TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 11167-4:2015
ISO/IEC 7816-4:2013

Xuất bản lần 1

THẺ DANH ĐỊNH - THẺ MẠCH TÍCH HỢP - PHẦN 4: TỔ CHỨC, AN NINH VÀ LỆNH TRAO ĐỔI

Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange

HÀ NỘI - 2015

Mục lục **Trang**

Lời nói đầu

TCVN 11167-4:2015 hoàn toàn tương đương với ISO/IEC 7816-4:2013, ISO/IEC 7816-4:2013/Cor.1:2014

TCVN 11167-4:2015 do Tiểu Ban kỹ thuật tiêu chuẩn quốc gia TCVN/JTC 1/SC 17 *"Thẻ nhận dạng"* biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ công bố.

Bộ tiêu chuẩn TCVN 11167 (ISO/IEC 7816) *Thẻ định danh – Thẻ mạch tích hợp* gồm các tiêu chuẩn sau:

- Phần 1: Thẻ tiếp xúc - Đặc tính vật lý;
- Phần 2: Thẻ tiếp xúc - Kích thước và vị trí tiếp xúc;
- Phần 3: Thẻ tiếp xúc - Giao diện điện và giao thức truyền;
- Phần 4: Tổ chức, an ninh và lệnh trao đổi;
- Phần 5: Đăng ký của bên cung cấp ứng dụng;
- Phần 6: Phần tử dữ liệu liên ngành trong trao đổi;
- Phần 7: Lệnh liên ngành đối với ngôn ngữ truy vấn thẻ có cấu trúc;
- Phần 8: Lệnh đối với hoạt động an ninh;
- Phần 9: Lệnh đối với quản lý thẻ;
- Phần 10: Tín hiệu điện và trả lời để thiết lập lại cho thẻ đồng bộ;
- Phần 11: Xác minh cá nhân bằng phương pháp sinh trắc học;
- Phần 12: Thẻ tiếp xúc - Thủ tục vận hành và giao diện điện tử USB;
- Phần 13: Lệnh đối với quản lý ứng dụng trong môi trường đa ứng dụng;
- Phần 15: Ứng dụng thông tin mã hóa.

Thẻ định danh - Thẻ mạch tích hợp - Phần 4: Tổ chức, an toàn và lệnh trao đổi

Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange

1 Phạm vi áp dụng

Tiêu chuẩn này áp dụng trong mọi lĩnh vực. Tiêu chuẩn này qui định:

- Nội dung cặp lệnh-hồi đáp được trao đổi tại giao diện,
- Biện pháp truy lục các phần tử dữ liệu và đối tượng dữ liệu trong thẻ,
- Cấu trúc và nội dung của các byte lịch sử mô tả các đặc tính hoạt động của thẻ,
- Cấu trúc đối với các ứng dụng và dữ liệu trong thẻ, được thể hiện tại giao diện khi xử lý lệnh,
- Phương pháp truy cập tệp và dữ liệu trong thẻ,
- Kiến trúc an toàn để xác định quyền truy cập tệp và dữ liệu trong thẻ,
- Biện pháp và cơ chế xác định và định địa chỉ các ứng dụng trong thẻ,
- Phương pháp truyền thông điệp an toàn,
- Phương pháp truy cập thuật toán được thẻ xử lý. Không mô tả các thuật toán này.

Tiêu chuẩn này không bao gồm các phần thực thi trong thẻ hoặc các phần thực thi của mọi đối tượng bên ngoài.

Tiêu chuẩn này độc lập với công nghệ giao diện vật lý và chỉ áp dụng đối với thẻ được truy cập theo một hoặc các phương pháp sau: tiếp xúc, kết nối và tần số vô tuyến. Nếu thẻ hỗ trợ sử dụng đồng thời nhiều giao diện vật lý, thì mối quan hệ giữa các sự việc xảy ra trên các giao diện vật lý khác nhau không thuộc phạm vi của tiêu chuẩn này.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau là rất cần thiết cho việc áp dụng tiêu chuẩn. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi.

TCVN 11167-3 (ISO/IEC 7816-3), *Thẻ định danh - Thẻ mạch tích hợp - Phần 3: Thẻ tiếp xúc - Giao diện điện và giao thức truyền*;

TCVN 11167-6 (ISO/IEC 7811-6), *Thẻ định danh - Thẻ mạch tích hợp - Phần 6: Phần tử dữ liệu liên ngành trong trao đổi*;

ISO/IEC 8825-1:2002, Information technology - ASN.1 encoding rules: Specification of basic encoding rules (BER), Canonical encoding rules (CER) and distinguished encoding rules (DER) *(Công nghệ*

thông tin - Quy tắc mã hóa ASN.1: Đặc điểm của quy tắc mã hóa cơ bản (BER), quy tắc mã hóa chính tắc (CER) và quy tắc mã hóa phân biệt (DER)).

3 Định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ, định nghĩa sau đây.

3.1

Quy tắc truy cập (access rule)

Phần tử dữ liệu bao gồm một chế độ truy cập liên quan đến hoạt động và các điều kiện an toàn cần thực hiện trước khi hành động.

3.2

Tệp answer-to-reset (answer-to-reset file)

EF tùy chọn chỉ ra các đặc tính hoạt động của thẻ, cũng là tệp thông tin.

3.3

Ứng dụng (application)

Các cấu trúc, phần tử dữ liệu và mô-đun chương trình cần thiết để thực hiện một hàm cụ thể.

3.4

DF ứng dụng (application DF)

Tệp chuyên dụng (DF) để tạo và quản lý ứng dụng trong thẻ.

3.5

Định danh ứng dụng (application identifier)

Phần tử dữ liệu (đến 16 byte) định danh ứng dụng.

3.6

Nhãn ứng dụng (application label)

Phần tử dữ liệu sử dụng tại giao diện người-máy.

3.7

Nhà cung cấp ứng dụng (application provider)

Thực thể cung cấp các cấu phần tạo nên ứng dụng trong thẻ.

3.8

Khuôn mẫu ứng dụng (application template)

Tập các đối tượng dữ liệu liên quan đến ứng dụng bao gồm một đối tượng dữ liệu định danh ứng dụng

3.9

Kỹ thuật mật mã không đối xứng (asymmetric cryptographic technique)

Kỹ thuật mật mã sử dụng hai phép tính liên quan: phép tính công khai được xác định bởi số hiệu công khai hoặc bởi khóa công khai và phép tính riêng được xác định bởi số hiệu riêng hoặc bởi khóa riêng (hai phép tính đều có thuộc tính là với phép tính công khai cho trước không thể tính ra phép tính riêng)

3.10

Khuôn mẫu cơ sở (base template)

Trường giá trị của đối tượng dữ liệu được xây dựng, ngoại trừ các DO là kết quả của việc phân tích tham chiếu gián tiếp.

3.11

Chứng thư (certificate)

Chữ ký số ràng buộc một người hoặc đối tượng nào đó với khóa công khai tương ứng (thực thể phát hành chứng thư là bên có thẩm quyền cấp phát thẻ bài liên quan đến các phần tử dữ liệu trong chứng thư).

3.12

Cặp lệnh-hồi đáp (command-response pair)

Tập hai thông điệp tại giao diện: Một APDU lệnh theo sau bởi APDU hồi đáp theo hướng ngược lại.

3.13

Nối chuỗi lệnh (command chaining)

Biện pháp được sử dụng bởi mọi đối tượng bên ngoài để báo cho thẻ rằng dữ liệu lệnh của một trình tự các cặp lệnh-hồi đáp phải được xử lý cùng nhau.

3.14

Lớp bối cảnh-cụ thể (context-specific class)

Lớp thẻ bài có byte đầu tiên hoặc duy nhất '80' đến 'BF'.

3.15

Khuôn mẫu hiện hành (current template)

Trình tự các đối tượng dữ liệu có thể được tham chiếu trực tiếp bằng thẻ bài duy nhất của các đối tượng đó trong một lệnh trao đổi, nghĩa là trường giá trị của DO được xây dựng hiện hành (có thể ảo)

3.16

Phần tử dữ liệu (data element)

Hạng mục thông tin được nhận biết tại giao diện; được qui định một tên, mô tả nội dung lô-gic, định danh và việc mã hóa.

3.17

Đối tượng dữ liệu (data object)

Thông tin được nhận biết tại giao diện bao gồm chuỗi nối kết trường thẻ bài bắt buộc, trường độ dài bắt buộc và trường giá trị có điều kiện.

3.18

Đơn vị dữ liệu (data unit)

Tập nhỏ nhất các bit có thể được tham chiếu rõ ràng trong một EF hỗ trợ các đơn vị dữ liệu.

3.19

Tệp dành riêng (dedicated file)

Cấu trúc bao gồm thông tin điều khiển tệp, là tùy chọn, sẵn có bộ nhớ để cấp phát.

3.20

Tên DF (DF name)

Phần tử dữ liệu (đến 16 byte) định danh duy nhất một DF trong thẻ.

3.21

Chữ ký số (digital signature)

Dữ liệu được nối thêm, hoặc biến đổi mật mã cho một chuỗi dữ liệu để chứng minh nguồn gốc và tính toàn vẹn của chuỗi dữ liệu và bảo vệ chống lại việc giả mạo, ví dụ : bởi người nhận chuỗi dữ liệu.

3.22

Tệp thư mục (directory file)

EP tùy chọn bao gồm danh sách các ứng dụng được hỗ trợ bởi thẻ và các phần tử dữ liệu tùy chọn liên quan.

3.23

Tệp sơ cấp (elementary flie)

Tập các đơn vị dữ liệu hoặc các bản ghi hoặc đối tượng dữ liệu cùng chia sẻ định danh tệp.

3.24

Tiêu đề mở rộng (extended header)

Phần tử dữ liệu tham chiếu một hoặc một vài DO trong DO được xây dựng.

3.25

Danh sách tiêu đề mở rộng (extended header list)

Chuỗi nối kết của các tiêu đề mở rộng.

3.26

Tệp (file)

Một cấu trúc cho ứng dụng và/hoặc dữ liệu trong thẻ, được nhận biết tại giao diện khi xử lý các lệnh.

3.27

Định danh tệp (file identifier)

Phần tử dữ liệu (2 byte) được sử dụng để định địa chỉ tệp.

3.28

Danh sách tiêu đề (header list)

Chuỗi nối kết các cặp trường và độ dài của thẻ bài mà không cần phân định.

3.29

Tệp thông tin (information file)

EF tùy chọn biểu thị các đặc tính hoạt động của thẻ, cũng là tệp answer-to-reset.

3.30

Liên ngành (interindustry)

Được tiêu chuẩn hóa trong bộ TCVN 11167 (ISO/IEC 7816).

3.31

EF nội bộ (internal EF)

EF để lưu giữ dữ liệu được dịch bởi thẻ.

3.32

Khóa (key)

Trình tự các ký hiệu điều khiển thao tác mật mã (ví d; mật hóa, giải mật mã, phép tính riêng hoặc công khai trong xác thực động, tạo chữ ký, xác minh chữ ký)

3.33

Tệp chủ (master file)

DF đơn nhất thể hiện gốc trong thẻ có sử dụng hệ phân cấp DF.

3.34

ốp-xét (offset)

Số tham chiếu theo trình tự đơn vị dữ liệu trong một EF hỗ trợ các đơn vị dữ liệu, hoặc một byte trong bản ghi.

3.35

Dữ liệu quá cỡ (oversize payload)

Dữ liệu vượt quá qui định kích cỡ hiện hành của APDU.

3.36

Tệp cha (parent file)

DF ở ngay trước tệp cho trước trong hệ phân cấp DF.

3.37

Mật khẩu (password)

Dữ liệu được yêu cầu bởi ứng dụng được thể hiện cho thẻ bởi người sử dụng thẻ với mục đích xác thực.

3.38

Đường dẫn (path)

Chuỗi nối kết định danh tệp mà không cần phân định.

3.39

Dữ liệu (payload)

Dữ liệu chiều dài tùy ý, được gửi tới thẻ hoặc bởi thẻ, được xử lý cùng nhau.

3.40

Khóa riêng (private key)

Khóa trong một cặp khóa không đối xứng của thực thể, chỉ được sử dụng bởi thực thể đó.

[ISO/IEC 9798-1]

3.41

Nhà cung cấp (provider)

Người có thẩm quyền hoặc người có quyền tạo DF trong thẻ.

3.42

Khóa công khai (public key)

Khóa trong một cặp khóa không đối xứng của thực thể mà có thể công khai.

[ISO/IEC 9798-1]

3.43

Bản ghi (record)

Chuỗi các byte được tham chiếu và xử lý bằng thẻ trong một EF có hỗ trợ bản ghi.

3.44

Định danh bản ghi (record identifier)

Số được sử dụng để tham chiếu một hoặc nhiều bản ghi trong một EF có hỗ trợ bản ghi.

3.45

Số bản ghi (record number)

Số tuần tự để định danh duy nhất từng bản ghi trong EF có hỗ trợ bản ghi.

3.46

Định danh nhà cung cấp ứng dụng đã đăng ký (registered application provider identifier)

Phần tử dữ liệu (5 byte) định danh duy nhất một nhà cung cấp ứng dụng.

3.47

Mã thiết lập lại (resetting code)

Dữ liệu được thể hiện cho thẻ để sửa đổi giá trị bộ đếm.

3.48

Chuỗi hồi đáp (response chaining)

Biện pháp được sử dụng bằng thẻ để báo cho mọi đối tượng bên ngoài biết rằng dữ liệu hồi đáp của mọi cặp lệnh-hồi đáp được theo sau bởi dữ liệu hồi đáp của trình tự cặp lệnh-hồi đáp GET RESPONSE nên được xử lý cùng nhau.

3.49

Khóa bí mật (secret key)

Khóa sử dụng các kỹ thuật mật mã hóa đối xứng bởi cặp thực thể xác định.

[ISO/IEC 11770-3]

3.50

Truyền thông điệp an toàn (secure messaging)

Tập các biện pháp bảo vệ mật mã của (các phần của) cặp lệnh-hồi đáp.

3.51

Thuộc tính an toàn (security attribute)

Điều kiện sử dụng đối tượng trong thẻ bao gồm dữ liệu được lưu giữ và các chức năng xử lý dữ liệu, được biểu thị như một phần tử dữ liệu gồm một hoặc nhiều quy tắc truy cập.

3.52

Môi trường an toàn (security environment)

Tập các cấu phần được yêu cầu bởi một ứng dụng trong thẻ đối với việc truyền thông điệp an toàn hoặc cho các thao tác an toàn.

3.53

DO tự điều khiển (self-controlled DO)

DO được xây dựng xếp lồng tại ít nhất một DO'62' lồng các thuộc tính an toàn.

3.54

Định danh EF ngắn (short EF identifier)

Phần tử dữ liệu (5 bit) được sử dụng để định địa chỉ một tệp sơ cấp.

3.55

Cấu trúc (structure)

DF, EF, bản ghi, chuỗi dữ liệu (DataString) hoặc DO.

3.56

Kỹ thuật mật mã đối xứng (symmetric cryptographic technique)

Kỹ thuật mật mã có sử dụng cùng khóa bí mật đối với cả thao tác của người tạo và của người nhận (không có khóa bí mật, không thể tính toán thao tác của người tạo và người nhận).

3.57

Danh sách thẻ bài (tag list)

Chuỗi nối kết các trường thẻ không phân định.

3.58

Trình bao được gắn thẻ (tagged wrapper)

Trình bao cung cấp một thẻ cho việc định địa chỉ cục bộ của DO mà thẻ đó tham chiếu.

3.59

Khuôn mẫu (template)

Chuỗi nối kết đối tượng dữ liệu BER-TLV, hình thành trường giá trị của một đối tượng dữ liệu được xây dựng BER-TLV.

3.60

Mở rộng khuôn mẫu (template extension)

Phần trường giá trị của một DO được xây dựng do phân tích tự động của tham chiếu gián tiếp.

3.61

Lựa chọn tạm thời (transient selection)

Việc lựa chọn cấu trúc cần thiết khi thực hiện một C-RP, không làm thay đổi vùng hiệu lực hiện hành nếu lựa chọn này thành công.

3.62

VA tạm thời (transient VA)

Vùng hiệu lực (VA) được thiết lập tạm thời trong quá trình thực hiện lệnh xử lý DO.

3.63

Người sử dụng (user)

Người sử dụng thẻ, cũng gọi là chủ thẻ.

3.64

Vùng hiệu lực (validity area)

Kết quả của tất cả các lựa chọn thành công được thực hiện trên kênh lô-gic

3.65

DO gốc ảo (virtual root DO)

DO'7F70' được xây dựng ảo được thực hiện hiện hành bằng cách lựa chọn một tệp, bản ghi hoặc chuỗi dữ liệu hỗ trợ xử lý DO

3.66

trình bao (wrapper)

Chuỗi nối kết các DO tham chiếu DO

3.67

EF hoạt động (working EF)

EF để lưu giữ dữ liệu không được thực hiện bởi thẻ.

4 Thuật ngữ viết tắt và kí hiệu

AID	Định danh ứng dụng
AMB	Byte chế độ truy cập
AMF	Trường chế độ truy cập
APDU	Đơn vị dữ liệu giao thức ứng dụng
ARR	Tham chiếu quy tắc truy cập
ASN.1	Ký hiệu cú pháp trừu tượng 1 (xem ISO/IEC 8825-1)
AT	Khuôn mẫu tham chiếu điều khiển đối với việc xác thực
ATR	Answer-to-Reset (Trả lời-để-Thiết lập)
BER	Quy tắc mã hóa cơ bản ASN.1 (xem ISO/IEC 8825-1)
CCT	Khuôn mẫu tham chiếu điều khiển đối với kiểm tra tổng mật mã
CLA	Byte lớp
CRT	Khuôn mẫu tham chiếu điều khiển
CT	Khuôn mẫu tham chiếu điều khiển dành cho bảo mật
CP	Thông số kiểm soát (thông số kiểm soát tệp hoặc thông số kiểm soát đối tượng dữ liệu)
CP DO	Đối tượng dữ liệu BER-TLV thông số kiểm soát
C-RP	Cặp lệnh-hồi đáp (command-response)
DF	Tệp dành riêng
DIR	Thư mục
DO	Đối tượng dữ liệu BER-TLV
DO'...'	Đối tượng dữ liệu BER-TLV, Thẻ bài có giá trị hệ cơ số 16 giữa các dấu nháy đơn
DST	Khuôn mẫu tham chiếu điều khiển đối với chữ ký số
EF	Tệp cơ sở
EF.ARR	Tệp tham chiếu quy tắc truy cập
EF.ATR/INFO	Tệp trả lời-để-thiết lập (Answer-to-Reset), hoặc tệp thông tin
EF.DIR	Tệp thư mục
FCI	Thông tin điều khiển tệp
FCP	Thông số kiểm soát tệp
FMD	Dữ liệu quản lý tệp
HT	Khuôn mẫu tham chiếu điều khiển đối với mã-băm
INS	Byte chỉ dẫn
KAT	Khuôn mẫu tham chiếu điều khiển đối với thỏa thuận về khóa
Trường L_c	Trường độ dài đối với mật mã số N_c
LCS	Trạng thái vòng đời
Trường L_e	Trường độ dài đối với mật mã số N_e
MF	Tệp chủ
N_c	Số byte trong trường dữ liệu lệnh
N_e	Số byte tối đa của byte được mong đợi trong trường dữ liệu hồi đáp

N_r	Số byte trong trường dữ liệu hồi đáp
OID	Định danh đối tượng, như được xác định bởi ISO/IEC 8825-1
PIX	Mở rộng định danh ứng dụng độc quyền
P1-P2	Byte thông số (được chèn với mục đích làm sáng tỏ, dấu gạch ngang không quan trọng)
RFU	Được giữ lại cho mục đích sử dụng trong tương lai
RID	Định danh nhà cung cấp ứng dụng đã đăng ký
SC	Điều kiện an toàn
SCB	Byte điều kiện an toàn
SCQL	Ngôn ngữ truy vấn thẻ có cấu trúc
SE	Môi trường an toàn
SEID	Định danh môi trường an toàn
SM	Thông điệp an toàn
SPT	Khuôn mẫu thông số an toàn
SW1-SW2	Byte trạng thái (được chèn với mục đích làm sáng tỏ, dấu gạch ngang không quan trọng)
TLV	Tệp, độ dài, giá trị
{T-L-V}	Đối tượng dữ liệu (được chèn với mục đích làm sáng tỏ, dấu gạch ngang và dấu ngoặc không quan trọng)
VA	Vùng hiệu lực
'XY'	Ký hiệu mà chữ in hoa từ G đến Z đại diện cho số hệ cơ số 16 từ '0' đến '9' hoặc 'A' đến 'F', tương đương với XY đến 16

5 Cặp lệnh-hồi đáp

5.1 Điều kiện hoạt động

Giao diện vật lý giữa thẻ và mọi đối tượng bên ngoài phải có khả năng hỗ trợ xử lý cặp lệnh-hồi đáp. Việc đảm bảo quá trình được xác định bằng các giao thức giao diện-cụ thể. Với các từ của các giao thức đó (giữa các ngoặc kép), các tiêu chuẩn sau xác định các thủ tục trợ giúp:

- TCVN 11167-3 (ISO/IEC 7816-3) xác định "kích hoạt tiếp xúc", "thiết lập nguội" hoặc "thiết lập nóng", và có thể "lựa chọn thông số và giao thức".
- TCVN 11167-12 (ISO/IEC 7816-12) xác định "kết nối điện" tiếp xúc tham chiếu với thông số USB, trạng thái "định dạng" và "ban đầu" của thiết bị, và "ATR".
- ISO/IEC 14443 (tất cả các phần) xác định cách thiết lập thẻ gần với trạng thái "ACTIVE".

Các tiêu chuẩn này cũng xác định thủ tục và tình huống vô hiệu hóa giao diện vật lý. Một giao diện vật lý bị vô hiệu hóa không hỗ trợ việc xử lý cặp lệnh-hồi đáp.

5.2 Cú pháp

Bảng 1 thể hiện cặp lệnh-hồi đáp (viết tắt trong tiêu chuẩn này là C-RP), được đặt tên là là APDU lệnh theo sau bởi một APDU hồi đáp theo hướng ngược lại (xem TCVN 11167-3). Không được có C-RP chen vào qua giao diện đó, nghĩa là APDU hồi đáp phải được nhận trước khi bắt đầu C-RP khác.

Trong mọi APDU lệnh bao gồm các trường L_c và L_e (xem TCVN 11167-3), không kết hợp các trường ngắn và trường độ dài mở rộng, tức là: hoặc cả hai trường đều ngắn, hoặc cả hai trường đều được mở rộng.

Nếu thẻ chỉ rõ khả năng xử lý "các trường L_e và L_c được mở rộng" (xem Bảng 119, Bảng chức năng phần mềm thứ ba) trong các byte lịch sử (xem 12.1.1) hoặc trong EF.ATR/INFO (xem 12.2.2), thì thẻ xử lý trường độ dài mở rộng và ngắn. Mặt khác (giá trị mặc định), thẻ chỉ xử lý các trường độ dài ngắn.

Trong một APDU lệnh dài hơn 5 byte, việc sử dụng trường độ dài mở rộng L được biểu thị bằng byte đầu tiên sau P2 bằng '00'.

N_c biểu thị số byte trong trường dữ liệu lệnh. Trường L_c mã hóa N_c.

- Nếu không có trường L_c, thì N_c bằng 0;
- Trường L_c ngắn bao gồm một byte không được đặt là '00'. Từ '01' đến 'FF', byte mã hóa N_c từ 1 đến 255.
- Trường L_c mở rộng bao gồm ba byte: một byte đặt là '00' sau 2 byte không đặt là '0000'. Từ '0001' đến 'FFFF', 2 byte mã hóa N_c từ 1 đến 65 535.

Bảng 1 - Cặp lệnh-hồi đáp (C-RP)

Trường	Mô tả	Số byte	Hướng
Tiêu đề lệnh	Byte lớp được biểu thị là CLA	1	Đến thẻ
	Byte chỉ dẫn được biểu thị là INS	1	
	Byte thông số được biểu thị là P1-P2	2	
Trường L_c	Không có đối với mã hóa $N_c = 0$, có đối với mã hóa $N_c > 0$	0, 1 hoặc 3	
Trường dữ liệu lệnh	Không có nếu $N_c = 0$, có khi là chuỗi byte N_c nếu $N_c > 0$	N_c	
Trường L_e	Không có đối với mã hóa $N_e = 0$, có đối với mã hóa $N_e > 0$	0, 1, 2 hoặc 3	
Trường dữ liệu hồi đáp	Không có nếu $N_r = 0$, có khi là chuỗi byte N_r nếu $N_r > 0$	N_r (tối đa N_e)	Từ thẻ
Người đò hồi đáp	Byte trạng thái được biểu thị SW1- SW2	2	

N_e biểu thị số byte tối đa trong trường dữ liệu hồi đáp, bất kể bất kỳ cấu trúc dữ liệu nào trong trường này. Trường L_e mã hóa là N_e.

- Nếu không có trường L_e, khi đó N_e là 0.
- Trường L_e ngắn bao gồm một byte có giá trị bất kỳ.
- Từ '01' đến 'FF', byte mã hóa N_e từ 1 đến 255
- Nếu byte được đặt là '00', khi đó N_e là 256
- Trường L_e mở rộng bao gồm mỗi ba byte (một byte đặt là '00' sau 2 byte có giá trị bất kỳ) nếu không có trường L_c, hoặc 2 byte (có giá trị bất kỳ) nếu có trường L_c mở rộng.
- Từ '0001' đến 'FFFF', 2 byte mã hóa N_e từ 1 đến 65 535
- Nếu 2 byte được đặt là '0000', khi đó N_e là 65 536

N_r biểu thị số byte trong trường dữ liệu hồi đáp. N_r phải nhỏ hơn hoặc bằng N_e. Vì vậy trong bất kỳ C-RP, việc không có trường L_e là cách thức tiêu chuẩn đối với nhận trường dữ liệu không hồi đáp. Nếu trường L_e bao gồm chỉ các byte đặt là '00', khi đó N_e là tối đa, nghĩa là trong giới hạn 256 đối với trường L_e ngắn, hoặc 65 536 đối với trường L_e mở rộng, tất cả các byte có sẵn phải được hoàn lại.

Nếu thủ tục bị hủy bỏ, khi đó thẻ có thể không hồi đáp. Tuy nhiên, nếu APDU hồi đáp diễn ra, khi đó trường dữ liệu hồi đáp phải không có và SW1- SW2 phải biểu thị lỗi.

P1-P2 biểu thị sự điều khiển và lựa chọn đối với xử lý lệnh. Byte thông số P1 hoặc P2 đặt là '00' thường không cung cấp nhiều định tính. Không có quy ước chung khác đối với mã hóa byte thông số.

Quy ước chung được xác định sau đây đối với mã hóa byte lớp được biểu thị CLA (xem 5.4), Byte chỉ dẫn được biểu thị INS (xem 5.5) và byte trạng thái được biểu thị SW1- SW2 (xem 5.6). Trong các byte này, bit RFU phải được đặt là 0 trừ khi có quy định khác.

5.3 Thủ tục nối chuỗi

5.3.1 Tổng quát

Thủ tục nối chuỗi được sử dụng hoặc để giúp phân đoạn dữ liệu hoặc đối với thủ tục liên quan đến một số C-RP liên tiếp.

5.3.2 Phân đoạn dữ liệu

Dữ liệu lệnh là dữ liệu có độ dài bất kỳ được gửi đến thẻ để được xử lý cùng nhau. Dữ liệu hồi đáp là dữ liệu có độ dài bất kỳ được nhận từ thẻ theo yêu cầu. Dữ liệu bị quá tải nếu độ dài lớn hơn độ dài có sẵn trong trường dữ liệu (xem Chú thích); nối chuỗi cần thiết để truyền các dữ liệu như vậy:

- Nối chuỗi lệnh hỗ trợ truyền đến thẻ dữ liệu lệnh quá tải. Dữ liệu được phân đoạn; mỗi đoạn là một trường dữ liệu lệnh tuân theo giới hạn kích cỡ.
- Nối chuỗi hồi đáp hỗ trợ phục hồi từ thẻ dữ liệu hồi đáp quá tải. Dữ liệu được phân đoạn; mỗi đoạn là một trường dữ liệu hồi đáp tuân theo giới giạn kích cỡ.

Bộ nhận phải nối với đoạn được truyền tải thành công để phục hồi dữ liệu.

CHÚ THÍCH Cú pháp APDU giới hạn kích cỡ của trường dữ liệu. Nhiều giới hạn kích cỡ hơn có thể được chỉ ra (xem 12.7.1); nếu trường L_e ('0000' hoặc '000000') biểu thị N_e = '010000', khi đó tất cả các thông tin được yêu cầu phải được phục hồi, đến 65 536 byte. Phân đoạn phải xảy ra với trường độ dài có định dạng ngắn nếu dữ liệu lệnh vượt quá 255 byte và/hoặc dữ liệu hồi đáp vượt quá 256 byte. Phân đoạn không xảy ra với trường có độ dài định dạng mở rộng nếu dữ liệu tuân theo giới hạn kích cỡ đã được chỉ ra (xem 12.7.1).

5.3.3 Nối chuỗi lệnh

Điều này xác định cơ chế mà nhờ đó trong lớp liên ngành (CLA < '80', xem Bảng 2 và Bảng 3) C-RP liên tiếp có thể được nối chuỗi. Nếu thẻ hỗ trợ cơ chế này, khi đó thẻ phải biểu thị (xem Bảng 119, Bảng chức năng phần mềm thứ ba) trong byte lịch sử (xem 12.1.1) hoặc trong EF.ATR/INFO (xem 12.2.2).

CHÚ THÍCH Nội dung của điều này không phụ thuộc vào giao thức truyền. TCVN 11167-3 (ISO/IEC 7816-3) mô tả nối chuỗi khi sử dụng giao thức T=0.

Đối với lập cuỗi trong lớp liên ngành, bit b5 của CLA phải được sử dụng trong khi bảy bit khác không đổi.

- Nếu bit b5 được đặt là 0, khi đó lệnh là duy nhất hoặc lệnh cuối cùng của chuỗi.

- Nếu bit b5 được đặt là 1, khi đó lệnh không phải là lệnh cuối cùng của chuỗi.

Cơ chế có thể được sử dụng:

- Để truyền dữ liệu lệnh quá tải:
- Tất cả các byte CLA của lệnh phải giống nhau, ngoại trừ bit b5 (xem ở trên).
- Nếu bit b5 được đặt là 1, khi đó trường L_e phải không có.
- Nếu bit b5 được đặt là 0, khi đó trường L_e phải có.
- Tất cả byte INS P1 P2 của lệnh phải giống nhau.
- Như đã được quy định trong tiêu chuẩn này (xem ví dụ trong phụ lục C)
- Đối với bất kỳ thủ tục xác định ứng dụng liên quan đến một số C-RP liên tiếp
- Bit b5 của CLA phải được sử dụng như được xác định ở trên
- Kênh lô-gic được biểu thị bằng CLA phải giống nhau
- Không có sự ràng buộc về giá trị của byte INS P1 P2 của lệnh.

Tiêu chuẩn này xác định hoạt động của thẻ chỉ trong trường hợp, khi được kích hoạt, chuỗi C-RP được xử lý thành công trước khi bắt đầu C-RP không phải là một phần của chuỗi. Nếu điều kiện này không được tuân theo, hoạt động của thẻ không thuộc phạm vi của tiêu chuẩn này, nhưng có thể được mô tả trong đặc tả.

Để hồi đáp lệnh không phải là lệnh cuối cùng của chuỗi, thiết lập SW1- SW2 đến '9000' nghĩa là quá trình đã được hoàn thành; sử dụng các chỉ dấu cảnh báo được xác định trong điều 5.6; các điều kiện lỗi cụ thể sau có thể xảy ra.

- Nếu SW1- SW2 được đặt là '6883', khi đó lệnh cuối cùng của chuỗi được chờ đợi.
- Nếu SW1- SW2 được đặt là '6884', khi đó nối chuỗi lệnh không được hỗ trợ.

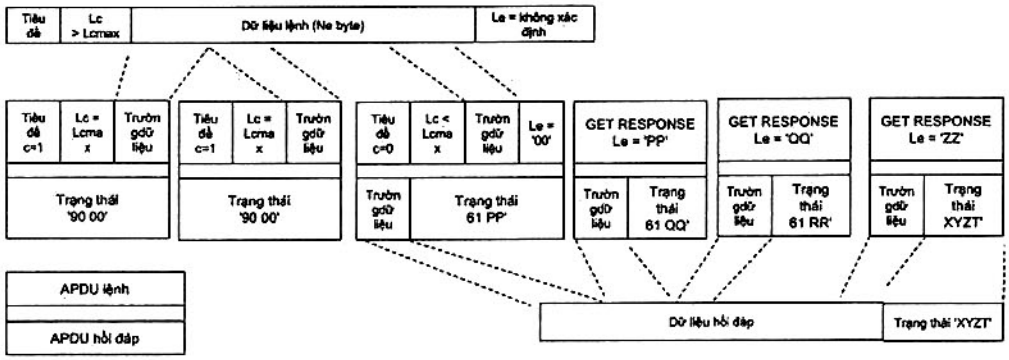
5.3.4 Nối chuỗi hồi đáp

SW1 = '61' và GET RESPONSE hỗ trợ truyền dữ liệu hồi đáp quá tải:

- Tất cả các byte CLA của lệnh liên quan đến hồi đáp, nối chuỗi phải giống nhau. Nối chuỗi hồi đáp xác định bắt đầu với C-RP trong đó SW1 được đặt là '61'.
- Ngoại trừ lệnh đầu tiên APDU của dãy, tất cả các byte INS P1-P2 của APDU lệnh phải là 'C0 00 00' (GET RESPONSE).
- Trong nối chuỗi lệnh, truyền dữ liệu bị gián đoạn bởi bất kỳ C-RP khác với GET RESPONSE, hoặc bởi bất kỳ C-RP nào trên kênh lô-gic khác.
- Ngược với nối chuỗi lệnh, sự kết thúc có thể xảy ra này là bình thường khi mọi đối tượng bên ngoài coi rằng nó đã nhận đủ dữ liệu: sự trao đổi tiếp tục xảy ra bình thường với C-RP tùy ý.
- Tuy nhiên, tiêu chuẩn này không xác định hoạt động của thẻ nếu mọi đối tượng bên ngoài cố nối lại nối chuỗi hồi đáp sau khi thực hiện lệnh trên kênh lô-gic khác. Hoạt động này có thể được xác định bằng ứng dụng.

Nếu được xác định bằng ứng dụng, nối chuỗi hồi đáp có thể được sử dụng để kiểm tra tính sẵn sàng của dữ liệu, mà việc này không cần thiết. Thẻ có thể biểu thị tính sẵn sàng bằng SW1- SW2 = '61XY', không gửi bất kỳ dữ liệu hồi đáp; mọi đối tượng bên ngoài phải hoặc phải không gửi (a) GET RESPONSE (s).

Trong hình 1, c = 0 và c = 1 biểu thị giá trị của bit b5 của CLA. Lcmax biểu thị giá trị tối đa của trường Lc mở rộng hoặc ngắn ICC hỗ trợ.



Cảnh báo Đây là mẫu mà thiết bị giao diện chọn để gửi trường dữ liệu lệnh dài nhất thẻ hỗ trợ và để phục hồi tất cả các dữ liệu đã có sẵn của thẻ. Tất cả các lựa chọn này đều không được ủy quyền.

Hình 1 – Việc truyền đến thẻ dữ liệu lệnh quá kích cỡ sử dụng nối chuỗi lệnh, tiếp theo bởi việc truyền bởi thẻ dữ liệu hồi đáp quá kích cỡ có sử dụng nối chuỗi hồi đáp.

5.4 Byte lớp

5.4.1 Mã hóa

CLA biểu thị lớp lệnh. Bit b8 của CLA phân biệt giữa lớp liên ngành và lớp dành riêng.

- Bit b8 đặt là 0 biểu thị lớp liên ngành
- Bit b8 đặt là 1 biểu thị lớp dành riêng, ngoại trừ giá trị 'FF' không có hiệu lực do quy định về đặc tính kỹ thuật trong TCVN 11167-3 (ISO/IEC 7816-3). Bối cảnh ứng dụng xác định các bit khác của CLA trong lớp dành riêng.

Giá trị 000x xxxx và 01xx xxxx được xác định sau đây. Giá trị 001x xxxx là RFU.

Bảng 2 xác định 000x xxxx là giá trị liên ngành đầu tiên.

- Bit b8, b7 và b6 được đặt là 000.
- Bit b5 điều khiển nối chuỗi lệnh (xem 5.3.3)
- Bit b4 và b3 biểu thị thông điệp an toàn (xem Điều 10)
- Bit b2 và b1 mã hóa số kênh lô-gic từ 0 đến 3 (xem 5.4.2).

Bảng 2 - Giá trị liên ngành đầu tiên của CLA

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	0	0	x	-	-	-	-	Điều khiển nối chuỗi lệnh (xem 5.3.3)
0	0	0	0	-	-	-	-	– lệnh là lệnh cuối cùng hoặc lệnh duy nhất của chuỗi
0	0	0	1	-	-	-	-	– lệnh không phải là lệnh cuối cùng của chuỗi
0	0	0	-	x	x	-	-	Chỉ báo thông điệp an toàn
0	0	0	-	0	0	-	-	– không SM hoặc không chỉ báo
0	0	0	-	0	1	-	-	– định dạng SM độc quyền
0	0	0	-	1	0	-	-	– SM theo Điều 10, Tiêu đề lệnh không được xử lý theo 10.2.3.1
0	0	0	-	1	1	-	-	– SM theo Điều 10, Tiêu đề lệnh được xác thực theo 10.2.3.1
0	0	0	-	-	-	x	x	Số kênh lô-gic từ không đến ba (xem 5.4.2)

Bảng 3 - Giá trị liên ngành tiếp theo của CLA

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	1	x	-	-	-	-	-	Chỉ báo thông điệp an toàn
0	1	0	-	-	-	-	-	– Không SM hoặc không chỉ báo
0	1	1	-	-	-	-	-	– SM theo Điều 10, Tiêu đề lệnh không được xử lý theo 10.2.3.1
0	1	-	x	-	-	-	-	Điều khiển nối chuỗi lệnh (xem 5.3.3)
0	1	-	0	-	-	-	-	– lệnh là lệnh cuối cùng hoặc lệnh duy nhất của chuỗi
0	1	-	1	-	-	-	-	– lệnh không phải là lệnh cuối cùng của chuỗi
0	1	-	-	x	x	x	x	Số kênh lô-gic từ bốn đến mười chín (xem 5.4.2)

Bảng 3 xác định 01xx xxxx là giá trị liên ngành hơn nữa

- Bit b8 và b7 được đặt là 01
- Bit b6 biểu thị thông điệp an toàn (xem Điều 10)
- Bit b5 điều khiển nối chuỗi lệnh (xem 5.3.3).

Bit b4 đến b1 mã hóa số từ không đến mười lăm; số này thêm bốn là số kênh lô-gic từ bốn đến mười chín (xem 5.4.2).

5.4.2 Kênh lô-gic

Điều này xác định cơ chế mà nhờ đó trong lớp liên ngành, C-RP có thể tham chiếu kênh lô-gic. Mỗi kênh lô-gic có trạng thái an toàn riêng (xem 9.3) và vùng hiệu lực (xem 7.2). Cách chia sẻ trạng thái an toàn không thuộc phạm vi của tiêu chuẩn này.

Nếu thẻ hỗ trợ cơ chế này, khi đó thẻ phải biểu thị số tối đa của kênh lô-gic có sẵn (xem Bảng 119, Bảng chức năng phần mềm thứ ba) trong byte lịch sử (xem 12.1.1) hoặc trong EF.ATR/INFO (xem 12.2.2).

- Nếu số được biểu thị là bốn hoặc ít hơn, khi đó chỉ áp dụng Bảng 2

- Nếu số được biểu thị là năm hoặc nhiều hơn, khi đó áp dụng Bảng 3.

Để tham chiếu kênh lô-gic trong lớp liên ngành, áp dụng các quy tắc sau.

- CLA mã hóa số kênh lô-gic của C-RP
- Giúp giao diện vật lý (xem 5.1) mở kênh lô-gic cơ bản mà kênh này phải mở cho đến khi làm mất khả năng hoạt động của giao diện vật lý. Nó có thể được thiết lập lại (xem bên dưới). Số kênh lô-gic cơ bản là 0.
- Thẻ không hỗ trợ kênh lô-gic bổ sung (giá trị mặc định) chỉ sử dụng kênh lô-gic cơ bản.
- Bất kỳ kênh lô-gic bổ sung nào phải được mở bằng cách hoàn tất lệnh hoặc SELECT hoặc SELECT DATA (xem 11.1.1 và 11.4.2) trong đó CLA mã hóa số kênh lô-gic chưa được sử dụng, hoặc lệnh MANAGE CHANNEL có hàm mở (xem 11.1.2).
- Bất kỳ kênh lô-gic bổ sung nào đều có thể bị đóng bằng cách hoàn tất lệnh MANAGE CHANNEL có hàm đóng. (xem 11.1.2). Sau khi đóng, kênh lô-gic phải luôn sẵn sàng cho việc sử dụng lại.
- Thậm chí nếu có nhiều kênh lô-gic được mở, không có sự đan xen của C-RP (xem 5.2).
- Nếu không loại bỏ hoàn toàn khả năng có thể chia xẻ bằng byte bộ mô tả tệp (xem bit b7 trong Bảng 11), thì kênh lô-gic nhiều có thể được mở cho cùng một cấu trúc (xem Điều 7), như là: cho DF, có thể cho DF ứng dụng, và có thể cho một EF.
- Nếu không loại bỏ hoàn toàn khả năng có thể chia xẻ bằng byte bộ mô tả tệp (xem bit b7 trong Bảng 13), thì kênh lô-gic nhiều có thể được mở cho cùng một DO
- Bất kỳ kênh lô-gic nào cũng có thể được thiết lập lại bằng cách hoàn tất lệnh MANAGE CHANNEL có hàm thiết lập lại (xem 11.1.2).

5.5 Byte chỉ dẫn

INS biểu thị lệnh xử lý. Do các đặc tính kỹ thuật trong TCVN 11167-3 (ISO/IEC 7816-3), giá trị '6X' và '9X' không có hiệu lực.

Bảng 4 liệt kê tất cả các lệnh được quy định trong TCVN 11167 (ISO/IEC 7816) tại thời điểm ban hành.

- Bảng 4.1, nghĩa là, bên trái, liệt kê các tên lệnh theo thứ tự Bảng chữ cái.
- Bảng 4.2, nghĩa là, bên phải, liệt kê các mã INS theo thứ tự số.

TCVN 11167 (ISO/IEC 7816) quy định sử dụng các lệnh này trong lớp liên ngành.

- Tiêu chuẩn này xác định lệnh đối với giao diện (xem Điều 11).
- TCVN 11167-7 (ISO/IEC 7816-7) quy định các lệnh đối với ngôn ngữ hỏi thẻ cấu trúc (SCQL).
- TCVN 11167-8 (ISO/IEC 7816-8) quy định các lệnh đối với thao tác an toàn.
- TCVN 11167-9 (ISO/IEC 7816-9) quy định các lệnh đối với quản lý thẻ.
- TCVN 11167-13 (ISO/IEC 7816-13) quy định các lệnh đối với quản lý ứng dụng trong môi trường nhiều ứng dụng.

Lớp liên ngành, bit b1 của INS biểu thị định dạng trường dữ liệu như sau.

- Nếu bit b1 được đặt là 0 (thậm chí mã INS), khi đó không cung cấp chỉ báo
- Nếu bit b1 được đặt là 1 (mã INS lẻ), dữ liệu (nếu có) phải được mã hóa trong BER-TLV (xem 8.1).

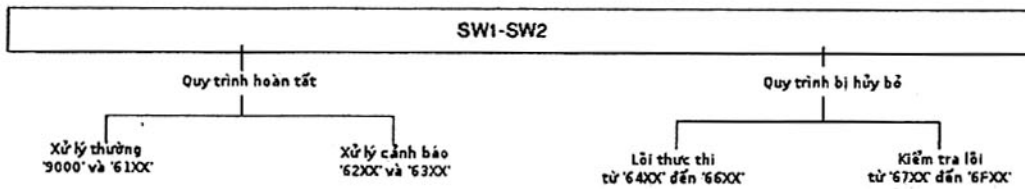
5.6 Byte trạng thái

SW1- SW2 biểu thị trạng thái xử lý. Do đặc tính kỹ thuật trong TCVN 11167-3 (ISO/IEC 7816-3), mọi giá trị khác với '6XXX' và '9XXX' không có hiệu lực; bất kỳ giá trị '60XX' cũng không có hiệu lực.

Các giá trị '61XX', '62XX', '63XX', '64XX', '65XX', '66XX', '68XX', '69XX', '6AXX' và '6CXX' là liên ngành.

Do các đặc tính kỹ thuật trong TCVN 11167-3 (ISO/IEC 7816-3), các giá trị '67XX', '6BXX', '6DXX', '6EXX', '6FXX' và '9XXX' là độc quyền, ngoại trừ giá trị '6700', '6701', '6702', '6B00', '6D00', '6E00', '6F00' và '9000' là liên ngành.

Hình 2 biểu thị sơ đồ cấu trúc của các giá trị '9000' và '61XX' đến '6FXX' đối với SW1- SW2.



Hình 2 - Sơ đồ cấu trúc các giá trị SW1- SW2

Tất cả các giá trị liên ngành SW1- SW2 không phụ thuộc với bất kỳ giao thức truyền nào. Bảng 5 liệt kê tất cả các giá trị liên ngành của SW1- SW2 và cho biết ý nghĩa chung của chúng. Tiểu ban SC 17 giữ lại cho mục đích sử dụng trong tương lai bất kỳ giá trị liên ngành của SW1- SW2 không được xác định trong TCVN 11167 (ISO/IEC 7816). Bảng 6 liệt kê tất cả điều kiện lỗi và cảnh báo liên ngành cụ thể được sử dụng trong TCVN 11167 (ISO/IEC 7816) tại thời điểm công bố.

Bảng 4.1 - Lệnh theo thứ tự Bảng chữ cái

Tên lệnh	INS	Tham khảo
ACTIVATE FILE	'44'	Phần 9
ACTIVATE RECORD	'08'	11.3.9
APPEND RECORD	'E2'	11.3.6
APPLICATION MANAGEMENT REQUEST	'40','41'	Phần 13
CHANGE REFERENCE DATA	'24','25'	11.5.7
COMPARE	'33'	11.6.1
CREATE FILE	'E0'	Phần 9
DEACTIVATE FILE	'04'	Phần 9
DELETE FILE	'E4'	7.6.2
DISABLE VERIFICATION REQUIREMENT	'26'	11.5.9
ENABLE VERIFICATION REQUIREMENT	'28'	0
ENVELOPE	'C2', 'C3	11.7.2
ERASE BINARY	'0E', '0F'	11.2.7
ERASE RECORD (S)	'0C'	11.3.8
EXTERNAL (/MUTUAL) AUTHENTICATE	'82'	11.5.4
GENERAL AUTHENTICATE	'86', '87'	11.5.5
GENERATE ASYMMETRIC KEY PAIR	'46','47'	Phần 8
GET ATTRIBUTE	'34','35'	11.6.2
GET CHALLENGE	'84'	11.5.3
GET DATA/GET NEXT DATA	'CA'/ 'CC'	11.4.3
GET DATA/GET NEXT DATA	CB'/ 'CD'	11.4.4
GET RESPONSE	'C0'	11.7.1
INTERNAL AUTHENTICATE	'88'	11.5.2
LOAD APPLICATION	'EA','EB'	Phần 13
MANAGE CHANNEL	'70'	11.1.2
MANAGE DATA	'CF'	Phần 9
MANAGE SECURITY ENVIRONMENT	'22'	11.5.11
PERFORM BIOMETRIC OPERATION	'2E','2F'	Phần 8
PERFORM SCQL OPERATION	'10'	Phần 7
PERFORM SECURITY OPERATION	'2A','2B'	Phần 8
PERFORM TRANSACTION OPERATION	'12'	Phần 7
PERFORM USER OPERATION	'14'	Phần 7
PUT DATA	'DA', 'DB	11.4.6
PUT NEXT DATA	'D8','D9'	11.4.7
READ BINARY	'B0', 'B1	11.2.3
READ RECORD (S)	'B2', 'B3'	11.3.3
REMOVE APPLICATION	'EC','ED'	Phần 13
RESET RETRY COUNTER	'2C','2D'	11.5.10
SEARCH BINARY	'A0', 'A1'	11.2.6
SEARCH RECORD	'A2'	11.3.7
SELECT	'A4'	11.1.1
SELECT DATA	'A5'	11.4.2
TERMINATE CARD USAGE	'FE'	Phần 9
TERMINATE DF	'E6'	Phần 9
TERMINATE EF	'E8'	Phần 9
UPDATE BINARY	'D6', 'D7'	11.2.5
UPDATE DATA	'DE','DF'	11.4.8

Bảng 4.2 - Lệnh theo thứ tự số

INS	Tên lệnh	Tham khảo
'04'	DEACTIVATE FILE	Phần 9
'06'	DEACTIVATE RECORD	11.3.10
'08'	ACTIVATE RECORD	11.3.9
'0C	ERASE RECORD (S)	11.3.8
'0E', '0F'	ERASE BINARY	11.2.7
'10'	PERFORM SCQL OPERATION	Phần 7
'12'	PERFORM TRANSACTION OPERATION	Phần 7
'14'	PERFORM USER OPERATION	Phần 7
'20', '21'	VERIFY	11.5.6
'22'	MANAGE SECURITY ENVIRONMENT	11.5.11
'24'	CHANGE REFERENCE DATA	11.5.7
'26'	DISABLE VERIFICATION REQUIREMENT	11.5.9
'28'	ENABLE VERIFICATION REQUIREMENT	0
'2A','2B'	PERFORM SECURITY OPERATION	Phần 8
'2C','2D'	RESET RETRY COUNTER	11.5.10
'2E','2F'	PERFORM BIOMETRIC OPERATION	Phần 8
'33'	COMPARE	11.6.1
'34','35'	GET ATTRIBUTE	11.6.2
'40','41'	APPLICATION MANAGEMENT REQUEST	Phần 13
'44'	ACTIVATE FILE	Phần 9
'46','47'	GENERATE ASYMMETRIC KEY PAIR	Phần 8
'70'	MANAGE CHANNEL	11.1.2
'82'	EXTERNAL (/MUTUAL) AUTHENTICATE	11.5.4
'84'	GET CHALLENGE	11.5.3
'86', '87'	GENERAL AUTHENTICATE	11.5.5
'88'	INTERNAL AUTHENTICATE	11.5.2
'A0', 'A1'	SEARCH BINARY	11.2.6
'A2'	SEARCH RECORD	11.3.7
'A4'	SELECT	11.1.1
'A5'	SELECT DATA	11.4.2
'B0', 'B1'	READ BINARY	11.2.3
'B2', 'B3'	READ RECORD (S)	11.3.3
'C0'	GET RESPONSE	11.7.1
'C2', 'C3'	ENVELOPE	11.7.2
'CA'/ 'CC'	GET DATA/GET NEXT DATA	11.4.3
'CB'/'CD'	GET DATA/GET NEXT DATA	11.4.4
'CF'	MANAGE DATA	Phần 9
'D0', 'D1'	WRITE BINARY	0
'D2'	WRITE RECORD	11.3.4
'D6', 'D7'	UPDATE BINARY	11.2.5
'D8','D9'	PUT NEXT DATA	11.4.7
'DA', 'DB'	PUT DATA	11.4.6
'DC', 'DD'	UPDATE RECORD	11.3.5
'DE','DF'	UPDATE DATA	11.4.8
'E0'	CREATE FILE	Phần 9
'E2'	APPEND RECORD	11.3.6
'E4'	DELETE FILE	Phần 9

Bảng 4.1 - Lệnh theo thứ tự Bảng chữ cái		
Tên lệnh	INS	Tham khảo
UPDATE RECORD	'DC', 'DD'	11.3.5
VERIFY	'20', '21'	11.5.6
WRITE BINARY	'D0', 'D1'	0
WRITE RECORD	'D2'	11.3.4

Bảng 4.2 - Lệnh theo thứ tự số		
INS	Tên lệnh	Tham khảo
'E6'	TERMINATE DF	Phần 9
'E8'	TERMINATE EF	Phần 9
'EA','EB'	LOAD APPLICATION	Phần 13
'EE'	DELETE DATA	Phần 9
'EC','ED'	REMOVE APPLICATION	Phần 13
'FE'	TERMINATE CARD USAGE	Phần 9

– Trong lớp liên ngành, bất kỳ mã INS có hiệu lực nào không được xác định trong TCVN 11167 (ISO/IEC 7816) đều là RFU.

Bảng 5 - Ý nghĩa tổng quát của giá trị liên ngành của SW1- SW2

	SW1- SW2	Ý nghĩa	
Xử lý thông thường	'9000'	Không thêm định tính	
	'61XX'	SW2 mã hóa số byte dữ liệu vẫn đang có sẵn (xem phần bên dưới)	
Xử lý cảnh báo	'62XX'	Trạng thái bộ nhớ không khả biến không thay đổi	(thêm định tính trong SW2, xem Bảng 6)
	'63XX'	Trạng thái bộ nhớ không khả biến có thể đã thay đổi	(thêm định tính trong SW2, xem Bảng 6)
Lỗi thực hiện	'64XX'	Trạng thái bộ nhớ không khả biến không thay đổi	(thêm định tính trong SW2, xem Bảng 6)
	'65XX'	Trạng thái bộ nhớ không khả biến có thể đã thay đổi	(thêm định tính trong SW2, xem Bảng 6)
	'66XX'	Các vấn đề liên quan đến an toàn	(thêm định tính trong SW2 là RFU)
Lỗi kiểm tra	'67XX'	Độ dài sai	(thêm định tính trong SW2, xem Bảng 6)
	'68XX'	Hàm trong CLA không hỗ trợ	(thêm định tính trong SW2, xem Bảng 6)
	'69XX'	Lệnh không được phép	(thêm định tính trong SW2, xem Bảng 6)
	'6AXX'	Thông số sai P1-P2	(thêm định tính trong SW2, xem Bảng 6)
	'6B00'	Thông số sai P1-P2	
	'6CXX'	Trường L_e sai: SW2 mã hóa số chính xác của byte dữ liệu có sẵn (xem bên dưới)	
	'6D00'	Mã chỉ báo không hỗ trợ hoặc không có hiệu lực	
	'6E00'	Lớp không hỗ trợ	
	'6F00'	Không có chuẩn đoán chính xác	

Bảng 6 - Các điều kiện lỗi và cảnh báo liên ngành cụ thể

SW1	SW2	Ý nghĩa
'62' (cảnh báo)	'00'	Không có thông tin được đưa ra
	'02' đến '80'	Gây ra bằng thẻ (xem 12.5.1)
	'81'	Phần dữ liệu phục hồi có thể bị lỗi
	'82'	Phần cuối của tệp hoặc bản ghi đạt được trước khi đọc byte N_e, hoặc tìm kiếm không thành công
	'83'	Tệp được lựa chọn bị giải hoạt
	'84'	Tệp hoặc thông tin điều khiển dữ liệu không được định dạng theo 7.4
	'85'	Tệp được lựa chọn trong trạng thái kết thúc
	'86'	Dữ liệu đầu vào không có sẵn từ cảm biến trên thẻ
	'87'	Ít nhất một trong các bản ghi được tham chiếu bị giải hoạt
'63' (cảnh báo)	'00'	Không có thông tin được đưa ra
	'40'	So sánh không thành công (ý nghĩa chính xác phụ thuộc vào lệnh)
	'81'	Tệp được làm đầy bởi lần ghi cuối cùng
	'CX'	Máy đếm từ 0 đến 15 được mã hóa bằng 'X' (ý nghĩa chính xác phụ thuộc vào lệnh)
'64' (lỗi)	'00'	Không có thông tin được đưa ra
	'01'	Hồi đáp ngay theo yêu cầu của thẻ
	'02' đến '80'	Gây ra bằng thẻ (xem 12.5.1)
	'81'	Truy cập chia sẻ kênh lô-gic bị từ chối
	'82'	Mở kênh lô-gic bị từ chối
'65' (lỗi)	'00'	Không có thông tin được đưa ra
	'81'	Bộ nhớ lỗi
'66' (lỗi)	'00'	Không có thông tin được đưa ra, các giá trị khác là RFU
'67' (lỗi)	'00'	Không có thông tin được đưa ra
	'01'	Định dạng APDU lệnh không theo tiêu chuẩn này (xem 5.1)
	'02'	Giá trị L_c không phải là giá trị được mong đợi
'68' (lỗi)	'00'	Không có thông tin được đưa ra
	'81'	Kênh lô-gic không được hỗ trợ
	'82'	Thông điệp an toàn không được hỗ trợ
	'83'	Lệnh cuối cùng của chuỗi được mong đợi
	'84'	Nối chuỗi lệnh không được hỗ trợ
'69' (lỗi)	'00'	Không có thông tin được đưa ra
	'81'	Lệnh không tương thích với cấu trúc tệp
	'82'	Trạng thái an toàn không thỏa đáng
	'83'	Phương pháp xác thực bị ngăn chặn
	'84'	Dữ liệu tham chiếu không thể sử dụng được

	'85'	Điều kiện sử dụng không thỏa đáng
	'86'	Lệnh không được phép (không EF hiện hành)
	'87'	DO thông điệp an toàn được mong đợi bị thiếu
	'88'	DO thông điệp an toàn không đúng
'6A' (lỗi)	'00'	Không có thông tin được đưa ra
	'80'	Thông số không đúng trong trường dữ liệu lệnh
	'81'	Hàm không được hỗ trợ
	'82'	Tệp hoặc ứng dụng không tìm thấy
	'83'	Bản ghi không tìm thấy
	'84'	Không đủ dung lượng bộ nhớ trong tệp
	'85'	N_c mâu thuẫn với cấu trúc TLV
	'86'	Thông số không đúng P1-P2
	'87'	N_c mâu thuẫn với thông số P1-P2
	'88'	Dữ liệu đã được tham chiếu hoặc dữ liệu tham chiếu không tìm thấy (ý nghĩa chính xác phụ thuộc vào lệnh)
	'89'	Tệp đã tồn tại
	'8A'	Tên DF đã tồn tại
Mọi giá trị khác của SW2 là RFU		

6 Đối tượng dữ liệu

Mục này xác định hai loại đối tượng dữ liệu: đối tượng dữ liệu SIMPLE-TLV và đối tượng dữ liệu BER-TLV, đối tượng dữ liệu BER-TLV được viết tắt là DO trong tiêu chuẩn này.

6.1 Đối tượng dữ liệu SIMPLE-TLV

Mỗi đối tượng dữ liệu SIMPLE-TLV bao gồm hai hoặc ba trường liên tiếp: trường thẻ bắt buộc, trường độ dài bắt buộc và trường giá trị điều kiện. Bản ghi (xem 11.3.1) có thể là đối tượng dữ liệu SIMPLE-TLV.

- Trường thẻ bao gồm một byte đơn nhất mã hóa số thẻ từ 1 đến 254. Giá trị '00' và 'FF' không có hiệu lực đối với trường thẻ. Nếu bản ghi là đối tượng dữ liệu SIMPLE-TLV, khi đó thẻ có thể được sử dụng là định danh bản ghi.
- Trường độ dài bao gồm một hoặc ba byte liên tiếp.
- Nếu byte đầu tiên không được đặt là 'FF', khi đó trường độ dài bao gồm một byte đơn nhất mã hóa số từ không đến 254 và được biểu thị là N.
- Nếu byte đầu tiên được đặt là 'FF', khi đó trường độ dài tiếp tục trên 2 byte tiếp sau có bất kỳ giá trị nào mã hóa số từ không đến 65 535 và được biểu thị là N.
- Nếu N là 0, không có trường giá trị, nghĩa là đối tượng dữ liệu trống. Mặt khác (N > 0), trường giá trị bao gồm các byte N liên tiếp.

CHÚ THÍCH Tiêu chuẩn này không xác định giá trị thẻ cũng không xác định trường giá trị của đối tượng dữ liệu SIMPLE-TLV. Do đó, xử lý đối tượng dữ liệu SIMPLE-TLV không thể dùng được đối với sự hoán đổi.

6.2 Đối tượng dữ liệu BER-TLV

Mỗi đối tượng dữ liệu BER-TLV (DO) bao gồm hai hoặc ba trường liên tiếp (xem quy tắc mã hóa cơ bản của ASN.1 trong ISO/IEC 8825-1): trường thẻ bắt buộc, trường độ dài bắt buộc và trường giá trị điều kiện. Bất kỳ DO không trống nào đều được biểu thị {T-L-V}.

Trường thẻ bao gồm một hoặc nhiều byte liên tiếp. Nó biểu thị một lớp và một mã hóa và mã hóa số thẻ. Giá trị '00' không có hiệu lực đối với byte đầu tiên của trường thẻ. ISO/IEC 7816 hỗ trợ trường thẻ của một, hai và ba byte; trường thẻ dài hơn là RFU.

Trường độ dài mã hóa độ dài, nghĩa là một số được biểu thị N, theo ISO/IEC 8825-1. Nếu N là 0, không có trường giá trị, nghĩa là DO trống, và được Chú thích {T-'00'}. Mặt khác (N > 0), trường giá trị bao gồm các byte liên tiếp N, và DO được Chú thích {T-L-V}. TCVN 11167 (ISO/IEC 7816).

a) Ngăn ngừa sử dụng "độ dài không xác định" (mã hóa '80'), theo quy tắc mã hóa DER;
b) Khuyến nghị sử dụng mã có thể ngắn nhất của trường độ dài, theo quy tắc mã hóa DER (xem ISO/ICE 8825-1);
c) Sử dụng trường độ dài bao gồm một đến 5 byte, trường độ dài dài hơn là RFU.

Chú thích 1 Để xác định độ dài của trường độ dài, đặc tả có thể theo khuyến nghị b), nghĩa là sử dụng trường độ dài ngắn nhất đối với mã độ dài được cho.

Chú thích 2 TCVN 11167-4 (ISO/IEC 7816-4) sử dụng '80' có ý nghĩa cụ thể trong trường giá trị của DO tiêu đề mở rộng (xem 8.4.5)

Chú thích 3 Phụ lục E cung cấp mã chi tiết của thẻ và trường độ dài.

6.3 DO được xây dựng so với DO ban đầu

Như được được xây dựng, DO không trống được biểu thị {T-L-{T1-L1-V1}...-{Tn-Ln-Vn}}. Thẻ T biểu thị cấu trúc của trường giá trị (xem phụ lục E). Trường giá trị này được gọi là bản mẫu, có thể:

- Hoặc bao gồm một DO, được gọi là "tổ" trong DO được xây dựng.
- Hoặc bao gồm sự kết nối của một số DO tổ, (n DO trong ví dụ ở trên), mà không có phần đệm (xem 8.1.1).

Trừ khi có quy định khác (ví dụ trình bao (xem 8.4.8) hoặc bộ bọc thẻ (xem 8.4.9), TCVN 11167-15 (ISO/IEC 7816-15), ISO/IEC 24727), thứ tự của DO trong bản mẫu không được xác định trong tiêu chuẩn này.

Xem phụ lục E đối với việc nhận dạng đối tượng dữ liệu ban đầu và được xây dựng bằng byte đầu tiên của thẻ. Cấu trúc hợp lý của trường giá trị của đối tượng dữ liệu ban dầu được xác định ở nơi khác.

7 Cấu trúc đối với ứng dụng và dữ liệu

7.1 Cấu trúc có sẵn

Mục này xác định cấu trúc đối với các ứng dụng và dữ liệu, như được nhận biết tại giao diện khi xử lý lệnh trong lớp liên công nghiệp. Vị trí lưu giữ thực sự của dữ liệu và thông tin cấu trúc ngoài cái được miêu tả trong mục này không thuộc phạm vi của ISO/IEC 7816. Cấu trúc sau được hỗ trợ:

- Tệp dành riêng (DF):

DF chủ các ứng dụng và/hoặc tập hợp tệp và/hoặc lưu giữ các DO. DF ứng dụng là DF chủ một ứng dụng. Một DF có thể là cha của các cấu trúc khác mà loại của chúng thuộc về tập hợp sau {DF, EF, DO}. Những cấu trúc khác này được cho là ngay dưới DF.

- Tệp cơ sở (EF)

EF lưu giữ dữ liệu. Một EF có thể là cha của các cấu trúc khác mà loại của chúng thuộc về tập hợp sau {DO, Record, DataString}. Những cấu trúc khác này được cho là ngay dưới EF. Hai loại EF được xác định.

- EF trong lưu giữ dữ liệu được thực hiện bởi thẻ, nghĩa là dữ liệu được sử dụng bởi thẻ dành cho mục đích điều khiển và quản lý.
- EF hoạt động lưu giữ dữ liệu không được thực hiện bởi thẻ, nghĩa là dữ liệu được sử dụngn bởi mọi đối tượng bên ngoài.
- Bản ghi:

Bản ghi lưu giữ dữ liệu. Một bản ghi có thể là cha của các cấu trúc khác mà loại của chúng thuộc về tập hợp sau {DO}. Những cấu trúc khác này được cho là ngay dưới bản ghi.

- Chuỗi dữ liệu:

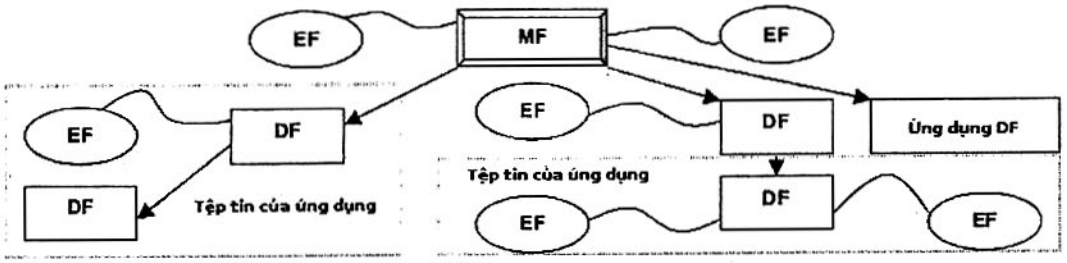
Chuỗi dữ liệu lưu giữ dữ liệu. Một chuỗi dữ liệu là một chuỗi các byte trong EF trong suốt. Một chuỗi dữ liệu có thể là cha của các cấu trúc khác mà loại của chúng thuộc về tập hợp sau {DO}. Những cấu trúc khác này được cho là ngay dưới chuỗi dữ liệu.

- Đối tượng dữ liệu (DO)

DO lưu giữ dữ liệu. Một DO có thể là cha của các cấu trúc khác mà loại của chúng thuộc về tập hợp sau {DO}. Những cấu trúc khác này được cho là ngay dưới DO.

Hai loại tổ chức lô-gic được cung cấp.

Hình 3 miêu tả hệ phân cấp của DF có cấu trúc an toàn tương ứng (xem mục 9). Trong tổ chức thẻ như vậy, DF tại gốc được gọi là tệp chủ (MF); bất kỳ DF nào cũng có thể là DF ứng dụng, có hoặc không có hệ phân cấp của chính nó thuộc các DF.



Hình 3 - Ví dụ về hệ phân cấp của các DF

- Hình 4 mô tả các DF ứng dụng song song, không có MF hiển thị tại giao diện, nghĩa là 0 có hệ phân cấp trong suốt của các DF. Tổ chức như vậy hỗ trợ các ứng dụng độc lập trong thẻ mà bất kỳ DF ứng dụng nào có thể có hệ phân cấp của chính nó thuộc các DF có cấu trúc an toàn tương ứng.

Hình 4 - Ví dụ về các DF ứng dụng độc lập

7.2 Vùng hiệu lực

7.2.1 Định nghĩa và thuộc tính

Vùng hiệu lực (VA) trên kênh lô-gic là kết quả của tất cả các lựa chọn thành công được thực hiện trên kênh lô-gic đó. Nó tạo ra khái niệm về tệp hiện hành được xác định trong bản trước thuộc TCVN 11167-4 (ISO/IEC 7816-4). VA xác định sự giải của thẻ DO và định danh tệp. VA bao gồm:

- curAppDF: tham chiếu hoặc DF hoặc DF ứng dụng. Luôn được thiết lập.
- curDF: tham chiếu DF, cái mà có thể là DF ứng dụng. Luôn được thiết lập.
- curEF: tham chiếu EF thuộc về DF hiện hành. Không luôn được thiết lập.
- curFile: tham chiếu tệp, luôn được thiết lập. Giá trị của nó phải đồng nhất với curDF nếu curDF không được thiết lập và đồng nhất với curEF nếu curEF được thiết lập.
- curRecord: tham chiếu với bản ghi, thuộc về EF hiện hành được cấu trúc trong các bản ghi. Không luôn được thiết lập.
- curDataString: tham chiếu chuỗi các byte là phần của EF hiện hành trong suốt. Không luôn được thiết lập.
- curConstructedDO: được thiết lập để xử lý DO. Khi được thiết lập, nó tham chiếu DO được xây dựng. Không luôn được thiết lập.
- curPrimitiveDO: tham chiếu DO ban đầu mà cha của DO ban đầu được tham chiếu bằng curConstructedDO. Không luôn được thiết lập.
- curDO: được thiết lập để xử lý DO. Khi được thiết lập, nó tham chiếu một DO, giá trị của nó phải đồng nhất với curConstructedDO nếu curPrimitiveDO không được thiết lập, và đồng nhất với curPrimitiveDO nếu curPrimitiveDO được thiết lập.

Chú thích 1 curFile có thể được tính từ curDF và curEF và ngược lại. Do vậy hoặc là curFile có thể bỏ qua hoặc curDF và curEF có thể bỏ qua. Lý do cho việc dư thừa này là một số hàm dễ dàng hơn mô tả bằng curFile (ví dụ ACTIVATE, DEACTIVATE) và các hàm khác dễ dàng hơn mô tả bằng curDF và curEF.

Chú thích 2 curDo có thể được tính từ curConstructedDO và curPrimitiveDO và ngược lại. Do vậy hoặc curDo có thể bỏ qua hoặc curConstructedDO và curPrimitiveDO có thể bỏ qua. Lý do cho việc dư thừa này là một số hàm dễ dàng hơn mô tả bằng curDO và các hàm khác dễ dàng hơn mô tả bằng curConstructedDO và curPrimitiveDO.

Chú thích 3 SE hiện hành không thuộc VA hiện hành.

7.2.2 Quy tắc cơ bản đối với sử dụng và xử lý VA

Liệt kê sau bao gồm liệt kê đầy đủ các quy tắc mô tả việc sử dụng VA. Các quy tắc khác được đưa ra trong các điều bao gồm sự mô tả lệnh:

a) Hỗ trợ giao diện vật lý (xem 5.1), mở kênh lô-gic cơ bản, thiết lập các giá trị của curAppDF và curDF đến giá trị đồng nhất, nghĩa là chúng tham chiếu hoặc MF hoặc ứng dụng hoàn toàn được lựa chọn.

b) Việc thiết lập lại kênh lô-gic thiết lập lại VA đến cùng tập hợp giá trị khi mở kênh lô-gic đó. Xem 11.1.2 đối với các kết quả thiết lập lại khác.

c) Mở kênh lô-gic thiết lập các giá trị của curAppDF và curDF đến giá trị đồng nhất (xem 11.1.1 và 11.1.2).

d) Lựa chọn một DF ứng dụng thiết lập curDF và curAppDF sao cho chúng tham chiếu DF ứng dụng được lựa chọn.

e) Lựa chọn một DF không phải là DF ứng dụng thiết lập curDF sao cho nó tham chiếu DF được lựa chọn. Nó thiết lập hoặc xác nhận curAppDF sao cho curAppDF tham chiếu hoặc DF ứng dụng gần nhất (nếu có) trong các tệp thủy tổ (cha, ông...) của DF được lựa chọn, hoặc MF nếu DF không ứng dụng tồn tại trong tệp thủy tổ.

f) Lựa chọn một EF thiết lập curEF sao cho nó tham chiếu EF được lựa chọn, và curDF sao cho nó tham chiếu tệp cha của EF được lựa chọn (xem quy tắc e)). Khi lựa chọn EF xuất hiện là tác động phụ của C-RP sử dụng tham chiếu bằng định danh EF ngắn, curEF có thể thay đổi trong khi curDF không thay đổi.

g) Lựa chọn bản ghi thiết lập curRecord sao cho nó tham chiếu bản ghi được lựa chọn làm bản ghi hiện hành, và curEF sao cho nó tham chiếu cha của bản ghi lựa chọn (xem quy tắc f)

h) Lựa chọn chuỗi dữ liệu trong EF trong suốt thiết lập curDataString sao cho nó tham chiếu DataString được lựa chọn và curEF sao cho nó tham chiếu cha của chuỗi dữ liệu được lựa chọn (xem quy tắc f).

   a. Lựa chọn cấu trúc bao gồm DO thiết lập curConstructedDO sao cho nó tham chiếu DO được lựa chọn theo cấu trúc quy định. Nếu cấu trúc được lựa chọn là DO được xây dựng, nó thiết lập curConstructedDO sao cho nó tham chiếu DO được lựa chọn. Nếu cấu trúc được quy định là {Application DF, DF, EF, record or DataString}, lựa chọn cấu trúc thiết lập curConstructedDO sao cho nó tham chiếu gốc ảo DO'7F70' làm DO được xây dựng hiện hành. DO này kết hợp với cấu trúc ... cuối cùng hỗ trợ DO trong danh sách ở trên.

i) Lựa chọn DO ban đầu thiết lập curPrimitiveDO sao cho nó tham chiếu DO xác định là Primitive DO hiện hành, và curConstructionDo sao cho nó tham chiếu cha của DO ban đầu được lựa chọn.

j) Đối với xử lý DO, khuôn mẫu hiện hành là giá trị của DO được tham chiếu bằng curConstructedDO (xem quy tắc i).

Lựa chọn hiện có thể thay đổi các phần tử của VA ngoài lựa chọn hiện do sự đệ quy. Lựa chọn ẩn có cùng kết quả như lựa chọn hiện.

Ví dụ Lựa chọn DO được xây dựng trong bản ghi phải thiết lập curConstructed DO (quy tắc i) hiện. Nó phải thiết lập ẩn hoặc xác nhận curRecord (quy tắc g)), curEF (quy tắc f)), curDF (quy tắc e)) và curAppDF (quy tắc d)).

7.3 Lựa chọn cấu trúc

7.3.1 Phương pháp lựa chọn cấu trúc

Lựa chọn cấu trúc cho phép truy cập dữ liệu và kết cấu bên dưới, nếu có. Các cấu trúc có thể được lựa chọn ẩn, nghĩa là tự động (xem 7.2.2, quy tắc a), g)) sau khi cho phép giao diện vật lý (xem 5.1). Khi một cấu trúc không thể được lựa chọn ẩn, nó phải được lựa chọn hiện, nghĩa là ít nhất một trong bốn phương pháp sau.

Lựa chọn theo tên DF - tên DF có thể t ham chiếu bất kỳ DF. Nó là một chuỗi đến 16 byte. Bất kỳ định danh ứng dụng nào (AID, xem 12.2.3) có thể được sử dụng làm tên DF. Để lựa chọn rõ ràng theo tên DF, ví dụ khi lựa chọn theo phương thức định danh ứng dụng, mỗi tên DF phải đơn nhất trong thẻ được cho.

Lựa chọn theo định danh tệp - định danh tệp có thể tham chiếu bất kỳ tệp nào. Nó bao gồm 2 byte. Giá trị '3F00' được lưu trữ (xem phần dưới và 11.4.1). giá trị '0000' được lưu trữ (xem 11.2.2 và 11.4.1). Để lựa chọn trong suốt bất kỳ tệp nào bằng định danh của chúng, tất cả các EF và DF ngay dưới DF được cho phải có định danh tệp khác nhau.

Lựa chọn theo đường dẫn - đường dẫn có thể tham chiếu bất kỳ tệp nào. Nó là sự kết nối định danh tệp. Đường dẫn bắt đầu bằng định danh DF (MF đối với đường dẫn tuyệt đối hoặc DF hiện hành đối với đường dẫn tương đối) và kết thúc bằng định danh của chính tệp đó. Giữa hai định danh này, đường dẫn bao gồm định danh của DF cha kế tiếp, nếu có. Thứ tự của định danh tệp luôn theo hướng cha đến con. Nếu định danh của DF hiện hành không biết, khi đó giá trị '3FFF' (giá trị lưu trữ) có thể được sử dụng tại điểm đầu tiên của đường dẫn. giá trị '3F002F00' và '3F002F01' được lưu trữ (xem 12.2.1 và 12.2.2). Đường dẫn cho phép lựa chọn rõ rệt bất kỳ tệp nào từ MF hoặc từ DF hiện hành (xem 12.3).

Lựa chọn theo định danh EF ngắn - định danh EF ngắn có thể tham chiếu bất kỳ EF nào. Nó bao gồm năm bit không bằng nhau, nghĩa là bất kỳ số nào từ 1 đến bao mươi. Khi được sử dụng làm định danh EF ngắn, số không, nghĩa là 00000 trong nhị phân, tham chiếu EF hiện hành. Tại mức MF, số ba mươi, nghĩa là 11110 trong nhị phân, được lưu trữ (xem 12.2.1). Định danh EF ngắn không thể được sử dụng trong đường dẫn hoặc làm định danh EF (ví dụ trong lệnh SELECT). Tất cả các định danh EF ngắn của EF ngay dưới DF được cho cùng với tất cả định danh EF ngắn được biểu thị trong FCP DO'A2' đi cùng với DF này phải đơn nhất.

Nếu được hỗ trợ, lựa chọn theo định danh EF ngắn phải được biểu thị.

- Nếu Bảng chức năng phần mềm đầu tiên (xem Bảng 117) có trong byte lịch sử (xem 12.1.1) hoặc trong EF.ATR/INFO (xem 12.2.2), khi đó chỉ báo có hiệu lực tại mức thẻ.
- Nếu định danh EF ngắn DO'88' (xem 10.2.3.1 và Bảng 10) có trong CP của EF, khi đó chỉ báo có hiệu lực tại mức EF.

Lựa chọn theo thẻ - DO có thể được lựa chọn theo thẻ đơn nhất, mà không cần thêm thông tin trên VA, nếu và chỉ khi nó thuộc về khuôn mẫu cơ sở của khuôn mẫu hiện hành nghĩa là giá trị của DO được xây dựng hiện hành.

Lựa chọn theo số bản ghi - nếu EF được chỉ theo curEF có hỗ trợ bản ghi, khi đó số bản ghi tham chiếu một bản ghi cụ thể trong EF đó. Số bản ghi là số nguyên dương.

Lựa chọn theo khoảng chừa trống - nếu EF được chỉ theo curEF trong suốt, khi đó khoảng chừa trống tham chiếu khởi đầu chuỗi của các byte trong EF đó. Khoảng chừa trống là số nguyên ≥ 0.

7.3.2 Phần tử dữ liệu tham chiếu tệp và DO

DO'51' liên ngành này (xem Bảng 7) tham chiếu một tệp. nó có thể có độ dài bất kỳ.

- DO trống tham chiếu MF
- Nếu độ dài là một và nếu bit b8 đến b4 của phần tử dữ liệu không bằng nhau và nếu bit b3 đến b1 được đặt là 000, khi đó bit b8 đến b4 mã hóa một số từ 1 đến ba mươi đó là định danh EF ngắn.

- Nếu độ dài là hai, khi đó phần tử dữ liệu là định danh tệp.
- Nếu độ dài nhiều hơn hai, khi đó phần tử dữ liệu là đường dẫn.
- Nếu độ dài chẵn và nếu 2 byte đầu tiên được đặt là '3F00', khi đó đường dẫn là tuyệt đối. Phần tử dữ liệu là kết nối của ít nhất hai định danh tệp bắt đầu bằng định danh MF.
- Nếu độ dài chẵn và nếu 2 byte đầu tiên không được đặt là '3F00', khi đó đường dẫn là tương đối. Phần tử dữ liệu là kết nối của ít nhất hai định danh tệp bắt đầu bằng định danh DF hiện hành.
- Nếu độ dài lẻ, khi đó đường dẫn được định tính. Phần tử dữ liệu hoặc là đường dẫn tuyệt đối không có '3F00',hoặc là đường dẫn tương đối không có định danh của DF hiện hành, theo sau byte sử dụng làm P1 trong một hoặc nhiều lệnh SELECT (xem 11.1.1 và 12.3).

Bảng 7 - Mã tham chiếu tệp DO'51'

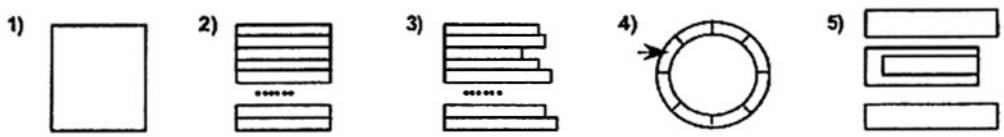
Thẻ	Độ dài	Giá trị
'51'	0	Đối tượng dữ liệu trống tham chiếu MF
	1	Định danh EF ngắn (bit b8 đến b4 mã hóa một số từ 1 đến ba mươi; bit b3 đến b1 được đặt là 000)
	2	Định danh tệp
		Đường dẫn tuyệt đối (2 byte đầu tiên được đặt là '3F00')
		Đường dẫn tương đối (2 byte đầu tiên không được đặt là '3F00')
	Lẻ, > 2	Đường dẫn định tính (byte cuối cùng được sử dụng làm P1 trong một hoặc nhiều lệnh SELECT)

7.3.3 Phần tử dữ liệu tham chiếu chung và DO

DO'60' liên ngành này (xem Bảng 86) và DO'7F72' (xembangr 37) có thể tham chiếu bất kỳ cấu trúc nào trong thẻ. Giá trị của DO'60' được sử dụng trong trường dữ liệu lệnh của nhiều CR-P xử lý DO (xem 11.4.2). Trong một số trường hợp, các lệnh này tác động tạm thời VA; trong các trường hợp khác, chúng sửa đổi VA.

7.3.4 Phương pháp tham chiếu dữ liệu trong tệp cơ sở

1) Cấu trúc trong suốt
2) Cấu trúc tuyến tính với bản ghi có kích cỡ cố định
3) Cấu trúc tuyến tính với bản ghi có kích cỡ thay đổi
4) Cấu trúc tuần hoàn với bản ghi có kích cỡ cố định (mũi tên tham chiếu bản ghi được viết gần nhất)



5) Cấu trúc SIMPLE-TLV or BER-TLV

Hình 5 - Cấu trúc EF

Phương pháp tham chiếu dữ liệu là một đặc tính phụ thuộc EF. EF hỗ trợ ít nhất một trong số các cấu trúc sau:

- Cấu trúc trong suốt - EF được nhận biết tại giao diện là chuỗi đơn đánh số, liên tục của đơn vị dữ liệu có thể truy cập được bằng lệnh xử lý đơn vị dữ liệu (xem 11.2). Kích cỡ đơn vị dữ liệu là một đặc tính phụ thuộc EF.
- Cấu trúc bản ghi - EF được nhận biết tại giao diện là chuỗi đơn liên tục của bản ghi định danh được có thể truy cập được bằng lệnh xử lý bản ghi (xem 11.3). Phương pháp đánh số bản ghi, cấu trúc SIMPLE-TLV hoặc BER-TLV của bản ghi là các đặc tính phụ thuộc EF. Ba đặc tính này được xác định: kích cỡ bản ghi, tổ chức bản ghi và bản ghi LCS.
- Kích cỡ của bản ghi hoặc cố định, hoặc thay đổi
- Tổ chức bản ghi hoặc chuỗi (cấu trúc tuyến tính) hoặc hình tròn (cấu trúc tuần hoàn).
- Bản ghi có thể có vòng đời bản ghi. Khi bản ghi có vòng đời, bản ghi LCS phân biệt ít nhất các trạng thái sau: ACTIVATED và DEACTIVATED. Mã bản ghi LCS không thuộc phạm vi của phần này thuộc ISO/IEC 7816. Trong phạm vi EF được cho, hoặc tất cả các bản ghi có vòng đời bản ghi hoặc không có bản ghi nào có vòng đời bản ghi. Sự có mặt của vòng đời bản ghi được biểu thị bằng CP (xem Bảng 10).
- Cấu trúc SIMPLE-TLV - EF được nhận biết tại giao diện khi tập hợp các đối tượng dữ liệu SIMPLE-TLV có thể truy cập được bằng các lệnh xử lý đối tượng dữ liệu (xem 11.4). Cấu trúc này ngăn cản cấu trúc BER-TLV
- Cấu trúc BER-TLV - EF được nhận biết tại giao diện khi tập hợp các DO có thể truy cập được bằng các lệnh xử lý DO (xem 11.4). Cấu trúc này ngăn cản cấu trúc SIMPLE-TLV.

Trong DF hoặc các ứng dụng, dữ liệu có thể được tham chiếu là DO (xem 6.2), cách thức tương tự như trong EF. Nếu EF, DF hoặc ứng dụng hỗ trợ tham chiếu này, sự lựa chọn của nó thiết lập curConstructedDO (xem 7.2.2 và 8.2.1).

7.4 Thông tin điều khiển dữ liệu và tệp

7.4.1 Phục hồi thông tin điều khiển tệp

Theo định nghĩa, thông tin điều khiển tệp là chuỗi byte có sẵn hồi đáp lệnh SELECT (xem 11.1.1); nó có thể có mặt trong bất kỳ tệp nào, nghĩa là bất kỳ DF và bất kỳ EF.

- Nếu byte đầu tiên được trị số từ '00' đến 'BF', khi đó chuỗi byte phải là BER-TLV được mã hóa. Tổ chức có trách nhiệm lưu trữ cho mục đích sử dụng trong tương lai tất cả các giá trị trong dãy '00' đến 'BF' các giá trị không được xác định trong tiêu chuẩn này.
- Nếu byte đầu tiên được trị số từ 'C0' đến 'FF', khi đó chuỗi byte không được mã hóa theo tiêu chuẩn này.

Bảng 8 cho thấy ba khuôn mẫu liên ngành:

- Khuôn mẫu FCP là tập hợp của CP DO thích hợp với các tệp, nghĩa là cá thuộc tính an toàn và cấu trúc, lô-gic như được liệt kê trong 'Bảng 10' và được xác định sau đây. Trong khuôn mẫu FCP, lớp ngữ cảnh cụ thể được lưu trữ đối với FCP; thẻ '85' và 'A5' tham chiếu thông tin độc quyền.
- Khuôn mẫu FMD là tập hợp của dữ liệu quản lý tệp, nghĩa là DO liên ngành như định danh ứng dụng như được xác định trong 12.2.3 và nhãn ứng dụng như được xác định trong 12.2.4 và ngày hết hạn ứng dụng như được xác định trong ISO/IEC 7816-6, khả năng lồng vào trong khuôn mẫu

ứng dụng như được xác định trong 12.2.4. trong khuôn mẫu FMD, thẻ '53' và '73' tham chiếu dữ liệu tùy ý.

- Khuôn mẫu FCI là tập hợp của tệp CP và dữ liệu quản lý tệp.

Bảng 8 - Khuôn mẫu liên ngành đối với thông tin điều khiển tệp

Thẻ	Giá trị
'62'	Tập hợp các thông số kiểm soát tệp (khuôn mẫu FCP)
'64'	Tập hợp dữ liệu quản lý tệp (khuôn mẫu FMD)
'6F'	Tập hợp các thông số kiểm soát tệp và dữ liệu quản lý tệp (khuôn mẫu FCI)

Ba khuôn mẫu có thể phục hồi theo lựa chọn của lệnh SELECT (xem Bảng 62).

- Nếu lựa chọn FCI được thiết lập, khi đó thẻ FCI tùy ý đưa vào khuôn mẫu trong trường dữ liệu hồi đáp.
- Nếu lựa chọn CP hoặc FMD được thiết lập, khi đó thẻ tương ứng bắt buộc đưa vào khuôn mẫu.

Phần thông tin điều khiển của DF có thể có mặt bổ sung trong EF dưới điều khiển ứng dụng và được tham chiếu bằng thẻ '87' trong tệp CP. Nếu có EF, thông tin điều khiển tệp phải được đưa vào bằng thẻ thích hợp, hoặc thẻ CP, hoặc thẻ FCI.

7.4.2 Phục hồi thông tin điều khiển dữ liệu

Theo định nghĩa, thông tin điều khiển dữ liệu là chuỗi byte có sẵn hồi đáp lệnh SELECT có P1='10' hoặc P1='13' (xem 11.1.1) hoặc lệnh SELECT DATA nếu bit b3 của P2 được đặt là 1 (xem 11.4.2); nó có thể có mặt đối với bất kỳ DO.

Bảng 9 - Khuôn mẫu liên ngành đối với thông tin điều khiển dữ liệu

Thẻ	Giá trị
'62'	Tập hợp thông số kiểm soát dữ liệu (CP DO, có khả năng bao gồm DO'62')

DO'62' xếp lồng CP DO

- Nó có thể có trong thông tin điều khiển dữ liệu của bất kỳ cấu trúc nào (tệp hoặc ứng dụng hỗ trợ cấu trúc BER-TLV, DO được xây dựng). Nó thuộc về và áp dụng đối với khuôn mẫu hiện hành sau khi lựa chọn cấu trúc.
- Khi có mặt trong khuôn mẫu cơ sở hiện hành (xem 8.2.2), nó áp dụng với, nó có thể được phục hồi bằng GET DATA hoặc GET NEXT DATA.
- Khi nó có trong khuôn mẫu khác, nó có thể được tham chiếu gián tiếp bằng trình bao thẻ (xem 8.4.8).

7.4.3 Thông số kiểm soát

Bảng 10 liệt kê CP DO đối với tệp và đối tượng dữ liệu, tất cả trong lớp ngữ cảnh cụ thể. Khi có CP, Bảng chỉ ra liệu xảy ra chỉ một lần (chỉ báo hiện) hoặc có thể được lặp lại (không chỉ báo).

Bảng 10 - Đối tượng dữ liệu tham chiếu tệp tin

Thẻ	Độ dài	Giá trị	Áp dụng với
'80'	Thay đổi	Số byte dữ liệu trong tệp, không bao gồm thông tin cấu trúc	Bất kỳ EP*

Thẻ	Độ dài	Giá trị	Áp dụng với
'81'	Thay đổi	Số byte dữ liệu trong tệp hoặc DO, bao gồm thông tin cấu trúc, nếu có	Tệp* hoặc DO*
'82'	1	Byte bộ mô tả tệp (xem 7.4.5 và Bảng 11)	Tệp*
	2	Byte bộ mô tả tệp và byte mã dữ liệu (xem Bảng 118)	
	3 hoặc 4	Byte bộ mô tả tệp, byte mã hóa dữ liệu, kích cỡ bản ghi tối đa trên một hoặc 2 byte	EF* hỗ trợ bản ghi
	5 hoặc 6	Byte bộ mô tả tệp, byte mã hóa dữ liệu, kích cỡ bản ghi tối đa trên 2 byte và số bản ghi trên một hoặc 2 byte (xem Chú thích)	
'83'	2	Định danh tệp	Tệp*
'84'	Đến 16	Tên DF	DF
'85'	Thay đổi	Thông tin độc quyền không được mã hóa trên BER-TLV	Tệp
'86	Thay đổi	Thuộc tính an toàn trong định dạng độc quyền	Tệp
'87'	2	Định danh của EF bao gồm mở rộng thông tin điều khiển tệp	DF*
'88'	0 hoặc 1	Định danh EF ngắn (xem 7.4.4)	EF*
'8A'	1	Trạng thái vòng đời (LCS, xem 7.4.10 và Bảng 14)	Tệp* hoặc DO*
'8B'	Thay đổi	Thuộc tính an toàn tham chiếu định dạng mở rộng (xem 9.3.3 và Bảng 38)	Tệp*
'8C'	Thay đổi	Thuộc tính an toàn trong định dạng khối, SE định hướng (xem Bảng 30)	Tệp*
'8D'	2	Định danh của một EF bao gồm khuôn mẫu môi trường an toàn (xem 10.3.3)	DF
'8E'	1	Thuộc tính an toàn kênh lô-gic (xem 9.3.7 và Bảng 47)	Tệp* hoặc DO*
'8F'	1	Chỉ báo tiết diện (xem Bảng 12)	EF có hỗ trợ bản ghi*
'92'	1	Byte bộ mô tả dữ liệu (xem 7.4.7)	DO* hoặc È* hỗ trợ cấu trúc BER-TLV
'96'	Thay đổi	Như được xác định trong ISO/IEC 7816-11	Xem ISO/IEC 7816-11
'97'	Thay đổi	Danh sách DF (xem 7.4.8)	DF*
'98'	Thay đổi	Số phiên bản (mã nhị phân)	DO*
Số EF trong DF (mã nhị phân) DF*'99'	Thay đổi	Số DO trong khuôn mẫu hiện hành sau khi lựa chọn DO hoặc tệp (mã nhị phân, xem 7.2.2 quy tắc i))	Tệp* hoặc DO*
'9B'Thay đổi	Thay đổi	Danh sách EF (xem 7.4.8)	DF*

Thẻ	Độ dài	Giá trị	Áp dụng với
'9A'			
'9C'	Thay đổi	Thuộc tính an toàn trong định dạng khối, SPT định hướng (xem Bảng 30). Chú thích chủ yếu dành cho xử lý DO	Tệp* hoặc DO*
'9D'	Thay đổi	Thẻ DO mà DO'62' áp dụng	DO
'A0'	Thay đổi	Khuôn mẫu thuộc tính an toàn đối với DO (xem 9.3.5)	Tệp* hoặc DO
'A1'	Thay đổi	Khuôn mẫu thuộc tính an toàn trong định dạng độc quyền	Tệp
'A2'	Thay đổi	Khuôn mẫu bao gồm một hoặc nhiều cặp DO: định danh EF ngắn (DO'88') - tham chiếu tệp (DO'51', L > 2, xem 7.3.2)	DF
'A3'	Thay đổi	Giao diện và thuộc tính an toàn phụ thuộc LCS (xem 7.4.12)	Tệp hoặc DO
'A5'	Thay đổi	Thông tin độc quyền được mã hóa trong BER-TLV	Tệp
'A6'	Thay đổi	Như được xác định trong ISO/IEC 7816-11	Xem ISO/IEC 7816-11
'AB'	Thay đổi	Khuôn mẫu thuộc tính an toàn trong định dạng mở rộng (xem 9.3.3)	Tệp*
'AC'	Thay đổi	Khuôn mẫu định danh cơ chế mật mã (xem 9.2)	DF
'AD'	Thay đổi	Khuôn mẫu thông số an toàn (xem 9.3.6.1)	DO
'AF'	Thay đổi	Khuôn mẫu tóm lược một hoặc nhiều DO'06' (OID) liên quan đến ứng dụng	DF*
* biểu thị rằng DO xuất hiện chỉ một lần dưới DO'62'. Hồi đáp SELECT và dưới thẻ '62' và '6F', Tổ chức có trách nhiệm lưu trữ bất kỳ DO khác của lớp ngữ cảnh cụ thể.			

7.4.4 Định danh EF ngắn

Các quy tắc sau áp dụng cho việc sử dụng DO'88' trong CP của bất kỳ EF.

- Nếu thẻ hỗ trợ lựa chọn theo định danh EF ngắn (xem 7.3.1) và nếu DO'88' không có, khi đó trong byte thứ hia của định danh tệp (tag '83'), bit b5 đến b1 mã hóa định danh EF ngắn.
- Nếu DO'88' có mặt có độ dài đặt là 0, khi đó EF không hỗ trợ định danh ngắn.
- Nếu DO'88' có mặt có độ dài đặt là một và nếu bit b8 đến b4 của phần tử dữ liệu không bằng và nếu bit b3 đến b1 được đặt là 000, khi đó bit b8 đến b4 mã hóa định danh EF ngắn (số từ 1 đến ba mươi).

7.4.5 Byte bộ mô tả tệp

DO'82' có thể xuất hiện trong CP của bất kỳ tệp nào (xem Bảng 10).

- Byte đầu tiên của giá trị là byte bộ mô tả tệp (xem Bảng 11).
- Nếu giá trị bao gồm hai hoặc nhiều byte hơn, khi đó byte thứ hai là byte mã dữ liệu (xem Bảng 118)
- Nếu thẻ cung cấp byte mã dữ liệu ở một số nơi, khi đó hiệu lực chỉ báo đối với tệp được cho là trong vị trí gần nhất với tệp đó trong đường dẫn đến tệp đó từ:
  1) MF, nếu có

2) DF tham chiếu với curAppDF, nếu có MF
3) Trong trường hợp không có chỉ báo trong đường dẫn, kích cỡ đơn vị dữ liệu được đặt là giá trị mặc định (xem Bảng 118).

Bảng 11 - Mã hóa byte bộ mô tả tệp

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	x	-	-	-	-	-	-	Tính có thể truy cập được tệp
0	0	-	-	-	-	-	-	- tệp không thể chia sẻ
0	1	-	-	-	-	-	-	- tệp có thể chia sẻ được
0	-	1	1	1	0	0	0	DF
0	-	Không phải tất cả đặt là 1			-	-	-	Loại EF
0	-	0	0	0	-	-	-	- EF để lưu giữ dữ liệu không được thực hiện bằng thẻ (EF hoạt động)
0	-	0	0	1	-	-	-	- EF để lưu giữ dữ liệu được thực hiện bằng thẻ (EF trong)
0	-	Mọi giá trị khác			-	-	-	- Loại EF độc quyền
0	-							Cấu trúc EF
0	-	Không phải tất cả đặt là 1			0	0	0	Không có thông tin được cho
0	-	Không phải tất cả đặt là 1			0	0	1	Cấu trúc trong suốt
0	-	Không phải tất cả đặt là 1			0	1	0	Cấu trúc tuyến tính, kích cỡ cố định, không có thêm thông tin
0	-	Không phải tất cả đặt là 1			0	1	1	Cấu trúc tuyến tính, kích cỡ cố định,, cấu trúc TLV
0	-	Không phải tất cả đặt là 1			1	0	0	Cấu trúc tuyến tính, kích cỡ thay đổi, không có thêm thông tin
0	-	Không phải tất cả đặt là 1			1	0	1	Cấu trúc tuyến tính, kích cỡ thay đổi, cấu trúc TLV
0	-	Không phải tất cả đặt là 1			1	1	0	Cấu trúc tuần hoàn, kích cỡ cố định, không có thêm thông tin
0	-	Không phải tất cả đặt là 1			1	1	1	Cấu trúc tuần hoàn, kích cỡ cố định, cấu trúc TLV
0	-	1	1	1	0	0	1	Cấu trúc BER-TLV
0	-	1	1	1	0	1	0	Cấu trúc SIMPLE-TLV

– Giá trị bất kỳ khác là RFU
– "Có thể chia sẻ được" nghĩa là tệp hỗ trợ truy cập đồng thời trên các kênh lô-gic khác nhau

7.4.6 Chỉ báo tiết diện

Các quy tắc sau áp dụng đối với sử dụng DO'8F' trong tệp CP của bất kỳ bản ghi hỗ trị EF:

- Nếu DO'8F' có mặt, khi đó trường giá trị chứa chỉ báo tiết diện theo Bảng 12;
- Nếu DO'8F' không có, khi đó tất cả các bản ghi trong EF ẩn trong trạng thái không thay đổi ACTIVATED

Bảng 12 - Mã hóa chỉ báo tiết diện

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	x	x	x	x	x	x	x	Mã hóa chỉ báo tiết diện được xác định bởi Tổ chức có trách nhiệm
0	-	-	-	-	-	-	x	Bản ghi LCS
0	-	-	-	-	-	-	0	Tất cả bản ghi trong tệp này đều trong trạng thái không thay đổi ACTIVATED
0	-	-	-	-	-	-	1	Mỗi bản ghi trong EF này có bản ghi riêng LCS, không thay đổi theo lệnh ACTIVATE RECORD, DEACTIVATE RECORD và ACTIVATE FILE
1	x	x	x	x	x	x	x	Mã hóa độc quyền chỉ báo tiết diện
– Giá trị bất kỳ khác là RFU								

7.4.7 Byte bộ mô tả dữ liệu

Được tham chiếu theo thẻ '92', phần tử dữ liệu liên ngành là CP DO bao gồm thông tin liên quan đến xử lý DO (xem Bảng 13). Thông tin có hiệu lực đối với tất cả các trường hợp (nếu nhiều hơn 1) của DO trong khuôn mẫu có liên quan. Nếu DO được tuyên bố là "không thể chia sẻ", chỉ một trường hợp của DO này có thể truy cập được trên một kênh lô-gic.

Bảng 13 - Mã hóa byte bộ mô tả dữ liệu

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	x	-	-	-	-	-	-	Tính có thể truy cập được dữ liệu
0	0	-	-	-	-	-	-	- DO không thể chia sẻ
0	1	-	-	-	-	-	-	- DO có thể chia sẻ được
0	-	x	x	-	-	-	-	Cấu trúc của DO trong khuôn mẫu
0	-	0	0	-	-	-	-	- không có thông tin được cho (mặc định)
0	-	0	1	-	-	-	-	- quản lý tuyến tính (xem 11.4.7)
0	-	1	0	-	-	-	-	- quản lý tuần hoàn đối với các trường hợp (xem 11.4.7)
0	-	1	1	-	-	-	-	- RFU
0	-	-	-	x	-	-	-	Các trường hợp
0	-	-	-	0	-	-	-	- thẻ xuất hiện chỉ một lần trong khuôn mẫu
0	-	-	-	1	-	-	-	- thẻ có thể xuất hiện nhiều lần trong khuôn mẫu (mặc định)
0	-	-	-	-	x	x	x	Đặc tính DO
0	-	-	-	-	0	0	0	- không có thông tin được cho
0	-	-	-	-	-	-	1	- có danh sách thẻ (DO được xây dựng) hoặc có trong danh sách thẻ (DO ban đầu)
0	-	-	-	-	-	1	-	- khuôn mẫu cơ sở có thể mở rộng được bằng trình bao (DO được xây dựng) hoặc phần mở rộng khuôn mẫu (DO ban đầu)
0	-	-	-	-	1	1-	-	- Giải tự động trình bao
– Giá trị bất kỳ khác là RFU – "Có thể chia sẻ được" nghĩa là DO hỗ trợ truy cập đồng thời trên các kênh lô-gic khác nhau								

7.4.8 Phần tử dữ liệu liệt kê DF và EF

Được tham chiếu theo thẻ '97', phần tử dữ liệu liên ngành liệt kê DF là một tệp CP cho biết các DF được chứa trong DF hoặc DF ứng dụng, và định danh EF ngắn của chúng. Thông tin của mỗi tệp được mã hóa trên ba byte liên tiếp. 2 byte đầu tiên bao gồm định danh tệp của một EF. Byte thứ ba hoặc là định danh EF ngắn của EF được mã hóa theo 7.4.4 hoặc byte được mã hóa '00' nếu tệp cơ sở không có định danh EF ngắn.

7.4.9 Phần tử dữ liệu số trường hợp

Được tham chiếu theo thẻ '98', phần tử dữ liệu liên ngành là CP DO, có thể xuất hiện chỉ khi có một số trường hợp DO trong khuôn mẫu. Giá trị của nó phải là số chuỗi dương được mã hóa nhị phân như được xác định theo ISO/IEC 8825-1 đối với loại INTEGER. Giản đồ số đối với quản lý tuần hoàn các trường hợp giống như đối với quản lý số bản ghi (xem 11.3.6). Xem 11.4.7 để biết thêm thông tin về giản đồ số.

7.4.10 Trạng thái vòng đời

Thẻ, tệp và các đối tượng khác, mỗi cái có vòng đời; trạng thái vòng đời (LCS) cho phép thẻ và thiết bị giao diện xác định trạng thái an toàn lô-gic khác nhau của thẻ, tệp và các đối tượng khác trong thẻ.

Để hỗ trợ quản lý thuận lợi vòng đời của tệp, bản ghi hoặc DO với tư cách là thuộc tính (xem TCVN 11167-9 (ISO/IEC 7816-9)), điều này xác định bốn trạng thái ban đầu của vòng đời theo trật tự sau.

1) Trạng thái tạo lập
2) Trạng thái giá trị ban đầu
3) Trạng thái hoạt động: được kích hoạt hoặc không được kích hoạt
4) Trạng thái kết thúc

LCS (1 byte) phải được thực hiện theo Bảng 14.

- Giá trị '00' đến '0F' là liên ngành
- Giá trị '10' đến 'FF' là độc quyền

Trạng thái mặc định là trạng thái hoạt động (đã được kích hoạt).

Bảng 14 - Mã hóa byte LCS dữ liệu hoặc tệp

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	0	0	0	0	0	0	0	Không có thông tin được cho
0	0	0	0	0	0	0	1	Trạng thái tạo lập
0	0	0	0	0	0	1	1	Trạng thái giá trị ban đầu
0	0	0	0	0	1	-	1	Trạng thái hoạt động (được kích hoạt)
0	0	0	0	0	1	-	0	Trạng thái hoạt động (không được kích hoạt)
0	0	0	0	1	1	-	-	Trạng thái kết thúc
Không phải tất cả bằng 0				x	x	x	x	Độc quyền
– Giá trị bất kỳ khác là RFU								

Theo thẻ '8A', LCS có thể xuất hiện trong CP của bất kỳ tệp hoặc DO (xem Bảng 10). Thẻ LCS có thể xuất hiện trong byte lịch sử (xem 12.1.1.11). Theo thẻ '48', thẻ LCS có thể xuất hiện trong EF.ATR/INFO (xem 12.2.2). Khi nó có MF, thẻ ít nhất trong trạng thái tạo lập.

Chú thích trừ khi có quy định khác, thuộc tính an toàn có hiệu lực đối với trạng thái hoạt động của tệp và trạng thái ACTIVATED của DO.

7.4.11 Tham chiếu gián tiếp theo định danh EF ngắn sử dụng DO'A2'

DO'88' dưới DO'A2' trong FCP của DF biểu thị rằng định danh EF ngắn lồng vào có hiệu lực khi DF là hiện hành. Lệnh sử dụng nó phải lựa chọn tạm thời EF được tham chiếu bằng đường dẫn lồng vào trong DO'51' sau DO'88'. Sự thành công của nó không có tác động đối với curDF và curAppDF (xem 7.2.2 quy tắc f)). Tác động đối với curEF được mô tả trong các phần giải quyết các lệnh sử dụng định danh EF ngắn (xem ví dụ 11.2.2 hoặc 11.3.2).

7.4.12 Khuôn mẫu thuộc tính an toàn phụ thuộc trạng thái vòng đời và giao diện

DO'A3' có thể xuất hiện trong CP của bất kỳ tệp hoặc DO và trong các khuôn mẫu có thể xuất hiện hơn một lần (xem Bảng 10).

DO'A3' bao gồm tối đa một DO'91' (xem 7.4.12.1). Nếu DO'91' không có, khi đó thuộc tính an toàn bao gồm trong DO'A3' áp dụng với tất cả các giao diện. Nếu DO'A3' gồm có DO'91', nó phải là DO đầu tiên trong khuôn mẫu.

DO'A3' bao gồm tối đa một DO'8A' (xem 7.4.12.2). Nếu DO'8A' không có khi đó thuộc tính an toàn bao gồm trong DO'A3' áp dụng với tất cả trạng thái vòng đời. Nếu DO'A3' bao gồm DO'8A' khi đó nó phải là

- DO đầu tiên trong khuôn mẫu nếu DO'91' xuất hiện, hoặc
- DO thứ hai trong khuôn mẫu nếu DO'91' không xuất hiện.

DO'A3' có thể bao gồm bất kỳ số nào của DO'8B', DO'8C', DO'9C', DO'A0', DO'AB' trong bất kỳ trật tự nào có cùng ý nghĩa và mã hóa như được xác định trong Bảng 10.

7.4.12.1 Bộ mô tả loại vận tải

Được tham chiếu theo thẻ '91' dưới DO'A3', phần tử dữ liệu này biểu thị cho giao diện thuộc tính an toàn bao gồm trong cùng DO'A3' áp dụng.

Bảng 15 - Mã hóa bộ mô tả loại vận chuyển (DO'91' dưới DO'A3')

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	-	-	-	-	-	-	-	0, các giá trị khác là RFU[a]
-	x	x	-	-	-	-	-	00, các giá trị khác là RFU
-	-	-	1	-	-	-	-	Giao tiếp bằng tiếp xúc C6 (xem TCVN 11167-3 (ISO/IEC 7816-3))
-	-	-	-	1	-	-	-	Giao tiếp trường gần (xem ISO/IEC 18092)
-	-	-	-	-	1	-	-	Giao diện USB (xem ISO/IEC 7816-2)
-	-	-	-	-	-	1	-	Giao diện không tiếp xúc đối với thẻ gần (xem ISO/IEC 14443)
-	-	-	-	-	-	-	1	Giao diện tiếp xúc (xem TCVN 11167-3 (ISO/IEC 7816-3))
[a] bản này xác định trường hợp khi một byte đủ để tham chiếu giao diện liên quan. Trong tương lai có thể cần thiết có nhiều byte								

Nếu trong phần tử dữ liệu này một bit được thiết lập đến

- 1 khi đó đối với giao diện tương ứng thuộc tính an toàn phải áp dụng
- 0 khi đó đối với giao diện tương ứng DO'A3' không liên quan

7.4.12.2 Biểu thị trạng thái vòng đời

Được tham chiếu theo thẻ '8A' dưới DO'A3', phần tử dữ liệu này biểu thị cho trạng thái vòng đời thuộc tính an toàn bao gồm trong cùng DO'A3' áp dụng. Phần tử dữ liệu này bao gồm một hoặc nhiều byte và mỗi byte phải được mã hóa và thực hiện theo 7.4.10 và Bảng 14, nghĩa là mỗi byte mã hóa một trạng thái vòng đời và tất cả các byte của phần tử dữ liệu tạo nên một tập hợp trạng thái vòng đời. Nếu vòng đời của tệp hoặc DO, được đưa ra trong DO'8A' trong khuôn mẫu thông số kiểm soát (nghĩa là khuôn mẫu có thẻ '62')

- Là phần tử của tập hợp này khi đó thuộc tính an toàn áp dụng đối với tệp hoặc DO
- Không phải là phần tử của tập hợp này khi đó DO'A3' không liên quan với tệp hoặc DO.

8 Sử dụng đặc thù DO và các khái niệm liên quan

8.1 Đệm và dữ liệu BER-TLV

Dữ liệu hoặc trường dữ liệu mã hóa BER-TLV là kết nối của BER-TLV DO, có khả năng đệm trước hoặc sau bất kỳ các DO nào.

Có hai phương thức tiêu chuẩn thể hiện mã hóa BER-TLV của một lệnh hoặc trường dữ liệu hồi đáp hoặc dữ liệu:

- CLA biểu thị thông điệp an toàn (xem Điều 10)
- Bit b1 của INS được đặt là 1 (mã INS lẻ).

Lệnh có mã INS chẵn có thể xác định mã hóa BER-TLV của trường dữ liệu và dữ liệu.

Trong dữ liệu lệnh, tiêu chuẩn này có thể xác định trật tự của DO (xem ví dụ Bảng 87). Trong dữ liệu hồi đáp, trật tự của DO hoặc không được xác định hoặc được kế thừa từ trật tự của DO có trong thẻ.

Do mã hóa trường độ dài BER-TLV (xem E.2) DO có thẻ n byte không thể có tổng độ dài ví dụ (n+1+128) byte hoặc (n+2+256) byte hoặc (n+3+65536) byte, vv... Trạng thái tổng độ dài không hiệu lực cũng có thể xảy ra nếu một số DO được truyền và DO cuối cùng tạo ra vấn đề tương tự. Trong tất cả các trường hợp này, nếu nhận lệnh N_e thiết lập với tổng độ dài không hiệu lực như vậy thẻ có thể gửi trong trường dữ liệu hồi đáp bao gồm DO byte N_e đầu tiên được yêu cầu theo lệnh và kết thúc bằng SW1-SW2 đặt là '61XY', trong đó 'XY' mã hóa số byte còn lại. Sau đấy chuỗi hồi đáp (xem 5.3.4) áp dụng.

8.1.1 Các điều kiện đệm

Khả năng đệm trong trường dữ liệu phụ thuộc vào lệnh. Thuật ngữ "kết nối DO" loại bỏ sự đệm. Đệm được phép:

- Khi xử lý cấu trúc dữ liệu qua đơn vị dữ liệu; ví dụ đệm có thể xuất hiện trong trường dữ liệu hồi đáp READ BINARY do xóa bỏ hoặc sửa đổi DO trong đơn vị dữ liệu hỗ trợ EF.
- Khi xử lý cấu trúc dữ liệu qua bản ghi; ví dụ đệm có thể xuất hiện trong trường dữ liệu hồi đáp READ RECORD do định dạng cố định của bản ghi trong bản ghi hỗ trợ EF.
- Khi được cho phép bởi tiêu chuẩn C-RP (CLA<'80')
- Khi được cho phép theo đặc tả của C-RP (CLA>'7F').

Nếu mã hóa BER-TLV được chỉ rõ, dữ liệu dữ liệu phải là BER-TLV được mã hóa, không có đệm. Mã hóa BER-TLV không áp dụng đối với trường dữ liệu đơn lẻ (a.k.a đoạn dữ liệu) của lệnh mà trong đó dữ liệu bị phân đoạn do sự phân đoạn dữ liệu khiến cho DO tách ra. Chèn vẫn bị loại bỏ trong đoạn dữ liệu.

CHÚ THÍCH Thông điệp an toàn có thể yêu cầu mã hóa BER-TLV của đoạn dữ liệu (xem 10.1).

8.1.2 Thủ tục đệm

Khi đệm được phép trong dữ liệu BER-TLV, byte đặt là '00' có thể có trước, giữa hoặc sau DO.

Khi có trong byte lịch sử (xem 12.1.1) hoặc trong EF.ATR/INFO (xem 12.2.2) hoặc trong thông tin điều khiển của bất kỳ tệp nào (xem thẻ '82' trong Bảng 10), byte mã hóa dữ liệu (xem Bảng 118) biểu thị liệu giá trị 'FF':

- Có hiệu lực đối với byte đầu tiên của trường thẻ dài của lớp riêng, mã hóa được xây dựng (câu lệnh rõ ràng), hoặc

- Không có hiệu lực đối với byte đầu tiên của trường thẻ (giá trị mặc định), nghĩa là được sử dụng cho cùng mục đích (đệm) và theo cùng điều kiện như giá trị '00".

8.2 Khuôn mẫu hiện hành và hệ số đối tượng dữ liệu

8.2.1 Khuôn mẫu hiện hành và DO hiện hành

Nếu được thiết lập, curConstructedDO tham chiếu DO được xây dựng. Trường giá trị của nó, như được xác định trong 7.2.2 quy tắc k), được gọi là khuôn mẫu hiện hành.

Bất kỳ DO nào trong khuôn mẫu hiện hành có thể được tham chiếu trực tiếp bằng thẻ đơn nhất trong lệnh chuyển đổi mà không cung cấp bất kỳ thông tin nào trên VA cùng với thẻ này.

Nếu bất kỳ DO nào được xây dựng, khuôn mẫu hiện hành không bao gồm bất kỳ DO xếp lồng trong DO được xây dựng.

Gốc ảo DO'7F70' thuộc về hệ 0, và là DO duy nhất trong hệ đó. Nếu curConstructed DO tham chiếu DO'XY" được xây dựng hệ n^{th}, khuôn mẫu hiện hành là chuỗi DO hệ $(n+1)^{th}$ lồng vào trong DO'XY'. Khuôn mẫu hiện hành không bao gồm DO có thể lồng vào trong bất kỳ DO hệ $(n+1)^{th}$. Ví dụ được đưa ra trong phụ lục F.

curDO (xem 7.2.1-9) được thiết lập bằng lệnh SELECT (xem 11.1.1) hoặc lệnh SELECT DATA (xem 11.4.2). Lựa chọn DO cũng xảy ra là tác động phụ của lệnh xử lý Do khác và được mô tả trong các phần liên quan, ví dụ 11.4.3 và 11.4.4 đối với lệnh GET DATA.

Để hỗ trợ phương pháp tham chiếu được xác định trong bản in này thuộc ISO/IEC 7816-4, thẻ phải có khả năng giải thẻ '7F70'.

Ngay sau khi hỗ trợ giao diện (xem 5.1), trước bất kỳ lựa chọn nào, khuôn mẫu hiện hành phụ thuộc vào ứng dụng được lựa chọn ẩn hoặc DF (curAppDF trong VA). Nó có thể bao gồm DO đặc thù để hỗ trợ ví dụ cho chế khám phá được xác định trong ISO/IEC 24727-2.

Nhiều lệnh xử lý DO bao hàm một hoặc một vài lựa chọn trong. Các lựa chọn này được cho là "tạm thời" và thiết lập "tệp hiện hành tạm thời" hoặc "khuôn mẫu hiện hành tạm thời", và "VA tạm thời". Trong một số trường hợp, tác động phụ của thành công lệnh có thể xác nhận các lựa trọn trong này, do vậy thiết lập VA tạm thời là VA hiện hành.

8.2.2 Mở rộng khuôn mẫu

Mở rộng khuôn mẫu là phần khuôn mẫu có thể truy cập được chỉ bằng giải tự động của trình bao thẻ, nhờ đó mở rộng khuôn mẫu cơ sở (xem phụ lục G hoặc ví dụ). tất cả trình bao DO'63' là phần khuôn mẫu cơ sở.

Nếu giải tự động của trình bao thẻ không được hỗ trợ, mở rộng khuôn mẫu trống. Tham chiếu gián tiếp chỉ mang tính cung cấp thông tin. Nếu cần thiết, mọi đối tượng bên ngoài có thể thực hiện thủ tục hai giai đoạn:

- Lựa chọn cấu trúc nơi DO được lưu giữ, khi cấu trúc này khác với cấu trúc hiện hành;
- Sau đó xử lý DO trong cấu trúc được lựa chọn.

8.2.3 Cây con đối tượng dữ liệu

DO được xây dựng có cấu trúc cây. Cây con của cấu trúc cây này đạt được bằng cách hủy bỏ DO lồng vào ở cây. Tiêu đề mở rộng cùng với DO được xây dựng tham chiếu cây con của DO (xem 8.4.6 và 8.4.7).

Ví dụ: DO hệ n^{th} được cho được biểu thị {T-L {T1-L1-{T2-L2-V2}-{T3-L3-V3}}-{T4-L4-V4}-{T5-L5-V5}}. Loại bỏ DO T2 hệ $(n+2)^{th}$ và DO T4 hệ $(n+1)^{th}$ đạt được cây con: {T-L'-{T1-L1'-{T3-L3-V3}}-{T5-L5-V5}}. L và L1 được thay bằng L' và L1' do hủy bỏ DO từ khuôn mẫu tác động đến độ dài của nó.

8.2.4 Vòng đời đối tượng dữ liệu

Bất kỳ DO nào lưu giữ trong thẻ đều có thể có vòng đời DO. Khi DO có vòng đời, LCS phải phân biệt ít nhất hai trạng thái: ACTIVATED và DEACTIVATED. Mã hóa LCS của DO và mã hóa LCS của tệp tương tự nhau (xem Bảng 14). Sự có mặt của LCS của DO được biểu thị trong DO'62' khuôn mẫu CP (xem Bảng 10).

8.3 Nhận dạng phần tử dữ liệu và đối tượng dữ liệu

8.3.1 Nguyên tắc

Tại giao diện giữa thẻ và thiết bị giao diện, phần tử dữ liệu thường xuất hiện trong trường giá trị của DO. Phần tử dữ liệu được cho là "dưới" thẻ của DO.

Nếu số bit đại diện phần tử dữ liệu không phải là bội số của tám, có thể sử dụng BITSTRING DO chung như ví dụ trong TCVN 11167-15 (ISO/IEC 7816-15). Nếu không, ánh xạ vào một byte hoặc một chuỗi byte phải được xác định cùng nhau với phần tử dữ liệu riêng. Trừ khi có quy định khác, số bit thích hợp được đặt là 1 trong byte cuối cùng bắt đầu từ bit b1.

Đối với mục đích phục hồi và tham chiếu trong trao đổi, phần tử dữ liệu phải được kết hợp với thẻ của đối tượng dữ liệu BER-TLV và phần tử dữ liệu có thể được gói gọn trong đối tượng dữ liệu này.

Phần tử dữ liệu có thể được tham chiếu trực tiếp bằng thẻ BER-TLV liên kết. Nó có thể được liên kết với phần tử dữ liệu khác mà phần tử dữ liệu này thiết lập ngữ cảnh nó thuộc về.

Một hoặc nhiều đối tượng dữ liệu lệnh để thực hiện có thể tham chiếu gián tiếp phần tử dữ liệu.

Lệnh liên ngành hỗ trợ nhiều phiên bản có cùng DO trong khuôn mẫu, như vậy trong ứng dụng và trong thẻ.

Tiêu chuẩn hoặc ứng dụng có thể giới hạn hoặc ngăn cấm nhiều phiên bản có cùng DO trong khuôn mẫu, trong cấu trúc hoặc trong ứng dụng.

8.3.2 Diễn giải thẻ trong trường dữ liệu hồi đáp và lệnh hoặc dữ liệu

DO có lớp chung (byte đầu tiên từ '01' đến '3F', xem phụ lục E) luôn có ý nghĩa chung của chúng.

Ý nghĩa của DO của lớp ứng dụng (byte đầu tiên từ '40' đến '7', xem phụ lục E) được xác định theo các tiêu chuẩn. Tiêu chuẩn mặc định là các tiêu chuẩn TCVN 11167 (ISO/IEC 7816) và Tổ chức có trách nhiệm (xem 8.3.3). Ý nghĩa của các DO này luôn giống nhau, mặc dù hàm của chúng được xác định theo lệnh chúng được sử dụng.

Cách thức thể hiện DO của lớp ngữ cảnh cụ thể (byte đầu tiên từ '80' đến 'BF', xem phụ lục E) được xác định:

- Bằng tổ của nó trong DO được xây dựng được xác định theo tiêu chuẩn, ví dụ DO lồng vào trong DO'62' (xem Bảng 10). Quy tắc này đệ quy và áp dụng, ví dụ với DO lồng vào trong DO'A0' lồng vào trong DO'62'.
- Bằng CLA: biểu thị thông điệp an toàn (xem 5.4 và 10.1).
- Bằng INS: lệnh có thể xác định các DO như vậy của lớp ngữ cảnh cụ thể đối với sử dụng cụ thể.
- Trong các trường hợp khác, diễn giải các DO này được xác định theo ứng dụng.

8.3.3 Phân phối thẻ

Tiêu chuẩn này xác định nhiều DO liên ngành và phân phối thẻ đối với lập mã BER-TLV của các DO này. Để xác định hơn nữa DO liên ngành, ISO/IEC 7816-6 duy trì một danh sách toàn diện bộ dữ liệu (tên của DO liên ngành, thẻ phân phối) được xác định trong ISO/IEC 7816 tại thời điểm công bố. Thẻ được phân phối trong tiêu chuẩn Tổ chức có trách nhiệm thuộc về:

- Hoặc lớp ứng dụng;
- Hoặc lớp ngữ cảnh cụ thể, khi DO tương ứng có thể được lồng vào trong DO được xây dựng thẻ đã được phân phối theo tiêu chuẩn.

Khi thẻ được xác định bằng tiêu chuẩn khác, cơ quan chức năng có trách nhiệm đối với tiêu chuẩn phải tìm kiếm thông tin của Tổ chức có trách nhiệm/WG 4 đối với thẻ hoặc các thẻ cần thiết, và phải chú giải kịp thời để bổ sung thẻ hoặc các thẻ này trong ISO/IEC 7816-6.

Được mô tả trong phụ lục A, cụm từ tiếp sau xác định sơ đồ phân phối thẻ định danh DO liên ngành trong trường dữ liệu. Khi cần thiết, sơ đồ phân phối thẻ này sử dụng DO liên ngành được thể hiện trong Bảng 16 để thông báo thẩm quyền có trách nhiệm đối với việc phân phối thẻ.

Bảng 16 - Đối tượng dữ liệu liên ngành đối với quyền phân phối thẻ

Thẻ	Giá trị
'06'	Định danh đối tượng (OID), mã hóa được xác định trong ISO/IEC 8825-1), xem ví dụ trong phụ lục A
'41'	Mã nước (mã hóa được xác định trong ISO 3166-1) và dữ liệu quốc gia tùy chọn
'42'	Số nhận dạng người phát hành (mã hóa và đăng ký được xác định trong ISO/IEC 7812-1 và dữ liệu người phát hành tùy chọn
'4F'	Định danh ứng dụng (AID, mã hóa được xác định trong 12.2.3)
'5F29'	Tiết diện trao đổi

8.3.4 Sơ đồ phân phối thẻ tiêu chuẩn

Trong lớp ứng dụng, Tổ chức có trách nhiệm phân phối hoặc lưu trữ sử dụng bất kỳ số thẻ lớp ứng dụng nào trong dải 0-127 hoặc lớn hơn 511 (số thập phân).

Số thẻ lớp ứng dụng trong dải 128 đến 511 (số thập phân) có thể được phân phối bằng bất kỳ tiêu chuẩn hoặc đặc tả nào được tham chiếu bằng OID, hoặc bằng ứng dụng được tham chiếu bởi AID.

Để định danh quyền phân phối thẻ trong dải này, DO'78' được xây dựng được sử dụng. DO này tạo tổ DO'80' trống sau hoặc DO'06' hoặc DO'4F'. Nếu DO'78' xuất hiện

- Trong chuỗi dữ liệu ban đầu (xem 12.1.2) hoặc trong EF.ATR/INFO (xem 12.2.2), khi đó quyền phải có hiệu lực đối với toàn bộ thẻ, ngoại trừ nếu bị bác bỏ bởi DO'78' khác trong tệp hoặc DO được xây dựng.

- Trong dữ liệu quản lý của EF hoặc DF, có khả năng hỗ trợ ứng dụng (xem 7.4) hoặc trong khuôn mẫu được thực hiện hiện hành bằng cách lựa chọn bất kỳ tệp nào, khi đó quyền phải có hiệu lực trong tệp đó hoặc ứng dụng, ngoại trừ nếu nó bị bác bỏ bởi DO'78' khác trong DO được xây dựng.
- Trong khuôn mẫu, nó phải có hiệu lực đối với tất cả các DO trong khuôn mẫu, và tất cả đối tượng bao gồm trong DO được xây dựng, (bất luận hệ của chúng), ngoại trừ nếu nó bị bác bỏ bởi DO'78' khác trong khuôn mẫu.

8.3.5 Sơ đồ phân phối thẻ tương thích

Các sơ đồ phân phối thẻ này sử dụng DO liên ngành và DO hơn nữa.

Các DO hơn nữa này phải được lồng vào trong DO liên ngành được tham chiếu bằng thẻ '70' đến '72' hoặc thẻ '74' đến '77'. Trong các DO này, ý nghĩa của thẻ lớp ứng dụng không được xác định trong ISO/IEC 7816 ngoại trừ đối với thẻ '41', '42' và '4F' để định danh quyền phân phối thẻ (xem Bảng 16).

Khi các DO hơn nữa sử dụng thẻ lớp ngữ cảnh cụ thể và thuộc về khuôn mẫu liên ngành được xác định ở trên, ý nghĩa của chúng được xác định bằng quyền phân phối thẻ.

Sử dụng lớp ngữ cảnh cụ thể trong khuôn mẫu liên ngành với thẻ '65' (dữ liệu liên quan đến người giữ thẻ), '66' (dữ liệu thẻ), '67' (dữ liệu xác thực) bị phản đối.

Để định danh sơ đồ phân phối thẻ tương thích và quyền trách nhiệm đối với sơ đồ, DO'78' liên ngành có thể được sử dụng. Khả năng xuất hiện và bác bỏ tương tự như trong 8.3.4. Nếu xuất hiện, giá trị của nó phải bao gồm một trong các DO liên ngành được thể hiện trong Bảng 16, để định danh quyền phân phối thẻ.

8.3.6 Sơ đồ phân phối thẻ cùng tồn tại

Trong sơ đồ như vậy, tất cả các DO liên ngành phải được lồng vào trong các DO'7E' liên ngành. Hơn nữa, thẻ '79' và ;7E' không được đưa lại sự diễn giải khác, cũng như thẻ '62', '64', '6F' (khuôn mẫu CP, FMD và FCI, xem 7.4) và '7D' (khuôn mẫu SM, xem 10.1).

Các sơ đồ phân phối thẻ này có thể sử dụng thẻ có sự diễn giải không được xác định trong TCVN 11167 (ISO/IEC 7816). Để định danh sơ đồ phân phối thẻ cùng tồn tại và quyền trách nhiệm đối với sơ đồ, DO'79' liên ngành được sử dụng. DO này phải tạo tổ một trong các DO liên ngành được thể hiện trong Bảng 16.

- Nếu quyền có hiệu lực đối với toàn bộ thẻ, khi đó DO'79' xuất hiện trong chuỗi dữ liệu ban đầu (xem 12.1.2) hoặc trong EF.ATR/INFO (xem 12.2.2).
- Nếu quyền có hiệu lực trong tệp hoặc ứng dụng, khi đó DO'79' xuất hiện trong dữ liệu quản lý DF ứng dụng hoặc EF, DF (xem 7.4) hoặc trong khuôn mẫu hiện hành được thiết lập bởi bất kỳ lựa chọn tệp nào.

8.3.7 Tránh sơ đồ phân phối thẻ độc lập

Bất kỳ sơ đồ phân phối thẻ độc lập nào sử dụng thẻ có sự diễn giải khác ISO/IEC 7816, nhưng không tuân theo 8.3.6. Các sơ đồ phân phối thẻ như vậy không tuân theo tiêu chuẩn này và không được phép trao đổi.

Bên cạnh việc sử dụng tính nhất quán sơ đồ phân phối cùng tồn tại và tương thích, có ba cách dành cho ứng dụng để tránh trạng thái như vậy và vẫn phù hợp với tiêu chuẩn này:

- Sử dụng các DO'53' tùy ý liên ngành để trình diễn DO tùy ý, và các DO'73' để tạo tổ DO độc quyền trong khuôn mẫu tùy ý.

- Sử dụng thẻ 3 byte được lưu trữ cho mục đích này (xem 8.3.4).
- Sử dụng DO có lớp ngữ cảnh cụ thể (xem 8.3.2).

8.4 Tham chiếu và phục hồi phần tử dữ liệu và DO

8.4.1 Tổng quát

Thẻ 'XY' tham chiếu trực tiếp phần tử dữ liệu mà là giá trị của DO'XY'. Đối với phục hồi DO trước khi lựa chọn ứng dụng xem 12.4.

Thông số kiểm soát và dữ liệu quản lý tệp có thể được phục hồi trong hồi đáp với lệnh SELECT hoặc SELECT DATA (xem 11.1.1, 11.4.2.1 và Bảng 87).

Ngay khi ứng dụng được lựa chọn, bất kỳ DO nào phải được phục hồi trực tiếp hoặc gián tiếp:

- Trong dữ liệu quản lý tệp (xem 7.4) của DF ứng dụng và từ EF cụ thể trong DF hiện hành.
- Trong khuôn mẫu hiện hành (xem 8.2) sau khi lựa chọn ứng dụng, sử dụng lệnh GET DATA hoặc GET NEXT DATA (xem 11.4.3) và 11.4.4). Dữ liệu quản lý tệp và/hoặc DO'62' (CP lồng) phải bao gồm trong khuôn mẫu này, để đảm bảo rằng các DO cụ thể này liên quan với ứng dụng.

Danh sách phần tử, danh sách thẻ, danh sách tiêu đề, tiêu đề mở rộng và danh sách tiêu đề mở rộng là các DO liên ngành tham chiếu gián tiếp phần tử dữ liệu, do vậy tham chiếu DO trong bất kỳ tệp nào. Các phần tử dữ liệu như vậy chỉ báo thẻ thể hiện một trường dữ liệu lệnh hoặc dựng một trường dữ liệu hồi đáp. Tính toán sự kết nối của phần tử dữ liệu hoặc DO từ tham chiếu gián tiếp được gọi là giải (hoặc phân tích) tham chiếu gián tiếp.

Sự diễn giải danh sách thẻ, danh sách tiêu đề, tiêu đề mở rộng hoặc danh sách tiêu đề mở rộng phụ thuộc vào khuôn mẫu mà trong đó chúng được xác định. Lồng một trong các DO này trong trình bao (cái xác định khuôn mẫu này), cho phép tham chiếu bất kỳ nơi nào trong thẻ. Thẻ tùy chọn trong trình bao cho phép tham chiếu kết quả của giải tham chiếu gián tiếp bằng thẻ này.

Cú pháp trường dữ liệu lệnh trong SELECT DATA, GET DATA, GET NEXT DATA thể hiện sử dụng các DO mà có thể gắn với cú pháp của trình bao.

8.4.2 Danh sách phần tử

Dưới thẻ '5F41', phần tử dữ liệu liên ngành này biểu thị rằng thông tin để phục hồi không xuất hiện là DO, mà dưới điều khiển ứng dụng. Nó được sử dụng chỉ trong khuôn mẫu trình bao. Cấu trúc của nó và thông tin hồi đáp không thuộc phạm vi của ISO/IEC 7816.

8.4.3 Danh sách thẻ

Được tham chiếu bằng thẻ '5C', phần tử dữ liệu liên ngành này là kết nối của trường thẻ không phân định. Nó tham chiếu sự kết nối của các DO bằng thẻ riêng, theo cùng trật tự như trong danh sách thẻ.

8.4.4 Danh sách tiêu đề

Dưới thẻ '5D', phần tử dữ liệu liên ngành này là kết nối của các bộ (trường thẻ T, trường độ dài L) không phân định. Chuỗi byte như được xác định trong danh sách thẻ ngoại trừ cắt cụt các giá trị. Khi L = '00', không xảy ra cắt cụt. Khi L > '00', giá trị bị cắt đến byte L, ngoại trừ khi nó đã ngắn hơn hoặc bằng với byte L. Mã hóa L là độ dài BER.

Cảnh báo: trong danh sách tiêu đề, tất cả các DO được tham chiếu bị cắt cụt phải là ban đầu do DO được xây dựng bị cắt cụt không phải là DO. Trích các phần của DO được xây dựng cần sử dụng tiêu đề mở rộng.

8.4.5 Tiêu đề mở rộng và danh sách tiêu đề mở rộng

Dưới thẻ '4D', '5F60' hoặc '5F61' (xem 8.4.8 đối với các khác biệt giữa các thẻ khác nhau), phần tử dữ liệu liên ngành này là danh sách tiêu đề mở rộng.

Danh sách tiêu đề mở rộng là

- Hoặc một tiêu đề mở rộng
- Hoặc kết nối của các tiêu đề mở rộng

Tiêu đề mở rộng là kết nối của các bộ (trường thẻ T, trường độ dài L) không phân định. Tiêu đề mở rộng tham chiếu thông tin trong DO mục tiêu. Một tiêu đề mở rộng hoàn toàn phải được suy ra từ DO mục tiêu theo thủ tục sau:

a) DO ban đầu không được tham chiếu:

Nếu tiêu đề mở rộng được gắn thẻ bằng

1) '4D', xóa bỏ thẻ, trường giá trị và độ dài.
2) '5F60' hoặc '5F61', xóa bỏ trường giá trị và thay thế trường độ dài bằng '00'.

b) DO ban đầu được tham chiếu mà không bị cắt bớt:

Xóa bỏ trường giá trị. Nếu tiêu đề mở rộng được gắn thẻ bằng

1) '4D', thay thế trường độ dài bằng '00'
2) '5F60' hoặc '5F61', thay thế trường độ dài bằng '80'.

c) DO ban đầu được tham chiếu bị cắt cụt

Xóa bỏ trường giá trị và thay thế trường độ dài bằng chỉ dấu cắt cụt (xem 8.4.6)

d) DO được xây dựng không được tham chiếu một chút nào

Xóa bỏ trường giá trị và thay thế trường độ dài bằng '00'.

e) DO được xây dựng được tham chiếu toàn bộ

Xóa bỏ trường giá trị và thay thế trường độ dài bằng '80'

f) DO được xây dựng mà phần thông tin được tham chiếu

Điều chỉnh giá trị của trường độ dài theo kết quả của việc áp dụng các thủ tục trên.

Như được thể hiện trong F.2, tham chiếu rõ ràng của DO mà không có gì được tham chiếu là 0 cần thiết, thậm chí khi một số phiên bản của DO như vậy tồn tại trong khuôn mẫu được cho. Tiêu chuẩn này cho phép loại bỏ tham chiếu không sử dụng.

8.4.6 Giải tiêu đề mở rộng

Để giải tiêu đề mở rộng, chuỗi byte tham chiếu cần được xây dựng như sau.

- Nếu thẻ biểu thị một mã hóa ban đầu, khi đó cặp trường thẻ và trường độ dài được thay thế bằng dữ liệu được thay thế bằng thẻ. Nếu tiêu đề mở rộng được gắn thẻ bằng '4D', độ dài '00' nghĩa là phần tử/DO hoàn thiện được bao gồm trong chuỗi byte. Nếu tiêu đề mở rộng được gắn thẻ bằng '5F60' hoặc '5F61', độ dài '80' có nghĩa là phần tử/DO hoàn thiện được bao gồm trong chuỗi byte. Độ dài không phải là '00' trong tiêu đề mở rộng được gắn thẻ bằng '4D', không phải là '80' trong tiêu đề mở rộng được gắn thẻ bằng '5F60' hoặc '5F61', biểu thị số tối đa các byte dữ liệu được phục hồi và do vậy có thể đòi hỏi cắt cụt như được xác định trong 8.4.4. Nếu chỉ báo cắt cụt biểu thị nhiều byte hơn sẵn có trong DO, cách xử lý phụ thuộc vào gắn thẻ:
- Dưới thẻ '4D', nằm ngoài phạm vi của tiêu chuẩn này.

- Dưới thẻ '5F60' và 5F61' tiêu đề mở rộng không hiệu lực. Nếu được sử dụng trong APDU lệnh, lệnh phải bị không chấp nhận bởi SW1-SW2 = '6985'.
- Thẻ biểu thị Bảng mã được xây dựng theo sau bởi độ dài không bằng 0, ngoại trừ '80', giới thiệu trường giá trị tiếp sau là danh sách tiêu đề mở rộng. Thẻ biểu thị Bảng mã được xây dựng theo sau bởi độ dài bằng 0 bị bỏ qua. Thẻ biểu thị Bảng mã được xây dựng theo sau bởi '80' có nghĩa là DO được xây dựng hoàn toàn/khuôn mẫu hoàn thiện được bao gồm trong chuỗi byte.
- Thẻ bỏ qua các phần tử của tiêu đề mở rộng không hợp với cấu trúc mục tiêu.

Vì lý do an toàn, thẻ có thể không chấp nhận lệnh SW1-SW2 = '6985' do thiếu tính nhất quán giữa cấu trúc được sử dụng trong trường dữ liệu lệnh và nội dung của thẻ. Điều này có thể làm mất hiệu lực thuộc tính an toàn.

Chuỗi byte bao gồm:

- Trường giá trị của DO ban đầu, có thể bị cắt cụt theo độ dài biểu thị (trường hợp 1), hoặc
- DO ban đầu, có thể bị cắt cụt theo độ dài biểu thị, và được lồng trong khuôn mẫu riêng, độ dài của nó tuân thủ theo quy tắc BER-TLV (trường hợp 2).
- Nếu xuất hiện, độ dài '80' phải được thay thế bằng độ dài thực tế. DO được xây dựng hoàn toàn/khuôn mẫu hoàn thiện được bao gồm trong chuỗi byte.

Mã hóa chuỗi byte tham chiếu, được đặt tên là DO (có khả năng được xây dựng) hoặc kết nối các phần tử dữ liệu (có khả năng bị cắt cụt), được biểu thị:

- Bằng mã INS thích hợp (lẻ/chẵn)
- Hoặc bằng thông số lệnh thích hợp, ví dụ hoặc mã hóa thích hợp trường dữ liệu (hoặc được xây dựng cho các cái bao gồm DO hoặc nguyên thủy đối với các cái chứa phần tử dữ liệu).
- Hoặc bằng cách gắn thẻ danh sách tiêu đề mở rộng theo thẻ khác '4D', như được thể hiện trong 8.4.8 và lệnh PERFORM SECURITY OPERATION (xem TCVN 11167-8 (ISO/IEC 7816-8)).

8.4.7 Giải danh sách tiêu đề mở rộng

Chuỗi byte được tham chiếu bằng danh sách tiêu đề mở rộng là kết nối của chuỗi byte được tham chiếu bằng các tiêu đề mở rộng, theo cùng trật tự như trong danh sách tiêu đề mở rộng. Khi phân tích danh sách tiêu đề mở rộng:

- Độ phân tích của một tiêu đề mở rộng phải được theo sau bởi độ phân tích của tiêu đề mở rộng tiếp theo nếu có.
- Trật tự trong chuỗi byte vì vậy được xác định theo trật tự của các tiêu đề mở rộng trong danh sách tiêu đề mở rộng mà hợp với trật tự trong mục tiêu (khuôn mẫu) để tránh vấn đề sau: như trong phân tích của tiêu đề mở rộng, thẻ bỏ qua các phần tử (các tiêu đề mở rộng) của danh sách tiêu đề mở rộng không tương thích cấu trúc mục tiêu (khuôn mẫu).

8.4.8 Trình bao

Dưới thẻ '63', DO liên ngành này phải lồng hai hoặc nhiều DO.

a) Do đầu tiên là tham chiếu gián tiếp bắt buộc. Chỉ một tham chiếu gián tiếp được cho trong trình bao. Nó là lựa chọn giữa:
   1) Danh sách phần tử (thẻ '5F41' hoặc '53');
   2) DO lồng danh sách phần tử (thẻ '73');
   3) Danh sách thẻ (thẻ '5C');

4) Danh sách tiêu đề (thẻ '5D');
5) Danh sách tiêu đề mở rộng (thẻ '4D');
6) Danh sách tiêu đề mở rộng tham chiếu chuỗi byte không có cấu trúc trạng thái (thẻ '5F60');
7) Danh sách tiêu đề mở rộng tham chiếu một DO hoặc kết nối của các DO (thẻ '5F61');
8) Chuỗi byte đồng nhất với dữ liệu hồi đáp của lệnh thực hiện cuối cùng (thẻ '80', DO trống), xem bên dưới.

Có thể theo sau bởi DO'7F71' bộ lọc (xem 11.4.2.3) trong trường hợp danh sách thẻ hoặc danh sách tiêu đề mở rộng. Sử dụng DO'5F60' hoặc sử dụng DO'5F61' cho phép bỏ qua chỉ báo DO ban đầu theo 8.4.5.

b) Số dư của trường giá trị trình bao phải là:
1) Hoặc định danh ứng dụng DO'4F' (xem 12.2.3). Tham chiếu gián tiếp có hiệu lực trong khuôn mẫu hiện hành sau khi lựa chọn ứng dụng.
2) Hoặc tham chiếu tệp DO'51' (xem 7.3.2 và Bảng 7). Tham chiếu gián tiếp có hiệu lực trong tệp được lựa chọn; nếu nó trống, nó có hiệu lực trong khuôn mẫu hiện hành.
3) Hoặc DO'4F' theo sau bởi DO'51' không trống tham chiếu tệp phải tồn tại trong ứng dụng. Tham chiếu gián tiếp có hiệu lực trong tệp này.
4) Hoặc một DO'52' (lệnh thực hiện). Tham chiếu gián tiếp có hiệu lực trong dữ liệu hồi đáp của lệnh này.
5) Hoặc một số DO'52'. Lệnh thực hiện được xử lý theo thứ tự trình bày. Tham chiếu gián tiếp có hiệu lực trong dữ liệu hồi đáp của lệnh cuối cùng hoặc trong VA tạm thời được thiết lập theo lệnh này.

Giải trình bao:

- Bắt đầu bằng giải phần thứ hai của trình bao, là cấu trúc tiêu chuẩn hoặc APDU hồi đáp. Nó kết thúc ở đó nếu tham chiếu gián tiếp là DO'80'.
- Nếu tham chiếu gián tiếp không phải là DO'80', nó kết thúc bằng giải tham chiếu gián tiếp được xác định trong 8.4.3, 8.4.4, 8.4.5.

Ví dụ: DO trình bao sau lồng danh sách thẻ và một lệnh thực hiện.

{'63'-L-{'5C'-L-(Tag1-Tag2-Tag3)}-{'52'-L-Command APDU}}

8.4.9 Trình bao được gắn thẻ

Dưới thẻ '63', DO mở rộng khuôn mẫu trong thẻ mà hỗ trợ giải tự động trình bao.

DO đầu tiên trong trường giá trị của DO'63' trình bao được gắn thẻ là DO'XY' trống. Thẻ 'XY' có hiệu lực trong GET DATA hoặc GET NEXT DATA C-RP khi khuôn mẫu mở rộng là khuôn mẫu hiện hành; 'XY' tôn trọng sơ đồ phân phối thẻ hiện hành. Số dư giá trị là giá trị của DO trình bao (xem 8.4.8). Kết quả của giải tham chiếu gián tiếp là giá trị của DO'XY' khi được giải quyết trong khuôn mẫu nó mở rộng (xem 8.2.2):

- Nếu trình bao tham chiếu DO'ZT', giá trị của DO'XY' là giá trị của DO'ZT' này (xem phụ lục G). Trình bao chỉ tham chiếu một DO, có khả năng được xây dựng.
- Nếu trình bao tham chiếu một chuỗi byte, giá trị của DO'XY' là chuỗi byte đó.

Chú thích 1 Cả ký hiệu 'XY' và 'ZT' đều không loại bỏ việc sử dụng thẻ bao gồm nhiều byte.

Chú thích 2 Giải tự động trình bao được gắn thẻ tạo ra trong khuôn mẫu hiện hành DO ảo. Thẻ của DO ảo này được lấy từ DO đầu tiên trong trình bao được gắn thẻ. Trường độ dài của DO này mã hóa độ dài của nội dung thao tác gián tiếp được giải. Giá trị của DO là nội dung của chính nó (xem ví dụ trong phụ lục G).

9 Cấu trúc an toàn

9.1 Tổng quát

Điều này mô tả trạng thái an toàn, thuộc tính an toàn và cơ chế an toàn.

Trạng thái an toàn - trạng thái an toàn mô tả trạng thái hiện hành có khả năng đạt được trên kênh lô-gic sau khi giao diện vật lý kích hoạt (xem 5.1) hoặc thiết lập lại kênh lô-gic và/hoặc thực hiện một hoặc một vài C-RP trên kênh lô-gic này có khả năng thực hiện thủ tục xác thực. Trạng thái an toàn cũng có thể dẫn đến hoàn thành thủ tục an toàn liên quan đến nhận dạng các thực thể liên quan, nếu có, ví dụ bằng cách chứng minh mật lệnh (ví dụ sử dụng lệnh VERIFY) hoặc khóa (ví dụ sử dụng lệnh GET CHALLENGE theo sau lệnh EXTERNAL AUTHENTICATE, hoặc sử dụng chuỗi lệnh GENERAL AUTHENTICATE) hoặc bằng thông điệp an toàn (ví dụ xác thực thông điệp). Năm trạng thái an toàn được xem xét.

- Trạng thái an toàn chung - trong thẻ sử dụng trật tự các DF, nó có thể được sửa đổi bằng cách hoàn thành thủ tục xác thực liên quan đến MF (ví dụ xác thực thực thể bằng mật lệnh hoặc khóa đi kèm với ứng dụng); nó có thể được duy trì, phục hồi hoặc bị mất do lựa chọn ứng dụng; sự sửa đổi này có thể chỉ liên quan đến ứng dụng mà thủ tục xác thực thuộc về. Nếu kênh lô-gic áp dụng, khi đó trạng thái an toàn ứng dụng cụ thể có thể phụ thuộc vào kênh lô-gic.
- Trạng thái an toàn tệp cụ thể - nó có thể được sửa đổi bằng cách hoàn thành thủ tục xác thực liên quan đến DF (ví dụ xác thực thực thể bằng mật lệnh hoặc khóa đi kèm với DF cụ thể); nó có thể được duy trì, phục hồi hoặc bị mất do lựa chọn tệp; sự sửa đổi này có thể chỉ liên quan đến các tệp trong ứng dụng mà thủ tục xác thực thuộc về. Nếu kênh lô-gic áp dụng, khi đó trạng thái an toàn tệp cụ thể có thể phụ thuộc vào kênh lô-gic.
- Trạng thái an toàn DO cụ thể - nó có thể được sửa đổi bằng cách hoàn thành thủ tục xác thực liên quan đến DO; nó có thể được duy trì, phục hồi hoặc bị mất do lựa chọn; sự sửa đổi này có thể chỉ liên quan đến DO trong ứng dụng mà thủ tục xác thực thuộc về. Nếu kênh lô-gic áp dụng, khi đó trạng thái an toàn DO cụ thể có thể phụ thuộc vào kênh lô-gic.
- Trạng thái an toàn lệnh cụ thể - nó chỉ tồn tại trong khi xử lý lệnh sử dụng thông điệp an toàn và xác thực bao hàm; lệnh như vậy có thể khiến cho trạng thái an toàn không đổi.

Thuộc tính an toàn - các thuộc tính an toàn, khi chúng tồn tại, xác định hành động nào được cho phép và theo điều kiện nào. Thuộc tính an toàn của cấu trúc phụ thuộc vào:

- Loại của chúng (DF, EF hoặc DO);
- CP tùy chọn trong DO'62' khuôn mẫu CP và/hoặc trong cấu trúc cha của nó;

Thuộc tính an toàn cũng có thể kết hợp với các lệnh, DO và Bảng và hiển thị. Đặc biệt, thuộc tính an toàn có thể

- Xác định trạng thái an toàn của thẻ có hiệu lực trước khi truy cập dữ liệu;
- Ngăn cản truy cập dữ liệu đến hàm cụ thể (ví dụ chỉ đọc) nếu thẻ có trạng thái cụ thể;
- Xác định hàm an toàn nào được thực hiện để đạt được trạng thái an toàn cụ thể.

Cơ chế an toàn - điều này xem xét cơ chế an toàn sau.

- Xác thực thực thể bằng mật lệnh - thẻ so sánh dữ liệu nhận được từ mọi đối tượng bên ngoài với dữ liệu mật bên trong. Cơ chế này có thể được sử dụng để bảo vệ quyền của người sử dụng.
- Xác thực thực thể bằng khóa - thực thể xác thực phải chứng minh sự nhận biết về khóa riêng hoặc bí mật có liên quan trong thủ tục xác thực (ví dụ lệnh GET CHALLENGE theo sau bởi lệnh EXTERNAL AUTHENTICATE, chuỗi các lệnh GENERAL AUTHENTICATE).
- Xác thực dữ liệu - sử dụng dữ liệu trong, hoặc khóa bí mật hoặc khóa công khai, thẻ kiểm tra dữ liệu dư nhận được từ mọi đối tượng bên ngoài. Cách khác, sử dụng dữ liệu mật bên trong, hoặc khóa mật hoặc khóa riêng, thẻ tính phần tử dữ liệu (kiểm tra tổng mã hóa hoặc chữ ký số) và chèn nó trong dữ liệu được gửi ra mọi đối tượng bên ngoài. Cơ chế này có thể được sử dụng để bảo vệ quyền của nhà cung cấp.
- Mã hóa dữ liệu - sử dụng dữ liệu mật bên trong, hoặc khóa mật hoặc khóa riêng, thẻ giải mã mật mã nhận được trong trường dữ liệu. Cách khác, sử dụng dữ liệu mật bên trong, hoặc khóa mật hoặc khóa riêng, thẻ tính tài liệu mã hóa và chèn vào trong trường dữ liệu, có thể cùng với dữ liệu khác. Cơ chế này có thể được sử dụng để cung cấp dịch vụ bảo mật, ví dụ quản lý khóa và truy cập có điều kiện. Cùng với cơ chế tài liệu mã hóa, tính bảo mật dữ liệu có thể đạt được bằng cách giấu dữ liệu. Trong trường hợp này, thẻ tính chuỗi byte ẩn và bổ sung nó bằng lệnh loại trừ -or đối với byte nhận được từ hoặc được gửi tới mọi đối tượng bên ngoài. Cơ chế này có thể được sử dụng để bảo vệ tính riêng tư và là biện pháp đối phó với nhận dạng mẫu.

Kết quả xác thực có thể được ghi bên trong theo các yêu cầu ứng dụng.

9.2 Khuôn mẫu định danh cơ chế mật mã

Một hoặc nhiều DO'AC' định danh cơ chế mật mã có thể xuất hiện trong CP của bất kỳ DF (xem Bảng 10). Mỗi cái biểu thị rõ ràng ý nghĩa của tham chiếu cơ chế mật mã trong DF và hệ phân cấp của nó. Khuôn mẫu bao gồm hai hoặc nhiều DO.

- DO đầu tiên là tham chiếu cơ chế mật mã, DO'80' (xem Bảng 55).
- DO thứ hai là định danh đối tượng, DO'06', như được xác định trong ISO/IEC 8825-1. Đối tượng định danh là cơ chế mật mã được xác định hoặc đăng ký trong tiêu chuẩn, ví dụ tiêu chuẩn ISO. Ví dụ về cơ chế mật mã là thuật giải mã hóa (ví dụ ISO/IEC 18033), mã xác thực thông điệp (ví dụ ISO/IEC 9797), giao thức xác thực (ví dụ ISO/IEC 9798), chữ ký số (ví dụ ISO/IEC 9796 hoặc ISO/IEC 14888), thuật giải mã hóa được đăng ký (ví dụ ISO/IEC 9979), vv...
- Nếu xuất hiện, một hoặc nhiều DO tiếp theo (DO'06' hoặc DO'13') hoặc định danh cơ chế được sử dụng bằng cơ chế trước đó (nghĩa là phương thức lựa chọn, ví dụ ISO/IEC 10116, hoặc hàm băm, ví dụ ISO/IEC 10118), hoặc thông số biểu thị (thẻ phụ thuộc vào cơ chế trước đó).

DO'13' đưa lại OID tương đối bắt rễ tại DO'06' gần nhất trước đấy như được xác định trong ISO/IEC 8825-1.

Ví dụ (xem giải thích trong phụ lục A và phụ lục B)

{'AC'-'0B'-{'80'-'01'-'01'}-{'06'-'06'-'28818C710201'}}

Khuôn mẫu cùng với tham chiếu địa phương '01' đối với thuật giải mã hóa đầu tiên trong ISO/IEC 18033-2

{'AC'-'11'-{'80'-'01'-'02'}-{'06'-'05'-'28CC460502'}-{'06'-'05'-'28CF060303'}}

Định danh đối tượng đầu tiên tham chiếu cơ chế xác thực thứ hai trong ISO/IEC 9798. Định danh đối tượng thứ hai tham chiếu hàm băm chuyên dụng thứ ba trong ISO/IEC 18033-3. Vì vậy, khuôn mẫu kết hợp tham chiếu địa phương '02' đến GQ2 sử dụng SHA-1.

9.3 Thuộc tính an toàn

Điều này xác định mã dữ liệu liên quan đến thuộc tính an toàn, và hai định dạng kết buộc thuộc tính an toàn và đối tượng: định dạng khối dựa trên ánh xạ bit và định dạng mở rộng mà mở rộng định dạng khối bằng quản lý danh sách TLV. Định dạng mở rộng có thể sử dụng mã được xác định đối với định dạng khối dưới các vỏ bọc khác nhau.

9.3.1 Mục tiêu thuộc tính an toàn

Được tham chiếu theo thẻ '86', '8B', '8C', '8E', '9C', 'A0', 'A1', 'A3', 'AB', thuộc tính an toàn có thể xuất hiện trong CP của bất kỳ tệp hoặc DO nào (xem Bảng 10). Bất kỳ đối tượng nào trong thẻ (ví dụ lệnh, tệp, DO, Bảng và hiển thị) có thể liên kết với hơn một thuộc tính an toàn và/hoặc với tham chiếu được bao gồm trong thuộc tính an toàn.

Trong môi trường SCQL (xem TCVN 11167-7 (ISO/IEC 7816-7), lệnh đối với ngôn ngữ hỏi thẻ cấu trúc), thuộc tính an toàn có thể được xác định trong hoạt động SCQL, ví dụ lệnh CREATE TABLE và CREATE VIEW. Nếu thuộc tính an toàn dựa trên mệnh đề này được sử dụng, khi đó chúng được truyền trong DO có thẻ '8B', '8C' hoặc 'AB' trong thông số thuộc tính san toàn của hoạt động SCQL.

Thuộc tính an toàn đối với DO BER-TLV được xác định trong 9.3.5. Thuộc tính an toàn đối với kênh lô-gic được xác định trong 9.3.7.

9.3.2 Định dạng khối

Trong định dạng khối, quy tắc truy cập bao gồm trường chế độ truy cập theo một hoặc nhiều byte điều kiện an toàn. Thuộc tính an toàn bao gồm một hoặc một số quy tắc truy cập kết nối.

Nếu một số quy tắc truy cập xuất hiện trong trường giá trị DO'8C' hoặc '9C' (xem Bảng 10), chúng đại diện cho điều kiện OR.

Trường chế độ truy cập - trường chế độ truy cập bao gồm hoặc một hoặc nhiều byte. Nếu trường chế độ truy cập bao gồm

- Một AMB, khi đó bit b7 đến b1 biểu thị hoặc không có byte điều kiện an toàn khi đặt là 0, hoặc có byte điều kiện an toàn trong cùng thứ tự (bit b7 đến b1) khi đặt là 1. Khi bit b8 được đặt là 1, bit b7 đến b4 có thể được sử dụng cho lệnh bổ sung, ví dụ lệnh ứng dụng cụ thể.
- Nhiều byte, byte đầu tiên của trường chế độ truy cập được đặt là '00'. Byte thứ hai và khả năng byte hơn nữa (xem Chú thích bên dưới) trong trường chế độ truy cập là AMB. Mỗi AMB biểu thị trong bit b8 liệu nó có là AMB cuối cùng hay không. Bit b8 được đặt là 0 trong AMB cuối cùng. Bit b8 được đặt là 1 trong tất cả các AMB khác. Bit b6 đến b1 biểu thị hoặc không có byte điều kiện an toàn khi đặt là 0, hoặc có byte điều kiện an toàn trong cùng thứ tự (bit b6 đến b1) khi đặt là 1 và trong cùng thứ tự như AMB. Khi bit b7 được đặt là 1, bit b6 đến b1 có thể được sử dụng cho lệnh bổ sung, ví dụ lệnh ứng dụng cụ thể.

Chú thích AMB hơn nữa không được xác định trong ISO/IEC 7816-4, và có thể được xác định trong bản in trong tương lai hoặc các phần khác của tiêu chuẩn này.

Bảng 17 đến Bảng 29 xác định byte chế độ truy cập riêng cho DF, EF, DO và Bảng và hiển thị.

Bảng 17 - Mã hóa byte đơn trong trường chế độ truy cập đối với DF

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	-	-	-	-	-	-	-	Bit b7 đến b1 theo Bảng này
1	-	-	-	-	-	-	-	Bit b3 đến b1 theo Bảng này (bit b7 đến b4 độc quyền)
0	1	-	-	-	-	-	-	DELETE FILE (bản thân)
0	-	1	-	-	-	-	-	TERMINATE CARD USAGE (MF), TERMINATE DF
0	-	-	1	-	-	-	-	ACTIVATE FILE
0	-	-	-	1	-	-	-	DEACTIVATE FILE
-	-	-	-	-	1	-	-	CREATE FILE (tạo DF)
-	-	-	-	-	-	1	-	CREATE FILE (tạo EF)
-	-	-	-	-	-	-	1	DELETE FILE (con)

Bảng 18 - Mã hóa byte đơn trong trường chế độ truy cập đối với EF

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	-	-	-	-	-	-	-	Bit b7 đến b1 theo Bảng này
1	-	-	-	-	-	-	-	Bit b3 đến b1 theo Bảng này (bit b7 đến b4 độc quyền)
0	1	-	-	-	-	-	-	DELETE FILE
0	-	1	-	-	-	-	-	TERMINATE EF
0	-	-	1	-	-	-	-	ACTIVATE FILE, ACTIVATE RECORD
0	-	-	-	1	-	-	-	DEACTIVATE FILE, DEACTIVATE RECORD
-	-	-	-	-	1	-	-	WRITE BINARY, WRITE RECORD, APPEND RECORD
-	-	-	-	-	-	1	-	UPDATE BINARY, UPDATE RECORD, ERASE BINARY, ERASE RECORD
-	-	-	-	-	-	-	1	READ BINARY/RECORD, SEARCH BINARY/RECORD, COMPARE BINARY/RECORD

Bảng 19 - Mã hóa byte đơn trong trường chế độ truy cập đối với DO

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	-	-	-	-	-	-	-	Bit b7 đến b1 theo Bảng này
1	-	-	-	-	-	-	-	Bit b3 đến b1 theo Bảng này (bit b7 đến b4 độc quyền)
0	1	-	-	-	-	-	-	DELETE DATA
0	-	1	-	-	-	-	-	MANAGE DATA Hủy bỏ
0	-	-	1	-	-	-	-	MANAGE DATA Kích hoạt
0	-	-	-	1	-	-	-	MANAGE DATA Giải hoạt
-	-	-	-	-	1	-	-	MANAGE SECURITY ENVIRONMENT
-	-	-	-	-	-	1	-	PUT DATA/PUT NEXT DATA/UPDATE DATA
-	-	-	-	-	-	-	1	GET DATA/GET NEXT DATA/COMPARE DATA

Bảng 20 - Mã hóa byte đơn trong trường chế độ truy cập đối với đối tượng an toàn

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	-	-	-	-	-	-	-	Bit b7 đến b1 theo Bảng này
1	-	-	-	-	-	-	-	Bit b3 đến b1 theo Bảng này (bit b7 đến b4 độc quyền)
0	x	-	-	-	-	-	-	0 (mọi giá trị khác là RFU)
0	-	1	-	-	-	-	-	*TERMINATE*[a]
0	-	-	1	-	-	-	-	*ACTIVATE*[a]
0	-	-	-	1	-	-	-	*DEACTIVATE*[a]
-	-	-	-	-	x	-	-	0 (mọi giá trị khác là RFU)
-	-	-	-	-	-	1	-	*PUT/UPDATE*[a]
-	-	-	-	-	-	-	1	*GET*[a]
[a] mô tả trong định dạng in nghiêng có nghĩa là hoạt động và không phải là lệnh								

Bảng 21 - Mã hóa byte đơn trong trường chế độ truy cập đối với Bảng và hiển thị

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	-	-	-	-	-	-	-	Bit b7 đến b1 theo Bảng này
CREATE USER, DELETE USER1	-	-	-	-	-	-	-	Bit b3 đến b1 theo Bảng này (bit b7 đến b4 độc quyền)
01 0	-	1	-	-	-	-	-	GRANT, REVOKE
0	-	-	1	-	-	-	-	CREATE TABLE, CREATE VIEW, CREATE DICTIONARY
0	-	-	-	1	-	-	-	DROP TABLE, DROP VIEW
-	-	-	-	-	1	-	-	INSERT
-	-	-	-	-	-	1	-	UPDATE, DELETE
-	-	-	-	-	-	-	1	FETCH

Bảng 22 - Mã hóa byte thứ hai trong trường chế độ truy cập (AMB đầu tiên) đối với DF

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	-	-	-	-	-	-	-	Byte cuối cùng của trường chế độ truy cập
1	-	-	-	-	-	-	-	Byte khác theo trong trường chế độ truy cập
-	0	-	-	-	-	-	-	Bit b6 đến b1 theo tiêu chuẩn này
-	1		-	-	-	-	-	Bit b6 đến b1 độc quyền
-	0	1	-	-	-	-	-	TERMINATE CARD USAGE (MF), TERMINATE DF
-	0	-	1	-	-	-	-	ACTIVATE FILE
-	0	-	-	1	-	-	-	DEACTIVATE FILE
-	0	-	-	-	1	-	-	CREATE FILE (tạo DF)
-	0	-	-	-	-	1	-	CREATE FILE (tạo EF)
-	0	-	-	-	-	-	1	DELETE FILE

Bảng 23 - Mã hóa byte thứ ba trong trường chế độ truy cập (AMB thứ hai) đối với DF

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	-	-	-	-	-	-	Cùng mã và ý nghĩa như trong Bảng 22
-	0	1	-	-	-	-	-	DELETE FILE (bản thân)
-	0	-	1	-	-	-	-	APPLICATION MANAGEMENT REQUEST
-	0	-	-	1	-	-	-	REMOVE APPLICATION
-	0	-	-	-	x	x	x	000 (mọi giá trị khác là RFU)

Bảng 24 - Mã hóa byte thứ tư trong trường chế độ truy cập (AMB thứ ba) đối với DF

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	-	-	-	-	-	-	Cùng mã và ý nghĩa như trong Bảng 22
-	0	x	x	x	x	-	-	000 (mọi giá trị khác là RFU)
-	0	-	-	-	-	1	-	Đối tượng dữ liệu tạo lệnh (xem TCVN 11167-9 (ISO/IEC 7816-9))
-	0	-	-	-	-	-	1	DELETE DATA

Bảng 25 - Mã hóa byte thứ hai trong trường chế độ truy cập (AMB đầu tiên) đối với EF

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	-	-	-	-	-	-	Cùng mã và ý nghĩa như trong Bảng 22
-	0	1	-	-	-	-	-	TERMINATE EF
-	0	-	1	-	-	-	-	ACTIVATE FILE, ACTIVATE RECORD
-	0	-	-	1	-	-	-	DE ACTIVATE FILE, DEACTIVATE RECORD
-	0	-	-	-	1	-	-	APPEND RECORD
-	0	-	-	-	-	1	-	UPDATE BINARY, UPDATE RECORD
-	0	-	-	-	-	-	1	READ BINARY/RECORD, SEARCH BINARY/RECORD

Bảng 26 - Mã hóa byte thứ ba trong trường chế độ truy cập (AMB thứ hai) đối với EF

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	-	-	-	-	-	-	Cùng mã và ý nghĩa như trong Bảng 22
-	0	1	-	-	-	-	-	DELETE EF
-	0	-	x	x	-	-	-	00 (mọi giá trị khác là RFU)
-	0	-	-	-	1	-	-	WRITE BINARY, WRITE RECORD
-	0	-	-	-	-	1	-	ERASE BINARY,ERASE RECORD
-	0	-	-	-	-	-	1	COMPARE BINARY/RECORD

Bảng 27 - Mã hóa byte thứ tư trong trường chế độ truy cập (AMB thứ ba) đối với EF

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	-	-	-	-	-	-	Cùng mã và ý nghĩa như trong Bảng 22
-	0	x	x	x	x	-	-	0000 (mọi giá trị khác là RFU)
-	0	-	-	-	-	1	-	Đối tượng dữ liệu tạo lệnh (xem TCVN 11167-9 (ISO/IEC 7816-9))
-	0	-	-	-	-	-	1	DELETE DATA

Bảng 28 - Mã hóa byte thứ hai trong trường chế độ truy cập (AMB đầu tiên) đối với DO

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	-	-	-	-	-	-	Cùng mã và ý nghĩa như trong Bảng 22
-	0	1	-	-	-	-	-	MANAGE DATA Hủy bỏ
-	0	-	1	-	-	-	-	MANAGE DATA Kích hoạt
-	0	-	-	1	-	-	-	MANAGE DATA Giải hoạt
-	0	-	-	-	1	-	-	MANAGE SECURITY ENVIRONMENT
-	0	-	-	-	-	1	-	PUT DATA/UPDATE DATA
-	0	-	-	-	-	-	1	GET DATA/GET NEXT DATA

Bảng 29 - Mã hóa byte thứ ba trong trường chế độ truy cập (AMB thứ hai) đối với DO

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	-	-	-	-	-	-	Cùng mã và ý nghĩa như trong Bảng 22
-	0	1	-	-	-	-	-	DELETE DATA
-	0	-	1	-	-	-	-	Đối tượng dữ liệu tạo lệnh (xem TCVN 11167-9 (ISO/IEC 7816-9))
-	0	-	-	x	x	-	-	00 (mọi giá trị khác là RFU)
-	0	-	-	-	-	1	-	PUT NEXT DATA
-	0	-	-	-	-	-	1	COMPARE DATA

Byte điều kiện an toàn - mỗi byte điều kiện an toàn xác định cơ chế an toàn nào cần thiết thích hợp với quy tắc truy cập. Bảng 30 thể hiện byte điều kiện an toàn. Bit b8 đến b5 biểu thị điều kiện an toàn yêu cầu. Nếu không phải là tất cả bằng nhau, bit b4 đến b1 định danh:

- Hoặc môi trường an toàn (xem 10.3.3, SEID từ '01' đến '0E').
- Hoặc DO'AD' (xem 9.3.6) theo số của nó từ '01' đến '0E'. DO'AD' là CP dưới cùng DO'62' là thuộc tính an toàn.

Bảng 30 - Mã hóa byte điều kiện an toàn

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa	
0	0	0	0	0	0	0	0	Luôn luôn	
1	1	1	1	1	1	1	1	Không bao giờ	
-	-	-	-	0	0	0	0	Không tham chiếu với môi trường an toàn, không tham chiếu với DO'AD'	
-	-	-	-	Không phải là tất cả bằng nhau				Dưới thẻ '8C'[1] hoặc '9E'[2]	SEID (xem 10.3.3)
								Dưới thẻ '9C'[1] hoặc '9D'[2]	Số chuỗi của SPT DO'AD' (xem Bảng 38)
0	-	-	-	-	-	-	-	Ít nhất một điều kiện	
1	-	-	-	-	-	-	-	Tất cả các điều kiện	
-	1	-	-	-	-	-	-	Thông điệp an toàn	
-	-	1	-	-	-	-	-	Xác thực ngoài	
-	-		1	-	-	-	-	Xác thực người sử dụng (ví dụ. mật lệnh)	

[1] đối với sử dụng trong định dạng khối (dưới thẻ '62', xem Bảng 10).

[2] đối với sử dụng trong định dạng mở rộng (xem Bảng 33).

Cơ chế được xác định trong môi trường an toàn, hoặc trong DO'AD' được sử dụng theo chỉ báo trong bit b7 đến b5 đối với bảo vệ lệnh và/hoặc xác thực bên ngoài và/hoặc xác thực người sử dụng.

- Nếu bit b8 được đặt là 1, khi đó tất cả các điều kiện được thiết lập trong bit b7 đến b5 được thỏa mãn.
- Nếu bit b8 được đặt là 0, khi đó ít nhất một trong các điều kiện được thiết lập trong bit b7 đến b5 được thỏa mãn.
- Nếu bit 7 được đặt là 1, trong điều kiện an toàn tham chiếu môi trường an toàn, khi đó khuôn mẫu tham chiếu điều khiển (xem 10.3.1) của môi trường an toàn mô tả liệu SM áp dụng với trường dữ liệu lệnh và/hoặc với trường dữ liệu hồi đáp (xem byte định tính sử dụng, Bảng 57). Nếu điều kiện an toàn biểu thị một số DO'AD', SEID liên quan khả dụng hoặc trong DO'AD' hoặc trong mở rộng thuộc tính an toàn lồng trong DO'AD'.
- Nếu b8 = b7 = b6 = b5 = 0, và nếu b4 b3 b2 b1 biểu thị số DO'AD' hiệu lực, DO biểu thức Boole xuất hiện trong DO'AD' (xem 9.3.6.11).

9.3.3 Định dạng mở rộng

9.3.3.1 Tổng quát

Trong định dạng mở rộng, quy tắc truy cập bao gồm DO chế độ truy cập theo sau bởi một hoặc nhiều DO điều kiện an toàn. Điều khiển truy cập đối với một đối tượng được quản lý bằng cách tham chiếu quy tắc truy cập từ đối tượng liên quan. DO'AB" có thể xuất hiện trong CP của bất kỳ tệp nào (xem Bảng 10) đối với các quy tắc truy cập như vậy.

DO chế độ truy cập - DO chế độ truy cập bao gồm hoặc trường chế độ truy cập (xem Bảng 17 đến Bảng 29 và Bảng 41 đến Bảng 44) hoặc danh sách các mô tả lệnh hoặc mô tả máy trạng thái độc

quyền; DO điều kiện an toàn tiếp theo thích hợp với tất cả các lệnh biểu thị. Bảng 31 thể hiện DO chế độ truy cập.

Bảng 31 - Mã hóa DO chế độ truy cập

Thẻ	Độ dài	Giá trị	Ý nghĩa
'80'	Thay đổi	Trường chế độ truy cập	Xem Bảng 17 đến Bảng 29 và Bảng 41 đến Bảng 44
'81' đến '8F'	Thay đổi	Mô tả tiêu đề lệnh	Danh sách (phần) tiêu đề lệnh (xem Bảng 32)
'9C'	Thay đổi		Mô tả máy trạng thái độc quyền

Nếu thẻ từ '81' đến '8F', khi đó phần tử dữ liệu chế độ truy cập đại diện danh sách các tập hợp có thể của giá trị bốn byte CLA, INS, P1 và P2 trong tiêu đề lệnh. Phụ thuộc vào bit b4 đến b1 của thẻ, danh sách bao gồm chỉ các giá trị như được mô tả trong Bảng 32. Một số nhóm có thể xuất hiện để xác định tập hợp lệnh, ví dụ giá trị của INS P1 P2, INS P1 P2, .. đối với thẻ '87'.

Bảng 32 - Mã hóa thẻ '81' đến '8F' đối với DO chế độ truy cập

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
1	0	0	0	x	x	x	x	Mô tả lệnh bao gồm
1	0	0	0	1	-	-	-	- (CLA), nghĩa là giá trị của CLA
1	0	0	0	-	1	-	-	- (INS), nghĩa là giá trị của INS
1	0	0	0	-	-	1	-	- (P1), nghĩa là giá trị của P1
1	0	0	0	-	-	-	1	- (P2), nghĩa là giá trị của P2
– Giá trị của CLA mã hóa không là số dành cho kênh lô-gic có ý nghĩa là mô tả độc lập với kênh lô-gic								

Đối tượng dữ liệu điều kiện an toàn - theo Bảng 33, DO điều kiện an toàn xác định hành động an toàn được yêu cầu để truy cập đối tượng được bảo vệ qua DO chế độ truy cập đặc biệt. Nếu được sử dụng là điều kiện an toàn, khuôn mẫu tham chiếu điều khiển (xem 10.3.1) được tham chiếu bởi thẻ 'A4' (AT), 'B4' (AT), 'B6' (DST) hoặc 'B8' (CT) bao gồm một DO định danh sử dụng (xem Bảng 57) biểu thị hành động an toàn.

Bảng 33 - Mã hóa DO điều kiện an toàn

Thẻ	Độ dài	Giá trị	Ý nghĩa
'90'	0	-	Luôn luôn
'97'	0	-	Không bao giờ
'9D', '9E'	1	Byte điều kiện an toàn	Xem Bảng 30
'A4'	Thay đổi	Khuôn mẫu tham chiếu điều khiển	Xác thực người sử dụng hoặc bên ngoài phụ thuộc vào định tính sử dụng
'AB'	Thay đổi	Khuôn mẫu điều kiện trạng thái đối tượng	Xem 9.3.3.2
'B4', 'B6', 'B8'	Thay đổi	Khuôn mẫu tham chiếu điều khiển	SM trong lệnh và/hoặc hồi đáp phụ thuộc vào định tính sử dụng
'A0'	Thay đổi	DO điều kiện an toàn	Ít nhất một điều kiện an toàn được thực hiện (khuôn mẫu OR)
'A7'	Thay đổi	DO điều kiện an toàn	Nghịch đảo của điều kiện an toàn (khuôn mẫu OR)
'A'	Thay đổi	DO điều kiện an toàn	Mọi điều kiện an toàn được thực hiện (khuôn mẫu AND)
'BE'	Thay đổi	Khuôn mẫu điều kiện an toàn Boole.	Tham chiếu giá trị của các điều xuất hiện trong thẻ

Một số DO điều kiện an toàn có thể được gắn với cùng hoạt động.

- Nếu DO điều kiện an toàn được lồng trong khuôn mẫu OR (thẻ 'A0'), khi đó ít nhất một điều kiện an toàn được thực hiện trước khi hành động.
- Nếu DO điều kiện an toàn không được lồng trong khuôn mẫu OR (thẻ 'A0') hoặc nếu chúng được lồng trong khuôn mẫu AND (thẻ 'AF'), khi đó mọi điều kiện an toàn được thực hiện trước khi hành động.
- Giá trị của điều kiện an toàn NOT (thẻ 'A7') là nghịch đảo lô-gic của giá trị của điều kiện an toàn nó lồng vào.

9.3.3.2 Khuôn mẫu điều kiện trạng thái đối tượng

Khuôn mẫu cung cấp khả năng khiến cho điều kiện an toàn phụ thuộc:

- Giá trị hiện hành của một đối tượng (EF, DO), được tham chiếu trong khuôn mẫu điều kiện trạng thái đối tượng.
- Giá trị hiện hành của một thuộc tính liên quan đến (EF, DF, DO, khóa hoặc mật lệnh) được tham chiếu trong khuôn mẫu điều kiện trạng thái đối tượng.
- Giá trị hiện hành của dữ liệu trong OS (ví dụ đồng hồ hệ thống)
- Giá trị hiện hành của (phần của) thông điệp lệnh

Khuôn mẫu được lập thành bốn phần khác nhau:

- Đối tượng dữ liệu điều kiện bắt buộc xác định hoạt động được thực hiện để so sánh giá trị tham chiếu với dữ liệu so sánh được cho trong khuôn mẫu.
- DO định vị đối tượng bắt buộc: bộ định vị đối tượng định danh rõ ràng dữ liệu được sử dụng để so sánh.

- Dữ liệu so sánh bắt buộc được so sánh với giá trị của đối tượng tham chiếu hoặc giá trị của một thuộc tính liên quan đến đối tượng tham chiếu.
- Bộ lọc nhị phân tùy chọn được áp dụng với dữ liệu để được so sánh (AND lô-gic) trước khi so sánh.

Bảng 34 thể hiện khuôn mẫu điều kiện trạng thái đối tượng

Bảng 35 cùng với Bảng 36 thể hiện đối tượng dữ liệu điều kiện

Bảng 34 - SC-DO giành cho mô tả các điều kiện truy cập phụ thuộc vào thuộc tính đối tượng

Bảng 34 - SC-DO giành cho mô tả

Thẻ	Độ dài	Giá trị	Ý nghĩa
'AB'	Thay đổi	Điều kiện DO'9E' Bộ định vị đối tượng theo Bảng 37 (thẻ '7F72') Bộ lọc nhị phân DO'5F71' (tùy chọn) Dữ liệu so sánh (thẻ '53')	Điều kiện trạng thái đối tượng

Bảng 35 - Mã hóa đối tượng dữ liệu điều kiện

Thẻ Độ dài	Giá trị	
'9E'	'01'	Quy tắc xác minh thuộc tính đối tượng (xem Bảng 36)

Bảng 36 - Giá trị mã hóa điều kiện

Giá trị	Điều kiện được thực hiện nếu
'01'	<, giá trị của thuộc tính/đối tượng tham chiếu nhỏ hơn giá trị được cho
'02'	≤, giá trị của thuộc tính/đối tượng tham chiếu nhỏ hơn hoặc bằng giá trị được cho
'03'	=, giá trị của thuộc tính/đối tượng tham chiếu bằng dữ liệu so sánh được cho
'04'	≥, giá trị của thuộc tính/đối tượng tham chiếu lớn hơn hoặc bằng dữ liệu so sánh được cho
'05'	>, giá trị của thuộc tính/đối tượng tham chiếu lớn hơn dữ liệu so sánh được cho
'06'	#, giá trị của thuộc tính/đối tượng tham chiếu không bằng dữ liệu so sánh được cho
Theo độ dài bằng của đối tượng	

Điều kiện an toàn được mô tả theo khuôn mẫu điều kiện trạng thái đối tượng không được thực hiện nếu giá trị thuộc tính/đối tượng tham chiếu không thực hiện điều kiện được xác định bởi DO điều kiện.

9.3.3.3 Bộ định vị đối tượng

Bộ định vị đối tượng cung cấp tham chiếu đối với đối tượng được lưu trữ trong thẻ. Loại đối tượng sau có thể được tham chiếu:

- Khóa cụ thể MF hoặc DF
- Mật lệnh cụ thể MF hoặc DF
- Đối tượng dữ liệu ứng dụng cụ thể
- EF hoặc DF
- Dữ liệu hệ thống đặc biệt được quản lý bằng thẻ
- Phần tử dữ liệu của thông điệp lệnh

Bộ định vị đối tượng được đại diện bằng khuôn mẫu '7F72'. Khuôn mẫu được soạn thảo bằng một DO tham chiếu đối tượng (bắt buộc) theo sau bởi DO tham chiếu thuộc tính (có điều kiện). Loại DO tham chiếu đối tượng phụ thuộc vào đối tượng được tham chiếu (EF, DF, DO, khóa, mật lệnh). Bảng 37 liệt kê DO tham chiếu đối tượng phụ thuộc vào loại đối tượng tham chiếu.

Khuôn mẫu tham chiếu mật mã (CRT) theo 10.3.1 được sử dụng để tham chiếu khóa hoặc mật lệnh. CRT phải chứa ít nhất một đối tượng dữ liệu tham chiếu (DO'83' hoặc '84'). Đối tượng dữ liệu hơn nữa từ Bảng 51 có thể được sử dụng (ví dụ định tính sử dụng) nếu được yêu cầu định tính tham chiếu hơn nữa. DO bắt buộc (trống) sau tham chiếu bằng thẻ của mình cho thuộc tính khóa dự định từ Bảng 40.

Bộ định vị đối tượng theo Bảng 37 được sử dụng để tham chiếu hoặc

- Một thông số kiểm soát của DF, EF hoặc DO
- (phần của) nội dung dữ liệu trong EF trong suốt
- (phần của) nội dung dữ liệu trong bản ghi EF cấu trúc
- Trường giá trị của DO

Nếu tham chiếu DF được xác định, đối tượng dữ liệu thứ hai phải tuân theo, biểu thị đối tượng thông số kiểm soát từ Bảng 10. Nếu EF hoặc DO được tham chiếu, DO thứ hai là tùy chọn. Nếu xuất hiện, nó phải biểu thị thông số kiểm soát của EF hoặc DO theo cùng cách thức như đối với DF. Nếu không xuất hiện, bộ định vị đối tượng tham chiếu nội dung dữ liệu của EF (EF trong suốt), nội dung dữ liệu của bản ghi trong EF hoặc trường giá trị của DO.

Để tham chiếu với dữ liệu hệ thống trong OS, DO'80' trống được sử dụng. DO bắt buộc sau biểu thị phần nào của APDU lệnh được thực hiện. DO'A1' được sử dụng để giải quyết hoặc

- (một phần của) trường dữ liệu, được xác định bằng khoảng chừa trống và độ dài
- (một phần của) trường dữ liệu của đối tượng dữ liệu được chứa trong trường dữ liệu.

Đối tượng dữ liệu dự định trong trường dữ liệu được xác định bằng danh sách thẻ. Nếu không có danh sách thẻ được cho, trường dữ liệu lệnh nằm trong phạm vi tiêu điểm của bộ định vị đối tượng. Sử dụng DO khoảng chừa trống và/hoặc DO độ dài, vùng liên quan đến trường dữ liệu lệnh/trường giá trị DO có thể bị cấm. Nếu DO khoảng chừa trống bị thiếu, giá trị khoảng chừa trống bằng 0 mặc nhiên được sử dụng. Nếu DO độ dài bị thiếu bộ định vị đối tượng tham chiếu với vùng đầy đủ bắt đầu từ vị trí được biểu thị bằng khoảng chừa trống đến cuối trường dữ liệu của APDU lệnh/trường giá trị của đối tượng dữ liệu.

Bảng 37 - Mã hóa bộ định vị đối tượng DO'7F72'

Loại đối tượng	DO tham chiếu đối tượng	DO tham chiếu thuộc tính
Khóa	CRT chứa ít nhất một DO('83' hoặc '84') tham chiếu khóa	DO trống (bắt buộc), thẻ tham chiếu thuộc tính khóa liên quan (xem Bảng 40)
Mật lệnh	CRT chứa ít nhất một DO'83' tham chiếu mật lệnh và DO'95' định tính sử dụng	DO trống (bắt buộc), thẻ tham chiếu thuộc tính khóa liên quan (xem Bảng 40)
DF	Khuôn mẫu tham chiếu chung '60' (xem Bảng 86) biểu thị một DF	DO trống (bắt buộc), thẻ tham chiếu đối tượng thông số kiểm soát liên quan (xem Bảng 10)
CP của EF hoặc DO	Khuôn mẫu tham chiếu chung '60' (xem Bảng 86) biểu thị một EF hoặc DO	DO trống (bắt buộc), thẻ tham chiếu đối tượng thông số kiểm soát liên quan (xem Bảng 10)
Bản ghi, chuỗi dữ liệu hoặc phần tử dữ liệu	Khuôn mẫu tham chiếu chung '60' (xem Bảng 86) biểu thị một bản ghi hoặc chuỗi dữ liệu n EF hoặc trường giá trị của đối tượng dữ liệu (có khả năng định vị trong EF)	Không có
Dữ liệu hệ thống	DO'80' (trống) biểu thị vùng dữ liệu hệ thống bên trong	Đối tượng dữ liệu (trống) biểu thị phần tử dữ liệu hệ thống dự định (độc quyền)
Thông điệp lệnh	DO'81' (trống) biểu thị APDU lệnh	Một trong các đối tượng dữ liệu sau (bắt buộc): '89': tham chiếu tiêu đề lệnh (DO trống) '96': tham chiếu giá trị N_e của APDU lệnh (DO trống) 'A1': Do dữ liệu lệnh; có thể chứa DO sau theo thứ tự được cho – Danh sách thẻ biểu thị một DO của trường dữ liệu lệnh (tùy chọn) – DO'54' khoảng chừa trống (tùy chọn) – DO'02' độ dài (tùy chọn) DO'A1' trống tham chiếu trường dữ liệu hoàn thành của APDU lệnh

9.3.3.4 Giá trị bộ lọc nhị phân (tùy chọn)

DO'5F71' bộ lọc nhị phân cung cấp mặt nạ nhị phân được sử dụng trong hoạt động AND lô-gic với dữ liệu được so sánh trước khi so sánh.

9.3.3.5 Dữ liệu so sanh

DO'53' dữ liệu so sánh cung cấp đại diện nhị phân của giá trị được so sánh với dữ liệu được xác định bằng bộ định vị.

9.3.4 Tham chiếu quy tắc truy cập

Quy tắc truy cập trong định dạng mở rộng có thể được lưu trữ trong EF hỗ trợ cấu trúc tuyến tính có bản ghi có kích cỡ biến đổi. EF như vậy được gọi là EF.ARR. Một hoặc nhiều quy tắc truy cập có thể được lưu trữ trong mỗi bản ghi được tham chiếu bằng số bản ghi. Số bản ghi như vậy được gọi là byte ARR. Bảng 38 mô tả bố cục của một EF.ARR.

Bảng 38 - Bố cục EF.ARR

Số bản ghi (byte ARR)	Nội dung bản ghi (một hoặc nhiều quy tắc truy cập)
1	DO chế độ truy cập, một hoặc nhiều DO điều kiện an toàn, DO chế độ truy cập, ...
2	DO chế độ truy cập, một hoặc nhiều DO điều kiện an toàn, ...
...	...
N	DO chế độ truy cập, một hoặc nhiều DO điều kiện an toàn, ...

DO'8B' thuộc tính an toàn tham chiếu định dạng mở rộng (xem Bảng 39) có thể xuất hiện trong CP của bất kỳ tệp nào hoặc DO (xem Bảng 10).

- Nếu độ dài là một, khi đó trường giá trị là một byte ARR tham chiếu bản ghi trong EF.ARR đã hoàn toàn biết.
- Nếu độ dài là ba, khi đó trường giá trị là một định danh tệp theo sau bởi một byte ARR; định danh tệp tham chiếu EF.ARR và byte ARR là số bản ghi trong EF.ARR.
- Nếu độ dài là chẵn và ít nhất là bốn, khi đó trường giá trị là định danh tệp theo sau bởi một hoặc nhiều cặp byte. Mỗi cặp bao gồm một SEID theo sau bởi một byte ARR; SEID định danh môi trường an toàn mà quy tắc truy cập được tham chiếu bằng byte ARR áp dụng.

Bảng 39 - DO thuộc tính an toàn tham chiếu định dạng mở rộng

Thẻ	Độ dài	Giá trị
'8B'	1	Byte ARR (một byte)
	3	Định danh tệp (2 byte) - byte ARR (một byte)
	Chẵn, > 3	Định danh tệp (2 byte) - SEID (một byte) - byte ARR (một byte) - (byte SEID - byte ARR) - ...

Byte ARR của SE hiện hành biểu thị quy tắc truy cập có hiệu lực đối với truy cập hiện hành vào DF ứng dụng.

CHÚ THÍCH Nếu không SE được thiết lập trong lệnh MANAGE SECURITY ENVIRONMENT trước đó, khi đó SE mặc định là SE hiện hành.

9.3.5 Thuộc tính an toàn đối với đối tượng dữ liệu

Chi tiết các đặc tính liên quan đến an toàn là DO, được định danh theo thẻ của nó trong khuôn mẫu hiện hành đi cùng với VA. Bất kỳ DO nào có thể có thông số kiểm soát được thể hiện tại giao diện thẻ là DO'62' lồng đặc tính an toàn đối với DO đó. Khi DO không có đặc tính thông số kiểm soát, thuộc tính an toàn của tệp cha phải được kế thừa.

Khi nó thuộc về mở rộng tệp, thuộc tính an toàn của DO phải không kế thừa từ tệp cha trình bao gắn thẻ. Thuộc tính an toàn của nó là các thuộc tính được xác định mà tham chiếu gián tiếp hướng vào.

Dưới thẻ 'A0', khuôn mẫu thuộc tính an toàn đối với DO có thể xuất hiện trong CP của bất kỳ tệp hoặc DO (xem Bảng 10). Khuôn mẫu như vậy:

- Bắt đầu với DO thuộc tính an toàn (thẻ '86', '8B', '8C', '8E', '9C', 'A0', 'A1', 'AB');
- Kết thúc với DO'5C' danh sách thẻ có thể để trống.

Danh sách thẻ chỉ bao gồm thẻ thuộc về khuôn mẫu cơ sở mà DO'62' lồng trong DO'A0' thuộc về, hoặc thẻ của DO được mong đợi bổ sung vào khuôn mẫu này. Khi danh sách thẻ trống, khuôn mẫu thuộc tính an toàn có hiệu lực đối với toàn bộ khuôn mẫu cơ sở mà DO'62' thuộc về.

9.3.6 Khuôn mẫu thông số an toàn

9.3.6.1 Đặc tính chung

Khuôn mẫu thông số an toàn, DO'AD' dưới DO'62', cung cấp sự mở rộng của thuộc tính an toàn đi cùng với đối tượng an toàn (ví dụ khóa, mật lệnh...) hoặc một DO chứng thực xử lý an toàn (xem 9.3.6.2). Bất kỳ DO'AD' nào hỗ trợ hàm này phải bao gồm hoặc trình bao hoặc trình bao được gắn thẻ DO'63' (xem 8.4.9 và 9.3.6.2) đưa lại tham chiếu gián tiếp với đối tượng an toàn hoặc DO. Nó có thể đưa lại thông số sử dụng dữ liệu mô tả đặc tính và điều kiện sử dụng của DO này.

Một DO'AD' lồng trong DO'AD' có cùng mã hóa như DO'AD' lồng trong DO'62'.

Như bất kỳ khuôn mẫu nào, khuôn mẫu thông số an toàn có thể lồng vào một DO'62'. Trong DO này, thuộc tính an toàn đối với DO có ý nghĩa được xác định trong 9.3.5. Tất cả các thuộc tính an toàn khác áp dụng đối với đối tượng an toàn (xem Bảng 20 về mã hóa byte chế độ truy cập).

Ví dụ: trong DO'62' dưới DO'AD', DO sau có thể xuất hiện cả:

- DO {A0 06 {8CXYZT}{5C01B3}có ý nghĩa thông thường, nghĩa là thuộc tính an toàn để truy cập DO'B3" bao gồm DO được xác định bằng một OID.
- DO {8CXYZ} hoặc {ABXY...} mã hóa thuộc tính an toàn để truy cập DO lồng trong đối tượng an toàn (xem Bảng 20).

DO'AD' cũng có thể được tham chiếu bằng bất kỳ lệnh nào sử dụng DO này hoặc đối tượng an toàn mà DO'AD' được kết nối.

Nếu biểu thức Boole được là TRUE để cho phép thực hiện C-RP, DO xác định biểu thức Boole này phải xuất hiện trong DO'AD' (xem 9.3.6.11).

9.3.6.2 Mở rộng thuộc tính an toàn

Tất cả các DO có thẻ từ 'A0' đến 'A5' định danh loại đối tượng an toàn. Mỗi loại có byte chế độ truy cập cụ thể (xem Bảng 41 đến Bảng 44). Thuộc tính an toàn đối với khóa Diffie-Hellman không liên quan, do vậy DO'A5' luôn trống.

Bất kỳ DO có thẻ từ 'A0' đến 'A4' phải lồng vào:

- Hoặc một DO'8C' lồng thuộc tính an toàn trong định dạng khối (xem 9.3.2), tham chiếu SE.
- Hoặc DO'9C' lồng thuộc tính an toàn trong định dạng khối (xem 9.3.2), tham chiếu SPT.
- Hoặc DO'AB' lồng thuộc tính an toàn trong định dạng mở rộng (xem 9.3.3), mà DO'9D' byte điều kiện an toàn có thể được sử dụng để tham chiếu SPT.

Bảng 40 - Thông số sử dụng dữ liệu trong khuôn mẫu thông số an toàn (thẻ 'AD' dưới thẻ '62')

Thẻ	Độ dài	Giá trị		Lần xuất hiện
'06'	Biến đổi	OID của tài liệu mô tả, ví dụ thuật giải và/hoặc sử dụng DO'B3'		Nhiều nhất là một lần
'63'	Biến đổi	Trình bao		Nhiều nhất là một lần
'7B'	Biến đổi	DO môi trường an toàn (xem Bảng 59)		Một lần
'80'	1	Số chuỗi (bắt buộc)		Một lần
'82'	Biến đổi	Đối tượng an toàn (mật lệnh/loại dữ liệu tham chiếu) số (mã nhị phân)		Nhiều nhất là một lần
'83'	Biến đổi	Đối tượng an toàn (khóa/loại chứng nhận) số (mã nhị phân)		Nhiều nhất là một lần
'84'	1	SEID		Bất kỳ
'86'	1	Bộ chỉ báo hạn chế sử dụng khóa (xem 9.3.6.4)		Nhiều nhất là một lần
'8A'	1	Byte LCS của đối tượng an toàn		Nhiều nhất là một lần
'90'	Biến đổi	Số tối đa của các lần thử của thủ tục xác thực (mã nhị phân)	Thay đổi được	Nhiều nhất là một lần
91			Không thay đổi được	
'92'	Biến đổi	Số còn loại của các lần thử của thủ tục xác thực (mã nhị phân)	Thay đổi được	Nhiều nhất là một lần
'93'			Không thay đổi được	
'94'	Biến đổi	Bộ đếm sử dụng tối đa (mã nhị phân)	Thay đổi được	Nhiều nhất là một lần
'95'			Không thay đổi được	
'96'	Biến đổi	Bộ đếm sử dụng còn lại (mã nhị phân)	Thay đổi được	Nhiều nhất là một lần
'97'			Không thay đổi được	
'98'	Biến đổi	Số tối đa của tạo chữ ký (mã nhị phân)	Thay đổi được	Nhiều nhất là một lần
'99'			Không thay đổi được	
'9A'	Biến đổi	Số còn lại của tạo chữ ký (mã nhị phân)		Nhiều nhất là một lần
'9B'				
'9C'	1	Cờ không phản đối (không được chứng thực nếu giá trị = '00')		Nhiều nhất là một lần
'9D'	Biến đổi	Số tối đa của tạo khóa (mã nhị phân)		Nhiều nhất là một lần
'9E'	Biến đổi	Số còn lại của tạo khóa (mã nhị phân)		Nhiều nhất là một lần
'A0'	Biến đổi	Mở rộng thuộc tính an toàn đối với đối tượng xác thực		Nhiều nhất là một lựa chọn trong số
'A1'	Biến đổi	Mở rộng thuộc tính an toàn đối với khóa riêng		

'A2'	Biến đổi	Mở rộng thuộc tính an toàn đối với khóa công khai	các giá trị này
'A3'	Biến đổi	Mở rộng thuộc tính an toàn đối với chứng nhận	
'A4'	Biến đổi	Mở rộng thuộc tính an toàn đối với khóa bí mật	
'A5'	0	Mở rộng thuộc tính an toàn đối với khóa[a] Diffie-Hellman riêng	
'AD'	Biến đổi	Khuôn mẫu thông số an toàn	Bất kỳ
'AF	Biến đổi	Khuôn mẫu đặc tính mật lệnh (xem 9.3.6.12)	Bất kỳ
'B3'	Biến đổi	DO được xác định bằng DO '06'	Bất kỳ
'BE'	Biến đổi	Biểu thức Boole	Nhiều nhất là một lần
– Các thẻ khác trong lớp ngữ cảnh cụ thể là RFU – Giá trị của bộ đếm không thay đổi được không liên quan với kênh vật lý hoạt động và không hoạt động – Giá trị của bộ đếm thay đổi được bị tác động bởi kênh vật lý hoạt động và không hoạt động – [a] sử dụng khóa như vậy không thuộc điều kiện sử dụng do nó thuộc về thông số miền công cộng			

Khi DO'AD' được tham chiếu trong DO'9C' hoặc DO'9D', DO'AD' này hoặc trình bao được gắn thẻ tham chiếu nó phải thuộc về cùng khuôn mẫu như mở rộng thuộc tính an toàn.

Byte chế độ truy cập trong mở rộng thuộc tính an toàn biểu thị các hàm hoặc lệnh nào được hỗ trợ bởi đối tượng an toàn. Khi nó không được sử dụng trong DO'AD', byte chế độ truy cập cũng có thể biểu thị những hoạt động nào có thể được thực hiện trên đối tượng an toàn.

Nếu không có SEID được cung cấp trong thuộc tính an toàn tham chiếu DO'AD', sự mở rộng thuộc tính an toàn này có thể cung cấp SEID nếu cần thiết.

Bảng 41 - Mã hóa byte chế độ truy cập đối với đối tượng xác thực

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	-	-	-	-	-	-	-	Bit b7 đến b1 theo Bảng này
1	-	-	-	-	-	-	-	Bit b3 đến b1 theo Bảng này (bit b7 đến b4 độc quyền)
0	1	-	-	-	-	-	-	ENABLE VERIFICATION REQUIREMENT
0	-	1	-	-	-	-	-	DISABLE VERIFICATION REQUIREMENT
0	-	-	1	-	-	-	-	Sử dụng độc quyền
0	-	-	-	1	-	-	-	Sử dụng độc quyền
-	-	-	-	-	1	-	-	RESET RETRY COUNTER
-	-	-	-	-	-	1	-	CHANGE REFERENCE DATE
-	-	-	-	-	-	-	1	VERIFY

Bảng 42 - Mã hóa byte chế độ truy cập đối với khóa không đối xứng riêng

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	-	-	-	-	-	-	-	Bit b7 đến b1 theo Bảng này
1	-	-	-	-	-	-	-	Bit b5 độc quyền, tất cả các bit khác theo Bảng này
-	1	-	-	-	-	-	-	PSO Tính chữ ký số
-	-	1	-	-	-	-	-	PSO Giải mã
0	-	-	x	-	-	-	-	0 (mọi giá trị khác là RFU)
-	-	-	-	1	-	-	-	GENERAL AUTHENTICATE
-	-	-	-	-	1	-	-	INTERNAL AUTHENTICATE
-	-	-	-	-	-	1	-	GENERATE ASYMMETRIC KEY PAIR
-	-	-	-	-	-	-	1	Độc quyền khi được sử dụng trong SPT, GET ATTRIBUTE khi được sử dụng ở nơi khác

Bảng 43 - Mã hóa byte chế độ truy cập đối với khóa không đối xứng công khai và chứng nhận

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	-	-	-	-	-	-	-	Bit b7 đến b1 theo Bảng này
1	-	-	-	-	-	-	-	Bit b5 độc quyền, tất cả các bit khác theo Bảng này
-	1	-	-	-	-	-	-	PSO xác minh chữ ký số, xác minh chứng nhận
-	-	1	-	-	-	-	-	PSO Mã hóa
0	-	-	x	-	-	-	-	0 (mọi giá trị khác là RFU)
-	-	-	-	1	-	-	-	GENERAL AUTHENTICATE
-	-	-	-	-	1	-	-	EXTERNAL AUTHENTICATE
-	-	-	-	-	-	1	-	GENERATE ASYMMETRIC KEY PAIR
-	-	-	-	-	-	-	1	Độc quyền khi được sử dụng trong SPT, GET ATTRIBUTE khi được sử dụng ở nơi khác

Bảng 44 - Mã hóa byte chế độ truy cập đối với khóa bí mật

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	-	-	-	-	-	-	-	Bit b7 đến b1 theo Bảng này
1	-	-	-	-	-	-	-	Bit b4 độc quyền, tất cả các bit khác theo Bảng này
-	1	-	-	-	-	-	-	PSO mã hóa, tính kiểm tra tổng mật mã
-	-	1	-	-	-	-	-	PSO giải mã, xác minh kiểm tra tổng mật mã
--x—0 (mọi giá trị khác là RFU)-	-	-	1	-	-	-	-	MUTUAL AUTHENTICATE/ GENERAL AUTHENTICATE
-- 0	-	-	-	-	1	-	-	EXTERNAL AUTHENTICATE/ MUTUAL AUTHENTICATE
-	-	-	-	-	-	1	-	INTERNAL AUTHENTICATE
-	-	-	-	-	-	-	1	Độc quyền khi được sử dụng trong SPT, GET ATTRIBUTE khi được sử dụng ở nơi khác

9.3.6.3 Số chuỗi

Phiên bản liên tiếp của DO'AD' tương ứng với giá trị gia tăng của số chuỗi. Giá trị DO'80' được mã hóa trong nhị phân, trên một byte. Các DO'AD' được tham chiếu trong byte điều kiện an toàn (xem Bảng 30) có số nằm trong dãy '01' đến '0E'.

9.3.6.4 Bộ chỉ báo hạn chế sử dụng khóa

Phần tử dữ liệu trong DO'86' biểu thị các hạn chế cụ thể đối với với sử dụng khóa (xem Bảng 45). Trong điều này, các định nghĩa sau được sử dụng:

- Giai đoạn chuẩn bị: giai đoạn chuẩn bị bao gồm một C-RP hoặc một chuỗi C-RP. Bản chất của lệnh được gửi trong giai đoạn chuẩn bị không thuộc phạm vi của tiêu chuẩn này.
- Giai đoạn sử dụng: giai đoạn sử dụng bao gồm một C-RP hoặc một chuỗi C-RP. Bản chất của lệnh được gửi trong giai đoạn sử dụng không thuộc phạm vi của tiêu chuẩn này.

Bảng 45 - Mã hóa các hạn chế sử dụng khóa

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
1	-	-	-	-	-	-	-	Nhiều nhất là một lần sử dụng
-	1	-	-	-	-	-	-	Sử dụng ngay lập tức
-	-	1	-	-	-	-	-	Chi tiết được cung cấp trong tham chiếu OID
-	-	-	x	x	x	x	x	00000 (mọi giá trị khác là RFU)

Nếu bit b8 được thiết lập đến

- 1 điều này biểu thị rằng đối với mỗi sử dụng khóa giai đoạn chuẩn bị phải được thực hiện
- 0 điều này biểu thị rằng khóa có thể sử dụng được hơn một lần đối với giai đoạn chuẩn bị.

Nếu bit b7 được thiết lập đến

- 1 điều này biểu thị rằng thiết bị giao diện không được phép gửi C-RP giữa giai đoạn chuẩn bị và giai đoạn sử dụng trên kênh lô-gic được sử dụng cho sử dụng khóa.
- 0 điều này biểu thị rằng thiết bị giao diện có thể gửi một hoặc một số C-RP giữa giai đoạn chuẩn bị và giai đoạn sử dụng, trên kênh lô-gic tùy ý.

Nếu bit b6 được thiết lập đến

- 1 khi đó SPT bao gồm DO'86' phải chứa DO'06' và tham chiếu OID phải cung cấp chi tiết cho hạn chế sử dụng khóa.
- 0 khi đó SPT bao gồm DO'86' có thể hoặc có thể không bao gồm DO'06'.

Bit b5 đến b1 của bộ chỉ báo hạn chế sử dụng khóa là RFU.

VÍ DỤ 1 Đối với khóa chữ ký cấp không phản đối giai đoạn chuẩn bị điển hình bao gồm xác nhận người sử dụng (ví dụ lệnh VERIFY) và giai đoạn sử dụng điển hình bao gồm ví dụ các lệnh số không, một hoặc nhiều PSO dữ liệu hỏng theo sau bởi ví dụ lệnh PSO COMPUTE DIGITAL SIGNATURE.

VÍ DỤ 2 Đối với khóa được sử dụng trong thủ tục xác nhận chứng minh tính xác thực của một thực thể bên ngoài giai đoạn chuẩn bị điển hình bao gồm sự phục hồi của thử thách từ thẻ (ví dụ bằng phương pháp lệnh GET CHALLENGE) và giai đoạn sử dụng điển hình bao gồm thủ tục xác nhận (ví dụ lệnh EXTERNAL AUTHENTICATE).

9.3.6.5 Số thử

Khi đối tượng an toàn được sử dụng để xác nhận, số thử được giới hạn đến giá trị của DO'90' hoặc '91' trong thông số sử dụng dữ liệu được lồng trong DO'AD'. Số thử còn lại cho phép được cho bởi giá trị của DO'92' hoặc '93'. Giá trị của DO'90', '91', '92' và '93' được mã hóa trong nhị phân.

9.3.6.6 Số sử dụng

Số sử dụng của đối tượng an toàn được giới hạn đến giá trị của DO'94' hoặc '95' trong thông số sử dụng dữ liệu được lồng trong DO'AD'. Số sử dụng còn lại cho phép được cho bởi giá trị của DO'96' hoặc '97'. Giá trị của DO'94', '95', '96' và '97' được mã hóa trong nhị phân.

9.3.6.7 Không phản đối

Khi cấp không phản đối, một hàm có thể dựa vào DO đối tượng an toàn có cờ này thiết lập trong DO'9C', nghĩa là đến giá trị > 0. Nếu giá trị này là '00', DO ('9C 01 00') không thể chứng thực không phản đối.

9.3.6.8 Đánh số đối tượng an toàn

Nếu cần thiết, đối tượng an toàn (mật lệnh/dữ liệu tham chiếu hoặc khóa/chứng nhận) có thể có số được chứa trong DO'82' ('83'). Giá trị của DO'82' và '83' được mã hóa trong nhị phân, trên một hoặc một số byte. Byte đầu tiên của giá trị có thể được sử dụng làm tham chiếu đối tượng trong lệnh xử lý an toàn cơ bản (xem 11.5 và Bảng 94). Trường giá trị cũng có thể được sử dụng khi tham chiếu đối tượng dữ liệu an toàn bằng CRT (xem DO'83', '84' trong Bảng 55).

CHÚ THÍCH Hạn chế từ Bảng 94 giới hạn dãy các giá trị có thể đối với byte đầu tiên của trường giá trị nếu byte đó được dự định sử dụng làm tham chiếu đối tượng trong lệnh xử lý an toàn cơ bản.

9.3.6.9 Tạo chữ ký

Nếu cần thiết, số tạo chữ ký bằng đối tượng an toàn được giới hạn đến giá trị của DO'98' hoặc '99' trong thông số sử dụng dữ liệu được lồng trong DO'AD'. Số tạo còn lại được phép được cho bằng giá trị của DO'9A' hoặc '9B'. Giá trị của DO'98', '99', '9A' và '9B' được mã hóa trong nhị phân.

9.3.6.10 Tạo khóa

Nếu cần thiết, số tạo khóa bằng đối tượng an toàn được giới hạn đến giá trị của DO'9D' trong thông số sử dụng dữ liệu được lồng trong DO'AD'. Số tạo còn lại được phép được cho bằng giá trị của DO'9E'. Giá trị của DO'9D' và '9E' được mã hóa trong nhị phân.

9.3.6.11 Biểu thức Boole

DO'BE' biểu thức Boole dưới DO'AD' bao gồm:

- DO'06' định danh đối tượng bắt buộc xác định sử dụng các DO như thế nào để xây dựng biểu thức Boole
- Một hoặc một số DO thuộc lớp ngữ cảnh cụ thể, dữ liệu tham chiếu hoặc DO có cùng cú pháp như DO'60' tham chiếu chung (xem 11.4.2.1) hoặc DO'7F72' bộ định vị đối tượng (xem 9.3.3.3).

CHÚ THÍCH Trong 9.3.2, gạch ngang cuối cùng bao gồm yêu cầu đối với sự xuất hiện của DO'BE'.

9.3.6.12 Khuôn mẫu đặc tính mật lệnh

DO'AF' khuôn mẫu đặc tính các mật lệnh dưới DO'AD' bao gồm các đặc tính mật lệnh. DO'06' có thể xuất hiện trong khuôn mẫu các đặc tính mật lệnh.

Nếu khuôn mẫu mật lệnh

- Bao gồm một OID trong DO'06, DO'06' đó là DO đầu tiên trong khuôn mẫu mật lệnh. Tiêu chuẩn hoặc đặc tả được tham chiếu bằng OID này xác định đối tượng dữ liệu hơn nữa đi kèm theo trong khuôn mẫu các đặc tính mật lệnh.
- Không bao gồm một DO'06' khi đó khuôn mẫu tuân theo TCVN 11167-15 (ISO/IEC 7816-15) và có thể bao gồm bất kỳ DO nào từ Bảng 46 theo bất kỳ thứ tự nào có ý nghĩa và mã hóa được xác định trong Bảng 46.

Bảng 46 - Khuôn mẫu các đặc tính mật khẩu (DO'AF' dưới thẻ 'AD')

Thẻ	Độ dài	Mô tả
'81'	1	Độ dài lịch sử dữ liệu xác minh: số tối đa của các giá trị dữ liệu xác minh được ghi lại và duy trì. Khi dữ liệu xác minh được thiết lập, nó phải khác với tất cả các giá trị trong lịch sử dữ liệu xác minh. Giá trị của độ dài lịch sử dữ liệu xác minh phải trong khoảng đóng [0, 8].
'82'	1	Định dạng vận chuyển đối với dữ liệu xác minh và dữ liệu tham chiếu mới – '00', trực tiếp: dữ liệu được truyền đến ICC được lấy nguyên như vậy (mã hóa nhị phân) – '01', bằng số: mỗi ký tự được mã hóa theo ISO/IEC 10646 (UTF-8) và là phần tử của khoảng đóng ['30', '39']. Dữ liệu được truyền đến ICC được đệm bằng 'FF' cho đến khi các ký tự có độ dài tối đa có sẵn. – '03', theo chữ cái con số, nghĩa là chữ số, ký tự viết hoa và ký tự thường ASCII: mỗi ký tự được mã hóa theo ISO/IEC 10646 (UTF-8) và phải là phần tử của khoảng đóng ['30', '39'] hoặc ['41', '5A'] hoặc ['61', '7A']. Dữ liệu được truyền đến ICC được đệm bằng 'FF' cho đến khi các ký tự có độ dài tối đa có sẵn. – Các giá trị khác là RFU
'83'	1	Độ dài tối thiểu: số tối thiểu các ký tự trong dữ liệu xác minh
'84'	1	Độ dài tối đa: số tối đa các ký tự trong dữ liệu xác minh
– Các thẻ khác trong lớp ngữ cảnh cụ thể là RFU		

9.3.7 Thuộc tính an toàn đối với kênh lô-gic

DO'8E' thuộc tính an toàn kênh lô-gic (nhiều nhất là một lần) có thể xuất hiện trong CP của bất kỳ tệp hoặc DO (xem Bảng 10) và trong bất kỳ môi trường an toàn thích hợp nào (SE, xem 10.3.3). Nó phải được thể hiện theo Bảng 47, trong đó:

- "không thể chia sẻ" có nghĩa là nhiều nhất một kênh lô-gic phải có sẵn. Công nghệ vật lý của kênh lô-gic có thể bị giới hạn.
- "bảo đảm an toàn" nghĩa là khóa SM (xem điều 10) phải có sẵn (ví dụ được thiết lập bằng xác thực trước).
- "người sử dụng được xác thực" nghĩa là người sử dụng phải được xác thực (ví dụ xác minh mật lệnh thành công)

Bảng 47 - Mã hóa thuộc tính an toàn kênh lô-gic

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	0	0	0	0	-	-	1	Không thể chia sẻ
0	0	0	0	0	-	1	-	Bảo đảm an toàn
0	0	0	0	0	1	-	-	Người sử dụng được xác thực
– Mọi giá trị khác là RFU								

9.4 Phần tử dữ liệu hỗ trợ an toàn

Điều này xác định tập hợp các phần tử dữ liệu hỗ trợ an toàn có các quy tắc quy định cách thức các giá trị của chúng được xử lý. Các phần tử dữ liệu hỗ trợ an toàn mở rộng và làm mịn DO tham chiếu điều khiển. Thẻ có thể cung cấp chúng làm hỗ trợ chung đối với cơ chế an toàn được thực hiện bằng

một ứng dụng. Các ứng dụng có thể tham chiếu chúng về thông điệp an toàn và các thao tác an toàn (xem ISO/IEC 7816-8). Điều này không xác định một số đặc tính của phần tử dữ liệu hỗ trợ an toàn, ví dụ độ dài của chúng, và không xác định thuật giải mà làm thay đổi giá trị của chúng.

Bảng 48 - DO hỗ trợ an toàn

Thẻ	Giá trị
'7A'	Tập hợp của DO hỗ trợ an toàn có các thẻ sau
'80'	Bộ đếm giao tiếp thẻ
'81'	Định danh giao tiếp thẻ
'82' đến '8E'	Bộ đếm lựa cọn tệp
'93'	Bộ đệm chữ ký số
'9F2X'	Giá trị cấp số trong ('X' là chỉ báo cụ thể, ví dụ chỉ báo tham chiếu bộ đếm lựa chọn tệp)
'9F3Y'	Giá trị cấp số ngoài ('Y' là chỉ báo cụ thể, ví dụ chỉ báo tham chiếu dấu thời gian bên ngoài)
– Dưới thẻ '7A', Tổ chức có trách nhiệm lưu trữ bất kỳ DO nào khác của lớp ngữ cảnh cụ thể	

Nguyên tắc - thẻ phải duy trì và sử dụng giá trị của phần tử dữ liệu hỗ trợ an toàn như sau.

- Cập nhật được thực hiện bằng các giá trị mới hoặc được tính bằng thẻ, hoặc được cung cấp bởi mọi đối tượng bên ngoài, phù hợp với quy tắc cụ thể đối với loại phần tử dữ liệu hỗ trợ an toàn cụ thể.
- Cập nhật được thực hiện trước bất kỳ kết quả nào được sản sinh đối với lệnh tạo ra cập nhật. Cập nhật không phụ thuộc vào trạng thái hoàn thiện của lệnh. Nếu giá trị được sử dụng bằng ứng dụng trong hoạt động gây ra cập nhật, cập nhật được thực hiện trước khi giá trị được sử dụng.
- Truy cập phần tử dữ liệu hỗ trợ ứng dụng - an toàn cụ thể bị hạn chế đối với các hàm được thực hiện bằng ứng dụng cụ thể.

CHÚ THÍCH An toàn thực sự cuối cùng đạt được trong C-RP phụ thuộc vào thuật giải và giao thức được xác định bởi ứng dụng; thẻ chỉ cung cấp hỗ trợ bằng các phần tử dữ liệu này và các quy tắc sử dụng đi cùng.

Phần tử dữ liệu - thẻ có thể hỗ trợ an toàn C-RP bằng phần tử dữ liệu được gọi là giá trị cấp số. Được gia tăng tại sự kiện cụ thể xuyên suốt đời thẻ, các giá trị này khác nhau mỗi thời điểm thẻ được kích hoạt. Hai giá trị cấp số được xác định: bộ đếm phiên thẻ và định danh phiên.

- Bộ đếm phiên thẻ được gia tăng ngay trong quá trình kích hoạt thẻ
- Định danh phiên được tính từ bộ đếm phiên thẻ và từ dữ liệu được cung cấp bởi mọi đối tượng bên ngoài.

Hai loại giá trị cấp số được xác định.

- Giá trị cấp số bên trong, nếu được xác định đối với một ứng dụng, đăng ký số lần sự kiện cụ thể được thực hiện. Phần tử dữ liệu được gia tăng sau sự kiện; thẻ có thể cung cấp hàm thiết lập lại cho các bộ đếm này mà nếu được xác định đối với một ứng dụng thiết lập giá trị của nó đến không. Giá trị cấp số trong không thể bị điều khiển bởi mọi đối tượng bên ngoài và phù hợp với việc sử dụng làm đại diện gần đúng trong thẻ được đảm bảo an toàn có thời gian thực. Giá trị của chúng có thể được sử dụng trong tính toán mật mã

- Các giá trị cấp số bên ngoài, nếu được xác định đối với một ứng dụng, phải chỉ được cập nhật bằng giá trị dữ liệu từ mọi đối tượng bên ngoài. Giá trị mới về số lượng lớn hơn giá trị hiện hành được lưu giữ trong thẻ.

Tham chiếu - thẻ có thể cung cấp truy cập đến giá trị phần tử dữ liệu hỗ trợ an toàn như sau.

- Một EF có thể xuất hiện trong MF,ví dụ đối với bộ đếm phiên thẻ, hoặc trong DF ứng dụng, ví dụ đối với các giá trị cấp số ứng dụng cụ thể.
- DO phụ, có thẻ '88', '92' và '93' (xem Bảng 54) có thể xuất hiện trong khuôn mẫu tham chiếu điều khiển. Các DO này có thể được sử dụng nếu SE hỗ trợ sử dụng rõ ràng các phần tử dữ liệu này.
- Trong DO'7A' liên ngành, lớp ngữ cảnh cụ thể được lưu trữ đối với DO hỗ trợ an toàn như được liệt kê trong Bảng 48.

10 Thông điệp an toàn

Thông điệp an toàn (SM) bảo vệ tất hoặc một phần của C-RP, hoặc kết nối các trường dữ liệu liên tiếp (phân đoạn dữ liệu, xem 5.3), bằng cách đảm bảo hai hàm an toàn cơ bản: bảo mật dữ liệu và xác nhận dữ liệu. Thông điệp an toàn đạt được bằng cách áp dụng một hoặc nhiều cơ chế an toàn. Có thể định danh rõ ràng bằng khuôn mẫu định danh cơ chế mật mã (xem 9.2) trong CP của bất kỳ DF nào (xem 7.4), mỗi cơ chế an toàn bao gồm một thuật giải mật mã, chế độ hoạt động, khóa, đối số (dữ liệu đầu vào) và dữ liệu ban đầu, luôn luôn.

- Truyền và nhận của trường dữ liệu có thể được đan xen với việc xử lý của cơ chế an toàn. Đặc tả này không loại trừ sự xác định bằng phân tích chuỗi của các cơ chế và điều an toàn được sử dụng để xẻ lý phần còn lại của trường dữ liệu.
- Hai hoặc nhiều cơ chế an toàn có thể sử dụng cùng thuật giải mật mã có chế độ hoạt động khác nhau. Quy tắc đệm xác định sau đây không loại trừ đặc tính như vậy.

10.1 Trường SM và SM DO

10.1.1 Bảo vệ SM thuộc dữ liệu lệnh

Dữ liệu SM là lệnh SM hoặc trường SM hồi đáp, không kể độ dài của nó. Nếu bảo vệ dữ liệu bằng thông điệp an toàn diễn ra trước khi có thể phân đoạn, dữ liệu SM quá khổ là trường hợp đặc biệt của dữ liệu được mã hóa BER-TLV quá khổ, mà theo đó các quy tắc được đưa ra trong 5.3 áp dụng.

Định dạng của dữ liệu được xác định như bên dưới (xem 10.4), ngoại trừ độ dài của nó không bị giới hạn bởi các hạn chế và định dạng độ dài được qui định nối chuỗi (xem 5.3).

10.1.2 Việc bảo vệ SM của hồi đáp và lệnh được nối chuỗi

Nếu có nhu cầu bảo vệ lệnh SM nối chuỗi hoặc trường dữ liệu hồi đáp, phân đoạn theo 5.3 phải diễn ra trước khi bảo vệ C-RP. Mỗi C-RP khi đó được bảo vệ (xem 10.4) theo các yêu cầu của môi trường an toàn.

Phân đoạn phải đạt được chuỗi lệnh hoặc các trường dữ liệu hồi đáp không có cấu trúc chắc chắn. Byte CLA INS P1 P2 phải tuân theo quy tắc nối chuỗi được sử dụng cho phân đoạn (xem 5.3).

10.1.3 SM DO

Bảng 49 cho thấy SM DO được xác định trong tiêu chuẩn này, tất cả trong lớp ngữ cảnh cụ thể. Một số SM DO (SM thẻ '82', '83', 'B0', 'B1') đệ quy, nghĩa là trường giá trị đơn giản (dễ hiểu) là trường SM.

Trong mỗi trường SM, bit b1 của byte cuối cùng của trường thẻ (tính chẵn lẻ thẻ) của mỗi SM DO (lớp ngữ cảnh cụ thể) biểu thị liệu SM DO được bao gồm (bit b1 đặt là 1, số thẻ lẻ) hoặc không bao gồm (bit b1 đặt là 0, số thẻ chẵn) trong tính toán phần tử dữ liệu đối với xác nhận: kiểm tra tổng mật mã (xem 10.2.3.1), hoặc chữ ký số (xem 10.2.3.2). Nếu xuất hiện, DO của các lớp khác (ví dụ DO liên ngành) phải được bao gồm trong phép tính. Nếu phép tính như vậy xảy ra, phần tử dữ liệu là trường giá trị của một SM DO đối với xác nhận (thẻ SM '8E', '9E') tại cuối trường SM.

Có hai loại SM DO

- Mỗi SM DO cơ bản (xem 10.2) truyền một giá trị đơn giản (dễ hiểu), hoặc một đầu vào hoặc kết quả của cơ chế an toàn.
- Mỗi SM DO phụ (xem 10.3) truyền một khuôn mẫu tham chiếu điều khiển, hoặc định danh môi trường an toàn, hoặc khuôn mẫu bộ mô tả hỏi đáp.

CHÚ THÍCH SM DO cơ bản cũng được sử dụng để điều khiển thao tác an toàn (xem ISO/IEC 7816-6). SM DO phụ cũng được sử dụng để quản lý môi trường an toàn (xem 11.5.11). Cách tiếp cận chung đối với an toàn bằng thông điệp an toàn chia sẻ một số vấn đề liên quan đến an toàn với thao tác an toàn, nghĩa là tiếp cận nguyên tử đối với an toàn. Phụ lục B mô tả tính đồng vận giữa hai cách tiếp cận.

Bảng 49 - Đối tượng dữ liệu SM

Thẻ	Giá trị
'80', '81'	Giá trị đơn giản (dễ hiểu) không được mã hóa trong BER-TLV
'82', '83'	Tài liệu viết bằng mật mã (giá trị đơn giản (dễ hiểu) được mã hóa trong BER-TLV và bao gồm SM DO nghĩa là trường SM)
'84', '85'	Tài liệu viết bằng mật mã (giá trị đơn giản (dễ hiểu) được mã hóa trong BER-TLV, nhưng không bao gồm SM DO)
'86', '87'	Byte bộ chỉ báo nội dung đệm theo sau bởi tài liệu viết bằng mật mã (giá trị đơn giản (dễ hiểu) không được mã hóa trong BER-TLV)
'89'	Tiêu đề lệnh (CLA INS P1 P2, bốn byte)
'8E'	Kiểm tra tổng mật mã (ít nhất bốn byte)
'90', '91'	Chế độ băm
'92', '93'	Chứng nhận (dữ liệu không được mã hóa trong BER-TLV)
'94', '95'	Định danh môi trường an toàn (SEID)
'96', '97'	Một hoặc 2 byte mã hóa L_e trong C-RP không an toàn (có thể để trống)
'99'	Trạng thái xử lý (SW1-SW2, 2 byte, có thể để trống)
'9A', '9B'	Phần tử dữ liệu đầu vào để tính toán chữ ký số (trường giá trị được ký)
'9C', '9D'	Khóa công khai
'9E'	Chữ ký số
'A0', 'A1'	Khuôn mẫu đầu vào để tính toán chế độ băm (khuôn mẫu được băm)
'A2'	Khuôn mẫu đầu vào để xác minh kiểm tra tổng mật mã (khuôn mẫu được bao gồm)
'A4', 'A5'	Khuôn mẫu tham chiếu điều khiển để xác thực (AT)
'A6', 'A7'	Khuôn mẫu tham chiếu điều khiển đối với thỏa thuận khóa (KAT)
'A8'	Khuôn mẫu đầu vào để xác minh chữ ký số (khuôn mẫu được bao gồm)

'AA', 'AB'	Khuôn mẫu tham chiếu điều khiển đối với chế độ băm (HT)
'AC', 'AD'	Khuôn mẫu đầu vào để tính toán chữ ký số (trường giá trị kết nối được ký)
'AE', 'AF'	Khuôn mẫu đầu vào để xác minh chứng nhận (trường giá trị kết nối được chứng nhận)
'B0', 'B1'	Giá trị đơn giản (dễ hiểu) được mã hóa trong BER-TLV và bao gồm SM DO, nghĩa là trường SM
'B2', 'B3'	Giá trị đơn giản (dễ hiểu) được mã hóa trong BER-TLV, nhưng không bao gồm SM DO
'B4', B5'	Khuôn mẫu tham chiếu điều khiển đối với tổng kiểm tra mật mã (CCT)
'B6', B7'	Khuôn mẫu tham chiếu điều khiển đối với chữ ký số (DST)
'B8', 'B9'	Khuôn mẫu tham chiếu điều khiển đối với tính bảo mật (CT)
'BA', 'BB'	Khuôn mẫu bộ mô tả hỏi đáp
'BC', 'BD'	Khuôn mẫu đầu vào để tính toán chữ ký số (khuôn mẫu được ký)
'BE'	Khuôn mẫu đầu vào để xác minh chứng nhận (khuôn mẫu được chứng nhận)
– Trong trường SM, Tổ chức có trách nhiệm lưu trữ bất kỳ DO khác của lớp ngữ cảnh cụ thể. – Để sử dụng các SM DO ngoài SM C-RP này, chúng phải được bao bọc trong DO'7D'	

10.2 SM DO cơ bản

10.2.1 SM DO để bao gói giá trị đơn giản (dễ hiểu)

Bao gói là bắt buộc đối với trường SM và đối với dữ liệu không được mã hóa trong BER-TLV. Nó mang tính tùy chọn đối với BER-TLV, không bao gồm SM, DO. Bảng 50 thể hiện SM DO để bao gói các giá trị đơn giản (dễ hiểu).

Bảng 50 - SM DO để bao gói các giá trị đơn giản (dễ hiểu)

Thẻ	Giá trị
'B0', 'B1'	Giá trị đơn giản (dễ hiểu) được mã hóa trong BER-TLV và bao gồm SM DO (nghĩa là trường SM)
'B2', 'B3'	Giá trị đơn giản (dễ hiểu) được mã hóa trong BER-TLV, nhưng không bao gồm SM DO
'80', '81'	Giá trị đơn giản (dễ hiểu) không được mã hóa trong BER-TLV
'89'	Tiêu đề lệnh (CLA INS P1 P2, bốn byte)
'96', '97'	Một hoặc 2 byte mã hóa L_e trong C-RP không an toàn (có thể để trống)
'99'	Trạng thái xử lý (SW1-SW2, 2 byte, có thể để trống)

10.2.2 SM DO đối với tính bảo mật

Bảng 51 thể hiện SM DO đối với tính bảo mật. Cơ chế an toàn đối với tính bảo mật bao gồm thuật giải mật mã thích hợp trong chế độ hoạt động thích hợp. Trong trường hợp không có chỉ báo rõ rệt và khi không có cơ chế nào được lựa chọn hoàn toàn đối với tính bảo mật, cơ chế mặc phải áp dụng.

– Để tính toán tài liệu viết bằng mật mã được đứng trước bằng một chỉ báo đệm, cơ chế mặc định là mật mã khối trong chế độ "sách mã điện tử" có thể bao gồm phần đệm. phần đệm đối với tính bảo mật có thể có ảnh hưởng đối với sự truyền: tài liệu viết bằng mật mã (một hoặc nhiều khối) có thể dài hơn giá trị đơn giản (dễ hiểu).

- Để tính toán tài liệu viết bằng mật mã không được đứng trước bằng một chỉ báo đệm, cơ chế mặc định là mật mã luồng. Trong trường hợp này, tài liệu viết bằng mật mã là loại trừ or của chuỗi các byte dữ liệu để giấu bằng chuỗi giấu có cùng độ dài. Do vậy, giấu yêu cầu không có phần đệm và chuỗi các byte dữ liệu được phục hồi bằng cùng hoạt động.

Nội dung đệm và/hoặc được biểu thị khi giá trị đơn giản (dễ hiểu) không được mã hóa trong BER-TLV. Nếu đệm áp dụng nhưng không được biểu thị, quy tắc được xác định trong 10.2.3.1 áp dụng.

Bảng 52 thể hiện byte bộ chỉ báo nội dung đệm

Bảng 51 - SM DO đối với tính bảo mật

Thẻ	Giá trị
'82', '83'	Tài liệu viết bằng mật mã (giá trị đơn giản (dễ hiểu) được mã hóa trong BER-TLV và bao gồm SM DO nghĩa là trường SM)
'84', '85'	Tài liệu viết bằng mật mã (giá trị đơn giản (dễ hiểu) được mã hóa trong BER-TLV, nhưng không bao gồm SM DO)
'86', '87'	Byte bộ chỉ báo nội dung đệm theo sau bởi tài liệu viết bằng mật mã (giá trị đơn giản (dễ hiểu) không được mã hóa trong BER-TLV)

Bảng 52 - Byte bộ chỉ báo nội dung đệm

Giá trị	Ý nghĩa
'00'	Không có thêm chỉ báo
'01'	Đệm như được xác định trong 10.2.3.1
'02'	Không đệm
'1X'	Một đến bốn khóa bí mật để mã hóa thông tin, không phải các khóa ('X' là ánh xạ bit với bất kỳ giá trị nào từ '0' đến 'F' '11' biểu thị khóa đầu tiên (ví dụ từ điều khiển "số chẵn" trong hệ thống TV trả giá '12' biểu thị khóa thứ hai (ví dụ từ điều khiển "số lẻ" trong hệ thống TV trả giá '13' biểu thị khóa đầu tiên theo sau bởi khóa thứ hai (ví dụ một cặp từ điều khiển trong hệ thống TV trả giá
'2X'	Khóa bí mật để mã hóa các khóa, không phải thông tin ('X' là tham chiếu với bất kỳ giá trị nào từ '0' đến 'F' (ví dụ trong hệ thống TV trả giá, hoặc khóa hoạt động để mã hóa các từ điều khiển hoặc khóa quản lý để mã hóa các khóa hoạt động)
'3X'	Khóa riêng của cặp khóa không đối xứng ('X' là tham chiếu với bất kỳ giá trị nào từ '0' đến 'F'
'4X'	Mật lệnh ('X' là tham chiếu với bất kỳ giá trị nào từ '0' đến 'F'
'80' đến '8E'	Độc quyền
– Mọi giá trị khác là RFU	

10.2.3 SM DO để xác nhận

Bảng 53 thể hiện SM DO để xác nhận

Bảng 53 - SM DO để xác nhận

Thẻ	Giá trị
'8E'	Kiểm tra tổng mật mã (ít nhất bốn byte)
'90', '91'	Chế độ băm
'92', '93'	Chứng nhận (dữ liệu không được mã hóa trong BER-TLV)
'9C', '9D'	Khóa công khai
'9E'	Chữ ký số
DO đầu vào (xem ISO/IEC 7816-8)	
'9A', '9B'	Phần tử dữ liệu đầu vào để tính toán chữ ký số (trường giá trị được ký)
'A0', 'A1'	Khuôn mẫu đầu vào để tính toán chế độ băm (khuôn mẫu được băm)
'A2'	Khuôn mẫu đầu vào để xác minh kiểm tra tổng mật mã (khuôn mẫu được bao gồm)
'A8'	Khuôn mẫu đầu vào để xác minh chữ ký số (khuôn mẫu được bao gồm)
'AC', 'AD'	Khuôn mẫu đầu vào để tính toán chữ ký số (trường giá trị kết nối được ký)
'AE', 'AF'	Khuôn mẫu đầu vào để xác minh chứng nhận (trường giá trị kết nối được chứng nhận)
'BC', 'BD'	Khuôn mẫu đầu vào để tính toán chữ ký số (khuôn mẫu được ký)
'BE'	Khuôn mẫu đầu vào để xác minh chứng nhận (khuôn mẫu được chứng nhận)

10.2.3.1 Phần tử dữ liệu kiểm tra tổng mật mã

Tính toán kiểm tra tổng mật mã bao gồm khối kiểm tra ban đầu, khóa bí mật và hoặc thuật giải mật mã khối (xem ISO/IEC 18033) hoặc hàm băm (xem ISO/IEC 10118).

Phương pháp tính toán có thể là phần đặc tả hệ thống. khuôn mẫu định danh cơ chế mật mã (xem 9.2) có thể định danh một tiêu chuẩn (ví dụ ISO/IEC 9797-1) quy định phương pháp tính toán.

Trừ khi có quy định khác, phương pháp tính toán sau được sử dụng. Thông số được sử dụng trong phương pháp tính toán này có thể được xác định trong CRT liên quan (xem Bảng 55). Tiêu chuẩn này không xác định CRT mặc định.

Dưới sự điều khiển của khóa, thuật giải về cơ bản biến đổi khối đầu vào hiện hành của k byte (điển hình là 8, 16 hoặc 20) thành khối đầu ra hiện hành có cùng kích cỡ. Phép tính được thực hiện trong các cấp liên tiếp sau.

- Khối vô hiệu, nghĩa là k byte được đặt là '00'
- Khối chuỗi, nghĩa là kết quả từ các phép tính trước, đối với lệnh, khối kiểm tra cuối cùng của lệnh trước và đối với hồi đáp, khối kiểm tra cuối cùng của hồi đáp trước đó.
- Khối giá trị ban đầu được cung cấp, ví dụ bởi mọi đối tượng bên ngoài.
- Khối phụ do biến đổi dữ liệu phụ dưới điều khiển của khóa. Nếu các dữ liệu phụ nhỏ hơn k byte, khi đó các bit được đặt là 0 hướng đến kích cỡ khối.

Cấp độ dãy - tiêu đề lệnh (CLA INS P1 P2) có thể được bao gói vì mục đích bảo vệ (thẻ SM '89'). Tuy nhiên, nếu bit b8 đến b6 của CLA được đặt là 000 và bit b4 và b3 đến 11 (xem 5.1), khi đó khối dữ liệu đầu tiên bao gồm tiêu đề lệnh (CLA INS P1 P2) theo sau bởi một byte đặt là '80' và k-5 byte đặt là '00'.

Kiểm tra tổng mật mã phải bao gồm bất kỳ DO thông điệp an toàn nào có số thẻ lẻ và bất kỳ DO nào có byte đầu tiên không phải từ '80' đến 'BF'. Các DO này phải được chứa theo từng khối dữ liệu theo khối dữ liệu trong khối kiểm tra hiện hành. Sự chia tách thành các khối dữ liệu được thực hiện như sau.

- Tạo khối phải tiếp tục tại biên giữa các DO liền kề để bao gộp
- Đệm phải áp dụng tại cuối mỗi Do để bao gộp hoặc bởi một DO không bao gộp, hoặc bởi DO không có thêm. Đệm bao gồm một byte bắt buộc đặt là '80' được theo sau, nếu cần thiết, bằng byte 0 đến k-1 được đặt là '00', cho đến khi khối dữ liệu tương ứng được lấp đầy đến byte k. Đệm để xác nhận không có ảnh hưởng đối với sự truyền do byte đệm không được truyền.

Trong cơ chế này, chế độ hoạt động là "chuỗi khối mã hóa" (xem ISO/IEC 10116). Đầu vào đầu tiên là lệnh loại trừ - or của khối kiểm tra ban đầu với khối dữ liệu đầu tiên. Đầu ra đầu tiên là kết quả của đầu vào đầu tiên. Đầu vào hiện hành là lệnh loại trừ - or của đầu ra trước với khối dữ liệu hiện hành. Đầu ra hiện hành là kết quả từ đầu vào hiện hành.

Cấp độ cuối cùng - khối kiểm tra cuối cùng là đầu ra cuối cùng. Cấp độ cuối cùng trích kiểm tra tổng mật mã (byte m đầu tiên, ít nhất là bốn) từ khối kiểm tra cuối cùng.

10.2.3.2 Phần tử dữ liệu chữ ký số

Sơ đồ chữ ký số dựa vào kỹ thuật mật mã không đối xứng (xem ISO/IEC 9796, ISO/IEC 14888). Phép tính bao hàm hàm bằm (xem ISO/IEC 10118). Đầu vào dữ liệu bao gồm trường giá trị của DO đầu vào chữ ký số, hoặc của kết nối các trường giá trị của DO tạo thành khuôn mẫu đầu vào chữ ký số. Nó có thể được xác định bằng cơ chế được quy định trong 10.2.3.1.

10.3 SM DO phụ

Bảng 54 thể hiện SM DO phụ

Bảng 54 - SM DO phụ

Thẻ	Giá trị
'94', '95'	Định danh môi trường an toàn (SEID)
'A4', 'A5'	Khuôn mẫu tham chiếu điều khiển để xác thực (AT)
'A6', 'A7'	Khuôn mẫu tham chiếu điều khiển đối với thỏa thuận khóa (KAT)
'AA', 'AB'	Khuôn mẫu tham chiếu điều khiển đối với chế độ băm (HT)
'B4', B5'	Khuôn mẫu tham chiếu điều khiển đối với tổng kiểm tra mật mã (CCT)
'B6', B7'	Khuôn mẫu tham chiếu điều khiển đối với chữ ký số (DST)
'B8', 'B9'	Khuôn mẫu tham chiếu điều khiển đối với tính bảo mật (CT)
'BA', 'BB'	Khuôn mẫu bộ mô tả hồi đáp

10.3.1 Khuôn mẫu tham chiếu điều khiển

Sáu khuôn mẫu tham chiếu điều khiển được xác định, có hiệu lực đối với xác nhận (AT), thỏa thuận khóa, mã-băm (HT), kiểm tra tổng mật mã (CCT), chữ ký số (DST) và tính bảo mật (CT) sử dụng hoặc kỹ thuật mật mã đối xứng hoặc kỹ thuật mật mã không đối xứng (CT-sym và CT-asym).

Mỗi cơ chế an toàn bao gồm một thuật giải mật mã trong chế độ hoạt động và sử dụng một khóa, và có khả năng, dữ liệu ban đầu. Các điều như vậy được lựa chọn hoặc ẩn, nghĩa là đã biết trước khi ban hành lệnh, hoặc hiện, nghĩa là bằng DO tham chiếu điều khiển được lồng trong khuôn mẫu tham chiếu

điều khiển. Trong khuôn mẫu tham chiếu điều khiển, lớp ngữ cảnh cụ thể được lưu trữ đối với DO tham chiếu điều khiển.

Trong trường SM, vị trí có khả năng cuối cùng của khuôn mẫu tham chiếu điều khiển chỉ ngay trước DO đầu tiên mà cơ chế tham chiếu áp dụng. Ví dụ, ví trị có khả năng cuối cùng của khuôn mẫu có hiệu lực đối với kiểm tra tổng mật mã (CCT) chỉ ngay trước DO đầu tiên bao gồm trong phép tính.

Mỗi tham chiếu điều khiển giữ nguyên hiệu lực cho đến khi một tham chiếu điều khiển mới được cung cấp đối với cùng cơ chế. Ví dụ, một lệnh được cung cấp tham chiếu điều khiển cho lệnh tiếp theo.

10.3.2 DO tham chiếu điều khiển trong khuôn mẫu tham chiếu điều khiển

Mỗi khuôn mẫu tham chiếu điều khiển (CRT) là tập hợp của các DO tham chiếu điều khiển: tham chiếu cơ chế mật mã, tham chiếu khóa và tệp, tham chiếu dữ liệu ban đầu, định tính sử dụng và, chỉ trong khuôn mẫu tham chiếu điều khiển đối với tính bảo mật, tham chiếu nội dung mật mã.

- Tham chiếu cơ chế mật mã biểu thị thuật giải mật mã trong chế độ hoạt động. CP hoặc bất kỳ DF (xem thẻ 'AC' trong Bảng 10) có thể bao gồm khuôn mẫu định danh cơ chế mật mã (xem 9.2). Mỗi cái biểu thị ý nghĩa của tham chiếu cơ chế mật mã.
- Tham chiếu tệp (giống như mã hóa trong 7.3.2) biểu thị tệp mà tham chiếu khóa có hiệu lực. Nếu tham chiếu tệp không xuất hiện, khi đó tham chiếu khóa có hiệu lực trong DF hiện hành, có khả năng là DF ứng dụng. Tham chiếu khóa định danh rõ ràng khóa sử dụng.
- Tham chiếu dữ liệu ban đầu, khi được áp dụng với kiểm tra tổng mật mã, biểu thị khối kiểm tra ban đầu. Nếu tham chiếu dữ liệu ban đầu không xuất hiện và khối kiểm tra ban đầu không được lựa chọn, khi đó khối trống áp dụng. Hơn nữa, trước khi truyền DO đầu tiên đối với tính bảo mật sử dụng mật mã luồng, khuôn mẫu đối với tính bảo mật phải cung cấp dữ liệu phụ để thiết lập ban đầu phép tính của dòng byte giấu.

Bảng 55 liệt kê các DO tham chiếu điều khiển và biểu thị khuôn mẫu tham chiếu điều khiển có liên quan. Tất cả các DO tham chiếu điều khiển thuộc lớp ngữ cảnh cụ thể.

Một CRT có thể bao gồm các DO liên ngành, ví dụ, quyền hạn người giữ chứng nhận (thẻ '5F4C', xem 10.3.3) trong AT, danh sách tiêu đề hoặc danh sách tiêu đề mở rộng (thẻ '5D' và '4D', xem 8.4.4 đến 8.4.7) trong HT hoặc DST. Trong bất kỳ khuôn mẫu tham chiếu điều khiển nào, khuôn mẫu sử dụng khóa dưới thẻ 'A3' có thể kết hợp một tệp và tham chiếu khóa với bộ đếm sử dụng khóa và/hoặc bộ đếm thử lại khóa. Khuôn mẫu sử dụng khóa bao gồm tập hợp các DO sử dụng khóa (xem Bảng 56)

Bảng 55 - DO tham chiếu điều khiển trong khuôn mẫu tham chiếu điều khiển

Thẻ	Giá trị	AT	KAT	HT	CCT	DST	CT-asym	CT-sym
'80'	Tham chiếu cơ chế mật mã	x	x	x	x	x	x	x
Tham chiếu đối tượng an toàn và tệp								
'81'	-tham chiếu tệp (để mã hoa, xem 7.3.2)	x	x	x	x	x	x	x
'82'	-tên DF (xem 7.3.1)	x	x	x	x	x	x	x
'83'	-tham chiếu khóa bí mật (để sử dụng trực tiếp)	x	x	x	x			x
	-tham chiếu khóa công khai	x	x	x		x	x	
	-dữ liệu tham chiếu	x						
'84'	-tham chiếu để tính khóa phiên	x	x		x			x
	-tham chiếu khóa riêng	x	x			x	x	
'A3'	Khuôn mẫu sử dụng khóa (xem phần bên dưới)	x	x	x	x	x	x	x
Tham chiếu dữ liệu ban đầu: khối kiểm tra ban đầu.								
'85'	-L=0, khối trống			x	x			x
'86'	-L=0, khối chuỗi			x	x			x
'87'	-L=0, khối giá trị ban đầu trước cộng với một L=k, khối giá trị ban đầu			 x	x x			x
Tham chiếu dữ liệu ban đầu: phần tử dữ liệu phụ (xem 10.2.3.1)								
'88'	-L=0, thách thức trao đổi trước cộng với một L>0, không thêm chỉ báo				x	x	x	x
'89' đến '8D'	-L=0, chỉ báo của phần tử dữ liệu độc quyền L>0, giá trị của phần tử dữ liệu độc quyền				x x			x
'90'	-L=0, chế độ băm được cung cấp bởi thẻ			x		x		
'91'	-L=0, số ngẫu nhiên được cung cấp bởi thẻ L>0, số ngẫu nhiên		x		x	x x	x x	
'92'	-L=0, dấu thời gian được cung cấp bởi thẻ L>0, dấu thời gian		x			x x	x x	
'93'	-L=0, bộ đếm chữ ký số trước cộng với một L>0, bộ đếm chữ ký số		x			x x	x x	x x
'94'	Thách thức hoặc phần tử dữ liệu để suy ra khóa	x			x			x
'95'	Byte định lượng sử dụng (xem phần bên dưới)	x	x		x	x	x	x
'8E'	Tham chiếu nội dung mật mã (xem phần bên dưới)						x	x
Trong khuôn mẫu tham chiếu điều khiển, Tổ chức có trách nhiệm lưu trữ bất kỳ DO nào khác của lớp ngữ cảnh cụ thể.								

Bảng 56 - DO sử dụng khóa

Thẻ	Giá trị
'80' đến '84'	Tham chiếu khóa và tệp như được xác định trong Bảng 55
'90'	Bộ đếm sử dụng khóa
'91'	Bộ đếm thử lại khóa
– Trong ngữ cảnh này, Tổ chức có trách nhiệm lưu trữ bất kỳ DO nào khác của lớp ngữ cảnh cụ thể	

Trong bất kỳ khuôn mẫu tham chiếu điều khiển để xác nhận (AT), đối với thỏa thuận khóa (KAT), đối với kiểm tra tổng mật mã (CCT), đối với tính bảo mật (CT) hoặc đối với chữ ký số (DST), byte định tính sử dụng (thẻ '95') có thể xác định sử dụng khuôn mẫu hoặc như điều kiện an toàn (xem 9.3.3 và Bảng 33), hoặc theo lệnh MANAGE SECURITY ENVIRONMENT (xem 11.5.11). Bảng 57 thể hiện byte định tính sử dụng.

Bảng 57 - Mã hóa byte định tính sử dụng

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
1	-	-	-	-	-	-	-	Xác minh (DST, CCT), mã hóa (CT), Xác nhận ngoài (AT), thỏa thuận khóa (KAT)
-	1	-	-	-	-	-	-	Phép tính (DST, CCT), giải mã (CT) Xác nhận trong (AT), thỏa thuận khóa (KAT)
-	-	1	-	-	-	-	-	Thông điệp an toàn trong trường dữ liệu hồi đáp (CCT, CT, DST)
-	-	-	1	-	-	-	-	Thông điệp an toàn trong trường dữ liệu lệnh (CCT, CT, DST)
-	-	-	-	1	-	-	-	Xác nhận người sử dụng, trên cơ sở mật lệnh (AT)
-	-	-	-	-	1	-	-	Xác nhận người sử dụng, trên cơ sở sinh trắc học (AT)
-	-	-	-	-	-	x	x	00 (mọi giá trị khác là RFU)

Trong bất kỳ khuôn mẫu tham chiếu điều khiển nào đối với tính bảo mật (CT), tham chiếu nội dung tài liệu viết bằng mật mã (thẻ '8E') có thể xác định nội dung của tài liệu viết bằng mật mã. Byte đầu tiên của trường giá trị là bắt buộc, tên của nó là byte bộ mô tả tài liệu viết bằng mật mã. Bảng 58 thể hiện byte bộ mô tả tài liệu viết bằng mật mã.

Bảng 58 - Byte bộ mô tả tài liệu viết bằng mật mã

Giá trị	Ý nghĩa
'00'	Không có thêm chỉ báo
'1X'	Một đến bốn khóa bí mật để mã hóa thông tin, không phải các khóa ('X' là ánh xạ bit với bất kỳ giá trị nào từ '0' đến 'F' '11' biểu thị khóa đầu tiên (ví dụ, từ điều khiển "số chẵn" trong hệ thống TV trả giá '12' biểu thị khóa thứ hai (ví dụ, từ điều khiển "số lẻ" trong hệ thống TV trả giá) '13' biểu thị khóa đầu tiên theo sau bởi khóa thứ hai (ví dụ, một cặp từ điều khiển trong hệ thống TV trả giá)
'2X'	Khóa bí mật để mã hóa các khóa, không phải thông tin ('X' là tham chiếu với bất kỳ giá trị nào từ '0' đến 'F') (ví dụ trong hệ thống TV trả giá, hoặc khóa hoạt động để mã hóa các từ điều khiển hoặc khóa quản lý để mã hóa các khóa hoạt động)
'3X'	Khóa riêng của cặp khóa không đối xứng ('X' là tham chiếu với bất kỳ giá trị nào từ '0' đến 'F')
'4X'	Mật lệnh ('X' là tham chiếu với bất kỳ giá trị nào từ '0' đến 'F')
'80' đến 'FF'	Độc quyền
– Mọi giá trị khác là RFU	

10.3.3 Môi trường an toàn

Điều này xác định môi trường an toàn (SE) để tham chiếu thuật giải mật mã, chế độ hoạt động, giao thức, thủ tục, khóa và bất kỳ dữ liệu bổ sung cần thiết nào đối với thông điệp an toàn và đối với thao tác an toàn (xem ISO/IEC 7816-8). Một SE bao gồm các phần tử dữ liệu được lưu giữ trong thẻ hoặc có kết quả từ một số phép tính, được xử lý bằng thuật giải xác định. Một SE có thể bao gồm cơ chế thiết lập ban đầu dữ liệu không ổn định được sử dụng trong môi trường, ví dụ, khóa phiên. Một SE có thể cung cấp hướng để xử lý kết quả phép tính , ví dụ lưu giữ trong thẻ. Khuôn mẫu SE liên ngành (thẻ '7B') mô tả một SE.

Định danh SE - một định danh SE (SEID) có thể tham chiếu bất kỳ môi trường an toàn nào, ví dụ đối với thông điệp an toàn và đối với lữu giữ và hồi phục bằng lệnh MANAGE SECURITY ENVIRONMENT (xem 11.5.11).

- Trừ khi có quy định khác theo ứng dụng, giá trị '00' biểu thị môi trường trống mà thông điệp an toàn và xác nhận không được xác định.
- Giá trị 'FF' biểu thị rằng không có hoạt động nào có thể được thực hiện trong môi trường này.
- Trừ khi có quy định khác theo ứng dụng, giá trị '01' được lưu giữ đối với SE mặc định, luôn có sẵn. Điều này không xác định nội dung của SE mặc định; nó có thể trống.
- Giá trị 'EF' là RFU.

Các hợp phần - khuôn mẫu tham chiếu điều khiển (CRT) có thể mô tả các hợp phần khác nhau của một SE. Bất kỳ tham chiếu điều khiển tương đối nào (tệp, khóa hoặc dữ liệu) được xác định bằng cơ chế trong định nghĩa môi trường được giải đối với curDF được lựa chọn trước khi sử dụng cơ chế này. Tham chiếu điều khiển tuyệt đối (ví dụ đường dẫn tuyệt đối) không cần phải giải. Trong SE, các hợp phần có thể có hai dạng: một là có hiệu lực đối với SM trong trường dữ liệu lệnh và đối với SM trong trường dữ liệu hồi đáp.

Tại bất kỳ thời điểm nào trong suốt quá trình hoạt động của thẻ, SE hiện hành hoạt động, hoặc theo mặc định hoặc do lệnh được thực hiện bằng thẻ. SE hiện hành bao gồm một hoặc nhiều hợp phần trong số các hợp phần sau.

- Một số hợp phần thuộc về SE mặc định kết hợp với curDF.
- Một số hợp phần được truyền trong lệnh sử dụng thông điệp an toàn.
- Một số hợp phần được truyền trong lệnh MANAGE SECURITY ENVIRONMENT.
- Một số hợp phần được dẫn ra bởi SEID trong lệnh MANAGE SECURITY ENVIRONMENT.

SE hiện hành có hiệu lực cho đến khi

- Ngăn chặn giao diện vật lý (xem 5.1), hoặc
- Thiết lập lại kênh lô-gic (xem 11.1.2), hoặc
- Thay đổi VA (ví dụ thay đổi curDF), hoặc
- Lệnh MANAGE SECURITY ENVIRONMENT. (xem 11.5.11) thiết lập hoặc thay thế SE hiện hành.

Trong SM, DO tham chiếu điều khiển được truyền trong CRT được quyền ưu tiên đối với bất kỳ DO tham chiếu điều khiển tương ứng xuất hiện trong SE hiện hành.

Quyền hạn người giữ chứng nhận - thủ tục xác thực có thể sử dụng chứng nhận có thể xác minh được thẻ, nghĩa là khuôn mẫu mà có thể được giải thích và xác minh bởi thẻ bằng hoạt động VERIFY CERTIFICATE sử dụng khóa công khai (xem ISO/IEC 7816-8). Trong các chứng nhận như vậy, quyền hạn người giữ chứng nhận (ví dụ định danh vai trò) có thể được truyền trong DO'5F4C' liên ngành. Nếu phần tử dữ liệu như vậy được sử dụng trong điều kiện an toàn để thực hiện truy cập dữ liệu hoặc hàm, khi đó DO'5F4C' phải xuất hiện trong khuôn mẫu tham chiếu điều khiển đối với xác thực (AT) mô tả thủ tục xác thực.

CHÚ THÍCH Trong bản in đầu tiên của TCVN 11167-9 (ISO/IEC 7816-9)), thẻ '5F4B' tham chiếu quyền hạn người giữ chứng nhận (phần tử dữ liệu của năm hoặc nhiều byte hơn nữa). trong bản sửa đổi bổ sung 1 của bản in đầu tiên của ISO/IEC 7816-6, thẻ '5F4B' tham chiếu định danh nhà sản xuất mạch tích hợp (phần tử dữ liệu 1 byte). Kết quả là thẻ '5F4B' bị phản đối trong TCVN 11167 (ISO/IEC 7816).

Điều khiển truy cập - thẻ có thể lưu giữ môi trường an toàn được sử dụng đối với điều khiển truy cập trong EF (xem thẻ '8D' trong Bảng 10) bao gồm khuôn mẫu SE liên ngành (thẻ '7B'). Ứng dụng có thể lưu giữ các DO'7B' trong VA được thiết lập bởi lựa chọn ứng dụng (ví dụ DO thế hệ đầu tiên). Trong khuôn mẫu SE liên ngành (thẻ '7B'), lớp ngữ cảnh cụ thể được lưu giữ đối với DO môi trường an toàn. Như được liệt kê trong Bảng 59 đối với mỗi SE được bao gộp, khuôn mẫu môi trường an toàn bao gồm một SEID DO'80', LCS DO'8A' tùy chọn, một hoặc nhiều khuôn mẫu định danh cơ chế mật mã (thẻ 'AC') và một hoặc nhiều CRT (thẻ 'A4', 'A6', 'AA', 'B4', 'B6', 'B8', như thẻ SM).

Bảng 59 - DO môi trường an toàn

Thẻ	Giá trị
'80'	SEID (1 byte, bắt buộc)
'8A'	LCS (1 byte, xem 7.4.10 và Bảng 14), tùy chọn
'AC'	Khuôn mẫu định danh cơ chế mật mã (xem 9.2), tùy chọn
'A4', 'A6', 'AA', 'B4', 'B6', 'B8'	CRT (xem 10.3.1)
– Dưới thẻ '7B', Tổ chức có trách nhiệm lưu trữ bất kỳ DO nào khác của lớp ngữ cảnh cụ thể	

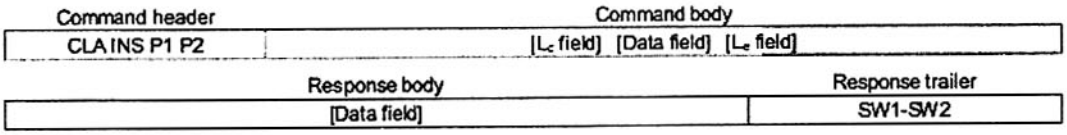
Một khuôn mẫu SE có thể áp dụng đối với cấu trúc (xem điều 7) chỉ khi giá trị của DO'8A' của khuôn mẫu SE đó tương thích LCS của cấu trúc (ví dụ, xem DO'8A' trong Bảng 10). Nếu không có DO'8A' xuất hiện trong khuôn mẫu SE, khi đó khuôn mẫu SE đó có hiệu lực chỉ với trạng thái hoạt động đã được kích hoạt.

10.3.4 Khuôn mẫu bộ mô tả hồi đáp

Mỗi trường dữ liệu lệnh có thể bao gồm một khuôn mẫu bộ mô tả hồi đáp. nếu xuất hiện trong trường dữ liệu lệnh, khuôn mẫu bộ mô tả hồi đáp biểu thị SM DO được yêu cầu trong trường dữ liệu hồi đáp. Trong khuôn mẫu bộ mô tả hồi đáp, cơ chế an toàn không được áp dụng; thực thể nhận phải áp dụng chúng để xây dựng trường dữ liệu hồi đáp. Các điều an toàn (thuật giải, chế độ hoạt động, khóa và dữ liệu ban đầu) được sử dụng để xử lý trường dữ liệu lệnh có thể khác với các điều được sử dụng để sản sinh trường dữ liệu hồi đáp. Các quy tắc sau áp dụng.

- Thẻ phải phù đầy mỗi DO SM cơ bản ban đầu trống
- Mỗi CRT xuất hiện trong khuôn mẫu bộ mô tả hồi đáp phải xuất hiện trong hồi đáp tại cùng địa điểm với cùng DO tham chiếu điều khiển đối với cơ chế an toàn, tập và kháo.
- Nếu khuôn mẫu mô tả hồi đáp cung cấp dữ liệu phụ, khi đó DO tương ứng phải trống trong hồi đáp.
- Nếu DO tham chiếu trống đối với dữ liệu phụ xuất hiện trong khuôn mẫu bộ mô tả hồi đáp, khi đó nó phải đầy trong hồi đáp.
- Theo cơ chế an toàn thích hợp, có các điều an toàn được lựa chọn, thẻ phải sản sinh tất các SM DO cơ bản được yêu cầu.

10.4 Tác động SM đối với cặp lệnh-hồi đáp



Hình 6 mô tả một C-RP

Hình 6 - Cặp lệnh-hồi đáp

Các quy tắc sau áp dụng để đảm bảo C-RP của lớp liên ngành (xem 5.4.1), nghĩa là khi chuyển hoặc bit b4 từ 0 đến 1 trong CLA mà tại đó bit b8, b7 và b6 được đặt là 000, hoặc bit b6 từ 0 đến 1 trong CLA mà tại đó bit b8 và b7 được đặt là 1. Ký hiệu CLA nghĩa là thông điệp an toàn được biểu thị bằng CLA.

- Trường dữ liệu lệnh an toàn là trường SM; nó được hình thành như sau.

- Nếu một trường dữ liệu lệnh xuất hiện (N_c>0), khi đó hoặc DO giá trị trống (thẻ SM '80', '81', 'B2', 'B3'), hoặc DO đối với tính bảo mật (thẻ SM '84', '85', '86', '87') phải truyền byte N_c.
- Tiêu đề lệnh (bốn byte) có thể được bao gói để bảo vệ (thẻ SM '89').
- Nếu trường L_e xuất hiện, khi đó trường L_e mới (chỉ bao gồm các byte được đặt là '00') và L_e DO (thẻ SM '96', '97') phải xuất hiện. Nếu xuất hiện, giá trị của L_e DO phải cung cấp L_e cho hồi đáp không được bảo vệ. L_e DO trống ('9600' hoặc '9700') có nghĩa là tối đa, nghĩa là 256 hoặc 65 536 phụ thuộc vào liệu trường L_e mới ngắn hoặc mở rộng. Mặt khác, nếu trường L_e đối với hồi đáp không bảo vệ bao gồm:
- Một byte, byte này phải trở thành trường giá trị của L_e DO.
- 2 byte, 2 byte này phải trở thành trường giá trị của L_e DO.
- Ba byte, nghĩa là một byte được đặt là '00' theo sau bởi 2 byte có giá trị bất kỳ, 2 byte phải trở thành trường giá trị của L_e DO.

Cảnh báo - một số hệ thống xử lý mã hóa trường L_e ba byte trong một L_e DO có trường giá trị 3 byte.

- Trường dữ liệu hồi đáp an toàn là trường SM; nó được diễn giải như sau.
- Nếu xuất hiện, DO giá trị trống (thẻ SM '80', '81', 'B2', 'B3') hoặc DO đối với tính bảo mật (thẻ SM '84', '85', '86', '87') truyền byte dữ liệu hồi đáp.
- Nếu xuất hiện, DO trạng thái xử lý (thẻ SM '99') truyền SW1- SW2 được bao gói để bảo vệ. DO trạng thái xử lý trống có nghĩa là SW1- SW2 được đặt là '9000'.

Hình 7 thể hiện C-RP an toàn tương ứng

Command header	Command body
CLA* INS P1 P2	[New L_c field] - {[Secured data field] = [T-N_c-Data bytes] - [T-'01' or '02'-L_e]} - [New L_e field]

Response body	Response trailer
[Secured data field] = [T-Nr-Data bytes] - [T-'02'-SW1-SW2]	SW1-SW2

Hình 7 - Cặp lệnh-hồi đáp an toàn

Khi bit b1 của INS được đặt là 1 (chế độ INS lẻ, xem 5.5), trường dữ liệu không an toàn được mã hóa trong BER-TLV và thẻ SM 'B2', 'B3', '84' và '85' được sử dụng đối với trình bao gói của chúng; trừ khi sử dụng thẻ '80', '81', '86' và '87' được xác định tại mức ứng dụng.

Cách khác (chế độ INS chẵn, xem 5.5), do định dạng của trường dữ liệu để bảo vệ luôn không biểu kiến, thẻ SM '80', '81', '86' và '87' được khuyến nghị.

- Trường dữ liệu an toàn là trường SM; chúng có thể bao gồm các DO SM khác hoặc hơn nữa, ví dụ kiểm tra tổng mật mã (thẻ SM '8E') hoặc chữ ký số (thẻ SM '9E') ở cuối.
- Trường L_c mới mã hóa số byte trong trường dữ liệu lệnh an toàn.
- Trường L_e mới không xuất hiện khi không có trường dữ liệu nào được mong đợi trong trường dữ liệu hồi đáp an toàn; mặt khác, nó phải bao gồm chỉ các byte được đặt là '00'.
- Bản ghi cuối hồi đáp biểu thị trạng thái của thực thể nhận sau khi xử lý lệnh an toàn. Các điều kiện lỗi cụ thể sau có thể xảy ra.
- Nếu SW1-SW2 được đặt là '6987', khi đó DO thông điệp an toàn được mong đợi bị thiếu.
- Nếu SW1-SW2 được đặt là '6988', khi đó DO thông điệp an toàn không đúng.

Phụ lục B cung cấp ví dụ mô tả thông điệp an toàn.

11 Lệnh trao đổi

Điều này xác định lệnh trao đổi. Nó không mang tính bắt buộc đối với tất cả các thẻ tuân theo tiêu chuẩn này để hỗ trợ tất cả các lệnh hoặc tất cả các lựa chọn của lệnh được hỗ trợ. Khi trao đổi được yêu cầu, tập hợp cung cấp thẻ ứng dụng độc lập và các lệnh liên quan và các lựa chọn được sử dụng như được xác định trong điều 12.

11.1 Lựa chọn

Sau khi kích hoạt giao diện vật lý (xem 5.1), VA trên kênh lô-gic cơ bản như được xác định trong 7.2.2. Byte lịch sử (xem 12.1.1) hoặc chuỗi dữ liệu ban đầu (xem 12.1.2) có thể biểu thị ứng dụng được lựa chọn ẩn.

Tiểu điều 11.1.1 bao gồm lựa chọn các tệp, ứng dụng và DO. Hàm lựa chọn DO bổ sung được bao gồm trong 11.4.2.

Chú thích Do không thể sử dụng định danh EF ngắn trong lệnh SELECT/SELECT DATA, FCP DO'A2' của DF không liên quan với lệnh SELECT/SELECT DATA. Do vậy, tham chiếu tệp gián tiếp (xem 7.4.11) không bao giờ xảy ra trong suốt quá trình xử lý lệnh SELECT/SELECT DATA.

11.1.1 Lệnh SELECT

Khi hoàn thành, lệnh mở kênh lô-gic (xem 5.4.2) được đánh số trong CLA (xem 5.4.1), nếu không được mở, và thiết lập cấu trúc hiện hành trong kênh lô-gic đó. Lệnh tiếp theo có thể tham chiếu ẩn với cấu trúc hiện hành qua kênh lô-gic.

DF được lựa chọn (MF, DF ứng dụng, DF) trở thành hiện hành trong kênh lô-gic (xem 7.2.2 các quy tắc d) và e)). DF được lựa chọn trước, nếu có, không được tham chiếu qua kênh lô-gic đó. Sau khi lựa chọn, EF hiện hành ẩn có thể được tham chiếu qua kênh lô-gic đó.

Lựa chọn EF thiết lập cặp tệp hiện hành: EF và DF cha của nó (xem 7.2.2 quy tắc f)).

Bảng 60 - Cặp lệnh-hồi đáp SELECT

CLA	Như được xác định trong 5.4.1
INS	'A4'
P1	Xem Bảng 61
P2	Xem Bảng 62
Trường L_c	Không xuất hiện đối với mã hóa $N_c = 0$, xuất đối với mã hóa $N_c > 0$
Trường dữ liệu	Không xuất hiện hoặc định danh tệp hoặc đường truyền hoặc tên DF hoặc tệp (theo P1)
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$, xuất đối với mã hóa $N_e > 0$
Trường dữ liệu	Không xuất hiện hoặc thông tin điều khiển (theo P2)
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6283', '6284', 6A81', '6A82', '6A86', '6A87', '6A88'

Bảng 61 - Mã hóa P1 trong lệnh SELECT

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa	Trường dữ liệu lệnh
0	0	0	0	0	0	x	x	Lựa chọn theo định danh tệp	
0	0	0	0	0	0	0	0	Lựa chọn MF, DF hoặc EF	Định danh tệp hoặc không xuất hiện
0	0	0	0	0	0	0	1	Lựa chọn DF con	Định danh tệp tham chiếu DF
0	0	0	0	0	0	1	0	Lựa chọn EF dưới DF hiện hành	Định danh tệp tham chiếu EF
0	0	0	0	0	0	1	1	Lựa chọn DF cha của DF hiện hành	Không xuất hiện
0	0	0	0	0	1	x	x	Lựa chọn theo tên DF	
0	0	0	0	0	1	0	0	Lựa chọn theo tên DF	Ví dụ định danh ứng dụng (cắt cụt)
0	0	0	0	1	0	x	x	Lựa chọn theo đường dẫn	
0	0	0	0	1	0	0	0	Lựa chọn từ MF	Đường dẫn không có định danh MF
0	0	0	0	1	0	0	1	Lựa chọn từ DF hiện hành	Đường dẫn không có định danh DF hiện hành
0	0	0	1	0	0	x	x	Lựa chọn DO	
0	0	0	1	0	0	0	0	Lựa chọn Do trong khuôn mẫu hiện hành	Thẻ thuộc khuôn mẫu hiện hành
0	0	0	1	0	0	1	1	Lựa chọn DO cha của DO được xây dựng thiết lập khuôn mẫu hiện hành	Không xuất hiện

- Mọi giá trị khác là RFU
- Khi xuất hiện trong byte lịch sử (xem 12.1.1) hoặc trong EF.ATR/INFO (xem 12.2.2), Bảng chức năng phần mềm đầu tiên (xem Bảng 117) biểu thị phương pháp lựa chọn được hỗ trợ bằng thẻ.

Bảng 62 - Mã hóa P2 trong lệnh SELECT

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	0	0	0	-	-	x	x	Tệp hoặc số lần DO
0	0	0	0	-	-	0	0	– Số lần đầu tiên hoặc duy nhất
0	0	0	0	-	-	0	1	– Số lần cuối cùng
0	0	0	0	-	-	1	0	– Số lần tiếp theo
0	0	0	0	-	-	1	1	– Số lần trước
0	0	0	0	x	x	-	-	Yêu cầu trường dữ liệu hồi đáp (xem 7.4.2 và Bảng 8)
0	0	0	0	0	0	-	-	- phục hồi khuôn mẫu FCI, sử dụng tùy chọn của độ dài và thẻ FCI
0	0	0	0	0	1	-	-	- phục hồi khuôn mẫu CP, sử dụng bắt buộc của độ dài và thẻ CP
0	0	0	0	1	0	-	-	- phục hồi khuôn mẫu FMD, sử dụng bắt buộc của độ dài và thẻ FMD - phục hồi thẻ thuộc khuôn mẫu được thiết lập bởi lựa chọn DO được xây dựng làm danh sách thẻ
0	0	0	0	1	1	-	-	- không có dữ liệu hồi đáp nếu trường L_e không xuất hiện, hoặc độc quyền nếu trường L_e xuất hiện
– Mọi giá trị khác là RFU								

Trừ khi có quy định khác, các quy tắc sau áp dụng với mỗi kênh lô-gic mở trong hệ phân cấp DF.

- Nếu EF hiện hành bị thay đổi, hoặc khi không có EF hiện hành, khi đó trạng thái an toàn, nếu có, đặc thù đối với EF được lựa chọn trước phải bị hủy bỏ.
- Nếu DF hiện hành là con, hoặc đồng nhất với DF được lựa chọn trước, khi đó trạng thái an toàn đặc thù với DF lựa chọn trước phải bị hủy bỏ. Trạng thái an toàn chung đối với tất cả thủy tổ của DF được lựa chọn trước và DF hiện hành mới phải được duy trì.

Nếu P1 được đặt là '00', khi đó thẻ biết liệu tệp lựa chọn là MF, DF hoặc EF, hoặc do mã hóa đặc thù định danh tệp, hoặc do ngữ cảnh xử lý lệnh. Nếu P2 cũng được đặt là '00' và trường dữ liệu lệnh

- Cung cấp định danh tệp, khi đó định danh tệp đó phải duy nhất trong ba môi trường sau: con trực tiếp của DF hiện hành, DF cha và con trực tiếp của DF cha.
- Xuất hiện hoặc được đặt là '3F00', khi đó MF phải được lựa chọn.

Nếu P1 được đặt là '04', khi đó trường dữ liệu lệnh là tên DF mà có thể là định danh tệp (xem 12.2.3) có khả năng bị cắt cụt. Nếu được hỗ trợ, kế tiếp, các lệnh như vậy có trường dữ liệu như nhau phải lựa chọn DF mà tên của chúng thích hợp với trường dữ liệu, nghĩa là bắt đầu với trường dữ liệu lệnh. Nếu thẻ chấp nhận lệnh SELECT mà không có trường dữ liệu, khi đó tất cả hoặc tập hợp con của các DF có thể được lựa chọn liên tiếp.

Nếu P1 được đặt là '10', khi đó trường dữ liệu lệnh là thẻ thuộc về khuôn mẫu hiện hành. DO được lựa chọn trở thành DO hiện hành. Nếu DO được lựa chọn được xây dựng, nó thiết lập khuôn mẫu của mình làm khuôn mẫu hiện hành. Để xử lý các nhiều phiên bản của DO, sử dụng bit b1 b2 trong P2 (xem Bảng 62) là bắt buộc.

Nếu trường L_e bao gồm chỉ các byte được đặt là '00', khi đó tất cả các byte tương ứng với sự lựa chọn phải quay lại trong giới hạn của 256 đối với trường L_e ngắn, hoặc 65 536 đối với trường L_e mở rộng. Nếu trường L_e không xuất hiện, thông tin điều khiển có sẵn (CP và/hoặc FMD) của cấu trúc được lựa chọn có thể được phục hồi qua xử lý DO (xem 11.4.3 và 11.4.4).

11.1.2 Lệnh MANAGE CHANNEL

Khi hoàn thành, lệnh mở hoặc đóng kênh lô-gic (xem 5.4.2) ngoại trừ lệnh cơ bản, nghĩa là kênh lô-gic được đánh số từ 1 đến mười chính (số lớn hơn là RFU). Hàm thiết lập lại có thể áp dụng đối với bất kỳ kênh lô-gic nào.

Hàm mở mở kênh lô-gic bổ sung ngoại trừ kênh lô-gic cơ bản. Các lựa chọn được cung cấp cho thẻ quy định số kênh, hoặc số kênh được cung cấp cho thẻ.

- Nếu bit b8 và b7 của P1 được đặt là 00 (nghĩa là P1 được đặt là '00' do sáu bit khác là RFU), khi đó MANAGE CHANNEL phải mở kênh lô-gic được đánh số từ 1 đến mười chín như sau.
- Nếu P2 được đặt là '00', khi đó trường L_e phải là '01' (định dạng ngắn) hoặc '000001' (định dạng mở rộng), và trường dữ liệu hồi đáp phải bao gồm một byte đơn lẻ mã hóa số kênh không phải là 0 được quy định bởi thẻ từ '01' đến '13'.
- Nếu P2 được thiết lập từ '01' đến '13', khi đó nó mã hóa số kênh không phải là 0 được quy định ngoài và trường L_e xuất hiện.
- Sau khi một hàm mở được thực hiện từ kênh lô-gic cơ bản (CLA mã hóa không làm số kênh), MF hoặc DF ứng dụng mặc định phải được lựa chọn ẩn làm DF hiện hành trên kênh lô-gic mới.
- Sau khi một hàm mở được thực hiện từ kênh lô-gic không cơ bản (CLA mã hóa số kênh không phải là 0), DF hiện hành trên kênh lô-gic được đánh số trong CLA phải được lựa chọn theo 7.2.2 quy tắc e) trên kênh lô-gic mới.

Hàm đóng đóng rõ ràng kênh lô-gic ngoại trừ kênh cơ bản. Trường L_e phải xuất hiện. Sau khi đóng, kênh lô-gic phải sẵn sàng để tái sử dụng. Nếu bit b8 và b7 của P1 được đặt là 10 (nghĩa là P1 được đặt là '80' do sáu bit khác là RFU), khi đó MANAGE CHANNEL phải đóng kênh lô-gic được đánh số từ 1 đến mười chín như sau.

- Nếu P2 được đặt là '00', khi đó kênh lô-gic được đánh số trong CLA (số kênh không phải là 0) phải được đóng
- Nếu P2 được thiết lập từ '01' đến '13', khi đó kênh lô-gic được đánh số trong P2 phải được đóng.

Cảnh báo - hàm đóng có thể bị hủy nếu CLA không biểu thị kênh lô-gic cơ bản và kênh lô-gic được đánh số trong P2. Mã hóa P1-P2 trong dãy '8001' đến '8013' phải bị phản đối trong tương lai.

Hàm thiết lập lại đóng và mở rõ ràng bất kỳ kênh lô-gic nào được xác định bằng CLA. Trường L_e phải không xuất hiện. Sau khi thiết lập lại, VA trên kênh lô-gic được xác định theo 7.2.2. Trạng thái an toàn được thiết lập trên kênh lô-gic phải bị thu hồi.

Lệnh thiết lập lại kênh lô-gic cơ bản và đóng tất cả các kênh lô-gic bổ sung phải được gửi trên kênh lô-gic cơ bản.

CHÚ THÍCH Tại mức APDU, hàm (P1-P2='4001') tương đương với cho phép giao diện vật lý (xem 5.1).

Bảng 63 - Cặp lệnh-hồi đáp MANAGE CHANNEL

CLA	Như được xác định trong 5.4.1	
INS	'70'	
P1-P2	'0000'	Mở kênh lô-gic được đánh số trong trường dữ liệu hồi đáp
	'0001' đến '0013'	Mở kênh lô-gic được đánh số trong P2
	'8000'	Đóng kênh lô-gic được đánh số trong CLA (ngoại trừ kênh lô-gic cơ bản)
	'8001' đến '8013'	Đóng kênh lô-gic được đánh số trong P2
	'4000'	Thiết lập lại kênh lô-gic được đánh số trong CLA
	'4001'	Thiết lập kênh lô-gic cơ bản và đóng tất cả kênh lô-gic bổ sung
	Các giá trị khác	RFU
Trường dữ liệu	Xuất hiện	
Trường L_e	Xuất hiện đối với mã hóa N_e = 0, xuất hiện đối với mã hóa N_e = 1	
Trường dữ liệu	Xuất hiện (P1-P2 không đặt là '0000'), hoặc '01' đến '13' (P1-P2 đặt là '0000'),	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6200', '6482', '6881', '6A81'	

11.2 Xử lý đơn vị dữ liệu

11.2.1 Đơn vị dữ liệu

Trong mỗi đơn vị dữ liệu hỗ trợ EF, khoảng chừa trống phải tham chiếu mỗi đơn vị dữ liệu. Từ không đối với đơn vị dữ liệu đầu tiên của EF, khoảng chừa trống được gia tăng theo một cho mỗi đơn vị dữ liệu tiếp theo. Phần tử dữ liệu khoảng chừa trống là nhị phân được mã hóa trên số byte tối thiểu. Tham chiếu với đơn vị dữ liệu không được bao gồm trong EF là sai số.

Thẻ có thể cung cấp byte mã hóa dữ liệu (xem Bảng 118) trong byte lịch sử (xem 12.1.1) trong EF.ATR/INFO (xem 12.2.2) và trong thông tin điều khiển của bất kỳ tệp nào (xem DO'82' trong Bảng 10). Byte mã hóa dữ liệu cố định kích cỡ đơn vị dữ liệu. Nếu thẻ cung cấp byte mã hóa dữ liệu trong một số địa điểm, khi đó 7.4.5 xác định byte mã hóa dữ liệu nào phải được tính đến.

11.2.2 Tổng quát

Bất kỳ lệnh nào của nhóm này phải bị hủy nếu được áp dụng với một EF không hỗ trợ đơn vị dữ liệu. Nó có thể được thực hiện trên EF chỉ khi trạng thái an toàn thỏa mãn thuộc tính an toàn được xác định đối với hàm, tên, đọc, viết, cập nhật, xóa, tìm kiếm hoặc so sánh.

Mỗi lệnh của nhóm này có thể sử dụng hoặc một định danh EF ngắn hoặc một định danh tệp. Nếu có một EF hiện hành tại thời điểm ban hành lệnh, khi đó quá trình có thể hoàn thành trên EF đó bằng cách thiết lập tất cả các bit tương ứng đến 0. Nếu quá trình hoàn thành, khi đó EF định danh trở thành hiện hành.

INS P1 P2 - tất cả các lệnh của nhóm này sử dụng bi b1 của INS và bit b8 của P1 như sau.

- Nếu bit b1 của INS được đặt là 0 và bit b8 của P1 đến 1, khi đó bit b7 và b6 của P1 được đặt là 00 (các giá trị khác là RFU), bit b5 đến b1 của P1 mã hóa định danh EF ngắn và P2 (tám bit) mã hóa khoảng chừa trống từ 0 đến 255 trong EF được tham chiếu bằng lệnh.
- Nếu bit b1 của INS được đặt là 0 và bit b8 của P1 đến 0, khi đó P1-P2 (mười lăm bit) mã hóa khoảng chừa trống trong EF hiện hành từ 0 đến 32 767.

- Nếu bit b1 của INS được đặt là 1, khi đó P1-P2 phải định danh một EF. Nếu bảy bit đầu tiên của P1-P2 được đặt là 0 và nếu bit b5 đến b1 của P2 không phải tất cả đều bằng nhau và nếu thẻ và/hoặc EF hỗ trợ lựa chọn bằng định danh EF ngắn, khi đó bit b5 đến b1 của P2 mã hóa định danh EF ngắn (số từ 1 đến ba mươi). Mặt khác, P1-P2 là một định danh tệp. P1-P2 được đặt là '0000' định danh EF hiện hành. Ít nhất một khoảng chừa trống DO'54' xuất hiện trong trường dữ liệu lệnh. Khi xuất hiện trong trường dữ liệu hồi đáp hoặc lệnh, dữ liệu phải được bao gói trong DO'53' tùy ý. ('73' bị phản đối đối với việc sử dụng này).

Trong nhóm lệnh này:

- SW1-SW2 được đặt là '63CX' biểu thị sự thay đổi thành công trạng thái nhớ, nhưng sau đoạn chương trình thử lại bên trong; 'X' > '0' mã hóa số lần thử lại; 'X' = '0' có nghĩa là bộ đếm không được cung cấp.
- SW1-SW2 được đặt là '6B00' được sử dụng để biểu thị rằng khoảng chừa trống chỉ bên ngoài của EF.

11.2.3 Lệnh READ BINARY

Trường dữ liệu hồi đáp mang lại (phần của) nội dung của đơn vị dữ liệu hỗ trợ EF. Nếu trường L_e bao gồm chỉ các byte được đặt là '00', khi đó tất cả các byte cho đến cuối của tệp được đọc trong giới hạn của 256 đối với trường L_e ngắn, hoặc 65 536 đối với trường L_e mở rộng.

Bảng 64 - Cặp lệnh-hồi đáp READ BINARY

CLA	Như được xác định trong 5.4.1		
INS	'B0' hoặc 'B1'		
P1-P2	INS = 'B0'	Khoảng chừa trống bắt buộc, định danh EF ngắn có khả năng	Xem 11.2.2
	INS = 'B1'	Định danh EF, hoặc định danh EF ngắn	
Trường L_c	Không xuất hiện đối với mã hóa $N_c = 0$, xuất hiện đối với mã hóa $N_c > 0$		
Trường dữ liệu	INS = 'B0'	Xuất hiện	
	INS = 'B1'	DO khoảng chừa trống	
Trường L_e	Xuất hiện đối với mã hóa $N_e > 0$		
Trường dữ liệu	INS = 'B0'		Đọc dữ liệu
	INS = 'B1'		DO tùy ý bao gói đọc dữ liệu
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6281', '6282', '6700', '6981', '6982, '6986, '6A81', '6A82', '6B00'		

11.2.4 Lệnh WRITE BINARY

Lệnh kích hoạt một trong các hoạt động sau trong EF theo thuộc tính tệp:

1) Lô-gic OR của các bit đã xuất hiện trong thẻ có bit được cho trong trường dữ liệu lệnh (trạng thái xóa bỏ lô-gic của các bit có tệp bằng 0);
2) Ghi một lần của các bit được cho trong trường dữ liệu lệnh (lệnh bị hủy nếu chuỗi đơn vị dữ liệu không trong trạng thái xóa bỏ lô-gic);

3) Lô-gic AND của các bit đã xuất hiện trong thẻ có bit được cho trong trường dữ liệu lệnh (trạnh thái xóa bỏ lô-gic của các bit có tệp bằng một).

Theo mặc định, nghĩa là khi byte mã hóa dữ liệu không có sẵn (xem 11.2.1), hoạt động 1) phải áp dụng trong EF đó.

Bảng 65 - Cặp lệnh-hồi đáp WRITE BINARY

CLA	Như được xác định trong 5.4.1		
INS	'D0' hoặc 'D1'		
P1-P2	INS = 'D0'	Khoảng chừa trống bắt buộc, định danh EF ngắn có khả năng	Xem 11.2.2
	INS = 'D1'	Định danh EF, hoặc định danh EF ngắn	
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$		
Trường dữ liệu	INS = 'D0'	Chuỗi đơn vị dữ liệu được viết	
	INS = 'D1'	DO khoảng chừa trống và DO tùy ý bao gói chuỗi đơn vị dữ liệu được viết	
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$		
Trường dữ liệu	Không xuất hiện		
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '63CX' (xem 11.2.2), '6581', '6700', '6981', '6982', '6B00'		

11.2.5 Lệnh UPDATE BINARY

Lệnh kích hoạt cập nhật các bit đã xuất hiện trong một EF có các bit được cho trong trường dữ liệu lệnh. Khi quá trình hoàn thành, mỗi bit của từng đơn vị dữ liệu xác định phải có giá trị được xác định trong trường dữ liệu lệnh.

Bảng 66 - Cặp lệnh-hồi đáp UPDATE BINARY

CLA	Như được xác định trong 5.4.1		
INS	'D6' hoặc 'D7'		
P1-P2	INS = 'D6'	Khoảng chừa trống bắt buộc, định danh EF ngắn có khả năng	Xem 11.2.2
	INS = 'D7'	Định danh EF, hoặc định danh EF ngắn	
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$		
Trường dữ liệu	INS = 'D6'	Chuỗi đơn vị dữ liệu được cập nhật	
	INS = 'D7'	DO khoảng chừa trống và DO tùy ý bao gói chuỗi đơn vị dữ liệu cập nhật	
Trường L_e	Xuất hiện đối với mã hóa $N_e = 0$		
Trường dữ liệu	Xuất hiện		
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '63CX' (xem 11.2.2), '6581', '6700', '6981', '6982', '6B00'		

11.2.6 Lệnh SEARCH BINARY

Lệnh kích hoạt tìm kiếm trong đơn vị dữ liệu hỗ trợ EF. Trường dữ liệu hồi đáp mang lại khoảng chừa trống của đơn vị dữ liệu: chuỗi byte tại khoảng chừa trống được phục hồi trong EF phải có cùng giá trị như chuỗi tìm kiếm trong trường dữ liệu lệnh. Trường dữ liệu hồi đáp xuất hiện hoặc do trường L_e xuất hiện, hoặc do không tìm thấy sự tương thích. Nếu chuỗi tìm kiếm không xuất hiện, khi đó trường dữ liệu hồi đáp mang lại khoảng chừa trống của đơn vị dữ liệu đầu tiên trong trạng thái xóa bỏ lô-gic.

Bảng 67 - Cặp lệnh-hồi đáp SEARCH BINARY

CLA	Như được xác định trong 5.4.1		
INS	'A0' hoặc 'A1'		
P1-P2	INS = 'A0'	Khoảng chừa trống bắt buộc, định danh EF ngắn có khả năng	Xem 11.2.2
	INS = 'A1'	Định danh EF, hoặc định danh EF ngắn	
Trường L_c	Không xuất hiện đối với mã hóa $N_c = 0$, xuất hiện đối với mã hóa $N_c > 0$		
Trường dữ liệu	INS = 'A0'	Không xuất hiện hoặc chuỗi tìm kiếm	
	INS = 'A1'	DO khoảng chừa trống và DO tùy ý bao gói chuỗi đơn vị tìm kiếm	
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$, xuất hiện đối với mã hóa $N_e > 0$		
Trường dữ liệu	INS = 'A0'	Không xuất hiện hoặc khoảng chừa trống của đơn vị dữ liệu đầu tiên khớp với trường dữ liệu lệnh	
	INS = 'A1'	DO khoảng chừa trống biểu thị đơn vị dữ liệu đầu tiên khớp với chuỗi tìm kiếm	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6282', '6982', '6B00', '6982', '6B00'		

11.2.7 Lệnh ERASE BINARY

Lệnh thiết lập (phần của) nội dung của một EF với trạng thái xóa bỏ lô-gic, liên tục, bắt đầu từ khoảng chừa trống được cho.

- Nếu INS = '0E', khi đó, nếu xuất hiện, trường dữ liệu lệnh mã hóa khoảng chừa trống của đơn vị dữ liệu đầu tiên không bị xóa. Khoảng chừa trống này phải cao hơn khoảng chừa trống được mã hóa trong P1-P2. Nếu trường dữ liệu không xuất hiện, khi đó lệnh xóa đến cuối tệp.
- Nếu INS = '0F', khi đó, nếu xuất hiện, trường dữ liệu lệnh phải bao gồm không, một hoặc hai DO khoảng chừa trống. Nếu không có khoảng chừa trống, khi đó lệnh xóa tất cả các đơn vị dữ liệu trong tệp. Nếu có một khoảng chừa trống, nó biểu thị đơn vị dữ liệu đầu tiên bị xóa; khi đó lệnh xóa đến cuối tệp. Hai khoảng chừa trống xác định một chuỗi các đơn vị dữ liệu: khoảng chừa trống thứ hai biểu thị đơn vị dữ liệu đầu tiên bị xóa; nó phải cao hơn khoảng chừa trống đầu tiên.

Bảng 68 - Cặp lệnh-hồi đáp ERASE BINARY

CLA	Như được xác định trong 5.4.1		
INS	'0E' hoặc '0F'		
P1-P2	INS = '0E'	Khoảng chừa trống bắt buộc, định danh EF ngắn có khả năng	Xem 11.2.2
	INS = '0F'	Định danh EF, hoặc định danh EF ngắn	
Trường L_c	Không xuất hiện đối với mã hóa $N_c = 0$, Xuất hiện đối với mã hóa $N_c > 0$		
Trường dữ liệu	INS = '0E'	Không xuất hiện hoặc khoảng chừa trống của đơn vị dữ liệu đầu tiên không bị xóa	
	INS = '0F'	Không xuất hiện hoặc một hoặc hai DO khoảng chừa trống	
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$		

Trường dữ liệu	Không xuất hiện
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '63CX' (xem 11.2.2), '6581', '6700', '6981', '6982', '6B00'

11.2.8 Hàm COMPARE BINARY

Hàm này được hỗ trợ bằng lệnh COMPARE (xem 11.6.1).

11.3 Xử lý bản ghi

11.3.1 Bản ghi

Trong mỗi bản ghi hỗ trợ EF, số bản ghi và/hoặc định danh bản ghi phải tham chiếu từng bản ghi. Tham chiếu đến một bản ghi không bao gồm trong EF là một sai số.

Tham chiếu bằng số bản ghi - mỗi số bản ghi là đơn nhất và liên tiếp.

- Trong mỗi EF hỗ trợ cấu trúc tuyến tính, số bản ghi được gán liên tiếp khi viết hoặc thêm vào, nghĩa là theo trật tự được tạo ra, bản ghi đầu tiên (số một) là bản ghi được tạo ra đầu tiên.
- Trong mỗi EF hỗ trợ cấu trúc tuần hoàn, số bản ghi được gán liên tiếp trong trật tự đối nhau, nghĩa là bản ghi đầu tiên (số một) là bản ghi được tạo ra gần nhất.

Quy tắc sau được xác định đối với cấu trúc tuyến tính và đối với cấu trúc tuần hoàn.

- Số không phải tham chiếu bản ghi hiện hành, nghĩa là bản ghi đó được tham chiếu bằng con trỏ bản ghi.

Tham chiếu bằng định danh bản ghi - mỗi định danh bản ghi được cung cấp bằng một ứng dụng. Một số bản ghi có thể có cùng định danh bản ghi, mà trong đó dữ liệu trường hợp chứa trong bản ghi có thể được sử dụng để phân biệt chúng. Nếu một bản ghi là một đối tượng dữ liệu SIMPLE-TLV trong trường dữ liệu, khi đó định danh bản ghi là byte đầu tiên của đối tượng dữ liệu, nghĩa là thẻ SIMPLE-TLV.

Tham chiếu bằng định danh bản ghi mang lại sự quản lý con trỏ bản ghi. Kích hoạt giao diện vật lý, thiết lập lại kênh lô-gic, lệnh SELECT và bất kỳ lệnh nào sử dụng định danh EF ngắn có hiệu lực để truy cập một EF có thể tác động đến con trỏ bản ghi. Tham chiếu bằng số bản ghi phải không ảnh hưởng con trỏ bản ghi.

Mỗi khi tham chiếu được thực hiện bằng định danh bản ghi, vị trí lô-gic của bản ghi mục tiêu được biểu thị: số lần đầu tiên hoặc cuối cùng, số lần tiếp theo hoặc trước đó liên quan đến con trỏ bản ghi.

- Trong mỗi EF hỗ trợ cấu trúc tuyến tính, vị trí lô-gic được gán liên tiếp khi viết hoặc thêm vào, nghĩa là theo trật tự được tạo ra. Bản ghi được tạo ra đầu tiên nằm ở vị trí lô-gic đầu tiên.
- Trong mỗi EF hỗ trợ cấu trúc tuần hoàn, vị trí lô-gic được gán liên tiếp trong trật tự đối nhau, nghĩa là bản ghi được tạo ra gần nhất nằm ở vị trí lô-gic đầu tiên.

Quy tắc sau được xác định đối với cấu trúc tuyến tính và đối với cấu trúc tuần hoàn.

- Số lần đầu tiên phải là bản ghi có định danh xác định và ở vị trí lô-gic đầu tiên; số lần cuối cùng phải là bản ghi có định danh xác định và ở vị trí lô-gic cuối cùng.
- Nếu có bản ghi hiện hành, khi đó số lần tiếp theo phải là bản ghi gần nhất có định danh xác định nhưng ở vị trí lô-gic lớn hơn bản ghi hiện hành; số lần trước phải là bản ghi gần nhất có định danh xác định nhưng ở vị trí lô-gic nhỏ hơn bản ghi hiện hành.
- Nếu không có bản ghi hiện hành, khi đó số lần tiếp theo phải tương đương với số lần đầu tiên; số lần trước phải tương đương với số lần cuối cùng.
- Số không tham chiếu bản ghi đầu tiên, cuối cùng, tiếp theo hoặc trước đó theo chuỗi số, độc lập với định danh bản ghi.

11.3.2 Tổng quát

Bất kỳ lệnh nào của nhóm này phải bị hủy nếu được áp dụng với EF không hỗ trợ bản ghi. Nó có thể được thực hiện trên một EF chỉ khi trạng thái an toàn thỏa mãn thuộc tính an toàn được xác định đối với hàm, tên, đọc, viết, thêm vào, cập nhật, tìm kiếm, xóa, kích hoạt hoặc giải hoạt.

Các bản ghi trong EF có thể hỗ trợ vòng đời bản ghi. Nếu vậy, nhìn chung các bản ghi được kích hoạt không thể truy cập được bằng lệnh READ RECORD, WRITE RECORD, UPDATE RECORD, ERASE RECORD, APPEND RECORD và COMPARE (RECORD). Nếu lệnh như vậy được sử dụng, lệnh tương ứng phục hồi với byte trạng thái '6287' (ít nhất một trong các bản ghi được tham chiếu bị giải hoạt). Hơn nữa, các bản ghi bị giải hoạt phải bị bỏ qua khi thực hiện lệnh SEARCH RECORD. Chi tiết hơn nữa và các ngoại lệ đối với các quy tắc chung được đề cập ở trên được đưa ra dưới đây.

Hai lệnh của nhóm này (READ, UPDATE) có thể sử dụng một chế độ INS lẻ (trường dữ liệu được mã hóa trong BER-TLV) để kích hoạt một hành động trên phần của bản ghi được cho (đọc một phần, cập nhật một phần). Sau đó, khoảng chừa trống phải tham chiếu mỗi byte trong bản ghi: từ 0 đối với byte đầu tiên của bản ghi, khoảng chừa trống được gia tăng theo một cho mỗi byte tiếp theo của bản ghi. Tham chiếu đến một byte không bao gồm trong bản ghi là một sai số. Khi cần thiết, phần tử dữ liệu

khoảng chừa trống là nhị phân được mã hóa và tham chiếu bởi thẻ '54'. Khi xuất hiện trong trường dữ liệu hồi đáp hoặc lệnh, dữ liệu phải được bao gói trong DO'53' tùy ý ('73' bị phản đối đối với việc sử dụng này).

Mỗi lệnh của nhóm này có thể sử dụng định danh EF ngắn. Nếu quá trình hoàn thành, khi đó EF định danh trở thành hiện hành và con trỏ bản ghi được thiết lập lại. Nếu có EF hiện hành tại thời điểm ban hành lệnh, khi đó quá trình có thể được hoàn thành mà không biểu thị EF (bằng cách thiết lập năm bit tương ứng đến 0).

P1 - mỗi số bản ghi hoặc định danh là một số từ 1 đến 254, được mã hóa bằng một giá trị của P1 từ '01' đến 'FE'. 0 (được mã hóa '00') được lưu trữ cho mục đích đặc biệt. 255 (được mã hóa 'FF') là RFU.

CHÚ THÍCH Nếu số bản ghi vượt quá dãy số ('01' đến 'FE') của bản ghi xử lý lệnh, bản ghi có thể được xử lý, ví dụ bằng cách sử dụng lựa chọn số lần tiếp theo của định danh bản ghi.

P2 - bit b8 đến b4 là định danh EF ngắn theo Bảng 69. Bit 3 đến 1 phụ thuộc vào lệnh.

Bảng 69 - Mã hóa định danh EF ngắn trong P2

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	0	0	0	0	-	-	-	EF hiện hành
Không phải tất cả đều bằng nhau					-	-	-	Định danh EF ngắn (một số từ 1 đến ba mươi)
1	1	1	1	1	-	-	-	RFU

Trong nhóm lệnh này, SW1-SW2 được đặt là '63CX' biểu thị sự thay đổi thành công của trạng thái nhớ, nhưng sau khi đoạn chương trình thử lại bên trong; 'X' > '0' mã hóa số lần thử lại; 'X' = '0' có nghĩa là bộ đếm không được cung cấp.

11.3.3 Lệnh READ RECORD

Trường dữ liệu hồi đáp mang lại (một phần) nội dung của bản ghi được xử lý (hoặc phần đầu của một bản ghi) trong một EF.

Nếu bất kỳ bản ghi nào được tham chiếu bởi P1 và P2 trong bản ghi LCS DEACTIVATED, lệnh được xử lý với cảnh báo '6287' và trường dữ liệu hồi đáp phải trống.

Nếu INS = 'B2' và nếu bản ghi là đối tượng dữ liệu SIMPLE-TLV (xem 6.1), khi đó hình 8 mô tả trường dữ liệu hồi đáp. So sánh N_r với cấu trúc TLV biểu thị liệu bản ghi đơn nhất (đọc một bản ghi) hoặc bản ghi cuối cùng (đọc tất cả bản ghi) là chưa hoàn thành, hoàn thành hoặc được đệm.

CHÚ THÍCH Nếu bản ghi không phải là đối tượng dữ liệu, khi đó hàm đọc tất cả bản ghi đưa lại việc nhận bản ghi mà không phân định.

Nếu INS = 'B3', khi đó lệnh không hỗ trợ lựa chọn "đọc tất cả bản ghi" trong P2. Nó đọc một phần bản ghi được tham chiếu bởi P1. Trường dữ liệu lệnh phải bao gồm DO'54' khoảng chừa trống biểu thị byte đầu tiên được đọc trong bản ghi. Trường dữ liệu hồi đáp phải bao gồm DO'53' tùy ý bao gói đọc dữ liệu.

Bảng 70 - Cặp lệnh-hồi đáp READ RECORD

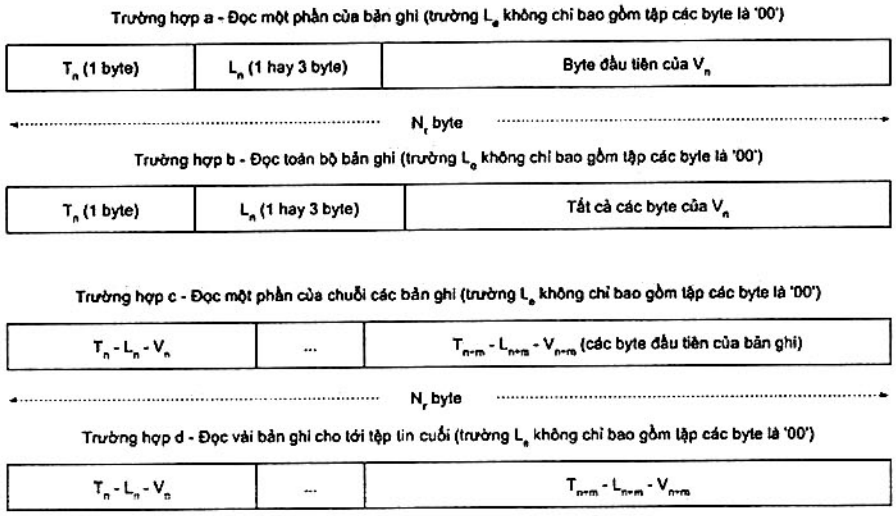
CLA	Như được xác định trong 5.4.1	
INS	'B2' hoặc 'B3'	
P1	Số bản ghi hoặc định danh bản ghi hoặc '00' tham chiếu bản ghi hiện hành	
P2	Xem Bảng 71	
Trường L_c	Không xuất hiện đối với mã hóa $N_c = 0$, xuất hiện đối với mã hóa $N_c > 0$	
Trường dữ liệu	INS = 'B2'	Không xuất hiện
	INS = 'B3'	DO khoảng chừa trống
Trường L_e	Xuất hiện đối với mã hóa $N_e > 0$	

Trường dữ liệu	INS = 'B2'	Đọc dữ liệu
	INS = 'B3'	DO tùy ý bao gói đọc dữ liệu
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6281', '6282', '6700', '6981', '6982', '6A81', '6A82', '6A83'	

Bảng 71 - Mã hóa P2 trong lệnh READ RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	x	x	x	-	-	-	Định danh EF ngắn theo Bảng 69
-	-	-	-	-	0	x	x	Định danh bản ghi trong P1
-	-	-	-	-	0	0	0	– Đọc số lần đầu tiên
-	-	-	-	-	0	0	1	– Đọc số lần cuối cùng
-	-	-	-	-	0	1	0	– Đọc số lần tiếp theo
-	-	-	-	-	0	1	1	– Đọc số lần trước
-	-	-	-	-	1	x	x	Số bản ghi trong P1
-	-	-	-	-	1	0	0	– Đọc bản ghi P1
-	-	-	-	-	1	0	1	– Đọc tất cả các bản ghi từ P1 cho đến bản cuối cùng (chỉ đối với INS = 'B2')
-	-	-	-	-	1	1	0	– Đọc tất cả các bản ghi từ bản cuối cùng cho đến P1 (chỉ đối với INS = 'B2')
					1	1	1	RFU

Nếu trường L_e bao gồm chỉ các byte được đặt là '00', khi đó lệnh phải đọc toàn bộ hoặc bản ghi được yêu cầu đơn lẻ, hoặc chuỗi các bản ghi được yêu cầu, phụ thuộc vào bit 3, 2 và 1 của P2 và trong giới hạn của 256 đối với trường L_e ngắn, hoặc 65 536 đối với trường L_e mở rộng.



Hình 8 - Trường dữ liệu hồi đáp có INS = 'B2' khi bản ghi là đối tượng dữ liệu SIMPLE-TLV

11.3.4 Lệnh WRITE RECORD

Lệnh kích hoạt một trong số các hoạt động sau trong EF theo thuộc tính tệp:

1) Ghi một lần bản ghi được cho trong trường dữ liệu lệnh (lệnh bị hủy nếu bản ghi không ở trạng thái xóa lô-gic);
2) Lô-gic OR của byte dữ liệu của bản ghi đã xuất hiện trong thẻ với byte dữ liệu của bản ghi được cho trong trường dữ liệu lệnh;
3) Lô-gic AND của byte dữ liệu của bản ghi đã xuất hiện trong thẻ với byte dữ liệu của bản ghi được cho trong trường dữ liệu lệnh.

Theo mặc định, nghĩa là khi byte mã hóa dữ liệu không có sẵn (xem 11.2.1), hoạt động 1) phải áp dụng trong EF đó.

Nếu bản ghi được tham chiếu bằng P1 và P2 nằm trong bản ghi LCS DEACTIVATED, lệnh được xử lý với cảnh báo '6287' mà không thay đổi nội dung bản ghi.

Khi sử dụng định địa chỉ bản ghi hiện hành, lệnh phải thiết lập con trỏ bản ghi trên bản ghi được viết thành công.

Nếu được áp dụng với EF hỗ trợ cấu trúc tuần hoàn có bản ghi có kích cỡ cố định, lựa chọn "trước" (bit 3, 2 và 1 của P2 được đặt là 011) hoạt động là APPEND RECORD.

Bảng 72 - Cặp lệnh-hồi đáp WRITE RECORD

CLA	Như được xác định trong 5.4.1
INS	'D2'
P1	Số bản ghi hoặc '00' tham chiếu bản ghi hiện hành
P2	Xem Bảng 73
Trường L_c	xuất hiện đối với mã hóa $N_c > 0$
Trường dữ liệu	Bản ghi được viết
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$
Trường dữ liệu	Xuất hiện
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '63CX' (xem 11.3.2), '6581', '6700', '6981', '6982', '6986', '6A81', '6A82', '6A83', '6A84', '6A85'

Bảng 73 - Mã hóa P2 trong lệnh WRITE RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	x	x	x	-	-	-	Định dạng EF ngắn theo Bảng 69
-	-	-	-	-	0	x	x	P1 được đặt là '00'
-	-	-	-	-	0	0	0	– Bản ghi đầu tiên
-	-	-	-	-	0	0	1	– Bản ghi cuối cùng
-	-	-	-	-	0	1	0	– Bản ghi tiếp theo
-	-	-	-	-	0	1	1	– Bản ghi trước
-	-	-	-	-	1	0	0	Số bản ghi trong P1
– Mọi giá trị khác là RFU								

Nếu bản ghi là đối tượng dữ liệu SIMPLE-TLV (xem 6.1), khi đó hình 9 mô tả trường dữ liệu lệnh

T_n (1 byte)	L_n (1 hay 3 byte)	Tất cả các byte của V_n

Hình 9 - trường dữ liệu APDU (một bản ghi hoàn chỉnh lồng trong đối tượng dữ liệu SIMPLE-TLV)

11.3.5 Lệnh UPDATE RECORD

Lệnh kích hoạt cập nhật bản ghi cụ thể với byte được cho trong trường dữ liệu lệnh. Khi sử dụng định địa chỉ bản ghi hiện hành, lệnh phải thiết lập con trỏ bản ghi trên bản ghi được cập nhật.

Nếu được áp dụng với EF hỗ trợ cấu trúc tuần hoàn hoặc tuyến tính có bản ghi có kích cỡ cố định, khi đó lệnh bị hủy nếu kích cỡ bản ghi sau khi cập nhật khác với kích cỡ của bản ghi đang có.

Nếu được áp dụng với EF hỗ trợ cấu trúc tuyến tính có bản ghi có kích cỡ thay đổi, khi đó lệnh có thể được thực hiện khi kích cỡ bản ghi sau khi cập nhật khác với kích cỡ của bản ghi đang có.

Nếu được áp dụng với EF hỗ trợ cấu trúc tuần hoàn có bản ghi có kích cỡ cố định, lựa chọn "trước" (bit 3, 2 và 1 của P2 được đặt là 011) hoạt động là APPEND RECORD

Nếu bản ghi được tham chiếu bằng P1 và P2 trong bản ghi LCS DEACTIVATED, lệnh được xử lý với cảnh báo '6287' mà không thay đổi nội dung bản ghi.

Nếu INS = 'DC' và nếu bản ghi là đối tượng dữ liệu SIMPLE-TLV (xem 6.1), khi đó hình 9 mô tả trường dữ liệu lệnh.

Nếu INS = 'DD', khi đó lệnh cập nhật một phần bản ghi được tham chiếu bằng P1. Trường dữ liệu lệnh phải bao gồm DO'54' khoảng chừa trống để biểu thị byte đầu tiên được cập nhật trong bản ghi và DO'53' ('73' bị phản đối đối với việc sử dụng này) để bao gói dữ liệu cập nhật.

Bảng 74 - Cặp lệnh-hồi đáp UPDATE RECORD

CLA	Được xác định trong 5.4.1	
INS	'DC' hoặc 'DD'	
P1	Số bản ghi hoặc '00' tham chiếu bản ghi hiện hành	
P2	Xem Bảng 73 (INS = 'DC') hoặc Bảng 75 (INS = 'DD')	
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$	
Trường dữ liệu	INS = 'DC'	Dữ liệu cập nhật
	INS = 'DD'	DO khoảng chừa trống và Do tùy ý để bao gói dữ liệu cập nhật
Trường L_e	Xuất hiện đối với mã hóa $N_e = 0$	
Trường dữ liệu	Xuất hiện	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '63CX' (xem 11.3.2), '6581', '6700', '6981', '6982', '6986', '6A81', '6A82', '6A83', '6A84', '6A85'	

Bảng 75 - Mã hóa của P2 trong lệnh UPDATE RECORD có INS = 'DD'

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	x	x	x	-	-	-	Định dạng EF ngắn theo Bảng 69
-	-	-	-	-	1	x	x	Số bản ghi trong P1
-	-	-	-	-	1	0	0	– Thay thế
-	-	-	-	-	1	0	1	– Lô-gic AND
-	-	-	-	-	1	1	0	– Lô-gic OR
-	-	-	-	-	1	1	1	– Lô-gic XOR
– Mọi giá trị khác là RFU								

11.3.6 Lệnh APPEND RECORD

Lệnh kích hoạt hoặc viết bản ghi mới tại cuối của cấu trúc tuyến tính, hoặc tại đầu của cấu trúc tuần hoàn. Khi sử dụng định địa chỉ bản ghi hiện hành, lệnh phải thiết lập con trỏ bản ghi trên bản ghi được thêm vào thành công.

Nếu lệnh áp dụng với cấu trúc tuyến tính đủ các bản ghi, khi đó lệnh bị hủy do không có đủ không gian bộ nhớ trong tệp.

Nếu lệnh áp dụng với cấu trúc tuần hoàn đủ các bản ghi, khi đó bản ghi có số bản ghi cao nhất bị xóa. Tất cả các số bản ghi khác được tăng theo một. Bản ghi thêm vào trở thành bản ghi số một. Nếu bản ghi có số bản ghi cao nhất nằm trong bản ghi LCS DEACTIVATED lệnh được xử lý với cảnh báo '6287' mà không thay đổi bất kỳ nội dung bản ghi hoặc số bản ghi.

Nếu các bản ghi trong EF có vòng đời bản ghi, LCS của bản ghi thêm vào được đặt là ACTIVATED trừ khi có quy định khác.

Nếu bản ghi là đối tượng dữ liệu SIMPLE-TLV (xem 6.1), khi đó hình 9 mô tả trường dữ liệu lệnh.

Bảng 76 - Cặp lệnh-hồi đáp APPEND RECORD

CLA	Như được xác định trong 5.4.1
INS	'E2'
P1	'00' (mọi giá trị khác đều không có hiệu lực)
P2	Xem Bảng 73 với bit 3 đến 1 được đặt là 000 (mọi giá trị khác là RFU)
Trường L_c	xuất hiện đối với mã hóa $N_c > 0$
Trường dữ liệu	Bản ghi được thêm vào
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$
Trường dữ liệu	Xuất hiện
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '63CX' (xem 11.3.2), '6287', '6581', '6700', '6981', '6982', '6986', '6A81', '6A82', '6A83', '6A84', '6A85'

11.3.7 Lệnh SEARCH RECORD

Lệnh kích hoạt tìm kiếm đơn giản hoặc nâng cao hoặc độc quyền trên các bản ghi được lưu giữ trong EF. Tìm kiếm có thể bị giới hạn đối với các bản ghi có định danh được cho hoặc đối với các bản ghi có số lớn hơn hoặc nhỏ hơn một số đã cho. Nó có thể được thực hiện trong trật tự tăng hoặc giảm của số bản ghi. Tìm kiếm bắt đầu hoặc từ byte đầu tiên của bản ghi (tìm kiếm đơn giản), hoặc từ khoảng chừa trống đã cho trong bản ghi (tìm kiếm nâng cao), hoặc từ số lần đầu tiên của byte được cho trong bản ghi (tìm kiếm nâng cao). Trường dữ liệu hồi đáp mang lại số bản ghi phù hợp với tiêu chí tìm kiếm trong bản ghi hỗ trợ EF. Lệnh phải thiết lập con trỏ bản ghi trên bản ghi đầu tiên phù hợp với tiêu chí tìm kiếm.

Trong một bản ghi hỗ trợ EF có kích cỡ thay đổi với cấu trúc tuyến tính, tìm kiếm phải không tính đến các bản ghi ngắn hơn cuối tìm kiếm. Trong bản ghi hỗ trợ EF có kích cỡ cố định với cấu trúc tuyến tính hoặc tuần hoàn, nếu chuỗi tìm kiếm dài hơn bản ghi, khi đó thẻ phải hủy lệnh.

Các bản ghi có LCS bản ghi được đặt là DEACTIVATED phải bị bỏ qua trong quá trình tìm kiếm.

Bảng 77 - Cặp lệnh-hồi đáp SEARCH RECORD

CLA	Như được xác định trong 5.4.1	
INS	'A2'	
P1	Số bản ghi hoặc định danh bản ghi ('00' tham chiếu bản ghi hiện hành)	
P2	Xem Bảng 78	
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$	
Trường dữ liệu	Bit 3 và 2 của P2 không được đặt là 11, tìm kiếm đơn giản	Chuỗi tìm kiếm
	Bit 3 và 2 và 1 của P2 được đặt là 110, tìm kiếm nâng cao	Chỉ báo tìm kiếm (2 byte, xem Bảng 79) theo sau bởi chuỗi tìm kiếm
	Bit 3 và 2 và 1 của P2 được đặt là 111, tìm kiếm độc quyền	Độc quyền
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$, xuất hiện đối với mã hóa $N_e > 0$	
Trường dữ liệu	Xuất hiện hoặc số bản ghi	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6282', '6982'	
– Trường dữ liệu hồi đáp xuất hiện hoặc do trường L_e xuất hiện, hoặc do không tìm thấy sự tương thích – Trường dữ liệu hồi đáp không mang lại định danh bản ghi do chúng có thể không phải là độc nhất.		

Trong tìm kiếm nâng cao (bit 3, 2 và 1 của P2 được đặt là 110), trường dữ liệu lệnh bao gồm một chỉ báo tìm kiếm trên 2 byte theo sau bởi chuỗi tìm kiếm. Bảng 79 xác định Byte chỉ dẫn tìm kiếm đầu tiên. Theo byte đầu tiên của chỉ báo tìm kiếm, byte thứ hai hoặc là khoảng chừa trống hoặc là một giá trị, nghĩa là tìm kiếm trong bản ghi phải bắt đầu hoặc từ khoảng chừa trống này (xem 11.3.2) hoặc sau số lần đầu tiên của giá trị này.

Bảng 78 - Mã hóa của P2 trong lệnh SEARCH RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	x	x	x	-	-	-	Định danh EF ngắn theo Bảng 69
-	-	-	-	-	0	x	x	Tìm kiếm đơn giản bằng định danh bản ghi trong P1
-	-	-	-	-	0	0	0	– Chuyển tiếp từ số lần đầu tiên
-	-	-	-	-	0	0	1	– Phục hồi từ số lần cuối cùng
-	-	-	-	-	0	1	0	– Chuyển tiếp từ số lần tiếp theo
-	-	-	-	-	0	1	1	– Phục hồi từ số lần trước
-	-	-	-	-	1	0	x	Tìm kiếm đơn giản bằng số bản ghi trong P1
-	-	-	-	-	1	0	0	– Chuyển tiếp từ P1
-	-	-	-	-	1	0	1	– Phục hồi từ P1
-	-	-	-	-	1	1	0	Tìm kiếm nâng cao
-	-	-	-	-	1	1	1	Tìm kiếm độc quyền

Bảng 79 - Mã hóa của byte đầu tiên của chỉ báo tìm kiếm

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	0	0	0	0	-	-	-	Byte tiếp theo là một khoảng chừa trống (bắt đầu từ vị trí đó)
0	0	0	0	1	-	-	-	Byte tiếp theo là một giá trị (bắt đầu sau số lần đầu tiên)
-	-	-	-	-	0	x	x	Định danh bản ghi trong P1
-	-	-	-	-	0	0	0	– Chuyển tiếp từ số lần đầu tiên
-	-	-	-	-	0	0	1	– Phục hồi từ số lần cuối cùng
-	-	-	-	-	0	1	0	– Chuyển tiếp từ số lần tiếp theo
-	-	-	-	-	0	1	1	– Phục hồi từ số lần trước
-	-	-	-	-	1	x	x	Số bản ghi trong P1
-	-	-	-	-	1	0	0	– Chuyển tiếp từ P1
-	-	-	-	-	1	0	1	– Phục hồi từ P1
-	-	-	-	-	1	1	0	– Chuyển tiếp từ bản ghi tiếp theo
-	-	-	-	-	1	1	1	– Phục hồi từ bản ghi trước
– Mọi giá trị khác là RFU								

11.3.8 Lệnh ERASE RECORD

Lệnh thiết lập một hoặc nhiều bản ghi của một EF đến trạng thái xóa bỏ lô-gic, hoặc bản ghi được tham chiếu bằng P1, hoặc chuỗi bản ghi từ P1, liên tục, cho đến cuối tệp. Bản ghi bị xóa không được bỏ đi, và vẫn có thể truy cập được bằng lệnh WRITE RECORD và UPDATE RECORD.

Nếu bất kỳ bản ghi nào được tham chiếu bằng P1 và P2 nằm trong bản ghi LCS DEACTIVATED, lệnh được xử lý với cảnh báo '6287' mà không thay đổi bất kỳ nội dung bản ghi nào.

Bảng 80 - Cặp lệnh-hồi đáp ERASE RECORD

CLA	Như được xác định trong 5.4.1
INS	'0C'
P1	Số bản ghi
P2	Xem Bảng 81
Trường L_c	Xuất hiện đối với mã hóa $N_c = 0$
Trường dữ liệu	Xuất hiện
Trường L_e	Xuất hiện đối với mã hóa $N_e = 0$
Trường dữ liệu	Xuất hiện
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6287', '63CX' (xem 11.3.2), '6581', '6700', '6981', '6982', '6986', '6A81', '6A82', '6A83', '6A84', '6A85'

Bảng 81- Mã hóa của P2 trong lệnh ERASE RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	x	x	x	-	-	-	Định danh EF ngắn theo Bảng 69
-	-	-	-	-	1	x	x	Số bản ghi trong P1
-	-	-	-	-	1	0	0	– Xóa bản ghi P1
-	-	-	-	-	1	0	1	– Xóa tất cả các bản ghi từ P1 cho đến bản cuối cùng
– Mọi giá trị khác là RFU								

11.3.9 Lệnh ACTIVATE RECORD

Lệnh thiết lập bản ghi được tham chiếu bằng P1 và P2 với bản ghi LCS ACTIVATED. Lệnh không ảnh hưởng đến con trỏ bản ghi.

Nếu EF được tham chiếu bằng P2 không hỗ trợ vòng đời bản ghi, lệnh phải bị hủy với byte trạng thái '6981'.

Nếu một bản ghi được xử lý đã được kích hoạt, lệnh phải phục hồi byte trạng thái '9000'.

Đối với việc kích hoạt tất cả các bản ghi trong bản ghi LCS DEACTIVATED, lệnh ACTIVATE FILE có thể được sử dụng. Không phụ thuộc vào sửa đổi của LCS tệp xuất hiện tùy chọn (xem 7.4.10) tất cả các bản ghi phải được kích hoạt.

Bảng 82 - Cặp lệnh-hồi đáp ACTIVATE RECORD

CLA	Như được xác định trong 5.4.1
INS	'08'
P1	Số bản ghi
P2	Xem Bảng 83
Trường L_c	Không xuất hiện
Trường dữ liệu	Không xuất hiện
Trường L_e	Không xuất hiện
Trường dữ liệu	Không xuất hiện
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6981', '6982', '6986', '6A82', '6A83'

Bảng 83 - Mã hóa của P2 trong lệnh ACTIVATE RECORD hoặc DEACTIVATE RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	x	x	x	-	-	-	Định danh EF ngắn theo Bảng 69
-	-	-	-	-	1	x	x	Số bản ghi trong P1
-	-	-	-	-	1	0	0	– Kích hoạt hoặc giải hoạt bản ghi P1
-	-	-	-	-	1	0	1	– Kích hoạt hoặc giải hoạt tất cả các bản ghi từ P1 cho đến bản cuối cùng
– Mọi giá trị khác là RFU								

11.3.10 Lệnh DEACTIVATE RECORD

Lệnh thiết lập bản ghi được tham chiếu bằng P1 và P2 với bản ghi LCS DEACTIVATED. Lệnh không ảnh hưởng đến con trỏ bản ghi.

Nếu EF được tham chiếu bằng P2 không hỗ trợ vòng đời bản ghi, lệnh phải bị hủy với byte trạng thái '6981'.

Nếu một bản ghi được xử lý đã được kích hoạt, lệnh phải phục hồi byte trạng thái '9000'.

Bảng 84 - Cặp lệnh-hồi đáp DEACTIVATE RECORD

CLA	Như được xác định trong 5.4.1
INS	'06'
P1	Số bản ghi
P2	Xem Bảng 83
Trường L_c	Không xuất hiện
Trường dữ liệu	Không xuất hiện
Trường L_e	Không xuất hiện
Trường dữ liệu	Không xuất hiện
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6981', '6982', '6986', '6A82', '6A83'

11.3.11 Hàm COMPARE RECORD

Hàm này được hỗ trợ bằng lệnh COMPARE (xem 11.6.1).

11.4 Xử lý đối tượng dữ liệu

11.4.1 Tổng quát

Trong nhóm lệnh này, SW1-SW2 được đặt là '63CX' biểu thị sự thay đổi thành công trạng thái bộ nhớ, nhưng sau đoạn chương trình thử lại bên trong; 'X' > '0' mã hóa số lần thử lại; 'X' = '0' có nghĩa là bộ đếm không được cung cấp.

11.4.1.1 Mã hóa của P1-P2 đối với mã INS chẵn

Bảng 85 - Mã hóa của P1-P2 xử lý đối tượng dữ liệu có mã INS chẵn

Giá trị của P1-P2	Ý nghĩa
'0000'	Kết xuất tệp (xem 12.4)
	Phục hồi truy vấn thẻ có nguồn gốc từ một thẻ hoặc gửi phản hồi đến thẻ (xem 12.5)
'0001' đến '00FE'	Thẻ BER-TLV (một byte) trong P2
'00FF'	Hàm đặc biệt (xem Bảng 89, Bảng 91, Bảng 92 và Bảng 93)
'0100' đến '01FF'	Độc quyền
'0200'	RFU
'0201' đến '02FE'	Thẻ SIMPLE-TLV trong P2
'02FF'	Hàm đặc biệt (xem 11.4.1.1)
'1F1F' đến 'FFFF'	Thẻ BER-TLV (2 byte) trong P1-P2
– Thẻ BER-TLV không hiệu lực trong dãy '01' đến 'FE' và '1F1F' đến 'FFFF' là RFU – Mọi giá trị khác là RFU	

Nếu P1 được đặt là '00', khi đó P2 từ '01' đến 'FE' phải là thẻ BER-TLV trên byte đơn.

Nếu P1 được đặt là '01', khi đó P2 từ '00' đến 'FF' phải là định danh đối với kiểm tra bên trong thẻ và đối với dịch vụ độc quyền có ý nghĩa trong ứng dụng được cho.

Nếu P1 được đặt là '02', khi đó P2 từ '01' đến 'FE' phải là thẻ SIMPLE-TLV. Giá trị '0200' là RFU. Giá trị '02FF' được sử dụng hoặc để đạt được tất cả các đối tượng dữ liệu SIMPLE-TLV thông thường có thể đọc được trong ngữ cảnh hoặc để biểu thị rằng trường dữ liệu lệnh được mã hóa trong SIMPLE-TLV.

Nếu P1-P2 nằm từ '1F1F' đến 'FFFF', khi đó chúng chỉ mã hóa thẻ BER-TLV có hiệu lực trên 2 byte.

Chú thích Nhiều giá trị trong dãy 1F1F' đến 'FFFF' là các thẻ BER-TLV có hiệu lực (xem phụ lục E).

11.4.1.2 Mã hóa của P1-P2 đối với mã INS lẻ

Nếu bit b1 của INS được đặt là 1, khi đó, ngoại trừ lệnh SELECT DATA, P1-P2 không được đặt là '0000' hoặc 'FFFF' phải định danh tệp:

- Nếu mười một bit đầu tiên của P1-P2 được đặt là 0 và nếu bit b5 đến b1 của P2 không phải tất cả bằng nhau và nếu thẻ và/hoặc tệp hỗ trợ lựa chọn theo định danh EF ngắn, khi đó bit b5 đến b1 của P2 mã hóa định danh EF ngắn (một số từ 1 đến ba mươi). Mặt khác, P1-P2 là định danh tệp 2 byte.
- P1-P2 được đặt là '3FFF' định danh DF hiện hành.

P1-P2 được đặt là '0000' định danh EF hiện hành, trừ khi trường dữ liệu lệnh cung cấp DO'51' tham chiếu tệp để định danh một tệp.

P1-P2 được đặt là 'FFFF' định danh khuôn mẫu hiện hành, trừ khi trường dữ liệu lệnh cung cấp tham chiếu của khuôn mẫu khác (xem đối số 1, 2 và 3 trong Bảng 86).

11.4.1.3 Trường dữ liệu

Nếu bit b1 của INS được đặt là 0, nếu DO được yêu cầu hoặc được cung cấp trong khuôn mẫu hiện hành, khi đó dữ liệu phải bao gồm trường giá trị của đối tượng dữ liệu, nghĩa là hoặc phần tử dữ liệu được tham chiếu trong trường hợp đối tượng dữ liệu SIMPLE-TLV hoặc đối tượng dữ liệu BER-TLV ban đầu, hoặc khuôn mẫu được tham chiếu trong trường hợp DO được xây dựng.

Không kể bit b1 trong INS, nếu một tập hợp các DO được cung cấp hoặc nếu nội dung của EF được yêu cầu, khi đó trường dữ liệu thích hợp phải bao gồm DO.

11.4.1.4 Truy cập phần mở rộng của khuôn mẫu hiện hành

Khi khuôn mẫu được mở rộng bằng trình bao được gắn thẻ (xem 8.4.8), phần mở rộng này chỉ có hiệu lực đối với lệnh GET DATA và GET NEXT DATA. Tất cả các lệnh khác xử lý DO bằng thẻ của chúng chỉ bị giới hạn đến khuôn mẫu cơ sở. Giải tự động của trình bao được gắn thẻ (xem 8.4.8) không làm biến đổi khuôn mẫu hiện hành.

Nếu khuôn mẫu bao gồm một hoặc một số trình bao, 8.4.8 mô tả cách phục hồi DO được mong đợi có liên quan với khuôn mẫu.

11.4.1.5 Các điều kiện phản đối hoặc thực hiện

Bất kỳ lệnh nào của nhóm này phải bị hủy nếu thông số lựa chọn DO được truy cập không tương thích với cấu trúc thực tế trong thẻ, ví dụ:

- Nếu được áp dụng với một cấu trúc (DF hoặc EF) không hỗ trợ đối tượng dữ liệu
- Nếu thông số không tương thích với cấu trúc đối tượng dữ liệu thực tế

Nó có thể được thực hiện chỉ khi trạng thái an toàn thỏa mãn điều kiện an toàn được xác định bằng ứng dụng trong ngữ cảnh đối với hàm.

11.4.2 Lệnh SELECT DATA

11.4.2.1 Tổng quát

Miễn là 0 làm biến đổi LCS của DO, lệnh SELECT DATA luôn được đưa ra.

Hàm của lệnh này là

- Để thiết lập DO lựa chọn đơn nhất, nghĩa là mục tiêu của lệnh, là DO hiện hành;
- Để thiết lập khuôn mẫu hiện hành làm trường giá trị của DO được lựa chọn nếu DO này được cấu trúc;
- Để thiết lập dữ liệu tham chiếu được so sánh, ví dụ với dữ liệu so sánh bằng lệnh COMPARE tiếp theo (xem 11.6.1);
- Để sửa đổi VA (xem 7.2.1) nếu DO được lựa chọn không thuộc VA hiện hành của khuôn mẫu hiện hành. Nếu lệnh truyền
- DO'4F' định danh ứng dụng, và DO'51' không tham chiếu tệp, nó lựa chọn DF ứng dụng (xem 7.2.2 quy tắc d)).
- Không phải DO'4F', mà là DO'51', nó lựa chọn một tệp (xem 7.2.2 quy tắc e) hoặc f)).
- DO'4F' và DO'51', nó lựa chọn DF ứng dụng (xem 7.2.2 quy tắc d)), và một tệp (xem 7.2.2 quy tắc e) hoặc f)).
- Số bản ghi (xem đối số 3 trong Bảng 86) nó sửa đổi curRecord (xem 7.2.2 quy tắc g)
- Khoảng chừa trống (xem đối số 3 trong Bảng 86) nó sửa đổi curDataString (xem 7.2.2 quy tắc h)

Bảng 86 - Giá trị của DO'60' tham chiếu chung (khuôn mẫu tham chiếu chung)

Arg	DO được lồng		Chú giải	
1	DO'4F' định danh ứng dụng		Tùy chọn	
2	DO'51' tham chiếu tệp (xem Bảng 7)		Tùy chọn, số byte chẵn. Có hiệu lực nếu đường dẫn tương thích với cấu trúc tệp của ứng dụng hiện hành, hoặc của ứng dụng được tham chiếu bằng DO'4F'	
3	Lựa chọn giữa	DO'02' số bản ghi theo sau bởi độ dài DO'02'	Tùy chọn. Tham chiếu một bản ghi hoặc DO'7F70' ảo giá trị của nó là bản ghi trong một EF	
		DO'54' khoảng chừa trống theo sau bởi độ dài DO'02'	Tùy chọn. Tham chiếu một chuỗi dữ liệu hoặc DO'7F70' ảo giá trị của nó là chuỗi dữ liệu trong một EF trong suốt	
4	Lựa chọn giữa	DO'5C' danh sách thẻ	Lồng một thẻ xuất hiện trong khuôn mẫu hiện hành	Đối số 4, bắt buộc trong DO tham chiếu. Áp dụng với khuôn mẫu hiện hành hoặc khuôn mẫu hiện hành tạm thời được thiết lập bởi đối số trước
		DO'4D' tiêu đề mở rộng hoặc '5F61' (xem 8.4.5 đối với tính hợp lý của lựa chọn)	Giá trị của tiêu đề mở rộng bắt đầu với thẻ xuất hiện trong khuôn mẫu hiện hành	
		DO'5F8400 thẻ che	Tham chiếu một DO bằng một phần thẻ	
		DO'7F71' bộ lọc	Tham chiếu một DO được xây dựng bằng nội dung của nó	
5	Số tùy ý của DO'5F8400 thẻ che và/hoặc DO'7F71' bộ lọc trong bất kỳ thứ tự nào; kết quả của áp dụng tất cả mạng che và tất cả bộ lọc là giao cắt của tất cả các tập hợp con đó		DO'5F8400' tham chiếu một DO bằng một phần thẻ; DO'7F71' tham chiếu DO được xây dựng bằng nội dung của nó	Tùy chọn nếu DO được tham chiếu bằng đối số 4 được cấu trúc

Bảng 87 - Cặp lệnh-hồi đáp SELECT DATA

CLA	Như được xác định trong 5.4.1	
INS	'A5'	
P1	< 'F0'	Số lần xuất hiện của phiên bản
	'F0'	Lựa chọn cha của DO được them chiếu bằng DO curConstructed
	> 'F0'	RFU
P2	Xem Bảng 88	
Trường L_c	Không xuất hiện đối với mã hóa $N_c > 0$, xuất hiện đối với mã hóa $N_c > 0$	
Trường dữ liệu	Có thể trống nếu P1 = 'F0'. Trong các trường hợp khác, ít nhất số đối 4 của DO'60' tham chiếu chung (xem Bảng 86). Các số đối khác tùy chọn. Tất cả các số đối phải theo cùng trật tự như trong khuôn mẫu tham chiếu chung.	
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$, xuất hiện đối với mã hóa $N_e > 0$ nếu dữ liệu hồi đáp được yêu cầu bởi P2 (xem Bảng 88)	
Trường dữ liệu	Không xuất hiện hoặc thông tin theo P2	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6202' đến '6280', '6281', '6700', '6981', '6982', '6985', '6A81', '6A88' (DO không tìm thấy, nghĩa là dữ liệu được tham chiếu không tìm thấy	

Bảng 88 - Mã hóa của P2 trong lệnh SELECT DATA

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	0	0	-	-	-	x	x	Số lần DO hoặc tệp trong khuôn mẫu hiện hành
0	0	0	-	-	-	0	0	– Số lần đầu tiên hoặc duy nhất của một DO sau khi bỏ qua số lần P1
0	0	0	-	-	-	0	1	– Số lần cuối cùng của một DO sau khi bỏ qua số lần P1
0	0	0	-	-	-	1	0	– Số lần tiếp theo của một DO sau khi bỏ qua số lần P1
0	0	0	-	-	-	1	1	– Số lần trước đó của một DO sau khi bỏ qua số lần P1
0	0	0	x	x	x	-	-	Các yêu cầu trường dữ liệu hồi đáp (xem 7.4.2 và Bảng 8)
0	0	0	0	0	1	-	-	Phục hồi thông tin điều khiển dữ liệu (DO'62')
0	0	0	0	1	0	-	-	Phục hồi danh sách thẻ của khuôn mẫu hiện hành (DO'5C') (hàm DIR)
0	0	0	1	0	0	-	-	Phục hồi danh sách thẻ của khuôn mẫu hiện hành (DO'5C') (hàm VIEW)
0	0	0	1	1	0	-	-	Phục hồi danh sách thẻ của khuôn mẫu hiện hành (DO'5C') (hàm DIR) theo sau bởi danh sách thẻ của khuôn mẫu hiện hành (DO'5C') (hàm VIEW)
– Mọi giá trị khác là RFU								

Ngoại trừ khi P1 được đặt là 'F0', xử lý lệnh này bao gồm một chuỗi các tìm kiếm tương thích trong khuôn mẫu hiện hành tạm thời. Tìm kiếm tương thích cuối cùng phải xảy ra:

- Trong DO được xây dựng hiện hành tạm thời cuối cùng (hệ cao nhất) được xác định bằng đối số, khi thẻ cuối cùng tham chiếu một DO được xây dựng bằng lựa chọn "next" hoặc "previous". Nếu sự tương thích được tìm thấy, DO được lựa chọn là anh em của DO được xây dựng tạm thời cuối cùng;

Trong ví dụ sau, "khuôn mẫu hiện hành tạm thời" biểu thị trường giá trị của DO được xây dựng hiện hành tạm thời mà trong đó sự tương thích cuối cùng diễn ra:

P1-P2='0000' lựa chọn số lần đầu tiên của DO trong khuôn mẫu hiện hành tạm thời.

P1-P2='0100' lựa chọn số lần thứ hai của DO trong khuôn mẫu hiện hành tạm thời.

P1-P2='0101' lựa chọn số lần gần cuối của DO trong khuôn mẫu hiện hành tạm thời.

P1-P2='0001' lựa chọn số lần cuối cùng của DO trong khuôn mẫu hiện hành tạm thời.

P1-P2='0102' lựa chọn hoặc số lần tiếp theo thứ hai của DO ban đầu trong khuôn mẫu hiện hành tạm thời hoặc anh em tiếp theo thứ hai của DO được xây dựng hiện hành.

C-RP SELECT DATA bị hỏng (SW1>'62', xem Bảng 6) không làm biến đổi VA hiện hành.

11.4.2.2 Định nghĩa mục tiêu cơ bản

Định nghĩa mục tiêu cơ bản sử dụng đối số 1, 2 và 4. Nếu mục tiêu, nghĩa là DO được lựa chọn:

- Không được bao gồm trong ứng dụng hiện hành, trường dữ liệu phải bao gồm một DO'4F' định danh ứng dụng,
- Không được bao gồm trong tệp hiện hành sau khi lựa chọn ứng dụng tạm thời có khả năng, trường dữ liệu phải bao gồm một DO'51' tham chiếu tệp khi tham chiếu tệp áp dụng trong ứng dụng.

Thẻ mục tiêu phải là:

- Hoặc được bao gói trong DO'5C' danh sách thẻ
- Hoặc được xác định bằng DO'4D' hoặc '5F61' danh sách tiêu đề mở rộng (xem 8.4.5 về lý do chọn lựa)
- Hoặc được xác định bằng DO'5F8400' thẻ được che
- Hoặc được xác định bằng nội dung của DO được xây dựng theo DO'7F71' bộ lọc

Đối số điều kiện 3 tham chiếu DO'7F70' ảo giá trị của nó hoặc là bản ghi trong EF được cấu trúc trong các bản ghi, hoặc chuỗi dữ liệu trong EF trong suốt. DO'7F70' hiện hành tạm thời phải trở thành DO được xây dựng hiện hành nếu đối số bắt buộc không tham chiếu DO được xây dựng.

11.4.2.3 Tham chiếu bằng DO thẻ được che và DO bộ lọc

Nếu lệnh tham chiếu một DO được xây dựng, thiết lập một khuôn mẫu hiện hành, đối số điều kiện 5, DO'5F8400' thẻ được che hoặc DO'7F71 bộ lọc có thể xuất hiện.

Nếu DO'5F8400' thẻ được che xuất hiện, lệnh phải hồi phục DO'5C' danh sách thẻ lồng vào kết nối của tất cả các thẻ của khuôn mẫu tương thích thẻ được che. Thẻ được che lồng hai phần tử dữ liệu có cùng độ dài, nghĩa là <mask value> theo sau bởi <target tag>. Sự tương thích với thẻ <matching tag> xảy ra khi:

<mask value> AND <matching tag> = <mask value> AND <target tag>

Nếu DO'7F71' bộ lọc xuất hiện, lệnh phải thành công nếu và chỉ khi giá trị của DO'7F71' bộ lọc:

- Hoặc là DO được xây dựng thuộc về khuôn mẫu hiện hành tạm thời; DO này trở thành hiện hành

- Hoặc là cây con (xem 8.2.3) của DO được xây dựng thuộc về khuôn mẫu hiện hành tạm thời; DO này trở thành hiện hành

11.4.2.4 Hàm GET DATA CONTROL PARAMETERS

Khi được yêu cầu bằng bit 3 được đặt là 1 trong P2, dữ liệu hồi đáp là DO'62' (xem Bảng 10) liên quan đến DO hiện hành (tạm thời hoặc cuối cùng), sau khả năng đổi của LCS dữ liệu. Nếu DO'62' không có sẵn, CP DO có thể xuất hiện dưới thẻ được lưu trữ cho quyền phân phối thẻ (xem 8.3.4).

11.4.2.5 Hàm DIR

Khi được yêu cầu bằng bit b4 được đặt là 1 trong P2, lệnh phải hồi phục DO'5C' danh sách thẻ lồng vào kết nối của tất cả các thẻ của khuôn mẫu hiện hành (có thể bao gồm mở rộng khuôn mẫu) được thiết lập theo lệnh.

Một DO danh sách thẻ thực tế có thể hoặc xuất hiện trong khuôn mẫu, hoặc được phát sinh do hệ thống xử lý. Trong cả hai trường hợp,

- Thẻ phải xuất hiện không kể thuộc tính an toàn hoặc giá trị của LCS dữ liệu của DO tương ứng
- Nếu một số phiên bản của cùng DO xuất hiện, thẻ phải được lặp lại
- Nếu xuất hiện, DO trình bao phải luôn xuất hiện.

Nếu hệ thống xử lý giải vô hướng, thẻ địa phương của các DO được xác định trong trình bao có thể xuất hiện trong danh sách thẻ (thể hiện khuôn mẫu mở rộng). Nếu không, chúng phải không xuất hiện (danh sách thẻ biểu thị khuôn mẫu cơ sở).

11.4.2.6 Hàm VIEW

Khi được yêu cầu bằng bit b5 được đặt là 1 trong P2, lệnh phải hồi phục DO'5C' danh sách thẻ lồng vào cùng kết nối của tất cả các thẻ như trong hàm DIR, nhưng theo nhu cầu của nó, ứng dụng có thể không bao gồm các thẻ như:

- Các DO không thể đọc được dưới trạng thái an toàn hiện hành
- Các DO không trong trạng thái được kích hoạt
- Trình bao được gắn thẻ khi giải tự động được ban hành (xem 8.4.8 và 11.4.2.6).

11.4.2.7 Hàm liên quan đến tệp

Khi đối số 4 không xuất hiện trong trường dữ liệu lệnh, và đối số 3 xuất hiện, lệnh SELECT DATA thành công phải

- Thiết lập curRecord trong trường hợp đối số 3 bao gồm số bản ghi, hoặc
- Thiết nối chuỗi dữ liệu được tham chiếu bằng đối số 3 làm curDataString trong trường hợp đối số 3 bao gồm DO khoảng chừa trống.

Khi đối số 3 và 4 xuất hiện trong trường dữ liệu lệnh, đối số 1 và 2 hỗ trợ lựa chọn ứng dụng, của một tệp trong ứng dụng hiện hành, hoặc tệp trong ứng dụng được cho.

11.4.3 Lệnh GET DATA/GET NEXT DATA - mã INS chẵn

Bảng 89 - Cặp lệnh-hồi đáp GET DATA/GET NEXT DATA (mã INS chẵn)

CLA	Như được xác định trong 5.4.1	
INS	'CA'	GET DATA
	'CC'	GET NEXT DATA
P1-P2	Xem Bảng 85, nếu giá trị đặc biệt '00FF' được sử dụng, lệnh đạt được tất cả các DO từ khuôn mẫu hiện hành	
Trường L_c	Không xuất hiện đối với mã hóa $N_c = 0$	
Trường dữ liệu	Không xuất hiện	
Trường L_e	Xuất hiện đối với mã hóa $N_c > 0$	
Trường dữ liệu	0, 1 hoặc nhiều hơn nữa byte dữ liệu theo P1-P2	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6202' đến '6280', '6281', '6700', '6981', '6982', '6985', '6A81', '6A88' (đối tượng dữ liệu không tìm thấy, nghĩa là dữ liệu được tham chiếu không tìm thấy)	

11.4.3.1 Tổng quát

Hàm chính của các lệnh này có mã INS chẵn là sự phục hồi của trường giá trị của DO thuộc khuôn mẫu hiện hành. Nó có thể là nội dung của DO hỗ trợ EF.

Nếu có một số lần xuất hiện của thẻ trong khuôn mẫu hiện hành, phần này không xác định DO nào được hồi phục bằng lệnh GET DATA thành công do phụ thuộc vào định nghĩa hoặc bản chất hoặc nội dung của DO. GET NEXT DATA có hoạt động chính xác (xem 11.4.3.4).

DO được yêu cầu hoặc phần tử dữ liệu phải không xuất hiện từ hồi đáp khi trạng thái an toàn không tương thích với thuộc tính an toàn của nó.

11.4.3.2 Hàm SELECT

Sau lệnh GET DATA thành công của DO được xây dựng, DO này trở thành DO được xây dựng hiện hành.

Lệnh GET NEXT DATA thành công phải không tác động đến DO hiện hành và khuôn mẫu hiện hành.

11.4.3.3 Hàm GET DATA CONTROL PARAMETERS

Khi đối số GET DATA/GET NEXT DATA INS chẵn là thẻ '62' khuôn mẫu CP, dữ liệu hồi đáp là kết nối của các CP DO (xem Bảng 10) được gắn với các DO trong cùng khuôn mẫu. Nếu DO'62' không có sẵn, CP DO có thể xuất hiện dưới thẻ được lưu trữ đối với quyền phân phối thẻ (xem 8.4.4).

11.4.3.4 Hàm cụ thể của GET NEXT DATA và xử lý con trỏ

Khi có một số lần xuất hiện của cùng thẻ trong khuôn mẫu, lệnh GET NEXT DATA kế tiếp phải lần lượt phục hồi giá trị của chúng. Thứ tự các giá trị được phục hồi phải giống như thứ tự của các thẻ được phục hồi bằng hàm DIR hoặc VIEW (xem 11.4.2.5 hoặc 11.4.2.6).

Trái với lệnh GET DATA, lệnh GET NEXT DATA thành công phải không tác động đến VA. Việc xử lý nhiều phiên bản có nghĩa là

- Khuôn mẫu được nhìn nhận là danh sách theo thứ tự của các DO tại giao diện giữa thẻ và thiết bị giao diện. Thuật ngữ "danh sách theo thứ tự" có nghĩa là danh sách này có phần tử đầu tiên và cuối cùng. Mỗi phần tử trong danh sách, ngoại trừ phần tử cuối cùng, có phần tử tiếp theo. Mỗi phần tử trong danh sách, ngoại trừ phần tử đầu tiên, có phần tử trước đó.
- Con trỏ được gắn với kênh lô-gic. Giá trị mặc định của con trỏ này là chưa được thiết lập. Con trỏ được thiết lập bằng lệnh GET NEXT DATA, PUT DATA, PUT NEXT DATA hoặc UPDATE DATA (xem 11.4.6, 11.4.7 và 11.4.8). Con trỏ này phải không được thiết lập nếu bất kỳ lệnh nào từ GET NEXT DATA hoặc PUT NEXT DATA được truyền trên cùng kênh lô-gic. Việc truyền lệnh trên kênh lô-gic không tác động đến con trỏ trên kênh lô-gic khác.

Khi một chuỗi các DO hỗ trợ quản lý tuần hoàn, lệnh GET DATA hoặc GET NEXT DATA phải đầu tiên hồi phục phiên bản gần nhất. Lệnh GET NEXT DATA tiếp phải hồi phục phiên bản gần nhất còn lại, vv...

Khi tất cả các phần tử dữ liệu hoặc DO đã được truyền bằng thẻ trong hồi đáp GET NEXT DATA kế tiếp, lệnh GET NEXT DATA tiếp theo phải bị phản đối bởi SW1-SW2 = '6A88'.

11.4.4 Lệnh GET DATA/GET NEXT DATA - mã INS lẻ

11.4.4.1 Tổng quát

Hàm chính của các lệnh này có mã INS lẻ là sự phục hồi của trường giá trị của một hoặc một vài DO theo các đối số của lệnh. Lựa chọn mục tiêu rất gần với lựa chọn SELECT DATA, ngoại trừ:

- Lệnh có thể phục hồi một số DO trong khi lệnh SELECT DATA lựa chọn một DO.
- Đối số 2 của SELECT DATA có thể được thay thế bằng một định danh tệp trong P1-P2, hàm tương đương với DO tham chiếu tệp bao gồm một định danh tệp. Nếu lựa chọn này được sử dụng, trường dữ liệu lệnh phải không mô tả đặc điểm đối số 1 (DO'4F').

Khi lệnh GET DATA/GET NEXT DATA yêu cầu một (hoặc một vài) DO được xây dựng, tất cả các DO được lồng ở trong phải xuất hiện trong hồi đáp, ngoại trừ:

1) Khi không có DO cùng với thẻ được yêu cầu có sẵn trong khuôn mẫu
2) Khi trạng thái an toàn không khớp với thuộc tính an toàn của nó
3) Nếu không được yêu cầu rõ rang khi đối số của lệnh là danh sách tiêu đề mở rộng.

Lệnh GET DATA/GET NEXT DATA có thể không bị phản đối nếu một hoặc một số DO được yêu cầu không có sẵn vì một trong các lý do đó. Nó phải bị phản đối chỉ khi không có DO nào có sẵn.

Nếu có một số lần xuất hiện của thẻ trong khuôn mẫu hiện hành, điều này không xác định DO nào được phục hồi bằng lệnh GET DATA thành công do việc đó phụ thuộc vào sự xác định hoặc bản chất hoặc nội dung của DO. GET NEXT DATA có chế độ chuẩn xác (xem 11.4.3.4)

Bảng 90 - Cặp lệnh-hồi đáp GET DATA/GET NEXT DATA (mã INS lẻ)

CLA	Như được xác định trong 5.4.1	
INS	'CB'	GET DATA
	'CD'	GET NEXT DATA
P1-P2	'0000'	Tệp hiện hành, ngoại trừ nếu trường dữ liệu tham chiếu một tệp
	'FFFF'	Tệp hiện hành hoặc tệp hiện hành tạm thời có thể được thiết lập bằng trường dữ liệu
	Các giá trị khác	Định danh tệp hoặc định danh EF ngắn (xem 11.4.1.2) Trường dữ liệu không bao gồm DO'4F' định danh ứng dụng và DO'51' tham chiếu tệp
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$	
Trường dữ liệu	Đồng nhất với trường dữ liệu của SELECT DATA, (xem Bảng 86 và Bảng 87) ngoại trừ nó có thể tham chiếu một vài DO	
Trường L_e	Xuất hiện đối với mã hóa $N_e > 0$	
Trường dữ liệu	0, 1 hoặc nhiều byte dữ liệu hơn nữa	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6202' đến '6280', '6281', '6700', '6981', '6982', '6985', '6A81', '6A88' (đối tượng dữ liệu không tìm thấy, nghĩa là dữ liệu được tham chiếu không tìm thấy)	

11.4.4.2 Đối số bắt buộc

Trường dữ liệu lệnh phải kết thúc bằng hoặc DO'5C' danh sách thẻ (xem 8.4.3) hoặc DO'5F61' hoặc DO'4D' danh sách tiêu đề mở rộng (xem 8.4.5), DO'5F8400' được che hoặc DO'7F71' bộ lọc (xem 11.4.2.3).

- Trong trường hợp danh sách thẻ, trường dữ liệu hồi đáp phải là kết nối của các DO được tham chiếu trong danh sách thẻ, trong cùng thứ tự. Thứ tự có thể khác với thứ tự của các DO trong khuôn mẫu. Khi một số DO trong khuôn mẫu có cùng thẻ, tất cả các DO này phải được phục hồi. Một hoặc nhiều DO có thể không xuất hiện do lý do trạng thái an toàn. Một danh sách thẻ trống yêu cầu tất cả các DO có sẵn.
- Trong trường hợp danh sách tiêu đề mở rộng, trường dữ liệu hồi đáp phải là kết nối của các DO có nguồn gốc từ danh sách tiêu đề mở rộng theo 8.4.6 và 8.4.7.
- Trong trường hợp thẻ được che hoặc trong trường hợp bộ lọc, trường dữ liệu hồi đáp phải là kết nối của các DO thích hợp.

11.4.4.3 Hàm SELECT

Nếu lệnh GET DATA với P1-P2 không bằng với 'FFFF' tham chiếu một tệp, hiệu ứng lề của sự thành công của nó là để thiết lập tệp này là hiện hành và tệp hiện hành là trường giá trị của DO'7F70' gốc.

Lệnh GET DATA thành công với cú pháp không được xác định trong bản in lần thứ hai của tiêu chuẩn này phải không tác động đến VA, nghĩa là:

- P1-P2 được đặt là 'FFFF'
- Đối số 1 và/hoặc đối số 3 xuất hiện,

- Đối số 4 khác với DO'4D' hoặc DO'5C'.

11.4.4.4 Hàm DIR và VIEW

Hàm DIR/VIEW được hỗ trợ bằng lệnh GET DATA/GET NEXT DATA INS lẻ khi đối số của nó là:

- '5C 01 5C' (thẻ '5C' lồng trong DO danh sách thẻ); dữ liệu hồi đáp phải là DO'5C' danh sách thẻ lồng dữ liệu hồi đáp được xác định trong 11.4.2.5 hoặc 11.4.2.6.
- '5C 01 5D' (thẻ '5D' lồng trong DO danh sách thẻ); dữ liệu hồi đáp phải là DO'5D' danh sách tiêu đề lồng dữ liệu hồi đáp được xác định trong 11.4.2.5 hoặc 11.4.2.6.

Lựa chọn giữa hàm DIR và VIEW không thuộc phạm vi của tiêu chuẩn này.

11.4.4.5 Hàm GET DATA CONTROL PARAMETER

Khi đối số của GET DATA INS lẻ là '5C 01 62' (thẻ '62' (thẻ khuôn mẫu CP) lồng trong DO danh sách thẻ), dữ liệu hồi đáp phải là DO'62'.

11.4.4.6 Hàm cụ thể của GET NEXT DATA (INS = 'CD')

Các đặc tính của GET NEXT DATA (INS='CD') liên quan đến GET DATA (INS='CB') đồng nhất với các đặc tính của GET NEXT DATA (INS='CC') liên quan đến GET DATA (INS='CA', xem 11.4.3.4), ngoại trừ C-RP có các mã INS lẻ phục hồi các DO, C-RP với mã INS chẵn phục hồi phần từ dữ liệu (các giá trị của DO).

11.4.5 Các đặc tính chung của lệnh PUT/PUT NEXT/UPDATE DATA

Các lệnh này khởi đầu sự biến đổi của nội dung khuôn mẫu hiện hành, bằng cách truyền một hoặc một vài DO, có thể được được xây dựng. PUT/ PUT NEXT/UPDATE DATA với bit 1 của INS:

- Được đặt là 0 phải chỉ hoạt động trong khuôn mẫu hiện hành
- Được đặt là 1 thiết lập khuôn mẫu tạm thời là giá trị của DO'7F70' gốc ảo, được lựa chọn theo P1-P2 không bằng với 'FFFF', trước khi xử lý thực tế của DO. Khuôn mẫu hiện hành tạm thời phải trở thành khuôn mẫu hiện hành nếu lệnh thành công.

Nếu con trỏ được thiết lập bằng lệnh GET NEXT DATA thành công hoặc C-RP PUT NEXT DATA (xem 11.4.3.4) nó xác định phiên bản nào phải bị ảnh hưởng bởi C-RP PUT DATA hoặc DATA UPDATE.

Nếu con trỏ không được thiết lập (xem 11.4.3.4) curDO (xem 7.2.1) xác định DO nào bị ảnh hưởng bởi UPDATE DATA hoặc C-RP PUT DATA.

Trong khi lệnh PUT DATA và UPDATA DATA có thể bao gồm một số DO trong trường dữ liệu lệnh, lệnh PUT NEXT DATA phải mô tả đặc tính một và chỉ một DO trong trường dữ liệu lệnh.

11.4.6 Lệnh PUT DATA

Bảng 91 thể hiện C-RP PUT DATA. Lệnh PUT DATA có thể có chế độ và mã hóa được xác định đối với UPDATE DATA (PUT NEXT DATA). Nhất quán với bản in lần thứ hai của tiêu chuẩn này, định nghĩa hoặc bản chất hoặc nội dung của các DO phải cảm sinh tác động đối với nội dung khuôn mẫu. Nếu INS được đặt là 'DB' và P1-P2 được đặt là 'FFFF', quy tắc sau được áp dụng:

- Nếu PUT NEXT DATA được hỗ trợ, PUT DATA của một DO thẻ của nó đã tồn tại trong khuôn mẫu phải thay thế mọt DO hiện có bằng một DO mới.
- Nếu UPDATE DATA được hỗ trợ, PUT DATA đảm bảo rằng toàn bộ DO được truyền được bổ sung vào khuôn mẫu. Điều này có thể đem lại kết quả là nhân đôi phiên bản trong khuôn mẫu.

Khi trường L_c không xuất hiện, lệnh PUT DATA INS chẵn phải bổ sung vào DO trống hoặc thay thế DO hiện có bằng một DO trống của cùng thẻ như được biểu thị bằng P1-P2.

Bảng 91 - Cặp lệnh-hồi đáp PUT DATA

CLA	Như được xác định trong 5.4.1	
INS	'DA' hoặc 'DB'	
P1-P2	INS = 'DA'	Xem Bảng 85, nếu giá trị đặc biệt '00FF' được sử dụng trường dữ liệu lệnh bao gồm kết nối của các DO được bổ sung hoặc thay thế trong khuôn mẫu hiện hành
	INS = 'DB'	Định danh tệp hoặc định danh EF ngắn (xem 11.4.1.2)
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$, không xuất hiện đối với mã hóa $N_c = 0$	
Trường dữ liệu	INS = 'DA'	Byte dữ liệu theo P1-P2, hoặc không xuất hiện để xóa bỏ giá trị của DO
	INS = 'DB'	Kết nối của các DO
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$	
Trường dữ liệu	Không xuất hiện	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '63CX' (xem 11.4.1), '6581', '6700', '6981', '6982', '6985', '6A80', '6A81', '6A84' '6A85'	

11.4.7 Lệnh PUT NEXT DATA

Lệnh khởi đầu bổ sung một DO trong khuôn mẫu hiện hành. Nếu một DO có cùng thẻ như DO đã được chèn tồn tại trong khuôn mẫu, nó phải bổ sung phiên bản mới này của DO trong khuôn mẫu. Nếu số phiên bản không đạt đến giá trị tối đa, PUT NEXT DATA phải bổ sung DO được truyền tới khuôn mẫu hiện hành, và thiết lập con trỏ trên DO đã được đặt. Kết quả của lệnh này phụ thuộc vào cấu trúc của DO như đã được đưa ra bởi byte bộ mô tả dữ liệu (xem Bảng 13). Nếu cấu trúc thuộc loại

- "không có thông tin được đưa ra" và số các phiên bản đã đạt đến giá trị tối đa, PUT NEXT DATA phải bị phản đối với SW1-SW2='6A84'. Mặt khác DO mới được chèn vào tại vị trí tùy ý trong danh sách theo thứ tự của DO.
- "quản lý tuyến tính" và số các phiên bản đã đạt đến giá trị tối đa, PUT NEXT DATA phải bị phản đối với SW1-SW2='6A84'. Mặt khác nếu con trỏ
  - Không được thiết lập, khi đó DO mới phải được thêm vào sau phần tử cuối cùng của danh sách.
  - Được thiết lập, khi đó DO mới phải được chèn vào sao cho nó trở thành phần tử danh sách trước đó đối với DO được chỉ.
- "quản lý tuần hoàn" và con trỏ
  - Không được thiết lập, khi đó DO mới phải được thêm vào sau phần tử đầu tiên của danh sách.
  - Được thiết lập, khi đó DO mới phải được chèn vào sao cho nó trở thành phần tử danh sách tiếp theo đối với DO được chỉ.

Hơn nữa, nếu cấu trúc thuộc loại "quản lý tuần hoàn" và sau khi chèn DO mới trong danh sách theo thứ tự số các phiên bản lớn hơn giá trị tối đa, khi đó DO có gần nhất với vị trí cuối của danh sách theo thứ tự có cùng thẻ như cái đã được chèn phải bị hủy bỏ.

Chú thích 1 Quy tắc chèn DO mới là sao cho cùng với quản lý tuyến tính và tuần hòa, một DO mới có thể được chèn vào tại vị trí bất kỳ trong danh sách theo thứ tự.

Chú thích 2 Nếu con trỏ không được thiết lập khi đó quản lý tuần hoàn hoạt động là APPEND RECORD đối với EF với cấu trúc tuần hoàn.

Chú thích 3 Nếu cấu trúc là quản lý tuần hoàn và con trỏ chỉ phần tử cuối cùng và số các phiên bản đã đạt đến giá trị tối đa khi đó quy tắc có nghĩa là chèn một DO mới không có ảnh hưởng đến danh sách theo thứ tự.

Chú thích 4 Nếu các phiên bản được đánh số rõ ràng, xử lý số phiên bản (xem Bảng 10) phải thuộc động lực học.

Chú thích 5 Tiêu chuẩn này không xác định số tối đa các phiên bản có thể thấy tại giao diện thẻ.

Nếu một số DO được truyền, lệnh phải bị hủy (SW1-SW2 = '6A80') mà không thay đổi bất kỳ cái gì trong khuôn mẫu hiện hành.

Bảng 92 - Cặp lệnh-hồi đáp PUT NEXT DATA

CLA	Như được xác định trong 5.4.1	
INS	'D8' hoặc 'D9'	
P1-P2	INS = 'D8'	Xem Bảng 85, nếu giá trị đặc biệt '00FF' được sử dụng trường dữ liệu lệnh bao gồm một DO được bổ sung vào khuôn mẫu hiện hành
	INS = 'D9'	Định danh tệp hoặc định danh EF ngắn (xem 11.4.1.2)
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$	
Trường dữ liệu	INS = 'D8'	Byte dữ liệu theo P1-P2
	INS = 'D9'	Một DO
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$	
Trường dữ liệu	Không xuất hiện	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '63CX' (xem 11.4.1), '6581', '6700', '6981', '6982', '6985', '6A80', '6A81', '6A84' '6A85'	

Bảng 93 - Cặp lệnh-hồi đáp UPDATE DATA

CLA	Như được xác định trong 5.4.1	
INS	'DE' hoặc 'DF'	
P1-P2	INS = 'DE'	Xem Bảng 85, nếu giá trị đặc biệt '00FF' được sử dụng trường dữ liệu lệnh bao gồm kết nối của các DO được xử lý trong khuôn mẫu hiện hành
	INS = 'DF'	Định danh tệp hoặc định danh EF ngắn (xem 11.4.1.2)
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$, không xuất hiện đối với mã hóa $N_c = 0$ (xem bên dưới)	
Trường dữ liệu	INS = 'DE'	Byte dữ liệu theo P1-P2, hoặc không xuất hiện để xóa bỏ giá trị của DO
	INS = 'DF'	Một DO (có thể được được xây dựng)
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$	
Trường dữ liệu	Không xuất hiện	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '63CX' (xem 11.4.1), '6581', '6700', '6981', '6982', '6985', '6A80', '6A81', '6A84' '6A85'	

Đối với mỗi DO được biểu thị trong trường dữ liệu, lệnh phải thực hiện:

a) Hoặc sửa đổi DO trong khuôn mẫu hiện hành. Nếu một số phiên bản của DO tồn tại, và:

1) Một trong số chúng là DO hiện hành, nó phải được cập nhật
2) Nếu DO hiện hành không phải là một trong số các phiên bản, tiêu chuẩn này không xác định phiên bản nào của DO được cập nhật

b) Hoặc xóa bỏ trường giá trị của DO, với cùng điều kiện như ở trên khi một số phiên bản tồn tại. Cập nhật DO không trống bằng một DO trống thay thế DO hiện có bằng một DO trống.

c) Hoặc tạo ra một DO trong khuôn mẫu hiện hành nếu không có DO nào có thẻ tương tự đã tồn tại. Cập nhật DO ban đầu thay thế DO hiện có bằng DO được truyền.

Để cập nhật DO được xây dựng (xem F.3), tất cả các khuôn mẫu xuất hiện trong DO được truyền phải được xử lý tiếp thoe, bắt đầu với số hiệu thế hệ thấp nhất. Các DO đã xuất hiện trong khuôn mẫu phải bị sửa đổi, và các DO không xuất hiện trong khuôn mẫu phải được tạo ra trong khuôn mẫu. Nếu một hoặc một vài DO bị sửa đổi được được xây dựng, thủ tục phải được lặp lại tại thế hệ tiếp theo và thủ tục tiếp tục như vậy.

CHÚ THÍCH Cập nhật DO trong DO được xây dựng mà không cần truyền lại toàn bộ DO được xây dựng.

11.4.9 Hàm COMPARE DATA

Hàm này được hỗ trợ bằng lệnh COMPARE (xem 11.6.1).

11.5 Xử lý an toàn cơ bản

11.5.1 Tổng quát

Các thủ tục liên quan đến an toàn, được hỗ trợ bởi các lệnh được mô tả trong điều này, thường liên quan đến chuỗi theo thứ tự bao gồm các lệnh đó và các lệnh được mô tả trong ISO/IEC 7816-8. Sử dụng mở rộng thuộc tính an toàn (xem 9.3.6.2) hỗ trợ mô tả các chuỗi như vậy tại giao diện.

Các lệnh thuộc nhóm này dự trữ P1-P2 để tham chiếu thuật toán và một số dữ liệu tham chiếu có liên quan (ví dụ, khóa). Nếu có khóa hiện hành và thuật toán hiện hành, khi đó lệnh có thể hoàn toàn sử dụng chúng.

P1 - trừ khi có quy định khác, P1 tham chiếu thuật toán để sử dụng: hoặc thuật toán mã hóa hoặc thuật toán sinh trắc (xem ISO/IEC 7816-11). P1 được đặt là '00' nghĩa là 0 có thông tin được cho, nghĩa là hoặc tham chiếu đã biết trước khi ban hành lệnh, hoặc trường dữ liệu lệnh cung cấp.

P2 - trừ khi có quy định khác, P2 định tính dữ liệu tham chiếu theo Bảng 94. P2 được đặt là '00' nghĩa là 0 có thông tin được cho, nghĩa là hoặc bộ định tính đã biết trước khi ban hành lệnh, hoặc trường dữ liệu lệnh cung cấp. Bộ định tính có thể là số mật lệnh hoặc số khóa hoặc một định danh EF ngắn.

Bảng 94 - Mã hóa bộ định tính dữ liệu tham chiếu trong P2

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	0	0	0	0	0	0	0	Không có thông tin được cho
0	-	-	-	-	-	-	-	Dữ liệu tham chiếu chung (ví dụ mật lệnh cụ thể MF hoặc khóa)
1	-	-	-	-	-	-	-	Dữ liệu tham chiếu cụ thể (ví dụ mật lệnh cụ thể DF hoặc khóa)
-	x	x	-	-	-	-	-	00 (bất kỳ giá trị nà khác là RFU)
-	-	-	x	x	x	x	x	Bộ định tính, nghĩa là số dữ liệu tham chiếu hoặc số bí mật

CHÚ THÍCH Lệnh MANAGE SECURITY ENVIRONMENT có thể thiết lập một tham chiếu thuật toán và/hoặc bộ định tính dữ liệu tham chiếu nhiều byte (xem Bảng 51).

Trong nhóm lệnh này, SW1-SW2 được đặt là '6300' hoặc '63CX' biểu thị rằng sự kiểm tra không đạt, 'X' >='0' mã hóa số các lần thử lại được phép. SW1-SW2 được đặt là '6A88' nghĩa là "dữ liệu tham chiếu không tìm thấy'.

11.5.2 Lệnh INTERNAL AUTHENTICATE

Lệnh khởi đầu phép tính dữ liệu xác thực bởi thẻ sử dụng dữ liệu thử thách được gửi bằng thiết bị giao diện và bí mật có liên quan (ví dụ, khóa) được lưu giữ trong thẻ.

Nếu bí mật có liên quan được gắn với MF, khi đó lệnh có thể được sử dụng để xác thực toàn bộ thẻ

- Nếu bí mật có liên quan được gắn với DF khác, khi đó lệnh có thể được sử dụng để xác thực DF đó.

Bất kỳ sự xác thực thành công nào đều có thể theo sự hoàn thành của các lệnh trước (ví dụ VERIFY, SELECT) hoặc các lựa chọn (ví dụ, bí mật có liên quan).

Thẻ có thể ghi lại số lần lệnh được ban hành để giới hạn số lần sử dụng hơn nữa của bí mật có liên quan hoặc thuật toán.

CHÚ THÍCH Trường dữ liệu hồi đáp có thể bao gồm dữ liệu có ích đối với các hàm an toàn (ví dụ, số ngẫu nhiên).

Bảng 95 - Cặp lệnh-hồi đáp INTERNAL AUTHENTICATE

CLA	Như được xác định trong 5.4.1
INS	'88'
P1-P2	Xem 11.5.1 và Bảng 94
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$
Trường dữ liệu	Dữ liệu liên quan đến xác thực (ví dụ, thử thách)
Trường L_e	Xuất hiện đối với mã hóa $N_e > 0$
Trường dữ liệu	Dữ liệu liên quan đến xác thực (ví dụ, hồi đáp một thử thách)
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6300' (xem 11.5.1), '63CX' (xem 11.5.1), '6581', '6700', '6982', '6983', '6984', '6A81', '6A82', '6A86' '6A88' (xem 11.5.1)

11.5.3 Lệnh GET CHALLENGE

Lệnh yêu cầu ban hành một thách thức (ví dụ, số ngẫu nhiên đối với xác thực mật mã hoặc một câu lệnh để nhắc xác thực sinh trắc sử dụng bản in giọng nói) để sử dụng trong thủ tục liên quan đến an toàn (ví dụ, lệnh EXTERNAL AUTHENTICATE). Thách thức có hiệu lực ít nhất đối với lệnh tiếp theo; điều này không xác định điều kiện hơn nữa.

Bảng 96 - Cặp lệnh-hồi đáp GET CHALLENGE

CLA	Như được xác định trong 5.4.1
INS	'84'
P1	Xem 11.5.1
P2	'00' (mọi giá trị khác là RFU)
Trường L_c	Không xuất hiện đối với mã hóa $N_c = 0$
Trường dữ liệu	Không xuất hiện
Trường L_e	Xuất hiện đối với mã hóa $N_e > 0$
Trường dữ liệu	Thử thách
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6700', '6A86' (xem 11.5.1)

11.5.4 Lệnh EXTERNAL AUTHENTICATE

Các hàm của lệnh này có thể được thực hiện chỉ khi trạng thái an toàn thỏa mãn thuộc tính an toàn đối với hoạt động này.

Lệnh này có một số vị. Bảng 97 thể hiện C-RP EXTERNAL AUTHENTICATE trong khi Bảng 98 thể hiện C-RP của hàm MUTUAL AUTHENTICATE. Lệnh cập nhật có điều kiện trạng thái an toàn sử dụng kết quả (có hoặc không) của phép tính bằng thẻ dựa trên thử thách được thẻ ban hành trước (ví dụ, bằng lệnh GET CHALLENGE), khóa có thể được lưu giữ bí mật trong thẻ và dữ liệu xác thực được truyền bằng thiết bị giao diện.

Bất kỳ xác thực thành công nào cũng đòi hỏi sử dụng thử thách cuối cùng đạt được từ thẻ. Thẻ có thể ghi lại các xác thực không thành công (ví dụ, để giới hạn số lần sử dụng hơn nữa của dữ liệu tham chiếu).

Không xuất hiện trường dữ liệu lệnh có thể được sử dụng hoặc để truy tìm số 'X' của các lần thử lại được cho phép (SW1-SW2 được đặt là '63CX'), hoặc để kiểm tra liệu việc xác nhận có được yêu cầu hay không) SW1-SW2 được đặt là '9000').

Hàm MUTUAL AUTHENTICATE - Hàm MUTUAL AUTHENTICATE sử dụng các chức năng giống như các lệnh EXTERNAL và INTERNAL AUTHENTICATE. Nó dựa trên lệnh GET CHALLENGE trước và khóa, có thể bí mật, được lưu giữ trong thẻ. Thẻ và thiết bị giao diện chia xẻ dữ liệu liên quan đến xác thực, bao gồm hai thử thách: một được thẻ ban hành, một thử thách khác do thiết bị giao diện ban hành.

CHÚ THÍCH Lệnh có thể được sử dụng để thực hiện xác thực như được xác định trong phần 2 và 3 của ISO/IEC 9798

Bảng 97 - Cặp lệnh-hồi đáp EXTERNAL AUTHENTICATE

CLA	Như được xác định trong 5.4.1
INS	'82'
P1-P2	Xem 11.5.1 và Bảng 94
Trường L_c	Không xuất hiện đối với mã hóa $N_c = 0$, xuất hiện đối với mã hóa $N_c > 0$
Trường dữ liệu	Không xuất hiện hoặc dữ liệu liên quan đến xác thực (ví dụ, hồi đáp một thử thách)
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$
Trường dữ liệu	Không xuất hiện
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6300' (xem 11.5.1), '63CX' (xem 11.5.1), '6581', '6700', '6982', '6983', '6984', '6A81', '6A82', '6A86' '6A88' (xem 11.5.1)

Bảng 98 - Cặp lệnh-hồi đáp đối với hàm MUTUAL AUTHENTICATE

CLA	Như được xác định trong 5.4.1
INS	'82'
P1-P2	Xem 11.5.1 và Bảng 94
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$
Trường dữ liệu	Dữ liệu liên quan đến xác thực (ví dụ, hồi đáp một thử thách)
Trường L_e	Xuất hiện đối với mã hóa $N_e > 0$
Trường dữ liệu	Dữ liệu liên quan đến xác thực
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6300' (xem 11.5.1), '63CX' (xem 11.5.1), '6581', '6700', '6982', '6983', '6984', '6A81', '6A82', '6A86' '6A88' (xem 11.5.1)

11.5.5 Lệnh GENERAL AUTHENTICATE

Lệnh làm mịn hàm EXTERNAL, INTERNAL và MUTUAL AUTHENTICATE; cụ thể là hoặc một thực thể trong mọi đối tượng bên ngoài xác thực một thực thể trong thẻ (hàm INTERNAL AUTHENTICATE), hoặc một thực thể trong thẻ xác thực mộ thực thể trong mọi đối tượng bên ngoài (hàm EXTERNAL AUTHENTICATE), hoặc cả hai (hàm MUTUAL AUTHENTICATE).

Trong khi phù hợp với cơ chế xác thực bao gồm các cặp thử thách-hồi đáp, các lệnh EXTERNAL và INTERNAL AUTHENTICATE ngăn ngừa cơ chế xác thực bao gồm bộ ba bằng chứng-thử thách-hồi đáp (xem ISO/IEC 9798) và các giao thức xác thực nhiều bước tổng quát hơn. Các giao thức này đòi hỏi hai hoặc nhiều C-RP GENERAL AUTHENTICATE: các C-RP như vậy có thể tạo chuỗi (xem 5.3.3).

Hàm (hoặc INTERNAL, hoặc EXTERNAL, hoặc MUTUAL AUTHENTICATE) có thể được thực hiện chỉ khi trạng thái an toàn thỏa mãn thuộc tính an toàn đối với hoạt động này. Bất kỳ xác thực thành công nào có thể phải theo sự hoàn thành của các lệnh trước (ví dụ, VERIFY, SELECT) hoặc các lựa chọn (ví dụ, bí mật có liên quan). Kết quả (có hoặc không) của một điều khiển được thực hiện bằng thẻ có thể cập nhật có điều kiện trạng thái an toàn. Thẻ có thể ghi lại số lần hàm được ban hành, để giới hạn số sử dụng hơn nữa bí mật có liên quan hoặc thuật toán. Thẻ có thể ghi lại các xác thực không thành công, ví dụ, để giới hạn số lần sử dụng hơn nữa của dữ liệu tham chiếu.

Bảng 99 - Cặp lệnh-hồi đáp GENERAL AUTHENTICATE

CLA	Như được xác định trong 5.4.1
INS	'86' hoặc '87'
P1-P2	Xem 11.5.1 và Bảng 94
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$
Trường dữ liệu	Dữ liệu liên quan đến xác thực
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$, xuất hiện đối với mã hóa $N_e > 0$
Trường dữ liệu	Không xuất hiện (hoặc do sự không xuất hiện của trường L_e, ví dụ lệnh cuối cùng của hàm EXTERNAL AUTHENTICATE, hoặc nếu quá trình bị hủy), hoặc dữ liệu liên quan đến xác thực
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6300' (xem 11.5.1), '63CX' (xem 11.5.1), '6581', '6700', '6982', '6983', '6984', '6A81', '6A82', '6A86' '6A88' (xem 11.5.1)

Bảng 100 - DO xác thực động lực đối với bộ ba bằng chứng-thử thách-hồi đáp

Thẻ		Giá trị
'7C'		Thiết lập DO xác thực động lực với các thẻ sau
	'80'	Bằng chứng (ví dụ, một hoặc nhiều số dương nhỏ hơn mô-đun công khai trong sử dụng)
	'81'	Thử thách (ví dụ, một hoặc nhiều số, có thể là 0 nhỏ hơn số mũ công khai trong sử dụng)
	'82'	Hồi đáp (ví dụ, một hoặc nhiều số dương nhỏ hơn mô-đun công khai trong sử dụng)
	'83'	Thử thách cam kết (ví dụ, mã-băm của một số bất kỳ lớn bao gồm một hoặc nhiều thử thách)
	'84'	Mã xác thực (ví dụ, mã-băm của một hoặc nhiều trường dữ liệu và DO bằng chứng)
	'85'	Một khóa công khai tạm thời đối với kỹ thuật quy ước khóa
	'86'	Dữ liệu mã hóa
	'06'	OID (xem phần dưới)
	'A0'	Khuôn mẫu dữ liệu định danh
– Theo thẻ '7C', Tổ chức có trách nhiệm lưu giữ bất kỳ DO nào khác của lớp ngữ cảnh cụ thể, nếu không có OID xác định ngữ cảnh		

Khi xuất hiện, mỗi trường dữ liệu phải bao gồm một khuôn mẫu leien công nghiệp được tham chiếu bằng thẻ '7C'.

Ngữ cảnh mặc định của lệnh GENERAL AUTHENTICATE liên quan đến giao thức mã hóa trong sử dụng được lưu giữ cho bộ ba bằng chứng-thử thách-hồi đáp (xem C.1). Trong trường hợp này, trong khuôn mẫu xác thực động lực, lớp ngữ cảnh cụ thể được lưu giữ cho các DO xác thực động lực như được liệt kê trong Bảng 100.

Trong trường hợp này, các DO ngữ cảnh cụ thể tương ứng phải được gửi trong các C-RP, được nhúng vào khuôn mẫu có thẻ '7C' (xem Bảng 100).

Nếu GENERAL AUTHENTICATE COMMAND được sử dụng cho giao thức xác thực nhiều bước (xem C.2), OID giao thức tương ứng hoặc tham chiếu thuật toán được kết hợp với một OID phải được bao gồm trong lệnh MANAGE SECURITY ENVIRONMENT có trước (xem 11.5.11) trong CRT AT đối với xác thực và/hoặc phải được bao gồm trong khuôn mẫu có thẻ '7C' biểu thị việc thực hiện giao thức cụ thể của DO ngữ cảnh cụ thể được nhúng vào bổ sung được gửi trong C-RP.

Đối với ngữ cảnh cụ thể, quy tắc sau áp dụng trong khuôn mẫu liên ngành đối với xác thực động lực.

- Nếu một DO trống trong khuôn mẫu, khi đó nó phải hoàn thành trong khuôn mẫu trong trường dữ liệu tiếp theo.
- Trong trường dữ liệu lệnh đầu tiên, khuôn mẫu biểu thị hàm xác thực động lực như sau.
  - Một yêu cầu bằng chứng, ví dụ một bằng chứng trống, biểu thị một hàm INTERNAL AUTHENTICATE.
  - Một yêu cầu thử thách, ví dụ một thử thách trốn, biểu thị một hàm EXTERNAL AUTHENTICATE.
  - Sự không xuất hiện của DO trống biểu thị hàm MUTUAL AUTHENTICATE. Khi đó, trừ khi thử hủy thủ tục, khuôn mẫu trong trường dữ liệu hồi đáp phải bao gồm các DO giống như khuôn mẫu trong trường dữ liệu lệnh. Hàm MUTUAL AUTHENTICATE cho phép hai thực thể thỏa thuận về khóa giao tiếp sử dụng cặp các phần tử dữ liệu "hàm số mũ" được tham chiếu bằng thẻ '85' (xem kỹ thuật quy ước khóa trong ISO/IEC 11770-3).

Xác thực động lực có thể bảo vệ trường dữ liệu được trao đổi trong suốt giao tiếp. Các thực thể duy trì một mã-băm hiện hành, được cập nhật bằng cách bao gồm một lệnh hoặc trường dữ liệu hồi đáp tại

cùng thời điểm. DO'84' chuyển mã xác thực là kết quả của việc cập nhật mã hiện hành bằng cách bao gồm DO'80' bằng chứng. Bộ xác minh lần lượt khôi phục một bằng chứng và một mã xác thực: nếu bằng chứng được khôi phục không phải là 0 và nếu hai mã đồng nhất, khi đó xác thực thành công.

Đối với ngữ cảnh mặc định, C.1 mô tả C-RP GENERAL AUTHENTICATE để thực hiện các hàm INTERNAL, EXTERNAL và MUTUAL AUTHENTICATE, mở rộng tới xác thực trường dữ liệu và quy ước khóa.

11.5.6 Lệnh VERIFY

Bảng 101 - Cặp lệnh-hồi đáp VERIFY

CLA	Như được xác định trong 5.4.1	
INS	'20' hoặc '21'	
P1	'00'	Hoạt động bình thường
	'FF'	Thiết lập trạng thái kiểm tra tới "không được xác minh;, xem đoạn cuối của điều này
	Mọi giá trị khác	RFU
P2	Xem Bảng 94	
Trường L_c	Không xuất hiện đối với mã hóa $N_c = 0$, xuất hiện đối với mã hóa $N_c > 0$	
Trường dữ liệu	INS = '20'	Dữ liệu kiểm tra hoặc không xuất hiện
	INS = '21'	DO dữ liệu kiểm tra, và, danh sách tiêu đề mở rộng, có điều kiện
Trường L_e	Xuất hiện đối với mã hóa $N_e = 0$	
Trường dữ liệu	Không xuất hiện	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6286', '6300' (xem 11.5.1), '63CX' (xem 11.5.1), '6581', '6700', '6982', '6983', '6984', '6A81', '6A82', '6A86' '6A88' (xem 11.5.1)	

Lệnh khởi đầu sự so sánh trong thẻ của dữ liệu tham chiếu lưu giữ với dữ liệu kiểm tra được gửi từ thiết bị giao diện (ví dụ, mật lệnh) hoặc từ cảm biến trên thẻ (ví dụ, dấu vân tay). Trạng thái an toàn có thể được sửa đổi do so sánh. Thẻ có thể ghi lại các so sánh không thành công (ví dụ, để giới hạn số lần sử dụng hơn nữa dữ liệu tham chiếu).

Nếu INS = '20', trường dữ liệu lệnh thường xuất hiện để chuyển dữ liệu kiểm tra. Sự không xuất hiện của trường dữ liệu lệnh được sử dụng để kiểm tra liệu việc kiểm tra cần đến (SW1-SW2 = '63CX' trong đó 'X' mã hóa số các lần thử lại cho phép), hoặc không (SW1-SW2 = '9000').

Nếu INS = '21', trường dữ liệu lệnh phải chuyển DO dữ liệu kiểm tra (ví dụ, thẻ '5F2E', xem ISO/IEC 7816-11), thông thường không trống. Sự xuất hiện của một DO dữ liệu kiểm tra trống và một danh sách tiêu đề mở rộng (thẻ '4D', xem 8.4.5) biểu thị rằng dữ liệu kiểm tra đến từ cảm biến trên thẻ. Danh sách tiêu đề mở rộng tham chiếu DO dữ liệu kiểm tra.

Với cả các giá trị INS, P1='FF' phải chỉ được sử dụng với L_c và trường dữ liệu lệnh không xuất hiện. Lệnh phải thiết lập trạng thái kiểm tra của dữ liệu tham chiếu liên quan là "không được kiểm tra".

11.5.7 Lệnh CHANGE REFERENCE DATA

Lệnh hoặc thay thế dữ liệu tham chiếu lưu giữ trong thẻ bằng dữ liệu tham chiếu mới được gửi từ thiết bị giao diện, hoặc khởi đầu so sánh với dữ liệu kiểm tra được gửi từ thiết bị giao diện và khi đó thay

thế có điều kiện chúng bằng dữ liệu tham chiếu mới được gửi từ thiết bị giao diện. Nó có thể được thực hiện chỉ khi trạng thái an toàn thỏa mãn thuộc tính an toàn đối với lệnh này.

Bảng 102 - Cặp lệnh-hồi đáp CHANGE REFERENCE DATA

CLA	Như được xác định trong 5.4.1		
INS	'24' hoặc '25'		
P1	'00' hoặc '01' (mọi giá trị khác là RFU)		
P2	Xem Bảng 94		
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$		
Trường dữ liệu	INS = '24'	P1 = '00'	Dữ liệu kiểm tra theo sau mà không phân định theo dữ liệu tham chiếu mới
		P1 = '01'	Dữ liệu tham chiếu mới
	INS = '25'	P1 = '00'	Do dữ liệu kiểm tra theo sau bởi DO dữ liệu tham chiếu mới
		P1 = '01'	Do dữ liệu tham chiếu mới
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$		
Trường dữ liệu	Không xuất hiện		
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6300' (xem 11.5.1), '63CX' (xem 11.5.1), '6581', '6700', '6982', '6983', '6984', '6A81', '6A82', '6A86' '6A88' (xem 11.5.1)		

11.5.8 Lệnh ENABLE VERIFICATION REQUIREMENT

Lệnh bật yêu cầu để so sánh dữ liệu tham chiếu với dữ liệu kiểm tra. Nó có thể được thực hiện chỉ khi trạng thái an toàn thỏa mãn thuộc tính an toàn đối với lệnh này.

Bảng 103 - Cặp lệnh-hồi đáp ENABLE VERIFICATION REQUIREMENT

CLA	Như được xác định trong 5.4.1	
INS	'28'	
P1	'00' hoặc '01' (bất kỳ giá trị nào là RFU)	
P2	Xem Bảng 94	
Trường L_c	Không xuất hiện đối với mã hóa $N_c = 0$, xuất hiện đối với mã hóa $N_c > 0$	
Trường dữ liệu	P1 = '00'	Dữ liệu kiểm tra
	P1 = '01'	Không xuất hiện
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$	
Trường dữ liệu	Không xuất hiện	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6300' (xem 11.5.1), '63CX' (xem 11.5.1), '6581', '6700', '6982', '6983', '6984', '6A81', '6A82', '6A86' '6A88' (xem 11.5.1)	

11.5.9 Lệnh DISABLE VERIFICATION REQUIREMENT

Bảng 104 - Cặp lệnh-hồi đáp DISABLE VERIFICATION REQUIREMENT

CLA	Như được xác định trong 5.4.1	
INS	'26'	
P1	'00', '01' hoặc 100xxxxx trong đó xxxxx là số dữ liệu tham chiếu (bất kỳ giá trị nào là RFU)	
P2	Xem Bảng 94	
Trường L_c	Không xuất hiện đối với mã hóa $N_c = 0$, xuất hiện đối với mã hóa $N_c > 0$	
Trường dữ liệu	P1 = '00' hoặc P1 = 100x xxxx	Dữ liệu kiểm tra
	P1 = '01'	Không xuất hiện
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$	
Trường dữ liệu	Không xuất hiện	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6300' (xem 11.5.1), '63CX' (xem 11.5.1), '6581', '6700', '6982', '6983', '6984', '6A81', '6A82', '6A86' '6A88' (xem 11.5.1)	

Lệnh tắt yêu cầu so sánh dữ liệu tham chiếu với dữ liệu kiểm tra, và có thể bật yêu cầu so sánh dữ liệu tham chiếu khác với dữ liệu kiểm tra. Nó có thể được thực hiện chỉ khi trạng thái an toàn thỏa mãn thuộc tính an toàn đối với lệnh này.

11.5.10 Lệnh RESET RETRY COUNTER

Lệnh hoặc thiết lập lại bộ đếm thử lại dữ liệu tham chiếu đến giá trị ban đầu của nó hoặc thay đổi dữ liệu tham chiếu khi hoàn thành thiết lập lại bộ đếm thử lại dữ liệu tham chiếu đến giá trị ban đầu. Nó có thể được thực hiện chỉ rkhi trạng thái an toàn thỏa mãn thuộc tính an toàn đối với lệnh này.

Bảng 105 - Cặp lệnh-hồi đáp RESET RETRY COUNTER

CLA	Như được xác định trong 5.4.1		
INS	'2C' hoặc '2D'		
P1	'00', '01' '02' hoặc '03' (mọi giá trị khác là RFU)		
P2	Xem Bảng 94		
Trường L_c	Không xuất hiện đối với mã hóa $N_c = 0$, xuất hiện đối với mã hóa $N_c > 0$		
Trường dữ liệu	INS = '2C'	P1 = '03'	Không xuất hiện
		P1 = '00'	Mã thiết lập lại theo sau mà không phân định bởi dữ liệu tham chiếu mới
		P1 = '01'	Mã thiết lập lại
		P1 = '02'	Dữ liệu tham chiếu mới
	INS = '2D'	P1 = '03'	Không xuất hiện
		P1 = '00'	DO mã thiết lập lại theo sau bởi DO dữ liệu tham chiếu mới
		P1 = '01'	DO mã thiết lập lại
		P1 = '02'	Dữ liệu tham chiếu mới
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$		
Trường dữ liệu	Không xuất hiện		
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6300' (xem 11.5.1), '63CX' (xem 11.5.1), '6581', '6700', '6982', '6983', '6984', '6A81', '6A82', '6A86' '6A88' (xem 11.5.1)		

11.5.11 Lệnh MANAGE SECURITY ENVIRONMENT

Lệnh chuẩn bị thông điệp an toàn (xem điều 10) lệnh an toàn (ví dụ, EXTERNAL, INTERNAL và GENERAL AUTHENTICAT, PERFORM SECURITY OPERATION trong ISO/IEC 7816-8). Lệnh hỗ trợ các hàm sau:

- SET, nghĩa là thiết lập hoặc thay thế một cấu phần của SE hiện hành;
- STORE, nghĩa là lưu SE hiện hành dưới SEID được cho trong P2;
- RESTORE, nghĩa là thay thế SE hiện hành bằng một SE được lưu giữ trong thẻ và được định danh bằng SEID được cho trong P2;
- ERASE, nghĩa là xóa bỏ một SE được lưu giữ trong thẻ và được định danh bằng SEID được cho trong P2;
- RESET, nghĩa là phục hồi SE mặc định sau khi lựa chọn DF hoặc DF ứng dụng;
- GET SE, nghĩa là truy tìm tất cả DO tham chiếu điều khiển thuộc về SE hiện hành
- GET CRT, nghĩa là truy tìm một khuôn mẫu tham chiếu điều khiển thuộc về SE hiện hành

Hàm KEY DERIVATION - sử dụng khái niệm khóa chính có thể yêu cầu nguồn gốc của khóa trong thẻ bao gồm khóa chính. Bảng 109 thể hiện việc sử dụng lệnh MANAGE SECURITY ENVIRONMENT để dẫn xuất khóa. Giả định rằng khóa chính và thuật toán được lựa chọn ẩn trong thẻ (mặt khác, lệnh MANAGE SECURITY ENVIRONMENT có thể lựa chọn bổ sung khóa và thuật toán).

CHÚ THÍCH Phụ thuộc vào tham chiếu thuật toán, dữ liệu dẫn xuất khóa từ khóa chính có thể là phần dữ liệu đầu vào của lệnh tiếp theo (ví dụ, EXTERNAL AUTHENTICATE). Trong trường hợp này, không cần thiết sử dụng lệnh MANAGE SECURITY ENVIRONMENT để dẫn xuất khóa.

Bảng 106 - Cặp lệnh-hồi đáp MANAGE SECURITY ENVIRONMENT

CLA	Như được xác định trong 5.4.1	
INS	'22'	
P1	Xem Bảng 107	
P2	Xem Bảng 108	
Trường L_c	Không xuất hiện đối với mã hóa $N_c = 0$, xuất hiện đối với mã hóa $N_c > 0$	
Trường dữ liệu	GET, STORE, RESTORE, ERASE, RESET	Không xuất hiện
	SET	Do tham chiếu điều khiển (SET)
Trường L_e	SET, STORE, RESTORE, ERASE, RESET	Không xuất hiện đối với mã hóa $N_e = 0$
	GET	Xuất hiện đối với mã hóa $N_e > 0$
Trường dữ liệu	GET SE	Kết nối DO tham chiếu điều khiển
	GET CRT	Một khuôn mẫu tham chiếu điều khiển
	Khác	Không xuất hiện
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6600', '6987', '6988', '6A88' (xem 11.5.1)	

Bảng 107 - Mã hóa P1 trong lệnh MANAGE SECURITY ENVIRONMENT

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
-	-	-	1	-	-	-	-	Thông điệp an toàn trong trường dữ liệu lệnh
-	-	1	-	-	-	-	-	Thông điệp an toàn trong trường dữ liệu hồi đáp
-	1	-	-	-	-	-	-	Tính toán, giải mã, xác thực bên trong và quy ước khóa
1	-	-	-	-	-	-	-	Xác thực, mã hóa, xác thực bên ngoài và quy ước khóa
-	-	-	-	0	0	0	1	SET
1	1	1	1	0	0	1	0	STORE
1	1	1	1	0	0	1	1	RESTORE
1	1	1	1	0	1	1	1	RESET
1	1	1	1	0	1	0	0	ERASE
0	0	0	0	1	0	0	0	GET CRT
0	0	0	0	0	0	0	0	GET SE
– Bất cứ giá trị nào khác là RFU								

Bảng 108 - Mã hóa P2 trong lệnh MANAGE SECURITY ENVIRONMENT

Giá trị	Ý nghĩa
'XX'	SEID có từ khoảng ['01' .. 'FE'] không có 'EF' (xem 10.3.3) nếu P1 biểu thị STORE, RESTORE hoặc ERASE
'A4', 'A6', 'AA', 'B4', 'B6', 'B8'	Thẻ CRT với ý nghĩa từ Bảng 54 xuất hiện trong trường dữ liệu lệnh nếu P1 biểu thị SET hoặc GET CRT
'00'	Nếu P1 biểu thị GET SE hoặc RESET
– Mọi giá trị khác là RFU	

Bảng 109 - Cặp lệnh-hồi đáp đối với hàm KEY DERIVATION

CLA	Như được xác định trong 5.4.1
INS	'22'
P1	'X1' (SET, xem Bảng 107)
P2	Thẻ CRT (ví dụ, 'A4' nếu EXTERNAL AUTHENTICATE theo sau, hoặc 'B4' nếu VERIFY CRYPTOGRAPHIC CHECKSUM theo sau)
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$
Trường dữ liệu	{'94' - L - dữ liệu để dẫn xuất khóa (bắt buộc)}; DO SM có thể xuất hiện
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$
Trường dữ liệu	Không xuất hiện
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6600', '6987', '6988', '6A88' (dữ liệu được tham chiếu không tìm thấy)

11.6 Các loại lệnh

11.6.1 Lệnh COMPARE

Lệnh khởi đầu sơ sánh của dữ liệu so sánh với dữ liệu tham chiếu mà phải là hoặc giá trị của DO ban đầu, hoặc nội dung của bản ghi, hoặc nội dung của chuỗi dữ liệu. Dữ liệu tham chiếu được xác định theo Bảng 86. Thẻ phải thực hiện bất kỳ phần tử đơn lẻ nào liên quan đến so sánh làm số mã hóa nhị phân. Khi một khoảng được cung cấp trong lệnh hoặc dữ liệu hồi đáp, điểm đầu nút của khoảng đó phải có cùng loại như dữ liệu mà chúng được so sánh.

Bảng 110 - Cặp lệnh-hồi đáp COMPARE

CLA	Như được xác định trong 5.4.1	
INS	'33'	
P1	'00'	Hàm COMPARE BINARY, giá trị tham chiếu được định vị trong EF trong suốt
	'01'	Hàm COMPARE RECORD, giá trị tham chiếu được định vị trong EF cấu trúc
	'02'	Hàm COMPARE DATA, giá trị tham chiếu được định vị Trong một DO
	Khác	RFU
P2	Bộ định tính hoạt động (xem chi tiết bên dưới)	
	'00'	So sánh được xác định bằng OID
	'01'	Bằng nhau
	'02'	Lớn hơn
	'03'	Nhỏ hơn
	'04'	Không bằng nhau
	'05'	Phần tử khoảng [điểm đầu nút thấp hơn, điểm đầu nút cao hơn]
	'06'	Không phải phần tử khoảng [điểm đầu nút thấp hơn, điểm đầu nút cao hơn]
	'07'	Dữ liệu so sánh phải thuộc về thiết lập của các giá trị có hạn được xác định bằng lệnh
	'08'	Dữ liệu so sánh phải không thuộc về thiết lập của các giá trị có hạn được xác định bằng lệnh
	['09' .. '7F']	RFU
	['80' .. 'FF']	Độc quyền
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$	
Trường dữ liệu	DO'06' OID có điều kiện, xuất hiện chỉ khi P2='00'	
	Lựa chọn bắt	DO'60' khuôn mẫu tham chiếu chung như được xác định trong Bảng 86

	buộc giữa	DO'78' theo sau bởi một DO có thẻ '70' đến '72' hoặc thẻ '74' đến '77' (xem 8.3.5), lồng ứng dụng DO xác định để tham chiếu mục tiêu của lệnh
		Bộ định vị đối tượng DO'7F72' như được xác định Bảng 37
		Trình bao DO'63' (xem 8.4.8)
	Trường dữ liệu kết thúc tùy chọn với dữ liệu so sánh được đóng kín dưới DO'53' hoặc DO'73'	
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$, hoặc xuất hiện đối với mã hóa $N_e > 0$	
Trường dữ liệu	Không xuất hiện hoặc xuất hiện (xem bên dưới)	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6282', '6340', '6982'	

Dữ liệu so sánh phải là:

- Hoặc được truyền trong trường dữ liệu lệnh
- Hoặc được nhận biết bởi thẻ

Theo định nghĩa, giá trị tham chiếu là số được mã hóa trong dữ liệu tham chiếu và giá trị so sánh là số được mã hóa trong dữ liệu so sánh.

Hàm của lệnh (COMPARE BINARY hoặc COMPARE RECORD hoặc COMPARE DATA) phải được mã hóa trong P1 được đặt là giá trị '00', '01', '02' tương ứng.

Loại hoạt động được xác định bằng P2 (bộ định tính hoạt động):

- P2 = '00': hàm so sánh được xác định bằng một DO'06' OID trong trường dữ liệu
- P2 = '01': so sánh thành công nếu giá trị tham chiếu bằng với giá trị so sánh,
- P2 = '02': so sánh thành công nếu giá trị tham chiếu lớn hơn giá trị so sánh,
- P2 = '03': so sánh thành công nếu giá trị tham chiếu nhỏ hơn giá trị so sánh,
- P2 = '04': so sánh thành công nếu giá trị tham chiếu không bằng với giá trị so sánh,
- P2 = '05': so sánh thành công nếu giá trị tham chiếu là phần tử khoảng đóng được xác định bằng lệnh
- P2 = '06': so sánh thành công nếu giá trị tham chiếu không là phần tử khoảng đóng được xác định bằng lệnh
- P2 = '07': so sánh thành công nếu giá trị tham chiếu là phần tử của tập hợp có hạn của các giá trị được xác định bằng lệnh
- P2 = '08': so sánh thành công nếu giá trị tham chiếu không là phần tử của tập hợp có hạn của các giá trị được xác định bằng lệnh.
- P2 có giá trị từ khoảng ['09' .. '7F'] là RFU.
- P2 có giá trị từ khoảng ['80' .. 'FF'] là độc quyền.

Kết quả được biểu thị bằng từ trạng thái trong hồi đáp lệnh. SW1-SW2 được đặt là '6340' biểu thị rằng dữ liệu so sánh không tương thích với dữ liệu tham chiếu.

Nếu dữ liệu so sánh được đưa ra trong trường dữ liệu lệnh, khi đó đối với P2 bằng

- '01' hoặc '02' hoặc '03' hoặc '04' giá trị phải được đưa ra trong trường giá trị của DO'53'.
- '05' hoặc '06' khoảng đóng phải được cung cấp trong trường giá trị của DO'73'. Trong trường hợp này DO'73' phải không bao gồm bất cứ cái gì ngoài hai DO'80'. DO'80' đầu tiên phải bao

gồm điểm đầu nút dưới của khoảng. DO'80' thứ hai phải bao gồm điểm đầu nút trên của khoảng.

- '07' hoặc '08' tập hợp phải được cung cấp trong trường giá trị của DO'73'. Trong trường hợp này, mỗi giá trị của tập hợp phải được đưa ra trong trường giá trị của DO'53'.

Khi lệnh thành công, trường dữ liệu hồi đáp tùy chọn có thể xuất hiện khi P2='01' hoặc '04' hoặc '05' hoặc '06'. Khi xuất hiện, nó phải là kết nối của hai DO'80' xác định điểm đầu nút của khoảng đóng mà trong đó một phần tử tương thích (P2='01' hoặc '05') hoặc trong đó không có phần tử tương thích (P2='04' hoặc '06') dữ liệu so sánh.

11.6.2 Lệnh GET ATTRIBUTE

Lệnh GET ATTRIBUTE truy tìm một thuộc tính đối tượng của đối tượng an toàn tham chiếu, nếu điều kiện truy cập đối với hoạt động tương ứng thỏa mãn. Đối tượng an toàn tương ứng phải được tham chiếu bằng bộ định vị đối tượng dữ liệu trong trường dữ liệu của lệnh. Nếu một EF hoặc DO được tham chiếu bằng lệnh tham chiếu thuộc tính trống là bắt buộc trong khuôn mẫu bộ định vị đối tượng. Thuộc tính tương ứng có thể liên quan tới môi trường an toàn riêng hoặc dịch vụ riêng được cung cấp bởi đối tượng an toàn tham chiếu. Thuộc tính có liên quan được truy tìm là đối tượng BER-TLV trong trường dữ liệu của APDU hồi đáp.

Bảng 111 - Cặp lệnh-hồi đáp GET ATTRIBUTE

CLA	Như được xác định trong 5.4.1	
INS	'34' hoặc '35'	
P1-P2	'0000'	
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$	
Trường dữ liệu	INS = '34'	Khuôn mẫu bộ định vị đối tượng (xem Bảng 37)
	INS = '35'	DO'7F72' bộ định vị đối tượng (xem Bảng 37)
Trường L_e	Xuất hiện đối với mã hóa $N_e > 0$	
Trường dữ liệu	Các thuộc tính được mã hóa trong BER-TLV	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan	

11.7 Xử lý truyền

11.7.1 Lệnh GET RESPONSE

Lệnh truyền (phần) APDU hồi đáp (xem 5.3.4).

Bảng 112 - Cặp lệnh-hồi đáp GET RESPONSE

CLA	Như được xác định trong 5.4.1
INS	'C0'
P1 - P2	'0000' (mọi giá trị khác là RFU)
Trường L_c	Không xuất hiện đối với mã hóa $N_c = 0$
Trường dữ liệu	Không xuất hiện
Trường L_e	Xuất hiện đối với mã hóa $N_e > 0$
Trường dữ liệu	Không xuất hiện trong bất kỳ trường hợp lỗi nào, hoặc (một phần của) APDU hồi đáp theo N_e
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '61XX' ('XX' mã hóa số byte thêm vẫn có sẵn bằng GET RESPONSE tiếp theo), '6281', '6700', '6A81', '6A82', '6A86', '6CXX'

11.7.2 Lệnh ENVELOPE

Với INS = 'C2', lệnh, hoặc chuỗi các lệnh như vậy truyền dữ liệu mà phải là một APDU lệnh.

Với INS = 'C3', lệnh, hoặc chuỗi các lệnh như vậy truyền dữ liệu mà phải là một DO. Sử dụng đặc biệt là:

- Khi DO là DO'52' (lệnh thực hiện), nó có cùng chức năng như 'C2', ngoại trừ hồi đáp phải là kết nối của các DO. Nếu hồi đáp được xác định bằng lệnh lồng là 0, nó phải được lồng vào trong DO'53'.
- Khi DO là DO'06' (định danh đối tượng), sự thành công của lệnh (SW1-SW2 = '9000') có nghĩa là thẻ sẵn sàng bắt đầu thủ tục được xác định theo tài liệu được tham chiếu bằng định danh đối tượng này. Thủ tục này, hoặc tập lệnh phải tuân theo cú pháp APDU tiêu chuẩn. Phần cuối của thủ tục phải được xác định trong thủ tục.

Ví dụ 1 để sử dụng gói dữ liệu IP tại giao diện, đặc tả đặc tham chiếu đến theo OID phải xác định sự đóng gói của các gói dữ liệu này trong dữ liệu lệnh và hồi đáp.

Ví dụ 2 để sử dụng tại giao diện cú pháp lệnh có nguồn gốc từ API được xác định theo ISO/IEC 24727-3, các yêu cầu và xác nhận được ghép nối BER-TLV (dữ liệu), cũng được xác định dtrong ISO/IEC 24727-3, được gói trong trường dữ liệu lệnh của C-RT ENVELOPE với INS = 'C3'.

CHÚ THÍCH Phụ lục B thể hiện sử dụng lệnh ENVELOPE đối với thông điệp an toàn

Bảng 113 - Cặp lệnh-hồi đáp ENVELOPE

CLA	Như được xác định trong 5.4.1	
INS	'C2' hoặc 'C3'	
P1-P2	'0000' (mọi giá trị khác là RFU)	
Trường L_c	Xuất hiện đối với mã hóa $N_c > 0$	
Trường dữ liệu	INS = 'C2'	(một phần của) APDU lệnh
	INS = 'C3'	DO hoặc đoạn DO
Trường L_e	Không xuất hiện đối với mã hóa $N_e = 0$, xuất hiện đối với mã hóa $N_e > 0$	
Trường dữ liệu	(một phần của) APDU hồi đáp (INS = 'C2'), hoặc (các phần của) DO'53' (INS = 'C3' với DO'52'), hoặc không xuất hiện	
SW1-SW2	Xem Bảng 5 và Bảng 6 khi có liên quan, ví dụ '6700'	

12 Dịch vụ thẻ ứng dụng-độc lập

mục đích của dịch vụ thẻ là để cung cấp cơ chế trao đổi giữa thẻ và thiết bị giao diện không nhận biết lẫn nhau ngoại trừ cả hai tuân theo tiêu chuẩn này. Dịch vụ thẻ là kết quả từ sự kết hợp của các byte lịch sử (xem 12.1.1), nội dung của EF.DIR và EF.ATR/INFO (xem 12.2.1 và 12.2.2) và chuỗi các lệnh. Trừ khi có quy định khác, mỗi APDU lệnh sử dụng CLA đặt là '00', nghĩa là 0 nối chuỗi lệnh, không thông điệp an toàn và kênh lô-gic cơ sở.

Một ứng dụng không cần thiết phải tuân theo điều này khi nó đã được định danh và lựa chọn trong thẻ. Một ứng dụng có thể sử dụng các cơ chế khác thích hợp với tiêu chuẩn này để đạt được các hàm tương tự. Vì vậy, các giải pháp như vậy có thể không đảm bảo được sự trao đổi.

Thông tin liên ngành cũng có thể được phục hồi bằng các lệnh được gửi trên kênh lô-gic bổ sung hơn là kênh lô-gic cơ sở. Hơn nữa, trong các lệnh như vậy, bất kỳ N_e nào cũng có thể được sử dụng. Câu lệnh này liên quan với đoạn trước cũng như sự truy tìm thông tin trong 12.1.1.1, 12.1.2, 12.2.1, 12.2.2 và 12.4.

12.1 Nhận dạng thẻ

Dịch vụ này cho phép thiết bị giao diện định danh thẻ và xử lý thẻ. Các byte lịch sử (xem 12.1.1) cung cấp hỗ trợ chung đối với định danh thẻ. Thẻ cung cấp thông tin với mọi đối tượng bên ngoài trên nội dung lô-gic của nó trực tiếp, ví dụ thông qua byte dữ liệu dịch vụ thẻ (xem Bảng 116), và/hoặc gián tiếp, ví dụ thông qua dữ liệu truy cập ban đầu (xem 12.1.1.6) biểu thị truy cập với tệp được lựa chọn ẩn ngay sau hỗ trợ giao diện vật lý (xem 5.1). Do đó, dữ liệu có sẵn tại điểm này, nghĩa là chuỗi dữ liệu ban đầu (xem 12.1.12) có thể không truy tìm được.

12.1.1 Byte lịch sử

12.1.1.1 mục đích và truy tìm

Các byte lịch sử (chuỗi của lên tới 15 byte, như được xác định trong TCVN 11167-3 (ISO/IEC 7816-3)) biểu thị các đặc tính hoạt động của thẻ. Khi thẻ hồi đáp để thiết lập lại, Answer-to-Reset có thể bao gồm các byte lịch sử.

Khi giao diện vật lý không cho phép thẻ hồi đáp để thiết lập lại, ví dụ nếu nó được truy cập bằng đường truyền dẫn tuần tự đa năng hoặc bằng tần số radio, lệnh GET DATA (xem 11.4.3) có thể truy tìm.

- Byte lịch sử là giá trị của DO'5F52'. APDU lệnh là '00CA 5F52 0F'. Đối với sử dụng thực tế, DO'5F52' thuộc về khuôn mẫu hiện hành sau khi hỗ trợ giao diện vật lý (xem 5.1).
- Answer-to-Reset là giá trị của DO'5F51'. APDU lệnh là '00CA 5F52 20'. Đối với sử dụng thực tế, DO'5F51' thuộc về khuôn mẫu hiện hành sau khi hỗ trợ giao diện vật lý (xem 5.1).

12.1.1.2 Cấu trúc và đối tượng dữ liệu COMPACT-TLV

Byte lịch sử đầu tiên là "Byte chỉ dẫn hạng mục". Nếu Byte chỉ dẫn hạng mục được đặt là '00' hoặc '8X', khi đó Bảng 114 tóm tắt định dạng của các byte lịch sử. Giá trị bất kỳ khác biểu thị định dạng độc quyền.

Nếu byte lịch sử đầu tiên được đặt là:

- '00' byte lịch sử còn lại phải bao gồm các đối tượng dữ liệu COMPACT-TLV theo sau bằng chỉ báo trạng thái bắt buộc (xem 12.1.1.11).

- '80' byte lịch sử còn lại phải bao gồm các đối tượng dữ liệu COMPACT-TLV liên tiếp tùy chọn; byte cuối cùng có thể chuyển chỉ báo trạng thái trong định dạng COMPACT-TLV (xem 12.1.1.11).

DO liên ngành bất kỳ bao gồm một trường thẻ được đặt là '4X', trường độ dài được đặt là '0Y' và trường giá trị của byte Y có thể được chuyển đổi thành đối tượng dữ liệu COMPACT-TLV bao gồm một byte được đặt là 'XY' được gọi là "tiêu đề compac" và trường giá trị của byte Y.

Phần tử dữ liệu liên ngành bất kỳ được xác định sau đây (xem 12.1.1.3 đến 12.1.1.10) có thể xuất hiện trong EF.ATR/INFO (xem 12.2.2). Nếu xuất hiện trong EF.ATR/INFO, nó phải xuất hiện trong DO, nghĩa là trường thẻ được đặt là '4X', trường độ dài được đặt là '0Y' và trường giá trị của byte Y.

Bảng 114 - Byte chỉ dẫn hạng mục

Giá trị	Ý nghĩa
'00'	Chỉ báo trạng thái phải xuất hiện là ba byte lịch sử cuối cùng (xem 12.1.1.11)
'80'	Chỉ báo trạng thái có thể xuất hiện trong đối tượng dữ liệu COMPACT-TLV (một, hai hoặc ba byte, xem 12.1.1.11)
'81' tới '8F'	RFU
– Mọi giá trị khác biểu thị định dạng độc quyền	

12.1.1.3 Chỉ báo người phát hành hoặc nước

Được tham chiếu bằng tiêu đề compact được đặt là hoặc '1Y' hoặc '2Y', phần tử dữ liệu liên ngành này là chỉ báo người phát hành hoặc nước (xem thẻ '41' và '42' trong Bảng 16). Bảng 115 thể hiện chỉ báo người phát hành hoặc nước

Bảng 115 - Chỉ báo người phát hành hoặc nước

Tiêu đề compact	Giá trị
'1Y'	Mã nước (xem ISO 3166-1) và dữ liệu quốc gia tùy chọn
'2Y'	Số định danh người phát hành (xem ISO/IEC 7812-1) và dữ liệu người phát hành tùy chọn

Chỉ báo nước bao gồm mã nước (ba nhóm bốn có giá trị từ '0' tới '9', xem ISO 3166-1) theo sau bởi dữ liệu tiếp theo (ít nhất một nhóm bốn). Cơ quan tiêu chuẩn hóa quốc gia liên quan phải chọn các dữ liệu tiếp theo này (số lẻ của nhóm bốn)

Chỉ báo người phát hành bao gồm số định danh người phát hành (xem ISO/IEC 7812-1) có thể theo sau bởi dữ liệu tiếp theo. Người phát hành thẻ phải chọn các byte tiếp theo này nếu có (để mã hóa, ví dụ số tài khoản ban đầu).

CHÚ THÍCH Trong ISO/IEC 7812-1:1993, số định danh người phát hành có thể bao gồm một số lẻ của nhóm bốn có giá trị từ '0' tới '9'. Khi đó nó được ánh xạ vào chuỗi byte bằng cách thiết lập các bit b4 tới b1 của byte cuối cùng đến 1111.

12.1.1.4 Định danh ứng dụng

Được tham chiếu bởi tiêu đề compact được đặt là 'FY', phần tử dữ liệu liên ngành này là một định danh ứng dụng (AID, xem 12.2.3, xem thẻ '4F' trong Bảng 16). Nếu xuất hiện trong byte lịch sử hoặc trong chuỗi dữ liệu ban đầu (xem 12.1.2), một AID biểu thị một ứng dụng được lựa chọn ẩn (xem 12.2.5.1).

12.1.1.5 Dữ liệu dịch vụ thẻ

Được tham chiếu bởi tiêu đề compact được đặt là '31', phần tử dữ liệu liên ngành này biểu thị phương pháp có sẵn trong thẻ để hỗ trợ dịch vụ được mô tả trong điều 12. Bảng 116 thể hiện byte dữ liệu thẻ. Nếu xuất hiện trong byte lịch sử hoặc trong chuỗi dữ liệu ban đầu (xem 12.1.2), byte dữ liệu dịch vụ thẻ biểu thị liệu EF.DIR và/hoặc EF.ATR/INFO (xem 12.2.1 và 12.2.2) xuất hiện hay không, và làm thế nào để truy cập được chúng. Sự không xuất hiện của byte dữ liệu dịch vụ thẻ trong byte lịch sử và trong chuỗi dữ liệu ban đầu biểu thị rằng thẻ chỉ hỗ trợ lựa chọn ứng dụng ẩn (giá trị mặc định).

12.1.1.6 Dữ liệu truy cập ban đầu

Được tham chiếu bởi tiêu đề compact được đặt là '4Y', phần tử dữ liệu liên ngành này biểu thị một APDU lệnh được giả định là lệnh đầu tiên sau khi hỗ trợ giao diện vật lý (xem 5.1). APDU lệnh được xác định trong 12.1.2.

12.1.1.7 Dữ liệu của người phát hành thẻ

Được tham chiếu bởi tiêu đề compact được đặt là '5Y', phần tử dữ liệu liên ngành này không được xác định trong ISO/IEC 7816. Người phát hành thẻ xác định độ dài, cấu trúc và mã hóa.

Bảng 116 - Mã hóa byte dữ liệu dịch vụ thẻ

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	-	-	-	-	-	-	Lựa chọn ứng dụng
1	-	-	-	-	-	-	-	- theo tên DF đầy đủ
-	1	-	-	-	-	-	-	- theo tên DF một phần
-	-	x	x	-	-	-	-	DO có sẵn
-	-	1	-	-	-	-	-	- trong EF.DIR (xem 12.2.1)
-	-	-	1	-	-	-	-	- trong EF.ATR/INFO (xem 12.2.2)
-	-	-	-	x	x	x	-	Dịch vụ truy cập EF.DIR và EF.ATR/INFO
-	-	-	-	1	0	0	-	- bằng lệnh READ BINARY (cấu trúc trong suốt)
-	-	-	-	0	0	0	-	- bằng lệnh READ RECORD (cấu trúc bản ghi)
-	-	-	-	0	1	0	-	- bằng lệnh GET DATA (cấu trúc BER-TLV)
-	-	-	-	Mọi giá trị khác			-	RFU
-	-	-	-	-	-	-	0	Thẻ có MF
-	-	-	-	-	-	-	1	Thẻ không có MF

12.1.1.8 Dữ liệu trước khi phát hành

Được tham chiếu bởi tiêu đề compact được đặt là '6Y', phần tử dữ liệu liên ngành này không được xác định trong TCVN 11167 (ISO/IEC 7816). Nhà sản xuất thẻ xác định độ dài, cấu trúc và mã hóa đối với nhà sản xuất thẻ, tên mạch tích hợp, nhà sản xuất mạch tích hợp, phiên bản che ROM, phiên bản hệ thống hoạt động, vv. Phần tử dữ liệu liên ngành này có thể bao gồm định danh nhà sản xuất mạch tích hợp (xem TCVN 11167-6 (ISO/IEC 7816-6)).

12.1.1.9 Khả năng thẻ

Được tham chiếu bởi tiêu đề thẻ được đặt là '71', '72' hoặc '73', phần tử dữ liệu liên ngành này bao gồm đến ba Bảng chức năng phần mềm. Nếu độ dài của phần tử dữ liệu là

- Một byte, khi đó phần tử dữ liệu phải bao gồm Bảng chức năng phần mềm đầu tiên (xem Bảng 117).
- 2 byte, khi đó phần tử dữ liệu phải bao gồm Bảng chức năng phần mềm đầu tiên là byte đầu tiên (xem Bảng 117) và Bảng chức năng phần mềm thứ hai là byte thứ hai (xem Bảng 118).
- Ba byte, khi đó phần tử dữ liệu phải bao gồm Bảng chức năng phần mềm đầu tiên là byte đầu tiên (xem Bảng 117) và Bảng chức năng phần mềm thứ hai là byte thứ hai (xem Bảng 118) và Bảng chức năng phần mềm thứ ba là byte thứ ba (xem Bảng 119).

Nội dung của Bảng chức năng phần mềm:

- Bảng chức năng phần mềm đầu tiên biểu thị phương pháp lựa chọn được hỗ trợ bằng thẻ.
- Bảng chức năng phần mềm thứ hai là "byte mã hóa dữ liệu". Byte mã hóa dữ liệu cũng có thể xuất hiện là byte thứ hai trong CP tệp được tham chiếu bằng thẻ '82' (xem Bảng 10).
- Bảng chức năng phần mềm thứ ba biểu thị khả năng tạo chuỗi các lệnh, để xử lý trường L_e và L_c mở rộng và để quản lý kênh lô-gic.

Bảng 117 - Mã hóa Bảng chức năng phần mềm đầu tiên (phương pháp lựa chọn)

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	x	x	x	-	-	-	Lựa chọn DF (xem 7.3)
1	-	-	-	-	-	-	-	- theo tên DF đầy đủ
-	1	-	-	-	-	-	-	- theo tên DF một phần
-	-	1	-	-	-	-	-	- theo đường dẫn
-	-	-	1	-	-	-	-	- theo định danh tệp
-	-	-	-	1	-	-	-	Lựa chọn DF ẩn
-	-	-	-	-	1	-	-	Định danh EF ngắn được hỗ trợ
-	-	-	-	-	-	1	-	Số bản ghi được hỗ trợ
-	-	-	-	-	-	-	1	Định danh bản ghi được hỗ trợ

Bảng 118 - Mã hóa Bảng chức năng phần mềm thứ hai (byte mã hóa dữ liệu)

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
1	-	-	-	-	-	-	-	EF của cấu trúc BER-TLV được hỗ trợ
-	x	x	-	-	-	-	-	Chế độ của hàm ghi
-	0	0	-	-	-	-	-	- Ghi một lần
-	0	1	-	-	-	-	-	- Độc quyền
-	1	0	-	-	-	-	-	- Ghi OR
-	1	1	-	-	-	-	-	- Ghi AND
-	-	-	-	x	x	x	x	Kích cỡ đơn vị dữ liệu trong nhóm bốn (từ một tới 32 768 nhóm bốn, nghĩa là 16 384 byte) (lũy thừa của 2, ví dụ, 0001 = 2 nhóm bốn = một byte, giá trị mặc định)
-	-	-	x	-	-	-	-	Giá trị 'FF' đối với byte đầu tiên của trwongf thẻ BER-TLV (xem 8.1.1)
-	-	-	0	-	-	-	-	- không có hiệu lực (được sử dụng để đệm, giá trị mặc định)
-	-	-	1	-	-	-	-	- có hiệu lực (thẻ riêng dài, mã hóa được xây dựng)

Bảng 119 - Mã hóa Bảng chức năng phần mềm thứ ba

(tạo chuỗi lệnh, trường độ dài và kênh lô-gic)

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
1	-	-	-	-	-	-	-	Tạo chuỗi lệnh (xem 5.3.3)
-	1	-	-	-	-	-	-	Trường L_c và L_e mở rộng (xem 5.1)
-	-	1	-	-	-	-	-	Thông tin độ dài mở rộng trong EF.ATR/INFO
-	-	-	x	x	-	-	-	Phép gán số kênh lô-gic (xem 5.4.2 và 11.1)
-	-	-	1		-	-	-	- theo thẻ
-	-	-		1		-	-	- theo thiết bị giao diện
-	-	-	0	0	-	-	-	Chỉ kênh lô-gic cơ sở có sẵn
-	-	-	-	-	y	z	t	Số tối đa của kênh lô-gic (xem 5.4.1) – y, z và t không phải tất cả được đặt là 1 có nghĩa 4y+2z+t+1, nghĩa là từ 1 đến bảy – y = z = t = 1 có nghĩa tám hoặc nhiều hơn

12.1.1.10 Định danh nhóm ứng dụng

Được tham chiếu bởi tiêu đề compact được đặt là '91', phần tử dữ liệu liên ngành này bao gồm một byte được xác định trong ISO/IEC 14443-3.

12.1.1.11 Chỉ báo trạng thái

Nếu Byte chỉ dẫn hạng mục được đặt là '00', khi đó ba byte lịch sử cuối cùng phải là chỉ báo trạng thái, cụ thể là LCS thẻ (1 byte) theo sau bởi 2 byte trạng thái xử lý được biểu thị SW1-SW2.

Nếu Byte chỉ dẫn hạng mục được đặt là '80', khi đó phần tử dữ liệu liên ngành được tham chiếu bởi tiêu đề compact được đặt là '81', '82' hoặc '83' có thể xuất hiện là chỉ báo trạng thái trên một, hai hoặc ba byte (độ dài khác bất kỳ là RFU) tại cuối của byte lịch sử.

- Nếu độ dài là một, khi đó phần tử dữ liệu là LCS thẻ.
- Nếu độ dài là hai, khi đó phần tử dữ liệu là SW1-SW2.
- Nếu độ dài là ba, khi đó phần tử dữ liệu là LCS theo sau bởi SW1-SW2.

LCS phải được giải thích theo 7.4.10 và Bảng 14; giá trị '00' biểu thị rằng trạng thái không được ghi lại. SW1-SW2 phải được giải thích theo 5.6, Bảng 5 và Bảng 6; giá trị '0000' biểu thị rằng trạng thái không được báo cáo.

12.1.2 Phục hồi chuỗi dữ liệu ban đầu

Được tham chiếu bởi tiêu đề compact được đặt là '4Y' trong byte lịch sử (xem 12.1.1) hoặc theo thẻ '44' trong EF.ATR/INFO (xem 12.2.2), phần tử dữ liệu liên ngành được gọi là "dữ liệu truy cập ban đầu" biểu thị một APDU lệnh.

- Nếu độ dài là một, khi đó APDU lệnh là một lệnh READ BINARY (xem 11.2.3) như sau: CLA INS P1 P2 được đặt là '00B0 0000' và một trường L_e được đặt là chỉ một byte đầu tiên của dữ liệu truy cập ban đầu.
- Nếu độ dài là hai, khi đó byte đầu tiên của dữ liệu truy cập ban đầu biểu thị cấu trúc (bit b8) và định danh EF ngắn (bit b5 tới b1) của EF để đọc, theo Bảng 120.
- Nếu bit 8 của byte đầu tiên được đặt là 1, khi đó APDU lệnh là lệnh READ BINARY (xem 11.2.3) như sau: CLA INS được đặt là '00B0'. Nếu bit b5 tới b1 được đặt là 00000, khi đó P1 phải được đặt là '00' mặt khác P1 phải được đặt là byte đầu tiên của dữ liệu truy cập ban đầu, P2 được đặt là '00' và trường L_e được đặt là byte thứ hai của dữ liệu truy cập ban đầu.
- Nếu bit 8 của byte đầu tiên được đặt là 0, khi đó APDU lệnh là lệnh READ RECORD (xem 11.3.3) như sau: CLA INS P1 được đặt là '00B2 01', P2 bao gồm bit b8 tới b4 được đặt là bit b5 tới b1 của byte đầu tiên của dữ liệu truy cập ban đầu (biểu thị EF hiện hành hoặc định danh EF ngắn) và bit b3 tới b1 được đặt là 110, và trường L_e được đặt là byte thứ hai của dữ liệu truy cập ban đầu.
- Nếu độ dài là năm hoặc nhiều hơn, khi đó APDU lệnh bao gồm các byte Y của dữ liệu truy cập ban đầu.

APDU lệnh phải được chuyển tới thẻ. Nếu thủ tục hoàn thành, khi đó trường dữ liệu hồi đáp là một chuỗi các DO liên ngành, mỗi ứng dụng có thể có liên quan, được gọi là "chuỗi dữ liệu ban đầu".

Bảng 120 - Mã hóa byte đầu tiên của dữ liệu truy cập ban đầu khi độ dài là hai

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	-	-	-	-	-	-	-	Cấu trúc EF
0	-	-	-	-	-	-	-	Cấu trúc bản ghi
1	-	-	-	-	-	-	-	Cấu trúc trong suốt
-	x	x	-	-	-	-	-	00 (mọi giá trị khác là RFU)
-	-	-	0	0	0	0	0	EF hiện hành
-	-	-	Không phải tất cả bằng nhau					Định danh EF ngắn

12.2 Định danh ứng dụng và lựa chọn

Dịch vụ này cho phép thiết bị giao diện biết ứng dụng nào được thẻ hỗ trợ, nếu có, cũng như làm thế nào để định danh và lựa chọn chúng.

Hai EF cụ thể cung cấp hỗ trợ chung cho lựa chọn và định danh ứng dụng, cụ thể là EF.DIR và EF.ATR/INFO. Chúng bao gồm một tập hợp các DO. Trong các EF này, các DO bị sửa đổi hoặc xóa bỏ có thể tạo phần đệm trước, giữa và sau các DO (xem 8.1.1) trong trường dữ liệu hồi đáp của lệnh READ BINARY/RECORD.

12.2.1 EF.DIR

EF này biểu thị danh sách các ứng dụng được thẻ hỗ trợ. Nó bao gồm một tập hợp các khuôn mẫu ứng dụng (xem 12.2.4) và/hoặc các DO định danh ứng dụng (xem 12.2.3) theo thứ tự bất kỳ. Nó xác định lệnh nào phải được thực hiện để lựa chọn ứng dụng được biểu thị.

Nếu một MF và một EF.DIR xuất hiện, EF.DIR phải có MF làm tệp cha và đường dẫn củ nó là '3F002F00'. Tại mức MF, định danh EF ngắn 30, nghĩa là 11110 trong nhị phân, tham chiếu EF.DIR.

Nếu một MF không xuất hiện, EF.DIR có thể xuất hiện và phải được giải quyết bằng định danh tệp '2F00' sau khi hỗ trợ giao diện vật lý (xem 5.1).

CHÚ THÍCH Lệnh (chuỗi) để truy tìm nội dung phụ thuộc vào cấu trúc của EF.DIR (ví dụ xem Bảng 116) và có thể được nhận biết ẩn bằng ứng dụng trong mọi đối tượng bên ngoài.

Nếu EF.DIR hỗ trợ xử lý DO, hoặc nếu nội dung của nó được lưu giữ trong một tệp, thẻ có thể cung cấp nội dung của nó bằng lệnh GET DATA (xem 11.4.3). dữ liệu hồi đáp đối với lệnh '00CB 2F00 02 5C00' là kết nối của tất cả các DO xuất hiện trong EF.DIR, hoặc phải xuất hiện nếu EF.DIR không thực sự tồn tại.

Nếu thẻ cung cấp dịch vụ này, lệnh phải thành công ít nhất ngay sau khi hỗ trợ giao diện vật lý (xem 5.1).

12.2.2 EF.ATR/INFO

EF biểu thị các đặc tính hoạt động của thẻ. Nó bao gồm một tập hợp các DO liên ngành mà không thể lồng trong EF.DIR, hoặc do không liên quan đến lựa chọn ứng dụng, hoặc do không có EF.DIR.

CHÚ THÍCH EF.ATR/INFO được gọi là EF.ATR trong bản xuất bản trước của tiêu chuẩn này. Do một số thẻ không tiếp xúc không cung cấp ATR, thuật ngữ này bị lầm lẫn trong thế giới thẻ không tiếp xúc. EF.ATR/INFO thuật ngữ mới được khuyến nghị sử dụng. Nó có thể vẫn được gọi là EF.ATR trong đặc tả hoặc tiêu chuẩn thẻ tiếp xúc, và hiện giờ có thể được gọi là EF.INFO trong đặc tả và tiêu chuẩn thẻ không tiếp xúc.

Nếu một MF và một EF.ATR/INFO xuất hiện, EF.ATR/INFO phải có MF là tệp cha và đường dẫn của nó phải là '3F002F01'.

Nếu một MF không xuất hiện, một EF.ATR/INFO có thể được định vị trong một ứng dụng có DF ứng dụng của nó là cha. Định danh tệp của nó phải là '2F01', trừ khi ứng dụng xác định khác.

CHÚ THÍCH lệnh (chuỗi) truy tìm nội dung phụ thuộc vào cấu trúc của EF.ATR/INFO (ví dụ, xem Bảng 116) và có thể được nhận biết ẩn bằng ứng dụng ở mọi đối tượng bên ngoài.

Nếu EF.ATR/INFO hỗ trợ xử lý DO hoặc nếu nội dung của nó không được lưu giữ trong tệp, thẻ có thể cung cấp nội dung của nó bằng lệnh GET DATA (xem 11.4.3). dữ liệu hồi đáp lệnh '00CB 2F01 02

5C00 00' là kết nối của tất cả các DO xuất hiện trong EF.ATR/INFO, hoặc phải xuất hiện nếu EF.ATR/INFO không thực sự tồn tại.

Nếu thẻ cung cấp dịch vụ này, lệnh phải thành công ít nhất ngay sau khi hỗ trợ giao diện vật lý (xem 5.1).

CHÚ THÍCH Thông tin được xuất hiện trong ATR tại hỗ trợ giao diện có thể thay thế cho EF.ATR/INFO hình thành thông tin, nếu xuất hiện.

12.2.3 Định danh ứng dụng

Được tham chiếu bằng tiêu đề compact được đặt là 'FY' trong byte lịch sử (xem 12.1.1.4), hoặc thẻ '4F' trong chuỗi dữ liệu ban đầu (xem 12.1.2), trong EF.ATR/INFO, trong EF.DIR và trong dữ liệu quản lý của DF bất kỳ (xem 7.4), phần tử dữ liệu liên ngành này định danh một ứng dụng.

Một định danh ứng dụng (AID) bao gồm tới mười sau byte. Bit b8 tới b5 của byte đầu tiên biểu thị một hạng mục theo Bảng 121.

Bảng 121- Hạng mục của định danh ứng dụng

Giá trị	Hạng mục	Ý nghĩa
'0' tới '9'	-	Được lưu trữ để tương thích ngược với ISO/IEC 7812-1 (xem phụ lục D)
'A'	Quốc tế	Đăng ký quốc tế của nhà cung cấp ứng dụng theo TCVN 11167-5 (ISO/IEC 7816-5)
'B', 'C'	-	RFU
'D'	Quốc gia	Đăng ký quốc gia (ISO 3166-1) của nhà cung cấp ứng dụng theo TCVN 11167-5 (ISO/IEC 7816-5)
'E'	Tiêu chuẩn	Định danh một tiêu chuẩn bằng định danh đối tượng theo theo ISO/IEC 8825-1
'F'	Độc quyền	Không đăng ký nhà cung cấp ứng dụng

Hình 10 thể hiện một AID quốc tế. Nó bao gồm một định danh nhà cung cấp ứng dụng đăng ký (RID quốc tế) trên 5 byte và tùy chọn, mở rộng ddinjhj danh ứng dụng độc quyền (PIX) trên tới bảy byte.

- RID quốc tế phải định danh duy nhất một nhà cung cấp ứng dụng (xem TCVN 11167-5 (ISO/IEC 7816-5)).
- Bit b8 tới b5 của byte đầu tiên phải được đặt là 1010, nghĩa là nhóm bốn đầu tiên phải được đặt là 'A'.
- Mỗi một trong chin nhóm bốn tiếp theo phải được thiết lập từ '0' tới '9'.
- Mở rộng có một mã hóa tự do. Nó cho phép nhà cung cấp ứng dụng định danh các ứng dụng khác nhau.

Định danh nhà cung cấp ứng dụng đăng ký RID quốc tế, 5 byte, byte đầu tiên được đặt là 'AX'	Mở rộng định danh ứng dụng độc quyền (PIX, tới bảy byte)

Hình 10 - AID quốc tế

Hình 11 thể hiện một AID quốc gia. Nó bao gồm một định danh nhà cung cấp ứng dụng đăng ký (RID quốc gia) trên 5 byte và tùy chọn, mở rộng định danh ứng dụng độc quyền (PIX) trên tới mười một byte.

- RID quốc gia phải định danh duy nhất một nhà cung cấp ứng dụng (xem TCVN 11167-5 (ISO/IEC 7816-5)).
- Bit b8 tới b5 của byte đầu tiên phải được đặt là 1101, nghĩa là nhóm bốn đầu tiên phải được đặt là 'D'.
- Ba nhóm bốn tiếp theo (từ '0' tới '9') phải hình thành mã nước (xem ISO 3166-1).
- Giá trị khuyến nghị của mỗi một trong sáu nhóm bốn cuối cùng là từ '0' tới '9'.
- Mở rộng có một mã hóa tự do. Nó cho phép nhà cung cấp ứng dụng định danh các ứng dụng khác nhau

Mã định danh bên cung cấp ứng dụng đã đăng ký (RID quốc tế, 5 byte, byte đầu đặt là 'AX'	Mở rộng mã định danh ứng dụng độc quyền (PIX, lên tới 11 byte)

Hình 11 - AID quốc gia

Hình 12 thể hiện AID tiêu chuẩn. Nó bao gồm tới 16 byte. Byte đầu tiên phải được đặt là 1110 1000, nghĩa là tới 'E8'. Giá trị 'E0' tới 'E7' và 'E9' tới 'EF' là RFU. Một định danh đối tượng (xem ISO/IEC 8825-1) theo sau để định danh một tiêu chuẩn xác định ứng dụng (xem ví dụ trong phụ lục A, ví dụ, TCVN 11167-11 (ISO/IEC 7816-11), kiểm tra cá nhân bằng phương pháp sinh trắc học, TCVN 11167-15 (ISO/IEC 7816-15), ứng dụng thông tin mật mã). Mở rộng định danh ứng dụng (được xác định theo tiêu chuẩn định danh) có thể theo để định danh hệ thống xử lý khác nhau.

'E8'	Mã định danh đối tượng (xem Phụ lục A)	Mở rộng mã định danh ứng dụng ứng dụng-cụ thể

Hình 12 - AID tiêu chuẩn

Hình 13 thể hiện một AID độc quyền. Nó bao gồm tới mười sau byte. Bit b8 tới b5 của byte đầu tiên phải được đặt là 1111, nghĩa là tới 'F'. Trong hạng mục độc quyền, khi nhà cung cấp ứng dụng không được đăng ký, nhà cung cấp ứng dụng khác có thể sử dụng cùng AID.

Mã định danh đối tượng (AID độc quyền lên tới 16 byte, byte đầu đặt là 'FX'

Hình 13 - AID độc quyền

T - một AID ngắn hơn 5 byte phù hợp với tiêu chuẩn này. Một số hệ thống xử lý có thể yêu cầu AID có ít nhất 5 byte dài. Điều này phải được tính đến khi gán một AID.

12.2.4 Khuôn mẫu ứng dụng và phần tử dữ liệu liên quan

Được tham chiếu bởi thẻ '61', khuôn mẫu liên ngành này có thể xuất hiện trong EF.ATR/INFO (xem 12.2.2), trong EF.DIR (xem 12.2.1) và trong dữ liệu quản lý của DF bất kỳ (xem 7.4).

- Khuôn mẫu như vậy phải bao gồm một và chỉ một định danh ứng dụng. Nếu một vài định danh ứng dụng có tên có hiệu lực đối với cùng DF, khi đó mỗi định danh phải xuất hiện trong khuôn mẫu ứng dụng khác nhau.
- Khuôn mẫu như vậy có thể tùy chọn bao gồm các DO liên ngành khác liên quan đến ứng dụng như được liệt kê trong Bảng 122 và được xác định sau đây.

Bảng 122 - DO liên ngành đối với lựa chọn và định danh ứng dụng

Thẻ	Giá trị	
'4F'	Định danh ứng dụng	
'50'	Nhãn ứng dụng	
'51'	Tham chiếu tệp	
'52'	APDU lệnh	
'53', '73'	Dữ liệu tùy chọn, khuôn mẫu tùy chọn	
'5F50'	Bộ định vị nguồn đồng nhất (xem IETF RFC 1738 và IETF RFC 2396	
'61'	Tập hợp các DO liên quan đến ứng dụng	
	'79'	Dưới DO'61' DO này biểu thị kế hoạch phân bổ thẻ cùng tồn tại

Các phần tử dữ liệu liên ngành sau cung cấp hỗ trợ chung cho lựa chọn và định danh ứng dụng.

Nhãn ứng dụng - được tham chiếu bằng thẻ '50', phần tử dữ liệu liên ngành không được xác định trong ISO/IEC 7816. Nhà cung cấp ứng dụng xác định nó để sử dụng tại giao diện người-máy, ví dụ nhãn hiệu để thể hiện.

Tham chiếu tệp - được tham chiếu bằng thẻ '51' (xem 7.3.2)

Dữ liệu tùy ý (hoặc khuôn mẫu) - được tham chiếu bằng thẻ '53' (hoặc '73'), phần tử dữ liệu liên ngành (hoặc khuôn mẫu) bao gồm các phần tử dữ liệu liên quan (hoặc lồng các DO) được xác định bởi nhà cung cấp ứng dụng.

Bộ định vị nguồn đồng nhất - được tham chiếu bởi thẻ '5F50', phần tử dữ liệu liên ngành này là một bộ định vị nguồn đồng nhất (URL) như được xác định trong IETF RFC 1738 và IETF RFC 2396. Nó hướng vào phần phần mềm được yêu cầu trong thiết bị giao diện để kết nối với ứng dụng trong thẻ.

12.2.5 Lựa chọn ứng dụng

Thẻ phải hỗ trợ ít nhất một trong các phương pháp lựa chọn ứng dụng sau.

1) Lựa chọn ứng dụng ẩn
2) Lựa chọn ứng dụng sử dụng định danh ứng dụng (AID, xem 12.2.3) là tên DF
3) Lựa chọn ứng dụng sử dụng EF.DIR hoặc EF.ATR/INFO

12.2.5.1 Lựa chọn ứng dụng ẩn

Nếu một ứng dụng được lựa chọn ẩn là kết quả của hỗ trợ giao diện vật lý, khi đó định danh ứng dụng phải xuất hiện trong byte lịch sử (xem 12.1.1) hoặc trong chuỗi dữ liệu ban đầu (xem 12.1.2). Sự xuất hiện như vậy biểu thị một ứng dụng được lựa chọn ẩn. Nếu một ứng dụng được lựa chọn ẩn mà không có định danh ứng dụng trong byte lịch sử và trong chuỗi dữ liệu ban đầu, khi đó định danh ứng dụng phải xuất hiện trong EF.ATR/INFO (xem 12.2.2).

12.2.5.2 Lựa chọn ứng dụng sử dụng AID là tên DF

Thẻ đa ứng dụng phải hỗ trợ lệnh SELECT với P1='04', P2='00' và trường dữ liệu bao gồm 5 tới 16 byte có AID của ứng dụng có thể thường trú trên thẻ. Lệnh phải hoàn thành thành công nếu ADI của ứng dụng thẻ giữ phù hợp với trường dữ liệu.

Nếu khả năng thẻ (xem 12.1.1.9 và Bảng 117) xác định thẻ hỗ trợ lựa chọn bằng AID cắt cụt, nó phải hỗ trợ lệnh SELECT với P1='04', P2='00' hoặc '02'. Trong trường hợp này, lệnh phải hoàn thành thành công nếu phần đầu tiên của AID của ứng dụng bất kỳ nó giữ, phù hợp với trường dữ liệu. Nếu có nhiều AID trong thẻ phù hợp dữ liệu đầu vào, thứ tự mà trong đó mỗi ứng dụng này thực sự được lựa chọn sau khi hoàn thành lệnh, phụ thuộc vào hệ thống xử lý. Nếu lệnh hoàn thành thành công với AID phù hợp một phần, nó phải phục hồi toàn bộ AID của ứng dụng được lựa chọn trong điều khiển tệp hoặc dữ liệu quản lý (là DO'84' hoặc DO'4F').

Thẻ có thể hỗ trợ cơ chế cho một ứng dụng để xác định yêu cầu đối với sự phù hợp hoàn toàn của AID để được lựa chọn thành công. Lệnh SELECT phải thất bại nếu AID ứng dụng phù hợp với AID cắt cụt khi do chỉ có ứng dụng có thể lựa chọn được trong thẻ, hoặc bỏ qua ứng dụng nếu các AID ứng dụng khác phù hợp và có thể được lựa chọn.

CHÚ THÍCH Thứ tự mà theo đó các ứng dụng trong thẻ được lựa chọn bằng lệnh SELECT liên tiếp với P1='02' có thể tĩnh hoặc động, ví dụ, dựa trên đó ứng dụng được lựa chọn gần nhất trong phiên bản trước.

Trong thẻ nhiều ứng dụng, một ứng dụng trong thẻ phải được định danh bằng

- AID đơn trong hạng mục độc quyền, quốc gia hoặc quốc tế, và/hoặc
- Một hoặc nhiều AID trong hạng mục tiêu chuẩn

Nếu ứng dụng được lựa chọn bằng cách xác định một AID trong hạng mục tiêu chuẩn, AID được phục hồi bằng lệnh SELECT là AID trong hạng mục độc quyền, quốc gia hoặc quốc tế, nếu AID như vậy được xác định đối với ứng dụng.

12.2.5.3 Lựa chọn ứng dụng sử dụng EF.DIR hoặc EF.ATR/INFO

Đối với thiết bị giao diện nhiều ứng dụng, sử dụng EF.DIR hoặc EF.ATR/INFO có thể hữu hiện hơn phương pháp trước.

- Nếu một DO định danh ứng dụng không phải là một phần của khuôn mẫu ứng dụng và không kết hợp với một tham chiếu tệp hoặc DO lệnh để thực hiện, khi đó lựa chọn phải sử dụng AID là tên DF.
- Nếu một DO định danh ứng dụng là một phần của khuôn mẫu ứng dụng cùng với một DO tham chiếu tệp (xem 7.3.2), trường giá trị của cái bao gồm hai hoặc nhiều byte, khi đó lựa chọn bằng đường dẫn phải được thực hiện theo 12.3.

- Nếu một DO định danh ứng dụng là một phần của khuôn mẫu ứng dụng cùng với một hoặc nhiều DO lệnh để thực hiện, khi đó lựa chọn ứng dụng được thực hiện bằng lệnh biểu thị. Nếu có một số lệnh, chúng phải được thực hiện theo thứ tự xuất hiện trong khuôn mẫu.

12.3 Lựa chọn bằng đường dẫn

Dịch vụ này cho phép lựa chọn EF và DF có định danh tệp bằng cách sử dụng đường dẫn, nghĩa là DO tham chiếu tệp (xem 7.3.2) bao gồm ba hoặc nhiều byte.

- Khi độ dài là số chẵn, đường dẫn hoặc là tuyệt đối hoặc là tương đối phụ thuộc vào liệu 2 byte đầu tiên được đặt là '3F00' hay không. 2 byte cuối cùng định danh hoặc DF hoặc EF.
- Đối với đường dẫn tới DF, lựa chọn phải được thực hiện bằng một hoặc nhiều lệnh SELECT, với CLA INS P1 P2 L_c được đặt là '00A4 0100 02'.
- Đối với đường dẫn tới EF, nếu độ dài là bốn hoặc nhiều hơn, lựa chọn phải được thực hiện bằng một hoặc nhiều lệnh SELECT, với CLA INS P1 P2 L_c được đặt là '00A4 0100 02'. Lựa chọn cuối cùng và có thể duy nhất sử dụng 2 byte cuối cùng của đường dẫn (một định danh EF) với CLA INS P1 P2 L_c được đặt là '00A4 0200 02'.
- Khi độ dài là số lẻ, đường dẫn được định tính. Nó bao gồm hoặc đường dẫn tuyệt đối không có '3F00', hoặc đường dẫn tương đối không có định danh của DF hiện hành, được theo sau bởi một byte sử dụng là P1 trong một hoặc nhiều lệnh SELECT. Giá trị của P1 cố định phương pháp lựa chọn.
- Nếu giá trị của P1 là '08' hoặc '09', khi đó thẻ phải hỗ trợ lệnh SELECT khi đường dẫn định tính xác định P1, L_c và trường dữ liệu và P2 được đặt là '00'.
- Nói cách khác, thẻ phải hỗ trợ một hoặc nhiều lệnh SELECT với P1 được đặt là byte cuối cung của đường dẫn định tính và P2 L_c được đặt là '0002'. Mỗi tệp cùng với đường dẫn phải được lựa chọn liên tục.

12.4 Truy tìm dữ liệu

Dịch vụ này cho phép thiết bị giao diện truy tìm phần tử dữ liệu liên ngành được sử dụng cho trao đổi, trước khi lựa chọn một ứng dụng. Các DO liên ngành phải được truy tìm trực tiếp hoặc gián tiếp từ các byte lịch sử (xem 12.1.1), chuỗi dữ liệu ban đầu (xem 12.1.2), EF. ATR/INFO (xem 12.2.2) và EF.DIR (xem 12.2.1), theo thứ tự khi xuất hiện. Các DO liên ngành này phải được giải thích theo kế hoạch phân bổ thẻ (xem 8.3). Các tiêu chuẩn được quyền khuyến nghị hoặc chỉ báo truy tìm các DO liên ngành bằng lệnh GET DATA (xem 11.4.3).

12.5 Chuỗi byte có nguồn gốc từ thẻ

Dịch vụ này cho phép thẻ phát xuất chuỗi byte. Điều này xác định câu hỏi khi (một phần của) chuỗi byte có nguồn gốc từ thẻ và hồi đáp khi (một phần của) chuỗi byte hồi đáp được gửi bằng thực thể ở mọi đối tượng bên ngoài; ví dụ, một tập hợp hoàn chỉnh các câu hỏi có thể hình thành APDU lệnh và một tập hợp hoàn chỉnh các APDU hồi đáp hồi đáp, do vậy cho phép kết nối dịch vụ từ thẻ tới thiết bị giao diện và đồng thời từ thẻ tới thẻ, có thể bằng mạng lưới.

Điều này xác định ba đặc tính sau.

- Làm thế nào thẻ sử dụng SW1-SW2 làm cơ cấu khởi động biểu thị rằng thẻ muốn ban hành câu hỏi, mà theo đó thẻ có thể mong đợi câu hỏi đáp.
- Làm thế nào thiết bị giao diện sử dụng lệnh GET DATA với mã INS chẵn (xem 11.4.3) để truy tìm câu hỏi từ thẻ và lệnh PUT DATA với mã INS chẵn (xem 11.4.6) để truyền câu hỏi đáp, nếu có, tới thẻ. Các lệnh GET DATA và PUT DATA phải thiết lập P1-P2 tới '0000' (xem Bảng 85).
- Câu hỏi và hồi đáp được định dạng như thế nào

12.5.1 Khởi động bằng thẻ

SW1-SW2 được đặt là '62XX' có giá trị của 'XX' từ '02' tới '80' có nghĩa rằng thẻ có câu hỏi của byte 'XX', thiết bị giao diện phải truy tìm và thẻ mong đợi câu hỏi đáp.

SW1-SW2 được đặt là '64XX' có giá trị của 'XX' từ '02' tới '80' có nghĩa rằng thẻ đã hủy lệnh; khả năng hoàn thành của lệnh phụ thuộc vào sự phục hồi của câu hỏi của byte 'XX' mà thẻ mong đợi câu hỏi đáp.

Nếu xuất hiện trong byte lịch sử có giá trị như ở trên, SW1-SW2 phải được giải thích như ở trên.

Nếu lệnh PUT DATA (xem 12.5.1, gạch ngang 2) để truyền một câu hỏi đáp bị hủy với SW1-SW2 được đặt là '64XX', khi đó

- Với '64XX' từ '6402' tới '6480', thẻ muốn gửi ít nhất một hoặc nhiều câu hỏi của byte 'XX';
- Với '64XX' được đặt là '6401', thẻ mong đợi câu hỏi đáp ngay lập tức.

12.5.2 Câu hỏi và hồi đáp

Để truy tìm một câu hỏi của byte 'XX' có sẵn trong thẻ, thiết bị giao diện phải gửi một lệnh GET DATA với INS được đặt là 'CA', P1-P2 được đặt là '0000' và trường L_e được đặt là 'XX'.

- SW1-SW2 được đặt là '62XX' có giá trị 'XX' từ '02' tới '80' nghĩa là thiết bị giao diện phải truy tìm hơn nữa câu hỏi của byte 'XX' và kết nối nó với câu hỏi đã truy tìm rồi trước khi xử lý chuỗi byte có nguồn gốc từ thẻ ở mọi đối tượng bên ngoài.
- SW1-SW2 được đặt là '9000' có nghĩa là chuỗi byte có nguồn gốc từ thẻ được hoàn thành; nó có thể được xử lý ở mọi đối tượng bên ngoài.

Để truyền một câu hỏi đáp tới thẻ, thiết bị giao diện phải gửi một lệnh PUT DATA với INS được đặt là 'DA', và P1-P2 được đặt là '0000'. Nếu chuỗi byte hồi đáp quá dài đối với một lệnh đơn, khi đó một số lệnh PUT DATA phải được kết chuỗi (xem 5.3.3). Mỗi lệnh PUT DATA truyền một câu hỏi đáp và kết nối của các câu hỏi đáp là chuỗi byte hồi đáp.

12.5.3 Định dạng

Giá trị của byte đầu tiên của chuỗi byte có nguồn gốc từ thẻ biểu thị định dạng như sau.

- Nếu byte đầu tiên được đặt là 'FF', khi đó các byte tiếp theo phải mã hóa định danh giao thức ban đầu theo ISO/IEC TR 9577; chuỗi byte phải tuân theo giao thức được biểu thị.
- Mặt khác (nghĩa là khi byte đầu tiên không được đặt là 'FF'), chuỗi byte có nguồn gốc từ thẻ cùng với câu hỏi đáp phải hình thành một C-RP.

Tất cả các điều kiện liên quan đến giao thức truyền do thẻ biểu thị, ngoại trừ sử dụng riêng lệnh GET DATA, lệnh PUT DATA và byte trạng thái SW1-SW2. Điều này không giả định về nhu cầu đối với câu hỏi đáp và trên thực thể chịu trách nhiệm về nội dung của câu hỏi đáp có khả năng.

12.6 Quản lý đặc tính chung

Dịch vụ này cho phép thẻ thông báo mọi đối tượng bên ngoài về các đặc tính hiện có trên thẻ theo một cách thức chung. Khuôn mẫu (DO'7F74') có khả năng mở rộng trong tương lai bằng cách thêm khuôn mẫu con bổ sung được định vị trong thẻ, ví dụ trong EF.ATR/INFO (xem 12.2.2) và/hoặc trong FCI của DF ứng dụng bất kỳ. Nhìn chung, thông tin có thể áp dụng với tất cả các ứng dụng. Các giá trị được xác định trong FCI ứng dụng chỉ áp dụng với ứng dụng đó, các giá trị có khả năng thay thế được xác định trong EF.ATR/INFO. EF.ATR/INFO hoặc một FCI ứng dụng phải không bao gồm nhiều phiên bản của DO'7F74'. Thông tin có thể được truy tìm bằng cách đọc EF.ATR/INFO hoặc trong trường dữ liệu hồi đáp của một lệnh lựa chọn ứng dụng.

Dịch vụ này hỗ trợ truy tìm thông tin cô đọng về các ứng dụng và đặc tính được cài đặt. Thiết bị giao diện có thể truy tìm thông tin bổ sung về các ứng dụng và đặc tính được cài đặt như được xác định theo các tiêu chuẩn khác.

12.6.1 Các dịch vụ trên thẻ

Dịch vụ này cho phép thẻ thông báo mọi đối tượng bên ngoài về các đặc tính hiện có trên thẻ. Được lồng trong khuôn mẫu quản lý đặc tính, khuôn mẫu con này bao gồm một chuỗi các nhóm tám liên tiếp của các bit. Mỗi bit biểu thị một đặc tính/cơ chế trên thẻ. Một bit tập hợp biểu thị sự tồn tại của đặc tính này trên thẻ. Bảng 123 thể hiện các dịch vụ trên thẻ đã được xác định trước.

12.6.2 Dịch vụ giao diện

Các tiêu chuẩn quốc tế xác định tính đa dạng lớn của các giao diện có thể hoạt động song song. Cơ chế giao tiếp của mỗi giao thức không đưa ra bất kỳ khả năng nào biểu thị sự tồn tại và sử dụng song song của nhiều giao diện. Khuôn mẫu con này trong khuôn mẫu quản lý đặc tính đưa ra thông tin về các giao thức đang tồn tại và cách thức xử lý giao tiếp (xem Bảng 123).

Bảng 123 - Khuôn mẫu đối với DO'7F74' quản lý đặc tính

Thẻ	Độ dài	Ý nghĩa								
'81'	Thay đổi	Định danh khuôn mẫu con đối với dịch vụ trên thẻ								
		Danh sách đặc tính [0..n], có thể mở rộng								
		b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa của các bit trong byte đầu tiên
		1	-	-	-	-	-	-	-	Hiển thị
		-	1	-	-	-	-	-	-	Cảm biến đầu vào sinh trắc
		-	-	x	x	x	x	x	x	000000 (mọi giá trị khác là RFU)

'82'	Thay đổi	Định danh khuôn mẫu con đối với dịch vụ giao diện								
		Danh sách đặc tính giao tiếp [0..n], có thể mở rộng								
		b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa của các bit trong byte đầu tiên
		1	-	-	-	-	-	-	-	Sử dụng đồng thời của giao diện biểu thị có khả năng
		0	-	-	-	-	-	-	-	Kích hoạt tối đa một trong các giao diện biểu thị có khả năng
		-	-	-	-	-	-	-	1	T=0 theo TCVN 11167-3 (ISO/IEC 7816-3)
		-	-	-	-	-	-	1	-	T=1 theo TCVN 11167-3 (ISO/IEC 7816-3)
		-	-	-	-	-	1	-	-	Không tiếp xúc theo ISO/IEC 14443
		-	-	-	-	1	-	-	-	USB theo ISO/IEC 7816-12
		-	-	-	1	-	-	-	-	SWP theo ETSI TS 102 613, TS 102 622
		-	x	x	-	-	-	-	-	00 (mọi giá trị khác là RFU)

12.6.3 Dịch vụ tiết diện

Tiêu chuẩn này xác định dịch vụ cắt ngắn đối với các ứng dụng, ví dụ, lựa chọn ứng dụng bằng AID hoặc đường dẫn (xem 12.2.5.2 và 12.3). Nhiều ứng dụng, đặc biệt hỗ trợ phiên bản di sản, phải cung cấp vi mạch phần cứng khác nhau có sự đa dạng các đặc tính. Thiết bị cuối của các ứng dụng này cần định danh ứng dụng và tập hợp đặc tính có khả năng của thẻ theo phương thức rất nhanh.

Định danh này được cung cấp bằng dịch vụ tiết diện, ví dụ trong một EF.DIR

Bảng 124 - DO liên ngành đối với định danh tiết diện ứng dụng

Thẻ	Giá trị
'73'	Chỉ báo tiết diện ứng dụng

12.6.4 Cung cấp thông tin bổ sung

Thông tin chi tiết trên ví dụ, ngoại vi hoặc giao thức có thể xuất hiện trong khuôn mẫu quản lý đặc tính chung. Thông tin này phải được cung cấp trong DO được xây dựng có thẻ trong lớp ngữ cảnh cụ thể. Thẻ và nội dung có thể được xác định trong các đặc tả hoặc tiêu chuẩn khác.

12.7 Quản lý APDU

12.7.1 Thông tin độ dài mở rộng

Sự xuất hiện của thông tin độ dài mở rộng (DO'7F66') được biểu thị trong Bảng chức năng phần mềm thứ ba của khả năng thẻ (xem Bảng 119).

DO'7F66' có thể xuất hiện trong EF.ATR/INIO (xem 12.2.2) và/hoặc trong FMD của DF ứng dụng bất kỳ. Trong trường hợp trước, thông tin áp dụng với tất cả các ứng dụng. Giá trị được xác định trong FMD ứng dụng chỉ áp dụng với ứng dụng đó, có khả năng thay thế các giá trị được xác định trong EF.ATR/INFO.

EF.ATR/INFO phải bao gồm nhiều nhất một phiên bản DO'7F66'; FMD ứng dụng phải bao gồm nhiều nhất một phiên bản DO'7F66'. Tất cả các DO được lồng trong DO'7F66' có độ dài thay đổi.

Giới hạn kích cỡ APDU lệnh và hồi đáp được xác định theo hai số nguyên, mỗi số được lồng trong DO'02'. Dưới thẻ '7F66':

- DO'02' đầu tiên phải bao gồm một số nguyên dương. Số các byte trong APDU lệnh phải không vượt quá số này.
- DO'02' thứ hai phải bao gồm một số nguyên dương. Nếu thẻ không hỗ trợ tạo chuỗi hồi đáp đối với một C-RP cụ thể khi đó C-RP N_e phải được thiết lập sao cho số các byte trong APDU hồi đáp không vượt quá số này.

12.7.2 Danh sách các mã INS hỗ trợ

Một DO'5F63' danh sách INS có thể xuất hiện trong EF.ATR/INFO (xem 12.2.2) và/hoặc trong FMD của DF ứng dụng bất kỳ. Trong trường hợp trước, thông tin áp dụng với tất cả các ứng dụng. Các giá trị được xác định trong FMD ứng dụng chỉ áp dụng đối với ứng dụng đó, có khả năng thay thế các giá trị được xác định trong EF.ATR/INFO.

Nếu DO'5F63' xuất hiện khi đó EF.ATR/INFO hoặc FMD ứng dụng bất kỳ phải bao gồm nhiều nhất một phiên bản.

DO'5F63' danh sách INS lồng vào kết nối của các byte INS được thẻ hoặc ứng dụng hỗ trợ.

Phụ lục A

(tham khảo)

Ví dụ về định danh đối tượng và kế hoạch phân bổ thẻ

A.1 Định danh đối tượng

Đối với tiêu chuẩn ISO, byte đầu tiên là '28', nghĩa là 40 trong số thập phân (xem ISO/IEC 8825-1). Một hoặc nhiều chuỗi byte theo sau; bit b8 được đặt là 0 trong byte cuối cùng của chuỗi và tới 1 trong byte trước, nếu có nhiều byte. Kết nối của bit b7 tới b1 của các byte có chuỗi mã hóa một số. Mỗi số phải được mã hóa trên byte có khả năng ít nhất, đó là, giá trị '80' không có hiệu lực đối với byte đầu tiên của chuỗi. Số đầu tiên là số tiêu chuẩn; số thứ hai, nếu xuất hiện, là phần trong tiêu chuẩn nhiều phần.

Như ví dụ đầu tiên, {iso(1) tiêu chuẩn (0) ic-thẻ(7816)} tham chiếu TCVN 11167 (ISO/IEC 7816).

- 7816 bằng với '1E88', nghĩa là 0001 1110 1000 1000, nghĩa là hai khối bit bảy: 0111101 0001000.
- Sau khi chèn giá trị thích hợp của bit b8 vào mỗi byte, mã hóa chuỗi đầu tiên là 1011 1101 0000 1000, bằng với 'BD08'.

Phần tử dữ liệu '28 BD08' có thể được sử dụng trong AID thuộc hạng mục tiêu chuẩn (xem 12.2.3).

AID = 'E8 28 BD08 0B XX ... XX' (ISO/IEC 7816-11 xác định mở rộng định danh ứng dụng 'XX ... XX').

AID = 'E8 28 BD08 0F XX ... XX' (TCVN 11167-15 (ISO/IEC 7816-15) xác định mở rộng định danh ứng dụng 'XX ... XX').

Như ví dụ thứ hai, {iso(1) tiêu chuẩn (0) e-auth(9798) phần (5)} tham chiếu ISO/IEC 9798. Chuỗi đầu tiên đạt được như sau.

- 9798 bằng với '2646', nghĩa là 0010 0110 0100 0110, nghĩa là hai khối bit bảy: 1001100 1000110.
- Sau khi chèn giá trị thích hợp của bit b8 vào mỗi byte, mã hóa chuỗi đầu tiên là 11001100 01000110, bằng với 'CC46'.

Phần tử dữ liệu '28 CC46 05 02' tham chiếu cơ chế thứ hai trong ISO/IEC 9798, nghĩa là GQ2. Định danh như vậy có thể được chuyển trong DO (thẻ '06', lớp chung, xem ISO/IEC 8825-1).

DO = {'06 05 28 CC 46 05 02'}

Như ví dụ thứ ba, {iso(1) tiêu chuẩn (0) mess(9992) phần (2)} tham chiếu ISO/IEC 9992-2. Chuỗi đầu tiên đạt được như sau.

- 9992 bằng với '2708', nghĩa là 0010 0111 0000 1000, nghĩa là hai khối bit bảy: 1001110 0001000.
- Sau khi chèn giá trị thích hợp của bit b8 vào mỗi byte, mã hóa chuỗi đầu tiên là 1100 1110 0000 1000, bằng với 'CE08'.

Phần tử dữ liệu là '28 CE08 02' (chuỗi thứ hai là '02'). Nó có thể được chuyển trong một DO.

DO = {'06 04 28 CE 08 02'}

A.2 Kế hoạch phân bổ thẻ

Ví dụ kế hoạch phân bổ thẻ mặc định

DO1 = {'59 02 95 02'}

DO2 = {'5F 24 03 97 03 31'}

DO1 (thẻ '59', ngày hết hạn thẻ) mã hóa tháng 2 năm 1995 làm ngày hết hạn thẻ (xem TCVN 11167-6 (ISO/IEC 7816-6)).

DO2 (thẻ '5F24', ngày hết hạn ứng dụng) mã hóa 31 tháng 3 năm 1997 là ngày hết hạn ứng dụng.

Ví dụ về kế hoạch phân bổ thẻ tương thích

DO1 = {'78 06' {'06 04 28 CE 08 02'}}

DO2 = {'5F 24 03 97 03 31'}

DO3 = {'70 04' {'80 02 XX XX'}}

DO4 = {'67 06' {'5F 29 03 XX XX XX'}}

DO1 (thẻ '78', thẩm quyền phân bổ thẻ tương thích) biểu thị kế hoạch phân bổ thẻ tương thích được xác định trong ISO 9992-2 được tham chiếu bởi định danh đối tượng của nó. Nếu DO1 xuất hiện hoặc trong chuỗi dữ liệu ban đầu (xem 12.1.2) hoặc trong EF.ATR/INFO (xem 12.2.2), khi đó thẩm quyền phân bổ thẻ có hiệu lực đối với toàn bộ thẻ. Nếu DO1 xuất hiện trong dữ liệu quản lý của một DF (xem 7.4), khi đó thẩm quyền phân bổ thẻ có hiệu lực trong DF đó.

DO2 (thẻ '5F24', ngày hết hạn ứng dụng) mã hóa 31 tháng 3 năm 1997 là ngày hết hạn ứng dụng.

DO3 (thẻ '70', khuôn mẫu liên ngành theo thẩm quyền phân bổ thẻ bao gồm) bao gồm một DO, thẻ '80', được xác định trong ISO 9992-2; ý nghĩa của thẻ '70' cũng được xác định trong ISO 9992-2.

DO4 (thẻ '67', khuôn mẫu dữ liệu xác thực) bao gồm DO tiết diện, thẻ '5F29'.

Ví dụ khác về kế hoạch phân bổ thẻ tương thích

DO1 = {'5F 24 03 97 03 31}

DO2 = {'70 0C' {'06 04 28 CE 08 02'}{'80 04 XX XX XX XX'}}

DO3 = {'67 06' {'5F 29 03 XX XX XX'}}

DO1 (thẻ '5F24', ngày hết hạn ứng dụng) mã hóa 31 tháng 3 năm 1997 là ngày hết hạn ứng dụng.

DO2 (thẻ '70', khuôn mẫu liên ngành được xác định định danh đối tượng bao gồm) bao gồm một DO, thẻ '06', xác định rằng DO tiếp theo, thẻ '80', được xác định trong ISO 9992-2. Ý nghĩa của thẻ '70' cũng được xác định trong ISO 9992-2.

DO3 (thẻ '67', khuôn mẫu dữ liệu xác thực liên ngành) bao gồm DO tiết diện trao đổi, thẻ '5F29'. Chú ý rằng nó không thể bao gồm các DO được xác định trong ISO 999-2 do lựa chọn không truyền DO liên ngành có thẻ '78'.

Ví dụ về kế hoạch phân bổ thẻ cùng tồn tại

DO1 = {'79 05'{'06 03 28 XX XX'}}

DO2 = {'7E 06' {'5F 24 03 97 03 31'}}

DO3 = {'70 06' {'XX XX XX XX XX XX'}}

DO1 (thẻ '79', thẩm quyền phân bổ thẻ cùng tồn tại) biểu thị kế hoạch phân bổ thẻ cùng tồn tại được xác định trong tiêu chuẩn được tham chiếu bằng định danh đối tượng bắt đầu bằng '28', một tiêu chuẩn ISO. Bắt buộc trong kế hoạch như vậy, DO1 phải xuất hiện hoặc

- Trong chuỗi dữ liệu ban đầu (xem 12.1.2) hoặc trong EF.ATR/INFO (xem 12.2.2) nếu thẩm quyền phân bổ thẻ có hiệu lực đối với toàn bộ thẻ, hoặc
- Trong dữ liệu quản lý của một DF (xem 7.4) nếu thẩm quyền phân bổ thẻ có hiệu lực trong DF đó.

DO2 (thẻ '7E') là một khuôn mẫu liên ngành để lồng các DO liên ngành. Chú ý rằng DO liên ngành "ngày hết hạn ứng dụng", thẻ '5F24', xuất hiện, mã hóa 31 tháng 3 năm 1997 là ngày hết hạn ứng dụng.

DO3 (thẻ '70', khuôn mẫu liên ngành được giải thích theo thẩm quyền phân bổ thẻ được biểu thị trong khuôn mẫu '79') chỉ có thể được giải thích theo tiêu chuẩn được biểu thị trong định danh đối tượng.

Phụ lục B
(tham khảo)

Ví dụ về thông điệp an toàn

B.1 Kiểm tra tổng mật mã

Điều này thể hiện việc sử dụng thông điệp an toàn (xem điều 10) và kiểm tra tổng mật mã (xem 10.2.3.1) đối với mỗi bốn trường hợp của C-RP được xác định trong TCVN 11167-3 (ISO/IEC 7816-3).

Trong các ví dụ, ký hiệu T* có nghĩa là bit b1 của byte cuối cùng của trường thẻ được đặt là 1 (số thẻ lẻ), nghĩa là SM DO phải được bao gồm trong phép tính của phần tử dữ liệu để xác thực.

Trong các ví dụ, ký hiệu CLA* có nghĩa là sử dụng thông điệp an toàn trong trường dữ liệu: trong CLA (xem 5.4.1), hoặc bit b8, b7 và b6 được đặt là 000 và bit b4 được đặt là 1, hoặc bit b8, b7 và b6 được đặt là 011.

Trong các ví dụ, ký hiệu CLA* có nghĩa là bit b8, b7 và b6 của CLA được đặt là 000 và bit b4 và b3 tới 11, nghĩa là tiêu đề lệnh phải được bao gồm trong phép tính của phần tử dữ liệu để xác thực.

Tiêu đề có thể được gói kín trong DO có thẻ '89', nghĩa là SM DO được bao gồm trong phép tính của phần tử dữ liệu để xác thực.

Trường hợp 1 thể hiện bit b3 trong mã hóa thứ nhất của CLA (xem Bảng 2) chỉ báo bảo vệ tiêu đề lệnh bằng kiểm tra tổng mật mã như thế nào, và hàm được hỗ trợ tùy chọn như thế nào khi sử dụng mã hóa thứ hai của CLA (xem Bảng 3). Trong trường hợp 1, bảo vệ nguồn áp dụng. Sử dụng bit b3 trong mã hóa đầu tiên của CLA nó không được thể hiện trong các trường hợp khác, để đơn giản ví dụ, và do kết quả luôn giống nhau: bổ sung một khối tại thời điểm bắt đầu của dữ liệu được phục hồi bằng kiểm tra tổng mật mã của APDU lệnh.

Trường hợp 1 - Không có dữ liệu lệnh, không có dữ liệu hồi đáp

Tiêu đề lệnh	Thân lệnh
CLA INS P1 P2	Không xuất hiện

Thân hồi đáp	Bản ghi cuối hồi đáp
Không xuất hiện	SW1-SW2

Trường hợp 1.a - Trạng thái không được bảo vệ

Giả định được thực hiện là tiêu đề lệnh phải được bảo vệ, do nó là điều duy nhất bảo vệ trong C-RP này.

Tiêu đề lệnh	Thân lệnh	b7 trong CLA*
CLA* INS P1 P2	Trường L_c mới - trường dữ liệu mới = {T-L-kiểm tra tổng mật mã}	0
	Trường L_c mới - trường dữ liệu mới = {T*-L-tiêu đề lệnh}{T-L-kiểm tra tổng mật mã}	1

Nếu độ dài của kiểm tra tổng mật mã là bốn byte, khi đó trường L_c mới được đặt là '06' (dòng trên cùng) hoặc '0C' (dòng dưới cùng).

Trường dữ liệu mới = một hoặc hai DO = có điều kiện {T* - L - tiêu đề lệnh} khi đó {T - L - kiểm tra tổng mật mã}

Dữ liệu được bao gói bằng kiểm tra tổng mật mã:

- Mã hóa đầu tiên của CLA, một khối = [CLA** INS P1 P2 phần đệm]
- Mã hóa thứ hai của CLA, một khối = [{T* - L - tiêu đề lệnh}- phần đệm]

APDU hồi đáp an toàn như sau

Thân hồi đáp	Bản ghi cuối hồi đáp
Không xuất hiện	SW1-SW2

Trường hợp 1.b - Trạng thái được bảo vệ

APDU lệnh an toàn như sau.

Tiêu đề lệnh	Thân lệnh	b7 trong CLA*
CLA* INS P1 P2	Trường L_c mới - trường dữ liệu mới = {T-L-kiểm tra tổng mật mã} = '00'	1
	Trường L_c mới - trường dữ liệu mới = {T-L-tiêu đề lệnh}{T-L-kiểm tra tổng mật mã}- trường L_e mới = '00'	0

Trường dữ liệu mới = một hoặc hai DO = có điều kiện {T - L - tiêu đề lệnh} luôn kết thúc với {T-L-kiểm tra tổng mật mã}

Sự khác nhau với trường hợp 1.a là trường L_e mới = '00', do kiểm tra tổng mật mã thuộc về dữ liệu hồi đáp mà dữ liệu này phải được yêu cầu theo sự xuất hiện của L_e. Dữ liệu được bao gói bằng kiểm tra tổng mật mã giống như trong trường hợp 1.a.

APDU hồi đáp an toàn như sau.

Thân hồi đáp	Bản ghi cuối hồi đáp
trường dữ liệu mới = {T*-L- SW1-SW2}-{T-L-kiểm tra tổng mật mã})	SW1-SW2

Trường dữ liệu mới = hai DO = {T*-L- SW1-SW2}-{T-L-kiểm tra tổng mật mã}

Dữ liệu được bao gói bằng kiểm tra tổng mật mã = một khối = [{T*-L- SW1-SW2} - phần đệm]

Trường hợp 2 - Không có dữ liệu lệnh, dữ liệu hồi đáp

C-RP không an toàn như sau.

Tiêu đề lệnh	Thân lệnh
CLA INS P1 P2	Trường L_e

Thân hồi đáp	Bản ghi cuối hồi đáp
trường dữ liệu	SW1-SW2

APDU lệnh an toàn như sau

Tiêu đề lệnh	Thân lệnh
CLA* INS P1 P2	Trường L_c mới - trường dữ liệu mới - trường L_e mới (một hoặc 2 byte được đặt là '00')

Trường dữ liệu mới = hai DO = {T* - L - N_e} - {T - L - kiểm tra tổng mật mã}

Dữ liệu được bao gói bằng kiểm tra tổng mật mã = một khối = [{T* - L - N_e}- phần đệm].

CHÚ THÍCH nếu trường L_e gốc là '00' hoặc '000000', trường giá trị có thể không xuất hiện, nghĩa là DO tương ứng phải là '97 00' (xem 10.4).

APDU hồi đáp an toàn như sau.

Thân hồi đáp	Bản ghi cuối hồi đáp
trường dữ liệu mới	SW1-SW2

Trường dữ liệu mới = ba DO = {T* - L - giá trị đơn giản} - {T* - L - SW1-SW2}-{T - L - kiểm tra tổng mật mã}

Dữ liệu được bao gói bằng tổng kiểm tra mật mã = một hoặc nhiều khối, phụ thuộc vào giá trị đơn giản, ví dụ:

- Một khối = [{T* - L - giá trị đơn giản}{T* - L - SW1-SW2}- phần đệm]
- Hai khối = [{T* - L - giá trị đơn giản, bắt đầu} - [giá trị đơn giản, kết thúc} - {T* - L - SW1-SW2}- phần đệm]

Trường hợp 3 - Dữ liệu lệnh, không có dữ liệu hồi đáp

C-RP không an toàn như sau.

Tiêu đề lệnh	Thân lệnh
CLA INS P1 P2	Trường L_c - trường dữ liệu

Thân hồi đáp	Bản ghi cuối hồi đáp
Không xuất hiện	SW1-SW2

Trường hợp 3.a - Trạng thái không được bảo vệ

APDU lệnh an toàn như sau.

Tiêu đề lệnh	Thân lệnh
CLA* INS P1 P2	Trường L_c mới - trường dữ liệu mới

Trường dữ liệu mới hoặc dữ liệu lệnh mới = hai DO = [{T* - L - giá trị đơn giản}- {T - L - kiểm tra tổng mật mã}

Dữ liệu được bao gói bằng kiểm tra tổng mật mã = một hoặc nhiều khối, phụ thuộc vào giá trị đơn giản:

1. [{T* - L - giá trị đơn giản}- phần đệm]
2. [{T* - L - giá trị đơn giản}] - [phần đệm]
3. [{T* - L - giá trị đơn giản, bắt đầu] - [giá trị đơn giản, kết thúc} - phần đệm]

Trong ví dụ 1, với khối 8 byte, L tối đa trong DO giá trị đơn giản là 5, trong trường hợp khối kết thúc với một byte phần đệm.

Trong ví dụ 2, với khối 8 byte, L trong DO giá trị đơn giản là 6. DO phủ đầy khối phải được theo sau bằng một khối đầy phần đệm.

Trong ví dụ 3, với khối 8 byte, L trong DO giá trị đơn giản trong khoảng 7 và 13, để lại ít nhất một byte phần đệm tại khối thứ hai.

APDU hồi đáp đồng nhất với APDU hồi đáp không an toàn:

Thân hồi đáp	Bản ghi cuối hồi đáp
Không xuất hiện	SW1-SW2

Trường hợp 3.b - Trạng thái được bảo vệ

APDU lệnh an toàn như sau

Tiêu đề lệnh	Thân lệnh
CLA* INS P1 P2	Trường L_c mới - trường dữ liệu mới - trường L_e mới (='00')

Trường dữ liệu mới hoặc dữ liệu lệnh mới = hai DO = [{T* - L - giá trị đơn giản}- {T - L - kiểm tra tổng mật mã}

Dữ liệu được bao gói bằng kiểm tra tổng mật mã = một hoặc nhiều khối, phụ thuộc vào giá trị đơn giản:

1. [{T* - L - giá trị đơn giản}- phần đệm]
2. [{T* - L - giá trị đơn giản}] - [phần đệm]
3. [{T* - L - giá trị đơn giản, bắt đầu] - [giá trị đơn giản, kết thúc} - phần đệm]

Trong ví dụ 4, với khối 8 byte, L tối đa trong DO giá trị đơn giản là 5, trong trường hợp khối kết thúc với một byte phần đệm.

Trong ví dụ 5, với khối 8 byte, L trong DO giá trị đơn giản là 6. DO phủ đầy khối phải được theo sau bằng một khối đầy phần đệm.

Trong ví dụ 6, với khối 8 byte, L trong DO giá trị đơn giản trong khoảng 7 và 13, để lại ít nhất một byte phần đệm tại khối thứ hai.

APDU hồi đáp an toàn như sau

Thân hồi đáp	Bản ghi cuối hồi đáp
trường dữ liệu mới (= {T*-L- SW1-SW2}-{T-L-kiểm tra tổng mật mã})	SW1-SW2

Trường dữ liệu mới = hai DO = {T*-L- SW1-SW2}-{T-L-kiểm tra tổng mật mã}

Dữ liệu được bao gói bằng kiểm tra tổng mật mã = một khối = [{T*-L- SW1-SW2} - phần đệm]

Trường hợp 4 - Dữ liệu lệnh, dữ liệu hồi đáp

C-RP không an toàn như sau.

Tiêu đề lệnh	Thân lệnh
CLA INS P1 P2	Trường L_c - trường dữ liệu - trường L_e

Thân hồi đáp	Bản ghi cuối hồi đáp
Trường dữ liệu	SW1-SW2

APDU lệnh an toàn như sau.

Tiêu đề lệnh	Thân lệnh
CLA* INS P1 P2	Trường L_c mới - trường dữ liệu mới - trường L_e mới (một hoặc 2 byte được thiết lập tới '00')

Trường dữ liệu mới hoặc dữ liệu lệnh mới = ba DO = {T* - L - giá trị đơn giản}- {T* - L - N_e}-{T - L - kiểm tra tổng mật mã}

Dữ được bao gói bằng kiểm tra tổng mật mã giống như trong trường hợp 3b.

APDU hồi đáp an toàn như sau.

Thân hồi đáp	Bản ghi cuối hồi đáp
trường dữ liệu mới (={T* - L - giá trị đơn giản}-{T*-L- SW1-SW2}-{T-L-kiểm tra tổng mật mã})	SW1-SW2

Trường dữ liệu mới = ba DO = {T* - L - giá trị đơn giản}-{T*-L- SW1-SW2}-{T-L-kiểm tra tổng mật mã}

Dữ liệu được bao gói bằng kiểm tra tổng mật mã = một hoặc nhiều khối = [{T* - L - giá trị đơn giản}-{T*-L- SW1-SW2} - phần đệm]

B.2 Mật mã

Sử dụng mật mã có hoặc không có phần đệm (xem 10.2.2) được thể hiện trong trường dữ liệu lệnh và hồi đáp. Thay cho DO giá trị đơn giản trong các ví dụ trước, các DO dành cho tính bảo mật phải được sử dụng như sau.

1) Trường hợp a - giá trị đơn giản không được mã hóa trong BER-TLV

   Trường dữ liệu = {T - L - Byte chỉ dẫn nội dung-phần đệm - mật mã}

   Giá trị đơn giản được chuyển bằng mật mã = một hoặc nhiều khối = giá trị đơn giản không được mã hóa trong BER-TLV, có khả năng được đệm theo Byte chỉ dẫn

2) Trường hợp b - giá trị đơn giản được mã hóa trong BER-TLV

   Trường dữ liệu = {T - L - mật mã}

   Giá trị đơn giản được chuyển bằng mật mã = chuỗi các byte mã hóa = DO BER-TLV (phần đệm phụ thuộc vào thuật toán và chế độ hoạt động của nó)

B.3 Tham chiếu điều khiển

Sử dụng tham chiếu điều khiển (xem 10.3.1 và 10.3.2) được thể hiện.

Trường dữ liệu lệnh = {T - L - khuôn mẫu tham chiếu điều khiển}, trong đó

Khuôn mẫu tham chiếu điều khiển = {T - L - tham chiếu tệp} - {T - L - tham chiếu khóa}

B.4 Bộ mô tả hồi đáp

Sử dụng bộ mô tả hồi đáp (xem 10.3.4) được thể hiện.

Trường dữ liệu lệnh = {T - L - bộ mô tả hồi đáp}, trong đó

Bộ mô tả hồi đáp = {T (giá trị đơn giản - '00' - T (kiểm tra tổng mật mã) - '00'}

Trường dữ liệu hồi đáp = {T - L - giá trị đơn giản} - {T - L - kiểm tra tổng mật mã}

B.5 Lệnh ENVELOPE

Sử dụng lệnh ENVELOPE (xem 11.7.2) được thể hiện.

Trường dữ liệu lệnh = {T - L - Byte chỉ dẫn nội dung-phần đệm - mật mã}

Giá trị đơn giản được chuyển bằng mật mã = APDU lệnh (bắt đầu bằng CLA*INS P1 P2), phần đệm theo Byte chỉ dẫn

Trường dữ liệu hồi đáp = {T - L - Byte chỉ dẫn nội dung-phần đệm - mật mã}

Giá trị đơn giản được chuyển bằng mật mã = APDU hồi đáp, phần đệm theo Byte chỉ dẫn.

B.6 Tính đồng vận giữa các thao tác an toàn và thông điệp an toàn

Trong điều này, các biểu tượng và thuật ngữ viết tắt sau được áp dụng

CC	tổng kiểm tra mật mã
CG	mật mã
CLA**	CLA với chỉ báo SM (bit b8, b7 và b6 được đặt là 000 và bit b4 và b3 được đặt là 11)
DS	chữ ký số
MSE	quản lý môi trường an toàn
PCI	Byte chỉ dẫn nội dung-phần đệm
PSO	thực hiện thao tác an toàn
SMC	thẻ mô-đun an toàn
USC	thẻ người sử dụng thông minh

Ví dụ giải thích sử dụng như thế nào thẻ mô-đun an toàn (SMC) mà thẻ này thực hiện các thao tác an toàn để sản sinh ra APDU lệnh an toàn để gửi tới thẻ người sử dụng (USC) và để xử lý APDU hồi đáp an toàn tương ứng nhận được ngay sau đó từ USC, nghĩa là để sản sinh và xử lý trường dữ liệu trong định dạng SM. Ví dụ mô tả tính đồng vận giữa hai cách tiếp cận: - tiếp cận nguyên tử bằng thao tác an toàn (xem ISO/IEC 7816-8) và - tiếp cận chung bằng thông điệp an toàn (xem điều 10).

Ví dụ giả định rằng USC và SMC đã hoàn thành thủ tục xác thực chung, dựa trên, ví dụ chứng nhận có thể kiểm tra được của thẻ. Thủ tục xác thực bao gồm một cơ chế quy ước khóa hoặc vận chuyển khóa sao cho sau thủ tục này hai khóa đối xứng có sẵn trong USC và trong SMC:

1. Khóa phiên đối xứng để tính kiểm tra tổng mật mã và
2. Kóa phiên đối xứng để tính tài liệu viết bằng mật mã

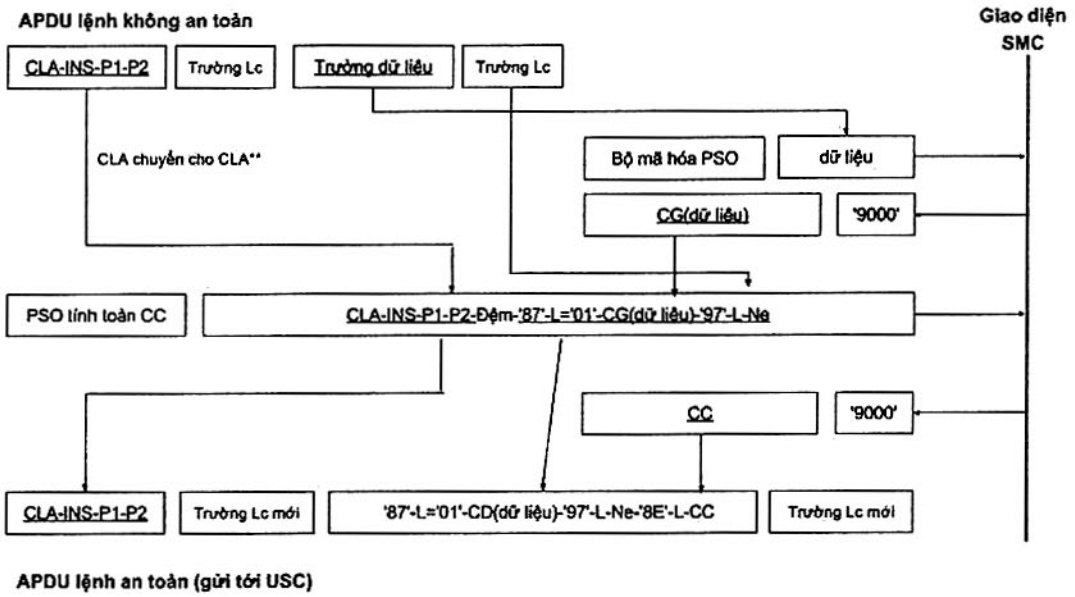
Thủ tục xác minh khởi đầu một hoặc nhiều bộ đếm trong USC và SMC. Ví dụ không thể hiện việc duy trì và sử dụng các bộ đếm như vậy bằng USC và SMC.

Tất cả các C-RP đối với SMC là các lệnh PSO, không sử dụng thông điệp an toàn, nhưng sử dụng DO SM (và khóa SM được thiết lập bằng lệnh MSE).

Tất cả các C-RP đối với USC sử dụng thông điệp an toàn và tiêu đề lệnh được bao gồm trong phép tính kiểm tra tổng mật mã, nghĩa là CLA được chuyển tới CLA**.

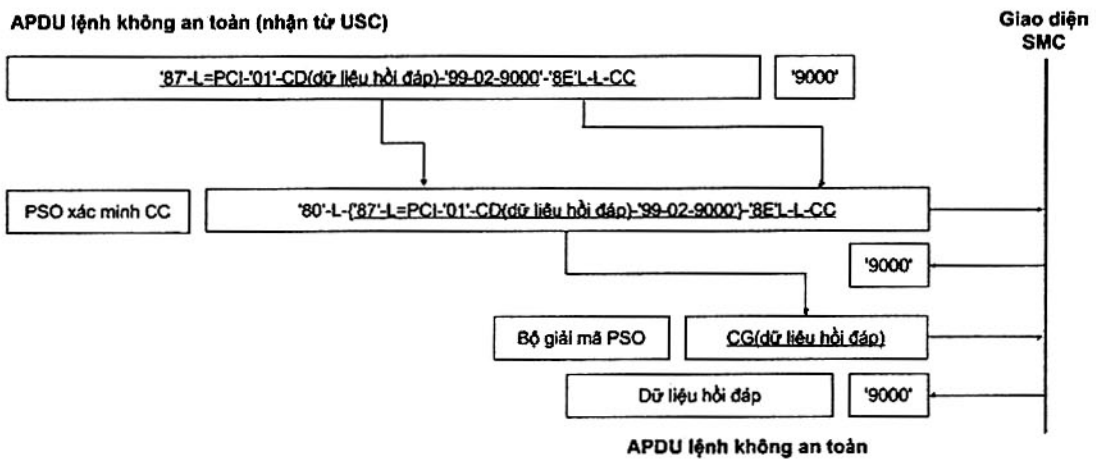
CHÚ THÍCH hoạt động mã hóa được thực hiện bằng các lệnh PSO COMPUTE CC, PSO VERIFY CC và PSO ENCIPHER có thể yêu cầu đầu vào có độ dài là bội số của độ dài khối của thuật toán mã hóa. Để thực hiện yêu cầu này, phần đệm áp dụng. Phần đệm này được áp dụng trong SMC. Hơn nữa, SMC loại bỏ các byte phần đệm trước khi hồi đáp lệnh PSO DECIPHER. Do vậy, phần đệm tại điểm cuối của dữ liệu đầu vào hoặc đầu ra không xảy ra trong các câu lệnh và hệ số sau.

Hình B.1 thể hiện nguyên tắc chung sản sinh một APDU lệnh an toàn



Hình B.1 - Sản sinh một APDU lệnh an toàn

Hình B.2 thể hiện nguyên tắc chung sản sinh một APDU hồi đáp an toàn



Hình B.2 - Sản sinh một APDU hồi đáp an toàn

Các kịch bản sau giải thích phép tính chữ ký số (DS) nhờ đó sử dụng khóa chữ ký riêng yêu cầu sự xuất hiện thành công của mật lệnh. Kịch bản thực hiện theo ba bước.

Bước 1 - Kiểm tra mật lệnh

1.1 lệnh tới SMC: MSE SET <CCT, {'83'-'01-'81'}>

Tham chiếu khóa phiên để tính kiểm tra tổng mật mã là '81' trong ví dụ.

Hồi đáp SMC: OK

1.2 lệnh tới SMC: MSE SET <CCT, {'83'-'01-'82'}>

Tham chiếu khóa phiên để tính tài liệu viết bằng mật mã là '82' trong ví dụ.

Hồi đáp SMC: OK

1.3 lệnh tới SMC: PSO ENCIPHER <mật lệnh>

Hồi đáp SMC: <CG (mật lệnh)>

1.4 lệnh tới SMC: PSO COMPUTE CC <CLA**-INS-P1-P2-phần đệm - {'87'-L-PCI-CG (mật lệnh)} - {'97'-L-N_e}>

Hồi đáp SMC: <CC>

Bây giờ thiết bị giao diện xây dựng APDU lệnh VERIFY an toàn.

1.5 lệnh tới USC: VERIFY <{'87'-L-PCI='01'-CG (mật lệnh)}- {'97'-L-N_e}-{'8E'-'04'-CC}>

Hồi đáp USC: <{'99'-'02'-SW1-SW2}-{'8E'-'04'-CC}>

1.6 lệnh tới SMC: PSO VERIFY CC<{'80'-'04'- {'99'-'02'-SW1-SW2}-{'8E'-'04'-CC}>

Hồi đáp SMC: OK

Bước 2 - Tính toán mã-băm

2.1 lệnh tới SMC: PSO COMPUTE CC <CLA**-INS-P1-P2-phần đệm - {'81'-L-({'90'-L-băm trung gian)} - {'80'-L-khối cuối cùng})}- {'97'-L-N_e}>

Hồi đáp SMC: <CC>

2.2 lệnh tới USC: PSO HASH <{'81'-L1 (=4+L2+L3)-({'90'-L2-băm trung gian)} - {'80'-L3-khối cuối cùng})}- {'8E'-'04'-CC}>

USC lưu giữ mã-băm làm kết quả bên trong để tính chữ ký số sau này.

Hồi đáp SMC: <{'99'-'02'-SW1-SW2}- {'8E'-'04'-CC}>

2.3 lệnh tới SMC: PSO VERIFY CC<{'80'-'04'- {'99'-'02'-SW1-SW2}-{'8E'-'04'-CC}>

Hồi đáp SMC: OK

Bước 3 - Tính toán chữ ký số

3.1 lệnh tới SMC: PSO COMPUTE CC <CLA**-INS-P1-P2-phần đệm - {'97'- '01'-'00'}>

Hồi đáp SMC: <CC>

3.2 lệnh tới USC: PSO COMPUTE DS <{'97'- '01'-'00'}- {'8E'-'04'-CC}>

Hồi đáp USC: <'81'-L-DS-'8E'-'04'-CC>

3.3 lệnh tới SMC: PSO VERIFY CC<{'80'-L1 (=2+L2)-('81'-L2-DS)}-{'8E'-'04'-CC}>

Hồi đáp SMC: OK

Phụ lục C

(tham khảo)

Ví dụ về hàm AUTHENTICATE theo lệnh GENERAL AUTHENTICATE

Hai hoặc nhiều C-RP GENERAL AUTHENTICATE thực hiện một hàm AUTHENTICATE

Nếu tạo chuỗi được sử dụng, khi đó CLA được đặt là 0xx1 xxxx trong lệnh đầu tiên của chuỗi cho đến gần cuối và tới 0xx0 xxxx trong thứ tự cuối cùng: sáu bit khác vẫn giữ nguyên không đổi trong chuỗi (xem 5.3.3).

INS P1 P2 được đặt là hoặc '86 00 00' hoặc '87 00 00'.

Giá trị của trường L_c phụ thuộc vào các DO trong trường dữ liệu lệnh. Phụ thuộc vào liệu một trường dữ liệu hồi đáp có được mong đợi hay không, trường L_e hoặc được đặt là '00', hoặc không xuất hiện.

C.1 GENERAL AUTHENTICATE sử dụng bộ ba bằng chứng-thử thách-hồi đáp

C.1.1 Giới thiệu

Phụ lục này mô tả trường dữ liệu của lệnh GENERAL AUTHENTICATE thực hiện cơ chế như được xác định trong ISO/IEC 9798-5, nghĩa là cơ chế sử dụng kỹ thuật nhận biết zero.

- bộ xác minh biết vấn đề chung và nguyên đơn biết giải pháp bí mật đối với vấn đề chung.
- Kết quả của giao thức nhận biết-zero, bộ xác minh bị thuyết phục rằng nguyên đơn biết giải pháp đối với vấn đề chung. Hơn nữa, giải pháp giữ nguyên bí mật.

CHÚ THÍCH ISO/IEC 9798-5 xác định hai kỹ thuật GQ

- Được cho khóa RSA chung trong đó số mũ v là nguyên tố như $257 = 2^8 + 1$, $65537 = 2^{16} + 1$ hoặc $2^{36} + 2^{13} + 1$, kỹ thuật GQ1 cho phép xác minh chữ ký RSA mà không nhận biết giá trị của nó, hoặc chứng minh nhận biết của chữ ký RSA mà không công khai giá trị của nó. Như được xác định bằng sử dụng tiêu chuẩn chữ ký RSA (ví dụ, xem ISO/IEC 14888-2), cơ chế định dạng biến đổi dữ liệu định danh nguyên đơn (khuôn mẫu) trong G số chung. Q số riêng tương ứng là chữ ký RSA của dữ liệu định danh. Nguyên đơn và bộ xác minh biết khóa RSA chung. Giao thức GQ1 chứng miinh rằng nguyên đơn biết chữ ký RSA của dữ liệu định danh.
- Được cho suất chung n, tích của hai thừa số nguyên tố, kỹ thuật GQ2 cho phép kiểm tra các thừa số mà không nhận biết chúng, hoặc chứng minh sự nhận biết của các thừa số mà không công khai chúng. Cơ chế abo gồm thông số an toàn $k > 0$ và số nguyên tố đầu tiên m, được gọi là số cơ sở m, như kxm là từ 8 tới 36. Mỗi số chung là bình phương của một số cơ sở: $G = g^2$. Q số riêng tương ứng là một modula 2^{k+1}-gốc th của G. Nếu có ít nhất một số cơ sở g như biểu tượng Jacobi của g đối với n là -1 và nếu n là đồng dư tới 1 mod 4, khi đó giao thức GQ2 chứng minh rằng n là đa hợp và nguyên đơn biết thừa số.

Giao thức trao đổi ba số, là bằng chứng, thử thách và hồi đáp.

- Nguyên đơn thực hiện trên hai bước: bước thứ nhất, nguyên đơn lựa chọn bí mật một số ngẫu nhiên và biến đổi nó thành bằng chứng theo "công thức bằng chứng"; bước thứ hai, sau khi đã nhận được thử thách, nguyên đơn hồi đáp thách thức từ số ngẫu nhiên và số bí mật, theo "công thức hồi đáp", và khi đó xóa bỏ số ngẫu nhiên.
- Bộ xác minh khôi phục bằng chứng từ thử thách và hồi đáp, theo "công thức kiểm tra".

Theo định nghĩa, bộ ba bao gồm ba số, gọi là bằng chứng, thử thách và hồi đáp, kiểm tra công thức kiểm tra. Thực thể bất kỳ có thể sản sinh ngẫu nhiên bộ ba trong "chế độ công khai", từ thử thách bất kỳ và hồi đáp. Phán đoán hoặc quan sát không thể phân biệt bộ ba ngẫu nhiên được sản sinh trong chế độ công khai, nghĩa là theo một thực thể không biết bí mật, và bộ ba ngẫu nhiên được sản sinh trong "chế độ bí mật", nghĩa là theo một thực thể biết bí mật.

Phần này của phụ lục mô tả ba hàm AUTHENTICATE.

- Hàm INTERNAL AUTHENTICATE - bộ xác minh trong mọi đối tượng bên ngoài xác thực nguyên đơn trong thẻ
- Hàm EXTERNAL AUTHENTICATE - bộ xác minh trong thẻ xác thực nguyên đơn trong mọi đối tượng bên ngoài
- Hàm MUTUAL AUTHENTICATE - các thực thể xác thực lẫn nhau.

C.1.2 Hàm INTERNAL AUTHENTICATE

Nếu trường dữ liệu đầu tiên chuyển một yêu cầu bằng chứng, hoặc một bằng chứng trống ('80 00'), hoặc một mã xác thực trống ('84 00') khi đó hàm là INTERNAL AUTHENTICATE.

Giao thức cơ bản (hai C-RP)

	chứng kiến từ thẻ
Command data field	{'7C'-'02'-{'80'-'00'}}
Response data field	{'7C'-L1 (=2+L2)-{'80'-L2-Witness}}
	thử thách từ thế giới bên ngoài và trả lời từ thẻ
Command data field	{'7C'-L1 (=4+L2)-{'81'-L2-Challenge}-{'82'-'00'}}
Response data field	{'7C'-L1 (=2+L2)-{'82'-L2-Response}}

Thử thách cam kết (hai C-RP)

	chứng kiến từ thẻ
Command data field	{'7C'-L1 (=4+L2)-{'83'-L2-Committed Challenge}-{'80'-'00'}}
Response data field	{'7C'-L1 (=2+L2)-{'80'-L2-Witness}}

CHÚ THÍCH thử thách cam kết đảm bảo rằng thử thách và bằng chứng được lựa chọn độc lập

Thử thách từ mọi đối tượng bên ngoài và hồi đáp từ thẻ

Command data field	{'7C'-L1 (=4+L2)-{'81'-L2-Challenge}-{'82'-'00'}}
Response data field	{'7C'-L1 (=2+L2)-{'82'-L2-Response} if the challenge is correct Absent if the challenge is incorrect

Mở rộng tới xác thực trường dữ liệu (hai C-RP)

Thẻ đã làm hỏng trường dữ liệu trao đổi trước: kết quả là mã-băm hiện hành. Thẻ bao gồm DO bằng chứng để nhận được mã xác thực và truyền với thẻ '84'.

	chứng kiến từ thẻ
Command data field	{'7C'-'02'-{'84'-'00'}}
Response data field	{'7C'-L1 (=2+L2)-{'84'-L2-Authentication code}}
	thử thách từ thế giới bên ngoài và trả lời từ thẻ
Command data field	{'7C'-L1 (=4+L2)-{'81'-L2-Challenge}-{'82'-'00'}}
Response data field	{'7C'-L1 (=2+L2)-{'82'-L2-Response}}

C.1.3 Hàm EXTERNAL AUTHENTICATE

Nếu trường dữ liệu đầu tiên chuyển một yêu cầu thử thách, hoặc một thử thách trống ('81 00'), hoặc một thử thách cam kết trống ('83 00') khi đó hàm là EXTERNAL AUTHENTICATE.

Giao thức cơ bản (hai C-RP)

	chứng kiến từ thế giới bên ngoài và thử thách từ thẻ
Command data field	{'7C'-L1 (=4+L2)-{'80'-L2-Witness}-{'81'-'00'}}
Response data field	{'7C'-L1 (=2+L2)-{'81'-L2-Challenge}}
	trả lời từ thế giới bên ngoài và kiểm tra bởi thẻ
Command data field	{'7C'-L1 (=2+L2)-{'82'-L2-Response}}
Response data field	Absent

Thử thách cam kết (ba C-RP)

	thử thách cam kết từ thẻ
Command data field	{'7C'-'02'-{'83'-'00'}}
Response data field	{'7C'-L1 (=4+L2)-{'83'-L2-Committed challenge)-{'80'-'00'}}
	chứng kiến từ thế giới bên ngoài và thử thách từ thẻ
Command data field	{'7C'-L1 (=4+L2)-{'80'-L2-Witness}-{'81'-'00'}}
Response data field	{'7C'-L1 (=2+L2)-{'81'-L2-Challenge}}
	trả lời từ thế giới bên ngoài và kiểm tra bằng thẻ
Command data field	{'7C'-L1 (=2+L2)-{'82'-L2-Response}}
Response data field	Absent

Mở rộng tới xác thực trường dữ liệu (hai C-RP)

Nguyên đơn đã làm hỏng trường dữ liệu trao đổi trước: kết quả là mã-băm hiện hành. Nó bao gồm DO bằng chứng để nhận được mã xác thực và truyền với thẻ '84'.

	chứng kiến từ thế giới bên ngoài và thử thách từ thẻ
Command data field	{'7C'-L1 (=4+L2)-{'84'-L2-Authentication code}-{'81'-'00'}}
Response data field	{'7C'-L1 (=2+L2)-{'81'-L2-Challenge}}
	trả lời từ thế giới bên ngoài và kiểm tra bằng thẻ
Command data field	{'7C'-L1 (=2+L2)-{'82'-L2-Response}}
Response data field	Absent

C.1.4 Hàm MUTUAL AUTHENTICATE

Nếu trường dữ liệu đầu tiên không chuyển DO trống, khi đó hàm là MUTUAL AUTHENTICATE; mọi đối tượng bên ngoài yêu cầu các DO giống nhau trong trường dữ liệu hồi đáp như trong trường dữ liệu lệnh.

Giao thức cơ bản (ba C-RP)

	chứng kiến
Command data field	{'7C'-L1 (=2+L2)-{'81'-L2-Witness}}
Response data field	{'7C'-L1 (=2+L2)-{'81'-L2-Witness}}
	thử thách
Command data field	{'7C'-L1 (=2+L2)-{'81'-L2-Challenge}}
Response data field	{'7C'-L1 (=2+L2)-{'81'-L2-Challenge}}
	trả lời
Command data field	{'7C'-L1 (=2+L2)-{'82'-L2-Response}}
Response data field	{'7C'-L1 (=2+L2)-{'82'-L2-Response}} if the response is correct Absent if the response is incorrect

Thử thách cam kết (bốn C-RP)

	thử thách cam kết
Command data field	{'7C'-L1 (=2+L2)-{'83'-L2-Committed challenge}}
Response data field	{'7C'-L1 (=2+L2)-{'83'-L2-Committed challenge}}
	chứng kiến
Command data field	{'7C'-L1 (=2+L2)-{'80'-L2-Witness}}
Response data field	{'7C'-L1 (=2+L2)-{'80'-L2-Witness}}
	thử thách
Command data field	{'7C'-L1 (=2+L2)-{'81'-L2-Challenge}}
Response data field	{'7C'-L1 (=2+L2)-{'81'-L2-Challenge}} if the challenge is correct Absent if the challenge is incorrect
	trả lời
Command data field	{'7C'-L1 (=2+L2)-{'82'-L2-Response}}
Response data field	{'7C'-L1 (=2+L2)-{'82'-L2-Response}} if the response is correct Absent if the response is incorrect

Mở rộng tới quy ước khóa (bốn C-RP)

Một cặp các phần tử dữ liệu số mũ cho phép quy ước khóa phiên (xem ISO/IEC 11770).

C-RP đầu tiên trao đổi khuôn mẫu xác thực động lực lòng vào phần tử dữ liệu "số mũ". Trong ví dụ, do không có thông điệp được trao đổi trước trong suốt phiên giao tiếp, mã-băm ban đầu là khối không có hiệu lực. Khi đó trường dữ liệu lệnh, nghĩa là khuôn mẫu xác thực động lực đầu tiên, được bao gồm để nhận được mã-băm hiện hành; khi đó trường dữ liệu hồi đáp, nghĩa là khuôn mẫu xác thực động lực thứ hai được bao gồm để cập nhật mã-băm hiện hành; mã-băm hiện hành phải giống nhau đối với các thực thể. Cuối cùng, một DO bằng chứng (không phải là zero và không được truyền, khác biệt đối với mỗi thực thể) được bao gồm để nhận được mã xác thực (khác với mỗi thực thể).

C-RP thứ hai trao đổi khuôn mẫu xác thực động lực lòng vào mã xác thực với thẻ '84'.

	số mũ
Command data field	{'7C'-L1 (=2+L2)-{'85'-L2-Exponential}}
Response data field	{'7C'-L1 (=2+L2)-{'85'-L2-Exponential}}
	chứng kiến
Command data field	{'7C'-L1 (=2+L2)-{'84'-L2-Authentication code}}
Response data field	{'7C'-L1 (=2+L2)-{'84'-L2-Authentication code}}
	thử thách
Command data field	{'7C'-L1 (=2+L2)-{'81'-L2-Challenge}}
Response data field	{'7C'-L1 (=2+L2)-{'81'-L2-Challenge}}
	trả lời
Command data field	{'7C'-L1 (=2+L2)-{'82'-L2-Response}}
Response data field	{'7C'-L1 (=2+L2)-{'82'-L2-Response}} if the response is correct Absent if the response is incorrect

C.2 GENERAL AUTHENTICATE đối với giao thức xác thực nhiều bước

C.2.1 Giới thiệu

Phần này thuộc phụ lục mô tả sử dụng lệnh GENERAL AUTHENTICATE đối với giao thức xác thực nhiều bước, nghĩa là mật lệnh dựa trên kế hoạch xác thực PACE v2 như được mô tả trong EN 14890-1.

Theo đó, giao thức xác thực nhiều bước bao gồm một vài hoạt động xác thực, ít nhất một hoặc nhiều GENERAL AUTHENTICATE: hoạt động PERFORM KEY AGREEMENT (PKA) khởi đầu sự tạo thành, quản lý và/hoặc sử dụng cặp khóa Diffie-Hellman và/hoặc thông số khóa trong thẻ, ví dụ để thiết lập kênh an toàn giữa ICC và mọi đối tượng bên ngoài bằng phương thức chỉ xác thực mật lệnh.

Theo sử dụng giao thức cụ thể một hoặc nhiều hoạt động PKA được sử dụng để

- Mã hóa và/hoặc ánh xạ nonce
- Tạo một cặp khóa Diffie Hellman (DH) không đối xứng đối với quy ước khóa và/hoặc
- Truy cập trước một cặp khóa DH không đối xứng và/hoặc thông số khóa được tạo ra trước trong thẻ
- Lưu giữ khóa chung DH từ thiết bị giao diện (IFD) dựa trên cùng thông số chung trong thẻ,
- Xử lý một quy ước khóa
- Và cung cấp khóa tạm thời trong thẻ, ví dụ được sử dụng đối với thông điệp an toàn.

Hoạt động được đặt trước bởi một hoặc nhiều hoạt động MANAGE SECURITY ENVIRONMENT để thiết lập định danh đối tượng tương ứng cũng như thông số liên quan đến tạo khóa (ví dụ tham chiếu thuật toán trong CRT AT theo giao thức res. giao thức biến thức được sử dụng (điều khiển truy cập mở rộng (EAC), trao đổi khóa số mũ mật lệnh đơn giản (SPEKE), PACE v2 theo EN 14890-1).

CHÚ THÍCH Như được xác định trong 10.3.2 trong khuôn mẫu tham chiếu điều khiển, một DO'80' được sử dụng để chuyển một tham chiếu cơ chế mã hóa. Trong C.2.2 bước 1 và C.2.3 bước 3, tham chiếu cơ chế mã hóa có chỉ định được chọn phải đồng nhất với giá trị của định danh đối tượng mô tả giao thức xác thực bằng gắn thẻ ẩn.

Một hoặc nhiều C-RP xác thực chung thực hiện một hoạt động xác thực.

- Nếu nối chuỗi được sử dụng, xem 5.3.3.
- INS P1 P2 được đặt là hoặc '86 00 00', hoặc '87 00 00'.
- Giá trị của trường L_c phụ thuộc vào các DO trong trường dữ liệu lệnh. Phụ thuộc vào liệu trường dữ liệu hồi đáp được mong đợi hay không, trường L_e hoặc được đặt là '00', hoặc không xuất hiện.

C.2.2 Sử dụng GENERAL AUTHENTICATE với byte INS chẵn ('86'): giao thức cơ sở mật lệnh ví dụ, ví dụ PACE v2

Bước 1: Môi trường SET SE (CRT AT)

Trường dữ liệu lệnh	{'80'-L-giá trị của mã định danh đối tượng đối với ánh xạ chung với thuật toán mã hóa cụ thể (ví dụ, TDES-3 hoặc AES) và ánh xạ trong trường hợp này (ánh xạ chung hoặc ánh xạ tích hợp} {'83'-L-tham chiếu mật lệnh} {'84'-L-tham chiếu thông số miền của khóa tạm thời riêng (khóa phiên giao tiếp)}
Trường dữ liệu hồi đáp	{} – Rỗng

Bước 2: mã hóa nonce

Trường dữ liệu lệnh	'7C' – L=0
Trường dữ liệu hồi đáp	{{'7C'-L2-{'80'-L-bất kỳ nonce)}

Bước 3: ánh xạ nonce (ví dụ, trao đổi khóa Diffie-Hellman (ánh xạ chung) hoặc ánh xạ cụ thể EC tới điểm (ánh xạ tích hợp)

Trường dữ liệu lệnh	{{'7C'-L2-{'81'-L-dữ liệu ánh xạ)}
Trường dữ liệu hồi đáp	{{'7C'-L2-{'82'-L-dữ liệu ánh xạ)} (ánh xạ chung) hoặc {} – Rỗng (ánh xạ tích hợp)

Bước 4: thực hiện quy ước khóa (PKA)

Trường dữ liệu lệnh	{{'7C'-L2-{'83'-L-khóa công khai tạm thời)}
Trường dữ liệu hồi đáp	{{'7C'-L2-{'84'-L- khóa công khai tạm thời)}

Bước 5: Xác thực chung

Trường dữ liệu lệnh	{{'7C'-L2-{'85'-L- mã thông báo xác thực)}
Trường dữ liệu hồi đáp	{{'7C'-L2-{'86'-L- mã thông báo xác thực)}

C.2.3 Sử dụng GENERAL AUTHENTICATE với byte INS chẵn ('86'): điều khiển truy cập mở rộng (EAC)

Giao thức EAC được phân tách thành hai phần: xác thực thiết bị cuối (TA) cho phép xác thực thiết bị giao diện hoặc máy chủ từ xa trong khi xác thực vi mạch (CA) chứng minh định danh của thẻ. Hai phiên bản được phân biệt theo EN 14890-1:

- EACv1 tham chiếu với chuỗi CA-TA;
- EACv2 tham chiếu với chuỗi TA-CA.

Giao thức xác thực thiết bị cuối đầu tiên nhập khóa công khai của thiết bị giao diện trong thẻ bằng phương thức chứng nhận kiểm tra thẻ. Trong bước thứ hai, giao thức thử thách-trả lời được thực hiện. Giao thức xác thực vi mạch xác định trao đổi khóa Diffie-Hellman với thiết lập kênh an toàn.

NA.1.1 Giao thức xác thực thiết bị cuối

Bước 1: môi trường SET SE (CRT DST)

Trường dữ liệu lệnh {'83'-L-tham chiếu khóa công khai

Trường dữ liệu hồi đáp {} – Rỗng

Bước 2: PERFORM SECURITY OPERATION (VERIFY CERTIFICATE)

Trường dữ liệu lệnh {'7F4E'-L-cấu trúc chứng nhận, được quy định trong ISO/IEC 7816-8}

{'5F37'-L-chữ ký số

Trường dữ liệu hồi đáp {} – Rỗng

Kiểm tra chứng nhận dọc theo chuỗi chứng nhận có thể tiếp tục cho đến khi khóa công khai của thẩm quyền xác minh tương ứng có sẵn trong thẻ được ban hành chứng nhận và chuyển khóa công khai của thiết bị giao diện. Nhóm giao thức EAC xác định PKI mức ba sao cho hai phép kiểm tra chứng nhận tiếp theo trở thành cần thiết.

Bước 3: Môi trường SET SE (CRT AT)

Trường dữ liệu lệnh {'80'-L-giá trị của mã định danh đối tượng} chỉ EACv2.0

{'83'-L-tham chiếu khóa công khai}

{'91'-L-khóa công khai tạm thời của IFD đối với CA} chỉ EACv2.0

Trường dữ liệu hồi đáp {} – Rỗng

Bước 4: GET CHALLENGE

Trường dữ liệu lệnh {} – Rỗng

Trường dữ liệu hồi đáp {dữ liệu ngẫu nhiên}

Bước 5: EXTERNAL AUTHENTICATE

Trường dữ liệu lệnh {dữ liệu hồi đáp – chữ ký số ký ngẫu nhiên và dữ liệu xác thực}

Trường dữ liệu hồi đáp {} – Rỗng

NA.1.2 Giao thức xác thực vi mạch

Bước 1[1]: môi trường SET SE (CRT AT)

Trường dữ liệu lệnh {'80'-L-giá trị của mã định danh đối tượng
{'84'-L-tham chiếu khóa riêng}

Trường dữ liệu hồi đáp {} – Rỗng

Bước 2: GENERAL AUTHENTICATE với khái niệm "thực hiện quy ước khóa (PKA)"

Trường dữ liệu lệnh {'7C'-L2-{'81'-L-dữ liệu ngẫu nhiên}- chỉ EACv2
{'82'-L-mã thông báo xác thực}}

Trường dữ liệu hồi đáp {'7C'-L2-{'80'-L-khóa công khai tạm thời của IFD}}

[1] CHÚ THÍCH:

Đối với EACv1 với 3DES chỉ lệnh sau sử dụng đối với bước 1. Trong trường hợp này bước 2 sẽ bị bỏ qua.

Bước 1: Môi trường SET SE (CRT KAT)

Trường dữ liệu lệnh {'91'-L-khóa công khai tạm thời của IFD} chỉ EACv1 với TDES
{'84'-L-tham chiếu khóa riêng} chỉ EACv1 với TDES

Trường dữ liệu hồi đáp {} – Rỗng

Phụ lục D

(tham khảo)

Định danh ứng dụng sử dụng số định danh người phát hành

D.1 Thông tin chung

Trong ISO/IEC 7816-5:1994, có thể sử dụng số định danh người phát hành trong định danh ứng dụng. Phụ lục này biểu thị định dạng của các AID như vậy.

D.2 Định dạng

Trong AID bất kỳ mà biet b8 tới b5 của byte đầu tiên được thiết lập từ '0' tới '9', trường đầu tiên và có thể duy nhất phải là số định danh người phát hành theo ISO/IEC 7812-1.

CHÚ THÍCH Trong ISO/IEC 7812-1:1993, số định danh người phát hành có thể bao gồm một số lẻ của nhóm bốn có giá trị từ '0' tới '9'. Khi đó nó được ánh xạ trong chuỗi byte bằng cách thiết lập bit b4 tới b1 của byte cuối cùng tới 1111.

Nếu mở rộng định danh ứng dụng độc quyền xuất hiện, khi đó byte được đặt là 'FF' phải phân tách hai trường.

Hình D.1 thể hiện một AID sử dụng một số định danh người phát hành: nó bao gồm tới mười bảy byte.

Số định danh bên phát hành theo ISO/IEC 7812-1 (hai hoặc nhiều byte)	'FF'	Mở rộng định danh ứng dụng độc quyền xuất (PIX)

Hình D.1 - AID sử dụng một số định danh người phát hành

Phụ lục E

(tham khảo)

Quy tắc mã hóa BER

E.1 Trường thẻ BER-TLV

Bit b8 và b7 của byte đầu tiên của trường thẻ biểu thị một lớp (xem ISO/IEC 8825-1).

- Giá trị 00 biểu thị một DO của lớp chung
- Giá trị 01 biểu thị một DO của lớp ứng dụng
- Giá trị 10 biểu thị một DO của lớp ngữ cảnh đặc biệt
- Giá trị 11 biểu thị một DO của lớp riêng

Bit b6 của byte đầu tiên của trường thẻ biểu thị một mã hóa (xem E.3).

Nếu bit b5 tới b1 của byte đầu tiên của trường thẻ không phải tất cả được đặt là 1, khi đó chúng mã hóa số thẻ từ zero tới ba mươi và trường thẻ bao gồm một byte đơn lẻ. Số thẻ 0 được loại trừ trong lớp chung.

Mặt khác (bit b5 tới b1 tất cả được đặt là 1), trường thẻ tiếp tục trên một hoặc nhiều byte tiếp theo.

- Bit b8 của mỗi byte tiếp theo phải được đặt là 1, trừ khi nó là byte tiếp theo cuối cùng.
- Bit b7 tới b1 của byte tiếp theo đầu tiên phải không được đặt là 0.
- Bit b7 tới b1 của byte tiếp theo đầu tiên, theo sau bởi biet b7 tới b1 của mỗi byte tiếp theo hơn nữa, cho đến và bao gồm bit b7 tới b1 của byte tiếp theo cuối cùng mã hóa số thẻ.

Bảng E.1 thể hiện byte đầu tiên của trường thẻ. Giá trị '00' là 0 có hiệu lực.

Bảng E.1 - Byte đầu tiên của trường thẻ BER-TLV trong TCVN 11167 (ISO/IEC 7816)

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	0	-	-	-	-	-	-	Lớp chung, không được xác định trong ISO/IEC 7816
0	1	-	-	-	-	-	-	Lớp ứng dụng, định danh được xác định trong tiêu chuẩn này
1	0	-	-	-	-	-	-	Lớp ngữ cảnh cụ thể, được xác định trong ISO/IEC 7816
1	1	-	-	-	-	-	-	Lớp riêng không được xác định trong ISO/IEC 7816
-	-	0	-	-	-	-	-	Mã hóa ban đầu
-	-	1	-	-	-	-	-	Mã hóa được xây dựng
-	-	-	Không phải tất cả được đặt là 1					Số thẻ từ zero tới ba mươi (trường thẻ ngắn, nghĩa là một byte đơn nhất)
-	-	-	1	1	1	1	1	Số thẻ lớn hơn ba mươi (trường thẻ dài, nghĩa là hai hoặc ba byte)

Trong trường thẻ của hai hoặc nhiều byte, giá trị '00' tới '1E' và '80' không có hiệu lực đối với byte thứ hai.

- Trong trường thẻ 2 byte, byte thứ hai bao gồm bit b8 được đặt là 0 và bit b7 tới b1 mã hóa một số lớn hơn ba mươi. Byte thứ hai có giá trị từ '1F' tới '7F'; số thẻ từ 31 tới 127.

- Trong trường thẻ 3 byte, byte thứ hai bao gồm bit b8 được đặt là 1 và bit b7 tới b1 không phải tất cả được đặt là 0; byte thứ ba bao gồm bit b8 được đặt là 0 và bit b7 tới b1 có giá trị bất kỳ. Byte thứ hai có giá trị từ '81' tới 'FF' và byte thứ ba từ '00' tới '7F'; số thẻ từ 128 tới 16 383.

E.2 Trường độ dài BER-TLV

Ở dạng ngắn, độ dài trường bao gồm một byte đơn nhất mà bit b8 được đặt là 0 và bit b7 tới b1 mã hóa số các byte trong trường giá trị. Một byte có thể mã hóa số bất kỳ từ zero tới 127..

CHÚ THÍCH số bất kỳ từ một tới 127 được mã hóa theo cùng cách thức trong trường độ dài BER-TLV như trong trường L_c và L_e. Mã hóa khác biệt đối với zero, 128 và nhiều hơn. Xem ví dụ, mã hóa của các DO trong lệnh GET DATA trong 11.4.3.

Ở dạng dài, trường độ dài bao gồm hai hoặc nhiều byte. Bit b8 của byte đầu tiên được đặt là 1 và bit b7 tới b1 không phải tất cả bằng nhau, do vậy mã hóa số các byte tiếp theo trong trườn độ dài. Các byte tiếp theo này mã hóa số các byte trong trường giá trị.

ISO/IEC 7816 hỗ trợ trường độ dài của một, hai, .. tới 5 byte (xem Bảng E.2). Trong ISO/IEC 7816, giá trị '80' và '85' tới 'FF' không có hiệu lực đối với byte đầu tiên của trường độ dài.

Bảng E.2 - Trường độ dài BER-TLV trong ISO/IEC 7816

	1st byte	2nd byte	3rd byte	4th byte	5th byte	N
1 byte	'00' to '7F'	-	-	-	-	0 to 127
2 bytes	'81'	'00' to 'FF'	-	-	-	0 to 255
3 bytes	'82'	'0000' to 'FFFF'		-	-	0 to 65 535
4 bytes	'83'	'000000' to 'FFFFFF'			-	0 to 16 777 215
5 bytes	'84'	'00000000' to 'FFFFFFFF'				0 to 4 294 967 295

E.3 Trường giá trị BER-TLV

Bit b6 của byte đầu tiên của trường thẻ biểu thị một mã hóa của trường giá trị:

- Giá trị 0 biểu thị mã hóa ban đầu của DO, nghĩa là 0 có thông tin được cung cấp trên mã hóa của trường giá trị, thậm chí nếu trường giá trị được mã hóa trong BER-TLV.
- Giá trị 1 biểu thị một mã hóa được xây dựng của DO, nghĩa là trường giá trị, nếu xuất hiện, được mã hóa trong BER-TLV. Trường giá trị không trống là một DO, hoặc kết nối của các DO mà không có phần đệm.

Phụ lục F

(tham khảo)

Xử lý đối tượng dữ liệu

F.1 Các thế hệ và khuôn mẫu trong DO được xây dựng

DO gốc (ảo) DO thế hệ 0		DO thế hệ 1		DO thế hệ 2		DO thế hệ 3		DO thế hệ 4	
'7F 70' L	*Giá trị =*								
		T1 L1'	Giá trị 1 =						
				T2 L2	V2				
				T3 L3'	Giá trị 3 =				
						T4 L4	V4		
						T6 L6	V6		
						T5 L5	Giá trị 5 =		
								T8 L8	V8
								T8 L8'	V8'
								T8 V8"	V8"
				T2 L2'	V2'				
				T14 L14	V14				
				T9 L9	Giá trị 9 =				
						T4 L4'			
						T6 L6"			
		T6 L6'	V6'						

Hình F.1 - Các thế hệ, DO và khuôn mẫu trong DO được xây dựng

Mỗi dòng của hình F.1 bao gồm một và chỉ một DO. Một DO sử dụng hai ô liên tiếp trên cùng một dòng, ô gần bên trái nhất bao gồm tiêu đề DO (thẻ, độ dài) và ô gần bên phải nhất bao gồm giá trị của nó.

Dòng kẻ đậm theo chiều thẳng gần bên trái nhất thể hiện khuôn mẫu hiện hành sau khi lựa chọn tệp, hoặc sau khi lựa chọn DO'7F70' ảo. Khuôn mẫu bao gồm DO'T1' và 'T6' xuất hiện ngay bên phải của dòng đơn kẻ đậm. Không có bộ dữ liệu Tn Ln xuất hiện ngay bên hải của dòng đứt đoạn kẻ đậm; dòng đứt đoạn thể hiện rằng khuôn mẫu chưa kết thúc.

Các DO thuộc dòng có đường bao đứt đoạn thuộc về kế cấu (tệp, bản ghi hoặc chuỗi dữ liệu), nhưng không thuộc về khuôn mẫu do chung được lồng vào các DO được xây dựng khác, nghĩa là 0 thuộc về thế hệ đầu tiên.

Sau khi lựa chọn DO'T1', khuôn mẫu hiện hành được thể hiện bằng dòng tô đậm, bắt đầu ngay bên phải của ô giữ "giá trị 1". Ô này được đóng khung bằng đường bao đậm để biểu thị rằng giá trị này là một khuôn mẫu, nghĩa là kết nối của các DO được lồng vào DO'T1' được xây dựng, tạo nên khuôn mẫu hiện hành sau khi lựa chọn DO'T1'. Khuôn mẫu này mô tả đặc tính của năm DO thế hệ thứ hai, DO'T2', 'T3', 'T2', 'T14', 'T19'. Khuôn mẫu cũng sử dụng đường đứt đoạn được tô đậm. Các DO thuộc về dòng có đường bao đứt đoạn thuộc về DO'T1', nhưng không thuộc về khuôn mẫu hiện hành sau khi lựa chọn DO'T1', do chúng được lồng vào trong các DO được xây dựng khác, nghĩa là 0 thuộc về thế hệ thứ hai.

Có hai phiên bản của DO'T2', có thẻ đồng nhất, nhưng có khả năng có giá trị và độ dài khác nhau. Điều này được cho phép, nhưng mang ý nghĩa rằng xử lý các DO này phải sử dụng DO theo thứ tự trong khuôn mẫu này. Khi hai phiên bản thuộc về cùng khuôn mẫu, sử dụng nhất quán thẻ để tham chiếu đảm bảo rằng chúng có cùng ý nghĩa.

Sau khi lựa chọn DO'T3', khuôn mẫu hiện hành được thể hiện bằng dòng tô đậm. Khuôn mẫu này mô tả đặc điểm ba DO thế hệ thứ ba, DO'T4', 'T6', 'T5'.

Sau khi lựa chọn DO'T9', khuôn mẫu hiện hành mô tả đặc điểm hai DO thế hệ thứ ba, DO'T4', 'T6'. Mặc dù trong cùng thế hệ như khuôn mẫu hiện hành sau khi lựa chọn DO'T3', nó là khuôn mẫu khác. Thế hệ thứ ba thể hiện hai phiên bản của DO'T6', nhưng chúng thuộc về các khuôn mẫu khác nhau và như vậy có thẻ có ý nghĩa khác nhau, ngoại trừ nếu có thêm thông tin xuất phát từ ví dụ, lớp thẻ 'T6'.

F.2 Tham chiếu bằng tiêu đề mở rộng

Tất cả các ví dụ thể hiện trong tiểu điều này phải mang lại kết quả chuỗi byte giống như hai cột gần bên trái nhất bị xóa bỏ tất cả các con số. Tiêu đề của tiểu điều này khi đó là "tham chiếu bằng một danh sách tiêu đề mở rộng". Điều này nhấn mạnh rằng DO mục tiêu và tiêu đề đầu tiên của tiêu đề mở rộng phải tương thích nhau, nghĩa là có cùng thẻ, để tham chiếu một chuỗi byte không trống.

'A1 37'	Value 1 =						
		'82 03'	'21 22 23'				
		'A3 1C'	Value 3 =				
				'84 04'	'40 41 42 43'		
				'86 02'	'61 62'		
				'A5 10'	Value 5 =		
						'88 03'	'81 82 83'
						'88 03'	'84 85 86'
						'88 04'	'87 88 89 8A'
		'82 04'	'24 25 26 27'				
		'8E 03'	'E0 E1 E2'				
		'A3 07'	Value 3' =				
				'84 01'	'46'		
				'86 02'	'63 64'		

Hình F.2 - DO mục tiêu của tất cả các tiêu đề mở rộng trong tiểu điều này

'A1 0C'	Value 1 =						
		'A3 06'	Value 3 =				
				'A5 04'	Value 5 =		
						'88 00'	
						'88 02'	
		'8E 00'					
		'A3 80'					

Hình F.3 - Phần tử dữ liệu tiêu đề mở rộng 1, bao gồm không bỏ qua sự tương thích trên DO ban đầu bất kỳ.

'A1 1B'	Value 1 =						
		'A3 0B'	Value 3 =				
				'A5 09'	Value 5 =		
						'88 03'	'81 82 83'
						'88 02'	'84 85'
		'8E 03'	'E0 E1 E2'				
		'A3 07'	Value 3' =				
				'84 01'	'46'		
				'86 02'	'63 64'		

Hình F.4 - Tương thích được tìm thấy với tiêu đề mở rộng 1 trong cây con của DO'A1'

Hình F.4 cho thấy rằng chỉ hai phiên bản đầu tiên của DO'88' là tương thích. Nếu tiêu đề mở rộng dưới thẻ '4D', không thể bao gồm phiên bản thứ hai mà không bao gồm phiên bản thứ nhất. Cắt cụt các giá trị của các DO ban đầu đã được thực hiện. Chuỗi byte tham chiếu là:

- Hoặc trong định dạng đối tượng dữ liệu:
- {88 03 81 82 83}{88 02 84 85}{8E 03 E0 E1 E2}{A3 07 {84 01 46}{86 02 63 64}}.
- Hoặc trong định dạng phần tử dữ liệu: '81 82 83 84 85 E0 E1 E2' {84 01 46} {86 02 63 64}

Hình F.5 thể hiện làm thế nào để bao gồm chỉ phiên bản thứ hai của DO'A3':

'A1 04'	Value 1 =						
		'8E 00'					
		'A3 80'					

Hình F.5 - Phần tử dữ liệu tiêu đề mở rộng 2, không gồm ẩn sự tương thích trên một DO được xây dựng

'A1 0E'	Value 1 =						
		'8E 03'	'E0 E1 E2'				
		'A3 07'	Value 3 =				
				'84 01'	'46'		
				'86 02'	'63 64'		

Hình F.6 - Sự tương thích được tìm thấy với tiêu đề mở rộng 2 trong cây con của DO'A1'

Phiên bản đầu tiên của DO'A3' không được tham chiếu do DO đầu tiên được tham chiếu là DO'8E' không bao gồm tham chiếu DO bất kỳ trước nó, theo 8.4.7. Hình F.7 thể hiện tiêu đề mở rộng phải có cùng kết quả là tiêu đề mở rộng hình F.5.

'A1 06'	Value 1 =						
		'A3 00'					
		'8E 00'					
		'A3 80'					

Hình F.7 - Mã dư của phần tử dữ liệu tiêu đề mở rộng 2

Trong trường hợp được thể hiện ở hình F.5, hình F.6 và hình F.7, chuỗi byte được tham chiếu là:

- Hoặc trong định dạng đối tượng dữ liệu: {8E 03 E0 E1 E2}{A3 07 {84 01 46}{86 02 63 64}}.
- Hoặc trong định dạng phần tử dữ liệu: 'E0 E1 E2'{84 01 46}{86 02 63 64}

'A1 04'	Value 1 =						
		'A3 00'					
		'A3 80'					

Hình F.8 - Phần tử dữ liệu tiêu đề mở rộng 3, bao gồm bỏ qua tương thích trên DO được xây dựng

'A1 09'	Value 1 =						
		'A3 07'	Value 3' =				
				'84 01'	'46'		
				'86 02'	'63 64'		

Hình F.9 - Sự tương thích được tìm thấy với tiêu đề mở rộng 3 trong cây con của DO'A1'

Trong trường hợp được thể hiện ở hình F.8 và hình F.9, chỉ báo tương thích với phiên bản đầu tiên của DO'A3' phải bị bỏ qua trở thành cần thiết do không có sự tương thích nào có thể xảy ra giữa các sự tương thích với hai phiên bản của DO'A3'. Chuỗi byte được tham chiếu là:

- Hoặc trong định dạng đối tượng dữ liệu: {A3 07{84 01 46}{86 02 63 64}}.
- Hoặc trong định dạng phần tử dữ liệu: {84 01 46}{86 02 63 64}

'A1 08'	Value 1 =						
		'A3 06'	Value 3 =				
				'A5 04'	Value 5 =		
						'88 00'	
						'88 80'	

Hình 10 - Phần tử dữ liệu tiêu đề mở rộng 4, bao gồm bỏ qua tương thích trên DO ban đầu

'A1 09'	Value 1 =						
		'A3 07'	Value 3 =				
				'A5 05'	Value 5 =		
						'88 03'	'84 85 86'

Hình 11 - Sự tương thích được tìm thấy với tiêu đề mở rộng 4 trong cây con của DO'A1'

Hình F.8 thể hiện rằng chỉ phiên bản thứ hai của DO'88' là tương thích. Cú pháp của tiêu đề mở rộng 4 không có khả năng dưới thẻ '4D'. Chuỗi byte được tham chiếu là:

- Hoặc trong định dạng đối tượng dữ liệu: {88 03 84 85 86}. Tiêu đề mở rộng được gắn thẻ bằng '5F61'.
- Hoặc trong định dạng phần tử dữ liệu: '84 85 86}. Tiêu đề mở rộng được gắn thẻ bằng '5F60'.

F.3 Sử dụng lệnh UPDATE DATA

Ví dụ này giả định rằng một và chỉ mọt DO'B1' xuất hiện trong VA. Nếu có nhiều phiên bản của DO'B1' xuất hiện, cập nhật một trong số chúng có thể được thực hiện:

- Hoặc bằng lựa chọn một phiên bản bằng C-RP SELECT DATA, sau đó cập nhật các DO trong thế hệ tiếp theo.
- Hoặc thiết lập một con trỏ trên phiên bản này bằng một hoặc một vài C-RP GET NEXT DATA.

Hình F.12 thể hiện mọt DO'B1' được cập nhật bằng C-RP UPDATE DATA. Cấu trúc cây của nó bao gồm:

Một DO'82' ban đầu (thế hệ thứ hai) và một DO'B2' được xây dựng (thế hệ thứ hai).

DO'B2' được xây dựng (thế hệ thứ hai) lồng vào hai DO'90' và '91' ban đầu, (thế hệ thứ ba) và một DO'B3' được xây dựng (thế hệ thứ ba).

DO'B3' được xây dựng (thế hệ thứ ba) lồng vào hai DO'84' và '86' ban đầu (thế hệ thứ tư).

'B1 1C'	Value 1 =						
		'82 04'	'21 22 23 24'				
		'B2 14'	Value 2 =				
				'90 03'	'01 02 03'		
				'91 04'	'11 12 13 14'		
				'B3 07'	Value 3 =		
						'84 01'	'46'
						'86 02'	'63 64'

Hình F.12 - DO'B1' được cập nhật

Hình F.13 thể hiện đối số của một lệnh UPDATE DATA. Nó là một DO được dựa trên DO'B1'. Nó là cây con đối với DO'B1' nguyên gốc:

- Một số "nhánh" (DO) có thể xuất hiện; các nhánh này phải được cập nhật.
- Một số bị thiếu; số này phải không được cập nhật, do đó được giữ làm DO'B0' nguyên gốc.
- Một số có thể được bổ sung, chúng phải được tạo ra.

'B1 10'	Value 1' =						
		'B2 09"	Value 2' =				
				'B3 07'	Value 3' =		
						'84 00'	
						'86 04'	'65 66 67 68'
		'8E 03'	'E1 E2 E3'				

Hình F.13 - Đối số của lệnh UPDATE DATA

Hình F.14 thể hiện nội dung của DO'B1' sau thanh công của C-RP UPDATE DATA:

Trong thế hệ thứ hai, DO'82' còn nguyên, DO'B2' được cập nhật và DO'8E' được tạo ra.

Trong thế thệ thứ ba, DO'90' và '91' ban đầu còn nguyên và DO'B3' được cập nhật.

Trong thế hệ thứ tư, DO'84' ban đầu hiện giờ trống và DO'86' được cập nhật. Giá trị mới của DO'86' được truyền trong lệnh (xem hình F.13) thay thế giá trị trước (xem hình F.12)

'B1 22'	Value 1'' =						
		'82 04'	'21 22 23 24'				
		'B2 15'	Value 2'' =				
				'90 03'	'01 02 03'		
				'91 04'	'11 12 13 14'		
				'B3 08'	Value 3'' =		
						'84 00'	
						'86 04'	'65 66 67 68'
		'8E 03'	'E1 E2 E3'				

Hình F.14 - DO'B1' cập nhật, trong đó các DO được bổ sung và biến đổi thể hiện bằng in đậm

F.4 Thuộc tính an toàn đối với một DO

'UV' L	Value					// constructed DO		
		'XY' L1	V1			// DO under DO'UV'		
		'62' L2	Value 2			// data control parameters DO		
				'A0 L3'	Value 3	// Security attribute for DOs		
						'9C' L4	V4	//Security attribute referencing security parameters template #1
						'5C01'	'XY'	// Tag list referencing DO'XY'
				'AD' L5	Value 5			// Security parameters template
						'8001'	'01'	// Security parameters template number
						'A1' L6	Value 6	// Protection uses of a private key
						'63' L7	Value 7	//Wrapper referencing the key

Hình F.15 - Khuôn mẫu hiện hành với DO'XY' và thuộc tính an toàn của nó (bố cục chung)

Hình F.15 mô tả mã hóa của thuộc tính an toàn của DO'XY' được lồng trong DO'UV'. DO'A0' thuộc tính an toàn được lồng trong DO'62' thông số kiểm soát, cũng lồng vào DO'AD' khuôn mẫu thông số an toàn. DO'62' có thể bao gồm các DO CP khác không đại diện trong hình do không có liên quan đến ví dụ này.

Thẻ được cho trong danh sách thẻ trong DO'A0' thuộc tính an toàn phải có nghĩa, nghĩa là chỉ tới một DO dưới DO'UV', nói cách khác một DO thế hệ thứ nhất nếu DO'UV' được lựa chọn. DO'AD' được tham chiếu bằng số của nó phải dưới DO'62' dưới DO'UV'.

F.5 Ví dụ tham chiếu khóa trong DO tự điều khiển

1st	2nd	3rd	4th	Thế hệ
62		Khuôn mẫu thông số kiểm soát		
	A0	Khuôn mẫu thuộc tính an toàn đối với các DO		
		90	AMF ‖SCB(ref#1) ‖SCB(ref#2) ‖SCB(ref#3)	Thẻ '9D' cũng có thể được sử dụng ở đây dưới thẻ 'AB' khi sử dụng định dạng mở rộng
		5C	Danh sách thẻ, nội dung không được chi tiết trong Bảng này	
	73	Thông tin độc quyền được mã hóa trong BER-TLV		
	AC	Khuôn mẫu định danh cơ chế mật mã		
	8A	LCS (trạng thái vòng đời)		
	AD	Khuôn mẫu thông số an toàn #1 được tham chiếu ở trên		
		06	OID hướng tới mô tả của ví dụ, thuật toán và sử dụng thông tin độc quyền	
		80	Giá trị = '01', số chuỗi của DO'AD'	
		A0	Mở rộng thuộc tính an toàn đối với đối tượng xác thực	
			8C	Thuộc tính an toàn trong định dạng compact, tham chiếu SE	Lựa chọn giữa các điều này
			AB	Thuộc tính an toàn trong định dạng mở rộng, tham chiếu SPT	
			9C	Định dạng compact thuộc tính an toàn, tham chiếu SPT	
			5C	Danh sách thẻ, nội dung không được chi tiết trong Bảng này	
		AD	Khuôn mẫu thông số an toàn, nội dung không được chi tiết trong Bảng này	
		...	Các DO hơn nữa không được chi tiết trong Bảng này, thế hệ thứ ba	
		B3	Thông tin liên quan đến OID được mã hóa trong BER-TLV	
		63	Trình bao, nội dung không được chi tiết trong Bảng này	
	AD	Khuôn mẫu thông số an toàn #2 được tham chiếu ở trên		
		80	Giá trị = '02', số chuỗi của DO'AD'	
		A4	Mở rộng thuộc tính an toàn đối với mã bí mật	
			'IJ'	Thuộc tính an toàn tham chiếu SE trong định dạng compact ('IJ'=8C') hoặc mở rộng ('IJ'='AB')
		63	Trình bao, nội dung không được chi tiết trong Bảng này	
	AD	Khuôn mẫu thông số an toàn #3 được tham chiếu ở trên		
		06	OID hướng tới mô tả của ví dụ, thuật toán và sử dụng thông tin độc quyền	
		80	Giá trị = '03', số chuỗi của DO'AD'	
		A1	Mở rộng thuộc tính an toàn đối với mã riêng	
			'ZT'	Thuộc tính an toàn trong định dạng compact ('ZT'=9C') hoặc mở rộng ('ZT'='AB')
		63	Trình bao, nội dung không được chi tiết trong Bảng này	
		73	Thông tin liên quan đến OID được mã hóa trong BER-TLV	

Hình F.16 - Giá trị của DO'XY' tự điều khiển với thuộc tính an toàn tham chiếu ba khóa

CHÚ THÍCH Hình F.16 không biểu thị trường độ dài của các DO mà các trường này mang thông tin nhỏ. Các dòng in đậm biểu thị ở bên trái thẻ của DO được xây dựng, ở bên phải thẻ của DO được lồng vào trong.

Hình F.16 mô tả mã hóa của thuộc tính an toàn trong DO'XY'. DO'A0' thuộc tính an toàn được lồng trong DO'62' thông số kiểm soát, cái mà cũng lồng ba phiên bản của DO'AD' khuôn mẫu thông số an toàn. DO'XY' và DO'62' có thể bao gồm các DO CP khác không được đại diện trong hình do không liên quan đến trong ví dụ này.

Thẻ được cho trong danh sách thẻ không trống được lồng trong DO'A0' thuộc tính an toàn phải có nghĩa, nghĩa là hướng vào một DO dưới DO'XY', nói cách khác DO thế hệ thứ nhất. DO'AD' khuôn mẫu thông số an toàn thuộc về cùng thế hệ như DO'A0' thuộc tính an toàn tham chiếu DO'AD'.

CHÚ THÍCH DO'A0' thuộc tính an toàn được lồng trong DO'62'. DO'A0' mở rộng thuộc tính an toàn được lồng trong DO'AD'. Cú pháp của chúng khác nhau.

Phụ lục G

(tham khảo)

Mở rộng khuôn mẫu bằng trình bao được gắn thẻ

G.1 Tổng quát

Mở rộng khuôn mẫu bằng trình bao được gắn thẻ cho phép thẻ mô phỏng, trong VA được cho, một hoặc một vài DO "xa" không thực sự thuộc về VA (xem 8.2.2 và 8.4.8 và 8.4.9). Phụ lục này giả định rằng trạng thái an toàn cho phép đọc một DO xa bằng C-RP GET DATA. Hình dưới đây thể hiện cả trình bao được gắn thẻ được tạo ra trong khuôn mẫu cơ sở (ví dụ bằng lệnh PUT DATA) và kết quả của trình bao được gắn thẻ này trong mở rộng khuôn mẫu. Chỉ các thẻ xuất hiện:

<table>
<tr><th>Thế hệ thứ n</th><th>Thế hệ thứ (n+1)</th><th colspan="2">Ý nghĩa</th></tr>
<tr><td>'63'</td><td></td><td colspan="2">Trình bao được gắn thẻ xuất hiện tong khuôn mẫu cơ sở</td></tr>
<tr><td></td><td>'XY' (trống)</td><td colspan="2">DO phải được tham chiếu cục bộ bằng thẻ 'XY'</td></tr>
<tr><td></td><td>'5C' hoặc '4D'</td><td colspan="2">Tham chiếu gián tiếp tới DO'ZT' trong VA tạm thời, xem 1) bên dưới</td></tr>
<tr><td rowspan="2"></td><td>'4F'</td><td>Tham chiếu curDF trong VA tạm thời</td><td rowspan="2">Giải tự động trình bao được gắn thẻ sử dụng các DO này để thiết lập VA tạm thời mà tham chiếu với DO'ZT' có hiệu lực. Xem 2) và 3) bên dưới.</td></tr>
<tr><td>'51'</td><td>Tham chiếu curEF trong VA tạm thời</td></tr>
<tr><td>'XY'</td><td></td><td colspan="2">Mô phỏng DO'ZT' trong mở rộng khuôn mẫu</td></tr>
</table>

Hình G.1 - Cú pháp và kết quả của trình bao được gắn thẻ

1) Các thẻ khác có sẵn để tham chiếu DO (xem 8.4.8).
2) Có các cách thức khác để thiết lập VA tạm thời (xem 8.4.8).
3) Khi các phần tử của VA tạm thời thuộc về VA hiện hành, không cần lặp lại chúng trong trình bao được gắn thẻ, chỉ xác nhận chúng khi cả hai không xuất hiện (xem các điều sau).

G.2 Tham chiếu trong EF hiện hành

Ví dụ dưới đây thể hiện nội dung của một EF'12 34' (định danh tệp) dưới một DF'A0 01 02 03 04' ứng dụng (định danh ứng dụng). Hình này thể hiện mã hóa hệ cơ số 16 của thẻ và trường độ dài. Ngoại trừ trong giá trị của trình bao được gắn thẻ, các giá trị của DO ban đầu không có nghĩa.

Thế hệ 1		Thế hệ 2		Thế hệ 3		Thế hệ 4		Thế hệ 5
'62 0E'	Giá trị							
		'A0 C0'	Giá trị					
				'5C 00'				
'80 01'	'XY'			'88 08'	'B1 B2 B3 B4 B5 B6 B7 B8'			
'A2 13'	Giá trị							
		'B2 11'	Giá trị					
				'80 04'				
				'81 02'				
				'82 03'				
				'63 0B'	Giá trị			
						'91 00'		
						'4D 05'		
							Giá trị	
						'51 00'		'7F 70 02 90 00'
				'91 01'	'XY'			
CHÚ THÍCH Phông chữ in đậm nghiêng '*9101XY*' chỉ ra phần mở rộng của khuôn mẫu được mã hóa trong DO '63' bên trên								

Hình G.2 - Nội dung của EF '12 34' dưới DF ứng dụng tên là 'A0 01 02 03 04'

Giá trị của DO'B2' dưới DO'A2' bao gồm một khuôn mẫu cơ sở (DO '80', '81', '82' và '63') và mở rộng khuôn mẫu (DO'91') do DO'63' trình bao được gắn thẻ tham chiếu theo mọt tiêu đề mở rộng, DO'80' trong thế hệ thứ nhất (cột gần bên trái nhất). DO'80' này phải được tham chiếu bằng thẻ '91' trong khuôn mẫu nó mở rộng, để tránh xung đột với thẻ '80' có khả năng tham chiếu các loại khác nhau. Thẻ '80' xuất hiện lần thứ hai trong loại in đậm, trong thế hệ thứ nhất (DO thuộc về khuôn mẫu cơ sở); và trong thế hệ thứ năm (trong phần tử dữ liệu tiêu đề mở rộng). Giá trị 'XY' xuất hiện hai lần trong loại in đậm, trong thế hệ thứ nhất (nơi nó được xác định); và trong thế hệ thứ ba, là giá trị của DO'91'. Thẻ '91' xuất hiện hai lần trong loại in đậm, trong thế hệ thứ tư nơi nó được xác định); và trong thế hệ thứ ba (DO'91' thuộc về mở rộng khuôn mẫu).

DO'51' tham chiếu tệp trống biểu thị rằng thao tác gián tiếp có hiệu lực trong DO'B2' tham chiếu VA, cái mà lồng vào DO'63', do vậy xác nhận rằng VA tạm thời tham chiếu ứng dụng 'A0 01 02 03 04' và EF'12 34'. Khi DO được xây dựng hiện hành là DO'B2', DO'80' có thể được xử lý cục bộ bằng thẻ '91'.

- APDU lệnh '00 CA 00 91 00' phải phục hồi 'XY 9000'.
- APDU lệnh '00 CB 00 00 03' {5C 01 91} phải phục hồi {91 01 XY} '9000'.

G.3 Tham chiếu trong DF ứng dụng hiện hành, ví dụ đầu tiên

Thế hệ 1		Thế hệ 2		Thế hệ 3		Thế hệ 4	
'62 0E'	Giá trị						
		'A0 0c'	Giá trị				
				'5C 00'			
				'8B 08'	'B1 B2 B3 B4 B5 B6 B7 B8'		
'80 01'	'XY'						
'A2 13'	Giá trị						
		'B2 11'	Giá trị				
				'80 04'	'11 12 13 14'		
				'81 02'	'21 22'		
				'82 03'	'31 32 33'		

Hình G.3 - Nội dung thay thế của EF'12 34' dưới DF ứng dụng được gọi là 'A0 01 02 03 04'

Trong hình G.3, nội dung của EF'12 34' không bao gồm trình bao được gắn thẻ có thể xuất hiện (nếu có hiệu lực) trong VA bất kỳ tham chiếu DF 'A0 01 02 03 04' ứng dụng, nhưng không phải EF'12 34'. Cú pháp của trình bao được gắn thẻ, tham chiếu DO giống như trong G.2 phải là:

'6309'			
	'92 00'		Trong ví dụ này, DO phải được tham chiếu cục bộ bằng thẻ '92'
	'5C 01'	'80'	Tham chiếu gián tiếp với DO'80' trong DO thế hệ đầu tiên trong EF '1234'
	'51 02'	'1234'	Tham chiếu EF'1234' dưới ứng dụng hiện hành

Hình G.4 - Cú pháp của trình bao được gắn thẻ tham chiếu một EF; sử dụng một danh sách thẻ

Như được so sánh với hình G.2:

- Tham chiếu hiện của EF biểu thị rằng tham chiếu gián tiếp có hiệu lực trong EF '12 34'.
- Do DO'80' thuộc về thế hệ thứ nhất trong EF'1234' tiêu đề mở rộng có thể được thay thế bằng danh sách thẻ.

Khi được ban hành từ VA bất kỳ tham chiếu ứng dụng được gọi là 'A0 01 02 03 04' và cha của trình bao được gắn thẻ ở trên, DO'80' có thể được xử lý cục bộ bằng thẻ '92':

- APDU lệnh '00 CA 00 92 00' phải phục hồi 'XY 9000'.
- APDU lệnh '00 CB 00 00 03' {5C 01 92} '00' phải phục hồi {92 01 XY} '9000'.

Hàm tương tự (nhưng không đồng nhất) có thể được hỗ trợ bằng C-RP GET DATA khác. Khi được ban hành từ cùng VA, APDU lệnh '00 CB **12 34** 03' {5C 01 **80**}'00' phải phục hồi {**80** 01 XY} '9000'. Sự khác biệt với C-RP ở trên được thể hiện ở dạng in đậm. Để sử dụng giải pháp thay thế này, mọi đối tượng bên ngoài phải biết định danh tệp '12 34', thẻ '80' của DO và thế hệ của nó. Tất cả điều này có thể phụ thuộc vào hệ thống xử lý.

G.4 Tham chiếu trong DF ứng dụng hiện hành, ví dụ thứ hai

Muốn xử lý DO'A0' dưới DO'62', cần có tiêu đề mở rộng; DO'A0' này thuộc về thế hệ thứ hai EF. Trình bao được gắn thẻ phải là:

'6309'			
	'A000'		Trong ví dụ này, DO phải được tham chiếu cục bộ bằng thẻ 'A0'
	'4D04'	'6202A080'	Tham chiếu gián tiếp với DO'A0' trong các DO thế hệ thứ hai dưới DO'62'
	'5102'	'1234'	Tham chiếu EF'1234' dưới ứng dụng hiện hành

Hình G.5 - Cú pháp của trình bao được gắn thẻ tham chiếu một EF; nó sử dụng tiêu đề mở rộng

Thẻ của DO'A0' dưới DO'62' có ý nghĩa tiêu chuẩn của thuộc tính an toàn đối với các DO. Xử lý nó cục bộ với cùng thẻ, dưới DO'62' khác, tránh sao chép thuộc tính an toàn này, ví dụ, nếu một số EF trong DF ứng dụng sử dụng cùng thuộc tính an toàn mặc định đối với các DO.

Khi được ban hành từ VA bất kỳ tham chiếu ứng dụng được gọi là 'A0 01 02 03 04' và trình bao được gắn thẻ ở trên,

- APDU lệnh '00 CA 00 A0 00' phải phục hồi {5C 00}{8B 08 B1 B2 B3 B4 B5 B6 B7 B8}'9000'.
- APDU lệnh '00 CB 00 00 03'{5C 01 A0'}'00' phải phục hồi {A0 0C {5C 00}{8B 08 B1 B2 B3 B4 B5 B6 B7 B8}'9000'.

G.5 Tham chiếu ngoài DF ứng dụng hiện hành

VA hiện hành không tham chiếu DF 'A0 01 02 03 04' ứng dụng. Vì vậy, tham chiếu ứng dụng và EF là cần thiết. Để tham chiếu DO giống như trong ví dụ đầu tiên của G.3, trình bao được gắn thẻ phải là:

'6310'			
	'9200'		Trong ví dụ này, DO phải được tham chiếu cục bộ bằng thẻ '92'
	'5C01'	'80'	Tham chiếu gián tiếp với DO'80' trong các DO thế hệ đầu tiên
	'4F05'	'A0 01 02 03 04'	Tham chiếu ứng dụng được gọi là 'A0 01 02 03 04'
	'5102'	'1234'	Tham chiếu EF'1234' dưới ứng dụng hiện hành

Hình G.6 - Cú pháp của trình bao được gắn thẻ tham chiếu một DF ứng dụng và một EF; nó sử dụng một danh sách thẻ

Khi được ban hành từ VA bất kỳ bao gồm trình bao được gắn thẻ ở trên,

- APDU lệnh '00 CA 00 92 00' phải phục hồi 'XY 9000'.
- APDU lệnh '00 CB 00 00 03' {5C 01 92} 00' phải phục hồi {92 01 XY} '9000'.

G.6 Cảnh báo

Tham chiếu gián tiếp một DO thuộc mở rộng khuôn mẫu có thể mang đến kết quả tham chiếu long vòng.

Sử dụng trình bao được gắn thẻ trao đổi tính phức tạp của lệnh so với tính phức tạp trong dữ liệu. Do vậy, cần phải chú ý cẩn thận khi chọn thẻ mà theo đó DO xa có thể được nhìn thấy cục bộ, để tránh phải xử lý:

- DO được xây dựng bằng thẻ biểu thị một DO ban đầu, cái mà khó khăn, nhưng có khả năng.

- DO ban đầu bằng thẻ biểu thị một DO được xây dựng; điều này phải gây ra DO hoặc khuôn mẫu có cú pháp không có hiệu lực.
- DO tiêu chuẩn, của dạng được xác định, bằng thẻ khác mà thẻ không biểu thị loại này. Điều này cho biết rằng đặc tả hoặc tiêu chuẩn sử dụng điều này để cập đến dạng.
- DO bằng thẻ đã được sử dụng trong cùng khuôn mẫu như trình bao được gắn thẻ, mà không nhận biết về việc sao chép các phiên bản.

Phụ lục H

(tham khảo)

Phân tích một tiêu đề mở rộng dựa vào DO mục tiêu

Thủ tục được mô tả trong phụ lục này tính đến ba trường hợp sử dụng của tiêu đề mở rộng:

- Hoặc hoàn thành tiêu đề mở rộng được xây dựng theo 8.4.5, biết DO được xây dựng tham chiếu.
- Hoặc được xây dựng theo 8.4.5, biết giá trị trước của DO tham chiếu, được cập nhật kể từ đó. Điều này có thể mang lại kết quả là các cấu trúc khác nhau đối với tiêu đề mở rộng và DO mục tiêu của nó.
- Hoặc xây dựng mà không tham chiếu dư với các DO bị bỏ qua, để rút ngắn tiêu đề mở rộng.

Để theo thủ tục, hiển thị tiêu đề mở rộng và DO mục tiêu như trong phụ lục F: một tiêu đề mỗi dòng trong Bảng tiêu đề, một DO mỗi dòng trong Bảng DO. Thứ tự của các dòng thể hiện thứ tự của các tiêu đề và DO, các thế hệ thể hiện sự dịch chuyển cột. Các quy tắc sau phải áp dụng lần lượt, trừ khi "chuyển tới..." được đề cập đến:

1) Nếu ít nhất một Bảng trống, thủ tục hoàn thành
2) Nếu tiêu đề mở rộng có nghĩa là chỉ tham chiếu một DO, thủ tục được hoàn thành nếu sự tương thích không bỏ qua (L≠'80' trong tiêu đề) với DO ban đầu, hoặc tương thích hoàn toàn (L='80' trong tiêu đề) với DO được xây dựng đạt được.
3) Đọc dòng đầu tiên (trên cùng) trong Bảng tiêu đề và tìm kiếm sự tương thích của tiêu đề trong Bảng DO. Trừ có quy định khác (xem 8)), việc tìm kiếm phải được thực hiện trong dòng đầu tiên (trên cùng) của Bảng DO.
4) Nếu tương thích (cùng thẻ, cùng thế hệ) đạt được, chuyển tới 10).
5) Nếu hệ DO thấp hơn hệ tiêu đề, chuyển tới 7).
6) Nếu tìm kiếm không đến được dòng cuối cùng của Bảng DO, tiếp tục tìm kiếm ở dòng tiếp theo. Chuyển tới 1).

CHÚ THÍCH khi tìm kiếm một khuôn mẫu, các DO ở thế hệ cao hơn hoặc có thẻ bị sai bị bỏ qua.

7) Nếu sự tương thích được tìm thấy trên DO ban đầu, xóa bỏ dòng từ Bảng tiêu đề. Chuyển tới 1).

CHÚ THÍCH DO tham chiếu không bao giờ ở trong khuôn mẫu được tìm kiếm, hoặc bị xóa bỏ sau khi tương thích (xem 10)).

8) Nếu sự tương thích được tìm kiếm ở trên DO được xây dựng, hoặc bỏ qua (L='00' trong tiêu đề) hoặc hoàn thành (L='80' trong tiêu đề), xóa bỏ dòng từ Bảng tiêu đề. Chuyển tới 1).

CHÚ THÍCH DO tham chiếu không bao giờ ở trong khuôn mẫu được tìm kiếm, hoặc bị xóa bỏ sau khi tương thích (xem 10)).

9) Xóa bỏ khỏi Bảng tiêu đề các dòng tham chiếu DO được xây dựng và nội dung của nó. Chuyển tới 1).

CHÚ THÍCH DO được xây dựng tham chiếu không bao giờ ở trong khuôn mẫu được tìm kiếm, hoặc bị xóa bỏ sau khi tương thích (xem 10)). Tham chiếu với nội dung của nó trở nên vô ích.

10) Áp dụng 8.4.6. Xóa bỏ dòng tương thích khỏi các bảng. Trong Bảng DO, xóa bỏ tất cả các dòng ở trên, nếu có.

CHÚ THÍCH Đóng góp bất kỳ của các DO bị xóa bỏ này đối với chuỗi byte phải không tương thích với thứ tự do tiêu đề mở rộng chỉ định.

11) Nếu đạt được sự tương thích với DO ban đầu, chuyển tới 1).

12) Nếu tương thích bị bỏ qua (L='00' trong tiêu đề) hoặc tương thích hoàn toàn (L-'80' trong tiêu đề) với DO được xây dựng đạt được, xóa bỏ khỏi Bảng DO tất cả các dòng của giá trị của DO tương thích. Chuyển tới 1).

13) Nếu tương thích khác với DO được xây dựng đạt được, chuyển tới 1).

CHÚ THÍCH Phân tích và tìm kiếm khi đó phải diễn ra ở thế hệ tiếp theo.

Thư mục tài liệu tham khảo

[1] EN 14890-1:2008, Application interface for smart cards used as secure signature creation device - Part 1: Basic services

[2] EN 14890-1:2012, Application interface for smart cards used as secure signature creation device - Part 1: Addition services

[3] TCVN 7217-1:2002 (ISO 3166-1:1997), Mã hóa đối với đại diện tên nước và phân vùng - Phần 1: mã nước

[4] ISO/IEC 7810:2003, Identification cards - Physical characteristics

[5] ISO/IEC 7812-1:2000, Identification cards - Identification of issuers - Part 1: Numbering system

[6] TCVN 11167 (ISO/IEC 7816) (tất cả các phần), Thẻ định danh - Thẻ mạch tích hợp

[7] ISO/IEC TR 9577:1999, Information technology - Protocol identification in the network layer

[8] ISO/IEC 9796 (tất cả các phần), Information technology - Security techniques - Digital signature schemes giving message recovery

[9] ISO/IEC 9797 (tất cả các phần), Information technology - Security techniques - Message authentication codes (MACs)

[10] ISO/IEC 9798 (tất cả các phần), Information technology - Security techniques - Entity authentication

[11] ISO/IEC 9979:1999, Information technology - Security techniques - Procedures for the registration of crytographic algorithms

[12] ISO 9992-2:1998, Financial transaction cards - Messages between the integrated circuit card and the card accepting device - Part 2: Function, messages (commands and responses), data elements and structures

[13] ISO/IEC 10116:1997, Information technology - Security techniques - Modes of operation for an n-bit block cipher

[14] ISO/IEC 10118 (tất cả các phần), Information technology - Security techniques - Hash - functions

[15] ISO/IEC 10536 (tất cả các phần), Identification cards - Contactless integrated circuit cards - Close-coupled cards

[16] TCVN 8271 (ISO/IEC 10646), Công nghệ thông tin - Tập hợp đặc tính được mã hóa chung (UCS)

[17] TCVN 7817 (ISO/IEC 11770) (tất cả các phần), Công nghệ thông tin - Kỹ thuật an toàn - Quản lý khóa

[18] ISO/IEC 14443 (tất cả các phần), Identification cards - Contactless integrated circuit cards - Proximity cards

[19] ISO/IEC 14888 (tất cả các phần), Information technology - Security techniques - Digital signatures with appendix

[20] ISO/IEC 15693 (tất cả các phần), Identification cards - Contactless integrated circuit cards - Vicinty cards

[21] ISO/IEC 18033 (tất cả các phần), Information technology - Security techniques - Encrytion algorithms

[22] ISO/IEC 18092, Information technology - Telecommunications and information exchange between systems - Near field communication - Interface and protocol (NFCIP-1)

[23] ISO/IEC 24727 (tất cả các phần), Identification cards - Integrated circuit card programming interfaces

[24] ISO/IEC 24727-2, Identification cards - Integrated circuit card programming interface - Part 2: Generic card interface

[25] ISO/IEC 24727-3, Identification cards - Integrated circuit card programming interface - Part 3: Application interface

[26] IETF RFC 1738:1994, Uniform resource locators (URL)

[27] IETF RFC 2396:1998, Uniform resource locators (URL): General syntax