TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 11167-13:2015
ISO/IEC 7816-13:2007

Xuất bản lần 1

THẺ DANH ĐỊNH - THẺ MẠCH TÍCH HỢP - PHẦN 13: LỆNH ĐỐI VỚI QUẢN LÝ ỨNG DỤNG TRONG MÔI TRƯỜNG ĐA ỨNG DỤNG

Identification cards - Integrated circuit cards - Part 13: Commands for application management in a multi-application environment

HÀ NỘI - 2015

Mục lục

Trang

Lời nói đầu

TCVN 11167-13:2015 hoàn toàn tương đương với ISO/IEC 7816-13:2007.

TCVN 11167-13:2015 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 13: Lệnh đối với quản lý ứng dụng trong môi trường đa ứng dụng

Identification cards – Integrated circuit cards –
Part 13: Commands for application management in multi-application enviroment

1 Phạm vi áp dụng

Tiêu chuẩn này quy định lệnh đối với quản lý ứng dụng trong môi trường đa ứng dụng. Các lệnh này bao trùm toàn bộ vòng đời ứng dụng trong một thẻ mạch tích hợp đa ứng dụng và các lệnh này có thể được dùng trước và sau khi được phát hành tới chủ thẻ. Tiêu chuẩn này không đề cập tới việc thiết lập trong thẻ và/hoặc thế giới bên ngoài.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên 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, bổ sung (nếu có).

TCVN 11167-4 (ISO/IEC 7816-4) Thẻ định danh - Thẻ mạch tích hợp - Phần 4: Tổ chức, an ninh và lệnh trao đổi,

TCVN 11167-9 (ISO/IEC 7816-9) Thẻ định danh - Thẻ mạch tích hợp - Phần 9: Lệnh đối với quản lý thẻ,

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).

3 Thuật ngữ và định nghĩa

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

3.1

Ứng dụng (application)

Cấu trúc, phần tử dữ liệu và các mô đun chương trình cần thiết nhằm thực hiện một chức năng cụ thể.

[TCVN 11167-4 (ISO/IEC 7816-4)]

3.2

Bên cung cấp ứng dụng (application provider)

Thực thể cung cấp các thành phần tạo nên một ứng dụng trên thẻ.

[TCVN 11167-4 (ISO/IEC 7816-4)]

3.3

Hạ tầng thẻ (card platform)

Thành phần trên thẻ chịu trách nhiệm với các chức năng cơ bản của thẻ.

3.4

Ứng dụng bộ quản lý thẻ (card manager application)

Ứng dụng thẻ cung cấp tính năng quản lý ứng dụng và giám sát việc ấn định tài nguyên thẻ.

4 Thuật ngữ viết tắt

Thuật ngữ	Tiếng Anh	Tiếng Việt
AID	application identifier	Mã định danh ứng dụng
APP	application	Ứng dụng
DF	dedicated file	Tệp tin dành riêng
DO	data object	Đối tượng dữ liệu
ICC	integrated circuit card	Thẻ mạch tích hợp
P1-P2	parameter bytes	Byte thông số
RID	registered application provider identifier	Mã định danh bên cung cấp ứng dụng đã đăng ký

5 Môi trường đa ứng dụng và vòng đời ứng dụng

5.1 Môi trường đa ứng dụng

Môi trường đa ứng dụng theo ngữ cảnh của tiêu chuẩn này có các đặc tính sau:

a) Một ứng dụng là một tập chức năng có thể định vị đơn nhất trong một thẻ đa ứng dụng nhằm cung cấp lưu trữ dữ liệu và các dịch vụ tính toán.

b) Một ứng dụng có thể thêm bởi thẻ trước hoặc sau khi được phát hành cho chủ thẻ.

c) Nhiều hơn một ứng dụng có thể thêm bởi thẻ.

d) Hạ tầng thẻ đưa ra các cơ chế đối với việc quản lý tài nguyên thẻ, ví dụ: bộ nhớ.

e) Hạ tầng thẻ đưa ra một cơ chế ranh giới an ninh đối với mỗi ứng dụng nhằm ngăn ngừa tương tác bất hợp pháp và vi phạm an ninh từ bất kỳ ứng dụng khác nào trên thẻ.

f) Bên cung cấp ứng dụng là một thực thể nhằm cung cấp cho chủ thẻ sử dụng một ứng dụng của thẻ và chịu trách nhiệm đối với hành vi của ứng dụng

g) Bên cung cấp ứng dụng đối với ứng dụng trên thẻ có thể khác biệt với bên phát hành thẻ.

h) Vòng đời của một ứng dụng độc lập với vòng đời của bất kỳ ứng dụng nào khác trên cùng thẻ.

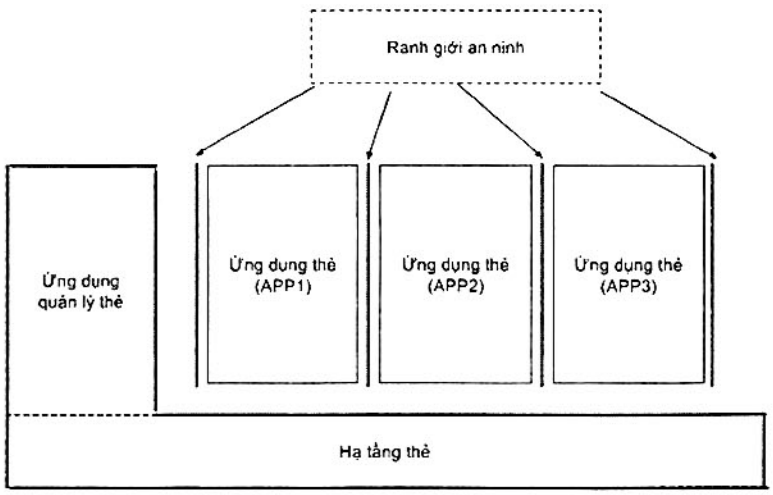
i) Vòng đời của một ứng dụng độc lập từ vòng đời của thẻ ngoại trừ lúc thẻ ở trạng thái hủy bỏ, được quy định trong TCVN 11167-9 (ISO/IEC 7816-9).

j) Tất cả ứng dụng phải có được chọn lựa ít nhất, dùng lệnh SELECT bằng cách quy định AID của nó như tên DF, được quy định trong TCVN 11167-4 (ISO/IEC 7816-4).

k) Một ứng dụng bộ quản lý thẻ phải là đơn nhất và có thể chọn lựa, dùng lệnh SELECT bằng cách quy định AID của nó như tên DF. Các ứng dụng khác trên thẻ có thể đưa ra tính năng quản lý ứng dụng.

l) AID mặc định của ứng dụng bộ quản lý thẻ là "E8 28 BD 08 0D".

Hình 1 là một biểu diễn khái niệm của một cấu trúc khả thi của thẻ mạch tích hợp đa ứng dụng.



Hình 1 - Cấu trúc khả thi của một thẻ đa ứng dụng

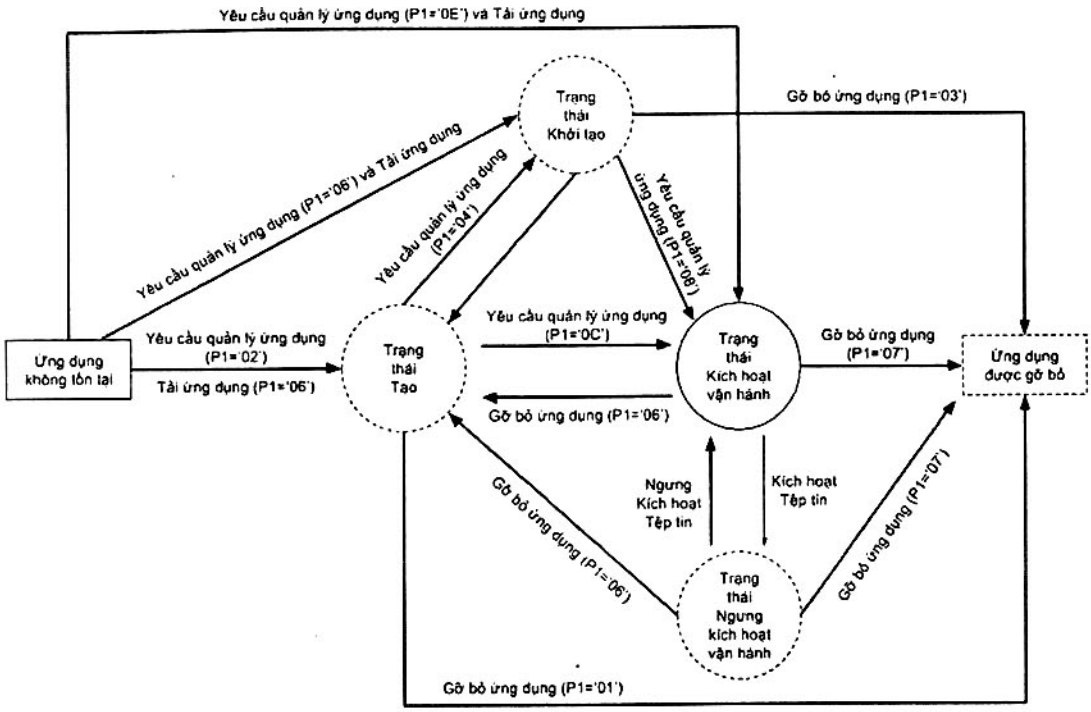
5.2 Vòng đời ứng dụng

Trạng thái vòng đời phải liên quan tới mỗi ứng dụng. Một ứng dụng có thể dùng trạng thái vòng đời của nó kết hợp với thuộc tính an ninh của nó nhằm đảm bảo rằng bất kỳ thao tác nào được thực hiện phù hợp với chính sách an ninh của ứng dụng. Ứng dụng quản lý thẻ phải cung cấp một đường dẫn truyền vòng đời từ trạng thái Không tồn tại thành trạng thái Kích hoạt vận hành.

Các lệnh sau khởi tạo các chuyển đổi trạng thái vòng đời:

- APPLICATION MANAGEMENT REQUEST;
- LOAD APPLICATION;
- REMOVE APPLICATION.

Hình 2 là một biểu diễn khái niệm về trạng thái vòng đời và các lệnh gọi từng chuyển đổi trạng thái. Lược đồ này chỉ trình bày các trạng thái ổn định (thường trú) mà một ứng dụng có thể đạt được khi hoàn thành chuyển đổi vòng đời. Mặt khác, các trạng thái trung gian có thể tồn tại trong một quá trình chuyển đổi vòng đời (ví dụ: từ trạng thái Không tồn tại thành trạng thái Tạo) nhưng không được duy trì khi quy trình này bị gián đoạn.



Hình 2 - Lược đồ vòng đời ứng dụng

CHÚ THÍCH 1 Lược đồ này đọc như sau: ví dụ: sau khi thực hiện lệnh APPLICATION MANAGEMENTREQUEST (P1 = '0E') và LOAD APPLICATION, các ứng dụng đặt ở trạng thái vòng đời Kích hoạt vận hành hoạt động, nghĩa là có thể thực thi và lựa chọn.

CHÚ THÍCH 2 Khối hình chữ nhật thể hiện trạng thái của bộ nhớ thẻ và khối hình tròn thể hiện trạng thái vòng đời ứng dụng. Khối hình tròn đứt đoạn thể hiện trạng thái vòng đời tùy chọn.

CHÚ THÍCH 3 Lệnh ACTIVATE FILE và DEACTIVATE FILE được quy định trong TCVN 11167-9 (ISO/IEC 7816-9).

Trạng thái vòng đời ứng dụng được quy định như trong Bảng 1.

Mã hóa của trạng thái vòng đời ứng dụng phải được thực hiện theo mã hóa các byte trạng thái vòng đời (byte LCS) được quy định trong TCVN 11167-4 (ISO/IEC 7816-4).

Bảng 1 - Trạng thái vòng đời ứng dụng

Ứng dụng Không tồn tại	Ứng dụng theo quan điểm của ứng dụng bộ quản lý thẻ, nếu không có
Trạng thái Tạo	Ứng dụng theo quan điểm của ứng dụng bộ quản lý thẻt, không thực thi và không được lựa chọn, nếu có.
Trạng thái Khởi tạo	Ứng dụng có thể thực thi với tính năng hạn chế và không được lựa chọn, nếu có.
Trạng thái Kích hoạt Vận hành	Ứng dụng có thể thực thi và lựa chọn, nếu có.
Trạng thái Bỏ kích hoạt vận hành	Ứng dụng có thể thực thi với tính năng hạn chế và lệnh SELECT trả về cảnh báo rằng ứng dụng bị bỏ kích hoạt, nếu có.
Ứng dụng bị gỡ bỏ	Ứng dụng không được lựa chọn và không được thực thi, nếu không có. Các tài nguyên bộ nhớ được ấn định trước đó có thể chỉ được giải phóng một phần và có thể tái sử dụng.
– Một vài nền tảng có thể có trạng thái đặc biệt trong vòng đời bổ sung. Các trạng thái bổ sung này không nằm trong phạm vi của tiêu chuẩn này. Nếu thẻ hỗ trợ các trạng thái vòng đời và chuyển đổi trạng thái, chúng không tham chiếu tới các trạng thái vòng đời và chuyển đổi trạng thái được mô tả trong Hình 2. – Trạng thái dưới dạng in nghiêng thể hiện các trạng thái bộ nhớ thẻ. Trạng thái dưới dạng in thường thể hiện trạng thái vòng đời ứng dụng.	

5.3 Đối tượng dữ liệu ấn định tài nguyên bộ nhớ đối với vận hành liên tục

Một khuôn mẫu ấn định tài nguyên bộ nhớ (thẻ '7F65') mô tả việc ấn định tài nguyên bộ nhớ cho một ứng dụng có thể được kết hợp với mỗi ứng dụng.

Bảng 2 quy định các đối tượng dữ liệu ấn định tài nguyên bộ nhớ với mỗi loại bộ nhớ: bộ lưu trữ liên tục hoặc dễ bay hơi, mà:

- **Bộ nhớ dành riêng** là số lượng bộ nhớ được ấn định riêng cho một ứng dụng;
- **Quota nhớ** là số lượng bộ nhớ tối đa bộ nhớ mà một ứng dụng được phép yêu cầu.

Một đối tượng dữ liệu tài nguyên bộ nhớ thể hiện một lượng tài nguyên bộ nhớ được tính theo byte, được mã hoá thành một giá trị nguyên, xem ISO/IEC 8825-1.

Bảng 2 - Đối tượng dữ liệu ấn định tài nguyên bộ nhớ

Thẻ	Mô tả	Yêu cầu
'80'	Lượng bộ nhớ dành riêng trong bộ lưu trữ cố định đối với mã ứng dụng. Nếu không có sự phân tách giữa mã và dữ liệu được yêu cầu thì '80' phải dùng để chỉ ra lượng bộ nhớ lưu trữ cố định được dành riêng đối với cả mã ứng dụng và dữ liệu.	Bắt buộc
'81'	Lượng bộ nhớ biến đổi được dành riêng tại thời điểm chọn lựa ứng dụng đối với dữ liệu ứng dụng.	Tùy chọn
'82'	Lượng bộ nhớ lưu trữ cố định được dành riêng đối với dữ liệu ứng dụng. Nếu '82' không được xem xét thì '80' chỉ ra tổng của bộ nhớ lưu trữ cố định đối với cả mã ứng dụng và dữ liệu.	Tùy chọn
'83'	Lượng quota bộ nhớ của bộ nhớ lưu trữ cố định đối với mã ứng dụng. Nếu không có sự phân tách giữa mã và dữ liệu được yêu cầu thì '83' phải được dùng để chỉ ra quota bộ nhớ của bộ nhớ lưu trữ cố định đối với cả mã ứng dụng và dữ liệu.	Tùy chọn
'84'	Lượng quota bộ nhớ của bộ nhớ dễ thay đổi tại thời điểm chọn lựa ứng dụng đối với dữ liệu ứng dụng.	Tùy chọn
'85'	Lượng quota bộ nhớ của lưu trữ cố định đối với dữ liệu ứng dụng. Nếu '85' không được xem xét thì '83' chỉ ra tổng của bộ nhớ lưu trữ cố định đối với cả mã ứng dụng và dữ liệu.	Tùy chọn
– Trong ngữ cảnh này, cơ quan tiêu chuẩn hóa quốc gia dành riêng các đối tượng dữ liệu khác của lớp ngữ cảnh cụ thể (byte đầu tiên từ '80' tới 'BF')		

Theo cách dùng giá trị của đối tượng dữ liệu ấn định tài nguyên bộ nhớ, các quy tắc sau phải được áp dụng:

- Việc ấn định được bộ nhớ dành riêng cho một ứng dụng làm suy giảm tài nguyên bộ nhớ có sẵn cho các ứng dụng khác trên thẻ.
- Việc ấn định quota bộ nhớ cho một ứng dụng không làm giảm tài nguyên bộ nhớ có sẵn cho các ứng dụng khác trên thẻ.
- Giá trị của quota bộ nhớ là lớn hơn hoặc bằng giá trị của bộ nhớ dành riêng.
- Tại thời điểm tạo thành công một ứng dụng (ví dụ: chuyển đổi từ trạng thái Không tồn tại thành Kích hoạt vận hành), số lượng bộ nhớ được ấn định cho ứng dụng này trước nhất là được nạp với bộ nhớ dành riêng được chỉ định cho ứng dụng đó cho đến khi nó hoàn toàn cạn kiệt. Khi bộ nhớ dành riêng của ứng dụng bị cạn kiệt, số lượng bộ nhớ được ấn định không làm giảm tài nguyên bộ nhớ sẵn có với ứng dụng khác trên thẻ miễn là nó không vượt quá quota bộ nhớ của ứng dụng đó. Khi một trong hai quota bộ nhớ vượt quá hay tài nguyên bộ nhớ hiện có trên thẻ đang cạn kiệt, việc tạo ứng dụng không thành công.
- Tại thời điểm loại bỏ thành công một ứng dụng (ví dụ: chuyển đổi sang trạng thái Gỡ bỏ ứng dụng), tài nguyên bộ nhớ sẵn có với các ứng dụng khác trên thẻ được tăng cường bởi số lượng bộ nhớ thực sự giải phóng và bất kỳ phần nào chưa sử dụng của bộ nhớ dành riêng được phân định theo tài nguyên bộ nhớ sẵn có cho ứng dụng khác trên thẻ.

6 Nhận dạng dịch vụ quản lý thẻ

6.1 Khuôn mẫu dịch vụ quản lý thẻ

Khuôn mẫu dịch vụ quản lý thẻ (thẻ "7F64") phải được xem xét. Bảng 3 quy định nội dung của khuôn mẫu dịch vụ quản lý thẻ.

Bảng 3 - Đối tượng dữ liệu dịch vụ quản lý thẻ

Thẻ	Độ dài / Định dạng	Mô tả	Yêu cầu
'80'	2 byte	Khả năng quản lý thẻ được hỗ trợ bởi thẻ: giá trị này là một kết hợp của các bit được quy định trong Bảng 4 và Bảng 5.	Bắt buộc
'81'	Thay đổi	Tên sơ đồ và phiên bản quản lý thẻ: Giá trị mã định danh đối tượng (xem ISO/IEC 8825-1) chỉ ra tên sơ đồ và phiên bản (chính và phụ) được dùng để quản lý thẻ và ứng dụng của nó.	Bắt buộc
'82'	Thay đổi	Mã định danh thủ tục định danh thẻ: Giá trị mã định danh đối tượng (xem ISO/IEC 8825-1) chỉ ra các thủ tục được dùng để định danh thẻ đơn nhất. Giá trị này quy định cách thức truy cập mã định danh cục bộ trên thẻ, ví dụ: số se-ri ICC và bất kỳ mã đinh danh nào là đơn nhất toàn phần.	Tùy chọn
'4F'	Thay đổi	Ứng dụng bộ quản lý thẻ AID: Mã định danh ứng dụng nhằm lựa chọn ứng dụng bộ quản lý thẻ khi có khác biệt từ 'E8 28 BD 08 0D'	Tùy chọn
– Trong ngữ cảnh này, cơ quan có thẩm quyền dành riêng bất kỳ đối tượng dữ liệu nào khác của lớp ngữ cảnh cụ thể (byte đầu tiên từ '80' tới 'BF')			

Bảng 4 – Khả năng quản lí thẻ: Byte đầu tiên

b8	b7	b6	b5	b4	b3	b2	b1	Giá trị của chuyển đổi trạng thái vòng đời được hỗ trợ
-	-	-	-	-	-	-	1	Không tồn tại thành Tạo
-	-	-	-	-	-	1	-	Tạo thành Khởi tạo
-	-	-	-	-	1	-	-	Khởi tạo thành Kích hoạt vận hành
-	-	-	-	1	-	-	-	Tạo thành Kích hoạt vận hành
-	-	-	1	-	-	-	-	Không tồn tại thành Kích hoạt vận hành
-	-	1	-	-	-	-	-	Kích hoạt vận hành thành Bỏ kích hoạt vận hành
-	1	-	-	-	-	-	-	Bỏ kích hoạt vận hành thành Kích hoạt vận hành
1	-	-	-	-	-	-	-	Kích hoạt vận hành thành Gỡ bỏ ứng dụng

Bảng 5 – Khả năng quản lí thẻ: Byte thứ 2

b8	b7	b6	b5	b4	b3	b2	b1	Giá trị của chuyển đổi trạng thái vòng đời được hỗ trợ
0	0	0	-	-	-	-	1	Tạo thành Gỡ bỏ ứng dụng
0	0	0	-	-	-	1	-	Khởi tạo thành Gỡ bỏ ứng dụng
0	0	0	-	-	1	-	-	Khởi tạo thành Tạo
0	0	0	-	1	-	-	-	Kích hoạt vận hành thành Tạo
0	0	0	1	-	-	-	-	Bỏ kích hoạt vận hành thành Gỡ bỏ ứng dụng
– Bất kỳ giá trị nào khác được dành riêng sử dụng sau này bởi cơ quan có thẩm quyền.								

6.2 Thu hồi khuôn mẫu dịch vụ quản lý thẻ

Việc thu hồi khuôn mẫu dịch vụ quản lý thẻ dùng dịch vụ thẻ độc lập với-ứng dụng được quy định theo TCVN 11167-4 (ISO/IEC 7816-4).

Trình tự mà các thủ tục thu hồi khác nhau quy định trong điều này không được quy định trong tiêu chuẩn này. Nếu tất cả thủ tục được mô tả sau đây không trả lại khuôn mẫu dịch vụ quản lý thẻ, thẻ không tuân thủ theo tiêu chuẩn.

Hai thủ tục có thể áp dụng nhằm thu hồi khuôn mẫu dịch vụ quản lý thẻ khi MF hay ứng dụng chọn mặc nhiên DF được chọn:

- Đọc EF.ATR, khi DO '7F64' có thể có xuất hiện;
- Lệnh GET DATA với P1-P2 đặt là '7F 64', có thể trả lại khuôn mẫu dịch vụ quản lý thẻ theo trường dữ liệu hồi đáp.

Thủ tục khác có thể áp dụng và bao gồm việc lựa chọn ứng dụng với AID 'E8 28 BD 08 0D' theo sau bởi lệnh GET DATA với P1-P2 đặt là '7F 64', có thể trả lại khuôn mẫu dịch vụ quản lý thẻ trong trường dữ liệu hồi đáp.

7 Lệnh đối với quản lý ứng dụng

Sau khi lựa chọn ứng dụng quản lý thẻ và thủ tục chứng thực tùy chọn, một thủ tục quản lý đối với một ứng dụng trên thẻ dẫn tới việc sử dụng một hay nhiều lệnh sau:

- Lệnh APPLICATION MANAGEMENT REQUEST;
- Lệnh LOAD APPLICATION;
- Lệnh REMOVE APPLICATION.

Ứng dụng quản lý thẻ phải hỗ trợ ít nhất hai lệnh đầu tiên.

Nếu ứng dụng quản lý thẻ hỗ trợ một lệnh được quy định trong điều này, ít nhất một tùy chọn của lệnh phải được hỗ trợ.

Một lệnh quản lý ứng dụng có thể được thực hiện chỉ nếu trạng thái an ninh thỏa mãn các điều kiện an ninh được quy đinh bởi ứng dụng quản lý thẻ.

7.1 Lệnh APPLICATION MANAGEMENT REQUEST

Lệnh APPLICATION MANAGEMENT REQUEST khởi tạo các thủ tục quản lý đối với một ứng dụng. Ứng dụng quản lý thẻ xác minh thông tin yêu cầu quản lý ứng dụng xuất hiện trong trường dữ liệu lệnh. Lệnh này có thể theo sau bởi lệnh LOAD APPLICATION được mô tả trong Điều 7.2. Nếu việc quản lý tài nguyên thẻ được hỗ trợ, việc ấn định tài nguyên bộ nhớ với một ứng dụng được mô tả trong khuôn mẫu ấn định tài nguyên bộ nhớ (thẻ '7F65') phải tuân thủ các quy tắc được quy định trong Điều 5.3.

Bảng 6 - Cặp lệnh-hồi đáp APPLICATION MANAGEMENT REQUEST

CLA INS P1 P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4). '40' hoặc '41' Kiểm soát trạng thái vòng đời ứng dụng theo Bảng 7. Kiểm soát quản lý ứng dụng theo Bảng 8.
Trường L_c	Số byte trong trường dữ liệu lệnh.
Trường dữ liệu	Thông tin yêu cầu quản lý ứng dụng mà định dạng và nội dung được biết tới bởi ứng dụng quản lý thẻ (INS='40') hoặc được mã hóa theo các đối tượng dữ liệu sau (INS='41'): AID (thẻ '4F') của ứng dụng đối tượng (bắt buộc) Phép ấn định tài nguyên bộ nhớ (thẻ '7F65') Một hay nhiều khối chữ ký số (thẻ '7F3D') bao gồm một chữ ký số DO (thẻ '9E') và các DO có thể, ví dụ: giá trị băm DO (thẻ '90') với mã băm ứng dụng;
Trường L_e	Rỗng đối với mã hóa $N_e = 0$, có giá trị đối với mã hóa $Ne > 0$
Trường dữ liệu	Thông tin bổ sung hoặc Rỗng
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 6 và 7 liên quan, ví dụ: '6982', '6985'.
– Thông tin yêu cầu quản lý ứng dụng có thể bao gồm các đối tượng dữ liệu khác, ví dụ: mã định danh bên phát hành (thẻ '42'), tham chiếu tệp tin (thẻ '51') hoặc dữ liệu tùy ý (thẻ '52' hoặc '73') – Việc mã hóa khối chữ ký số (thẻ '7F3D') không nằm trong phạm vi tiêu chuẩn.	

Bảng 7 - Kiểm soát trạng thái đối tượng vòng đời ứng dụng trong P1

b8	b7	b6	b5	b4	b3	b2	b1	Giá trị của chuyển đổi trạng thái vòng đời được hỗ trợ
0	0	0	0	0	0	0	0	Không thông tin nào được đưa ra
0	0	0	0	0	0	1	0	Chuyển đổi từ trạng thái Không tồn tại thành trạng thái Tạo
0	0	0	0	0	1	0	0	Chuyển đổi từ trạng thái Tạo thành Khởi tạo
0	0	0	0	0	1	1	0	Chuyển đổi từ trạng thái Không tồn tại thành Khởi tạo
0	0	0	0	1	0	0	0	Chuyển đổi từ trạng thái Khởi tạo thành Kích hoạt vận hành
0	0	0	0	1	1	0	0	Chuyển đổi từ trạng thái Tạo thành Kích hoạt vận hành
0	0	0	0	1	1	1	0	Chuyển đổi từ trạng thái Không tồn tại thành Kích hoạt vận hành
– Bất kỳ giá trị nào khác được dành riêng sử dụng sau này bởi cơ quan tiêu chuẩn hóa quốc gia								

Bảng 8 - Kiểm soát quản lý ứng dụng trong P2

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	0	0	0	0	0	0	0	Không có thông tin đưa ra
0	0	0	0	0	0	0	1	Xác minh yêu cầu quản lý ứng dụng
0	0	0	0	0	0	1	0	Gửi yêu cầu quản lý ứng dụng
0	0	0	0	0	0	1	1	Xác minh và gửi yêu cầu quản lý ứng dụng
– Bất kỳ giá trị nào khác được dành riêng sử dụng sau này bởi cơ quan có thẩm quyền.								

7.2 Lệnh LOAD APPLICATION

Lệnh LOAD APPLICATION truyền một ứng dụng vào thẻ. Một ứng dụng có thể được phân chia thành nhiều thành phần và mỗi thành phần có thể được phân chia thành nhiều khối để chuyển cho thẻ. Mỗi lệnh LOAD APPLICATION truyền một khối vào thẻ. Lệnh này có thể được bắt đầu bằng lệnh APPLICATION MANAGEMENT REQUEST, xem Điều 7.1.

Nếu lệnh LOAD APPLICATION được bắt đầu bằng lệnh APPLICATION MANAGEMENT REQUEST thì việc ấn định tài nguyên bộ nhớ được thực hiện ngay trước lệnh APPLICATION MANAGEMENT REQUEST. Việc thực thi thành công chuỗi lệnh thực hiện chuyển đổi vòng đời ngay trước lệnh APPLICATION MANAGEMENT REQUEST.

Nếu lệnh LOAD APPLICATION không bắt đầu bằng lệnh APPLICATION MANAGEMENT REQUEST thì việc ấn định tài nguyên bộ nhớ và thiết lập trạng thái vòng đời ứng dụng đến một giá trị thích hợp được thực hiện trên cơ sở thông tin được cung cấp bởi chuỗi lệnh LOAD APPLICATION.

Nếu việc quản lý tài nguyên bộ nhớ được hỗ trợ, số lượng bộ nhớ được ấn định cho một ứng dụng được tạo thành công phải tuân thep theo quy tắc được quy định trong Điều 5.3.

Bảng 9 - Cặp lệnh-hồi đáp LOAD APPLICATION

CLA INS P1-P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4). 'EA' hoặc EB' Xem Bảng 10.
Trường Lc	Số byte trong trường dữ liệu lệnh.
Trường dữ liệu	Thành phần ứng dụng mà định dạng và nội dung được biết tới bởi ứng dụng bộ quản lý thẻ (INS='EA') hoặc được mã hóa thành các đối tượng dữ liệu riêng lẻ (INS='EB')
Trường Lc	Rỗng đối với mã hóa $N_e = 0$, có giá trị đối với mã hóa $N_e > 0$
Trường dữ liệu	Thông tin bổ sung hoặc Rỗng
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 6 và 7 liên quan, ví dụ: '6982', '6985'.

Bảng 10 - Số chuỗi hoặc Offset trong P1 và P2

P1								P2	Mô tả
b8	b7	b6	b5	b4	b3	b2	b1		
0	0	0	0	0	0	0	0	00	Không có thông tin.
-	X	X	X	X	X	X	X	XX	Số chuỗi hoặc offset.
-	0	X	X	X	X	X	X	XX	– Offset
-	1	X	X	X	X	X	X	XX	– Số chuỗi
0	-	-	-	-	-	-	-	-	Nhiều khối
1	-	-	-	-	-	-	-	-	Khối cuối

– Nếu b7 của P1 được đặt là 0 thì phần còn lại của P1-P2 (14 bit) mã hóa một offset từ 0 tới 16383 và nếu b7 của P1 được đặt là 1 thì phần còn lại của P1-P2 (14 bit) mã hóa một số chuỗi của lệnh.

– Nếu b8 của P1 được đặt là 0 thì một khối kế tiếp được mong đợi, và nếu b8 của P1 được đặt là 1 thì lệnh này chứa khối cuối.

– Offset được đếm theo các byte từ lúc bắt đầu chuyển đổi ứng dụng.

– Số chuỗi được tăng +1 với mỗi khối đối từ lúc bắt đầu chuyển đổi ứng dụng.

7.3 Lệnh REMOVE APPLICATION

Lệnh REMOVE APPLICATION xóa một ứng dụng và có thể lấy lại tài nguyên bộ nhớ được ấn định cho ứng dụng.

Ứng dụng quản lý thẻ xác minh thông tin gỡ bỏ ứng dụng, khi có trong trường dữ liệu lệnh.

Nếu việc quản lý tài nguyên bộ nhớ được hỗ trợ, việc gỡ bỏ thành công một ứng dụng phải gia tăng tài nguyên bộ nhớ sẵn có với các ứng dụng trên thẻ theo các quy tắc được quy định trong Điều 5.3.

Bảng 11 - Cặp lệnh-hồi đáp REMOVE APPLICATION

CLA INS P1 P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4). 'EC' hoặc ED' Gỡ bỏ kiểm soát trạng thái theo Bảng 12 '00' không có thông tin được đưa ra. (bất kì giá trị nào được dành riêng sử dụng sau này bởi cơ quan có thẩm quyền)
Trường Lc	Rỗng hoặc số byte trong trường dữ liệu lệnh.
Trường dữ liệu	Rỗng hoặc ứng dụng gỡ bỏ thông tin mà định dạng và nội dung được biết đến bởi ứng dụng bộ quản lý thẻ (INS='EC') hoặc ứng dụng gỡ bỏ thông tin được mã hóa trong các đối tượng dữ liệu sau (INS='ED'): – AID (thẻ '4F') của ứng dụng đối tượng (bắt buộc); – Một hay nhiều khối chữ ký số (thẻ '7F3D') bao gồm một chữ ký số DO (thẻ '9E')
Trường Lc	Rỗng đối với mã hóa $N_e = 0$, có giá trị đối với mã hóa Ne > 0
Trường dữ liệu	Thông tin bổ sung hoặc Rỗng
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 6 và 7 liên quan, ví dụ: '6982', '6985'.
– Ứng dụng gỡ bỏ thông tin có thể bao gồm các đối tượng dữ liệu khác, ví dụ: dữ liệu tùy chọn (thẻ '53' hoặc '73') – Mã hóa khối chữ ký số (thẻ '7F3D') nằm ngoài phạm vi của tiêu chuẩn.	

Bảng 12 - Kiểm soát trạng thái gỡ bỏ trong P1

b8	b7	b6	b5	b4	b3	b2	b1	Giá trị của chuyển đổi trạng thái vòng đời được hỗ trợ
0	0	0	0	0	0	0	0	Không có thông tin đưa ra
0	0	0	0	0	0	0	1	Chuyển đổi từ trạng thái Tạo thành Gỡ bỏ ứng dụng
0	0	0	0	0	0	1	0	Chuyển đổi từ trạng thái Khởi tạo thành trạng thái Tạo
0	0	0	0	0	0	1	1	Chuyển đổi từ trạng thái Khởi tạo thành Gỡ bỏ ứng dụng
0	0	0	0	0	1	1	0	Chuyển đổi từ trạng thái Vận hành (Kích hoạt/Bỏ kích hoạt) thành trạng thái Tạo
0	0	0	0	0	1	1	1	Chuyển đổi từ trạng thái Vận hành (Kích hoạt/Bỏ kích hoạt) thành Gỡ bỏ ứng dụng
– Bất kỳ giá trị nào khác được dành riêng sử dụng sau này bởi cơ quan tiêu chuẩn hóa.								

7.4 Cân nhắc quản lý ứng dụng

Lược đồ quản lý thẻ và/hoặc các chính sách bên phát hành thẻ quy định loại và số lượng chữ ký được yêu cầu, như:

- Chữ ký của bên phát hành thẻ,
- Chữ ký bên cung cấp ứng dụng,
- Chữ ký của quyền lược đồ quản lý thẻ.

Thẻ phải có khả năng bắt buộc các chính sách này và quản lý các khóa xác minh chữ ký tương ứng.

Một chính sách quản lý ứng dụng giữa bên phát hành thẻ và bên cung cấp ứng dụng, và việc thiết lập chính này này nằm ngoài phạm vi của tiêu chuẩn.

Phụ lục A

(tham khảo)

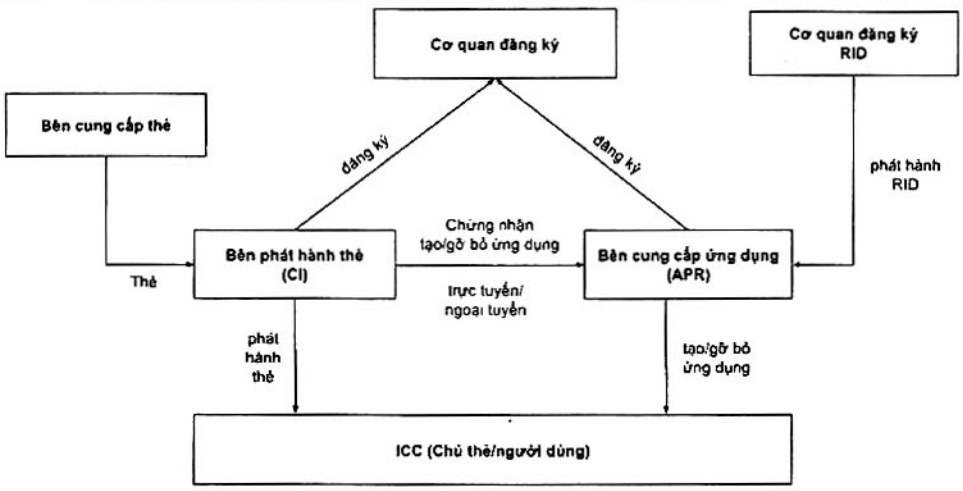
Ví dụ về quản lý ứng dụng thẻ theo bên phát hành thẻ độc lập và mô hình bên cung cấp ứng dụng

A.1 Giới thiệu

Ví dụ này trình bày cách thức quản lý một ứng dụng trên thẻ theo bên phát hành thẻ độc lập và mô hình bên cung cấp ứng dụng. Có các giả định sau:

- Một ứng dụng có thể được thêm vào thẻ bởi bên cung cấp ứng dụng độc lập sau khi phát hành thẻ. Mô hình được trình bày trong Hình A.1.
- Chứng nhận tạo ứng dụng có thể được phát hành trong quá trình kết nối trực tuyến hay ngoại tuyến.

CHÚ THÍCH Nhóm nghiên cứu hệ thống thẻ mạch tích hợp (NICSS) thế hệ kế tiếp dùng mô hình này.



Hình A.1 - Mô hình của bên phát hành thẻ độc lập và bên cung cấp ứng dụng

A.2 Ví dụ về thủ tục quản lý ứng dụng

A.2.1 Trường hợp của APR độc lập với CI (CI từ xa): xác minh chứng nhận trước khi tải

a) SELECT ứng dụng với AID 'E8 28 BD 08 0D'.

b) GET DATA để thu hồi khuôn mẫu dịch vụ quản lý thẻ (thẻ '7F64').

c) SELECT ứng dụng quản lý thẻ với AID (thẻ '4F') được chỉ ra trong khuôn mẫu dịch vụ quản lý thẻ.

d) Chứng thực hai chiều.

e) Nhận một chứng nhận tạo ứng dụng từ bên phát hành thẻ (trực tuyến/ngoại tuyến). Chứng nhận có thể chứa AID, một giá trị băm của ứng dụng, ID phê duyệt, ID thẻ và chữ ký số của bên phát hành thẻ.

f) APPLICATION MANAGEMENT REQUEST với chứng nhận.

g) LOAD APPLICATION bằng lệnh LOAD APPLICATION.

A.2.2 Trường hợp của CI từ xa: xác minh chứng nhận sau khi tải

a) SELECT ứng dụng với AID 'E8 28 BD 08 0D'.

b) GET DATA để thu hồi khuôn mẫu dịch vụ quản lý thẻ (thẻ '7F64').

c) SELECT ứng dụng quản lý thẻ với AID (thẻ '4F') được chỉ ra trong khuôn mẫu dịch vụ quản lý thẻ.

d) Chứng thực hai chiều.

e) Nhận được một chứng nhận tạo ứng dụng từ bên phát hành thẻ.

f) APPLICATION MANAGEMENT REQUEST không có giấy chứng nhận để cấp phát bộ nhớ.

g) Tải ứng dụng bằng LOAD APPLICATION.

h) APPLICATION MANAGEMENT REQUEST với chứng nhận.

A.3 Ví dụ về thủ tục gỡ bỏ

A.3.1 Trường hợp của CI từ xa: xác minh chứng nhận trong suốt quá trình gỡ bỏ

a) SELECT ứng dụng với AID 'E8 28 BD 08 0D'.

b) GET DATA để thu hồi khuôn mẫu dịch vụ quản lý thẻ (thẻ '7F64').

c) SELECT ứng dụng quản lý thẻ với AID (thẻ '4F') được chỉ ra trong khuôn mẫu dịch vụ quản lý thẻ.

d) Chứng thực hai chiều.

e) Nhận chứng nhận loại bỏ ứng dụng từ bên phát hành thẻ (trực tuyến/ngoại tuyến). Chứng nhận có thể chứa AID, ID phê duyệt, ID thẻ và chữ ký số của bên phát hành thẻ.

f) REMOVE APPLICATION với chứng nhận.

A.3.2 Trường hợp của CI từ xa: xác minh chứng nhận trước khi gỡ bỏ

a) SELECT ứng dụng với AID 'E8 28 BD 08 0D'.

b) GET DATA để thu hồi khuôn mẫu dịch vụ quản lý thẻ (thẻ '7F64').

c) SELECT ứng dụng quản lý thẻ với AID (thẻ '4F') được chỉ ra trong khuôn mẫu dịch vụ quản lý thẻ.

d) Chứng thực hai chiều.

e) Nhận chứng nhận loại bỏ ứng dụng từ bên phát hành thẻ.

f) APPLICATION MANAGEMENT REQUEST với chứng chỉ.

g) REMOVE APPLICATION không có giấy chứng nhận.

Phụ lục B

(tham khảo)

Ví dụ thực hành của quản lý ứng dụng thẻ

B.1 Giới thiệu

Ví dụ này trình bày mô hình hai-bước cho việc tạo và kích hoạt ứng dụng: tải mã của ứng dụng trước tiên, sau đó cài đặt và kích hoạt một trường hợp ứng dụng.

CHÚ THÍCH GlobalPlatform (GP) sử dụng mô hình này.

Một ứng dụng gồm các mã ứng dụng và dữ liệu ứng dụng. Mã ứng dụng (nhưng không phải dữ liệu ứng dụng) được tải vào thẻ bằng cách dùng một Load Object. Việc cài đặt một ứng dụng tạo ra một trường hợp theo Load Object cộng với một số dữ liệu ứng dụng có thể.

Trong ví dụ này, việc tạo và kích hoạt một ứng dụng đòi hỏi phải bổ sung:
- Chứng thực trước đó của hệ thống quản lý ứng dụng thẻ (CAMS),
- Bảo vệ các lệnh và hồi đáp bằng thông điệp an toàn,
- Xác minh chứng nhận của bên phát hành thẻ.

B.2 Lệnh đối với quản lý ứng dụng

B.2.1 Lệnh APPLICATION MANAGEMENT REQUEST

Lệnh APPLICATION MANAGEMENT REQUEST được phát hành nhằm khởi tạo và thực hiện các bước khác nhau được yêu cầu cho việc tải một Load Object, cài đặt và kích hoạt một trường hợp ứng dụng.

Bảng B.1 - Cặp lệnh-hồi đáp APPLICATION MANAGEMENT REQUEST

CLA INS P1 P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4). '40' Kiểm soát trạng thái đối tượng vòng đời ứng dụng: Xem Bảng B.2 Kiểm soát quản lý ứng dụng: xem Bảng B.3
Trường Lc	Số byte trong trường dữ liệu lệnh.
Trường dữ liệu	Thông tin yêu cầu quản lý ứng dụng
Trường Le	Rỗng đối với mã hóa Ne = 0, có giá trị đối với mã hóa Ne > 0
Trường dữ liệu	Rỗng hoặc thông tin xác nhận quản lý ứng dụng
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 6 và 7 liên quan, ví dụ: '6982', '6985'.

Tham số P1 của lệnh APPLICATION MANAGEMENT REQUEST mô tả mục đích của lệnh này và được mã hóa theo Bảng B.2.

Bảng B.2 Kiểm soát trạng thái đối tượng vòng đời ứng dụng trong P1

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	0	0	0	1	1	0	0	Chuyển đổi từ trạng thái Tạo thành Kích hoạt vận hành
0	0	0	0	1	0	0	0	Chuyển đổi từ trạng thái Khởi tạo thành Kích hoạt vận hành
0	0	0	0	0	1	0	0	Chuyển đổi từ trạng thái Tạo thành trạng thái Khởi tạo
0	0	0	0	0	0	1	0	Chuyển đổi từ trạng thái Không tồn tại thành trạng thái Tạo
X	X	X	X	-	-	-	-	RFU

b4 = 1 chỉ ra việc kích hoạt ứng dụng được quy định trong trường dữ liệu lệnh. Điều này áp dụng cho một ứng dụng mà chỉ được tạo ra (trạng thái vòng đời hiện tại = Tạo) hay đã là Khởi tạo (trạng thái vòng đời hiện tại = Khởi tạo).

b3 = 1 chỉ ra việc khởi tạo ứng dụng được quy định trong trường dữ liệu lệnh (trạng thái vòng đời = Tạo).

b2 = 1 chỉ ra việc tạo ứng dụng được quy định trong trường dữ liệu lệnh (trạng thái vòng đời hiện tại = Không tồn tại).

Bảng B.3 - Kiểm soát quản lý ứng dụng trong P2

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	0	0	0	0	0	0	1	Xác minh yêu cầu quản lý ứng dụng
0	0	0	0	0	0	1	1	Xác minh và gửi yêu cầu quản lý ứng dụng

Trong ví dụ này, lệnh APPLICATION MANAGEMENT REQUEST được cấp hai lần.

- Với b2 = 1 trong thông số P1 và P2 đặt là '01', để khởi tạo viêc tải mã ứng dụng (Load Object). Trường dữ liệu lệnh gồm việc định danh Load Object, định danh bên cung cấp ứng dụng, thông tin ấn định tài nguyên bộ nhớ theo Load Object, việc băm Load Object và một chứng nhận tạo ứng dụng được ban hành bởi bên phát hành thẻ. Không có trường dữ liệu hồi đáp trả về trong thông điệp hồi đáp. Một hay nhiều lệnh LOAD APPLICATION theo sau. Khi thực thi thành công lệnh LOAD APPLICATION cuối cùng, việc tạo yêu cầu quản lý ứng dụng là mặc nhiên cam kết và trạng thái vòng đời ứng dụng được đặt là Tạo.
- Với sự kết hợp của b4 = 1 và b3 = 1 trong thông số P1 và P2 đặt là '03', việc cài đặt và kích hoạt đồng thời một trường hợp ứng dụng. Các trường dữ liệu lệnh gồm việc định danh của Load Object đã được tải, định danh của trường hợp ứng dụng, thông tin ấn định tài nguyên bộ nhớ theo trường hợp ứng dụng và một chứng nhận khởi tạo-và-kích hoạt ứng dụng của bên phát hành thẻ. Khi thực thi thành công lệnh này, trạng thái vòng đời được thay đổi từ Tạo thành Kích hoạt vận hành. Một trường dữ liệu hồi đáp có thể được trả lại trong các thông điệp hồi đáp. Nội dung của trường dữ liệu hồi đáp chứa độ dài (được mã hóa theo các quy tắc ASN.1 được quy định trong ISO/IEC 8825-1) và giá trị của việc xác nhận Khởi tạo-và-Kích hoạt ứng dụng.

B.2.2 Lệnh LOAD APPLICATION

Load Object được chia thành nhiều khối Load Block để truyền tới thẻ. Lệnh LOAD APPLICATION khởi tạo việc truyền Load Block vào thẻ. Các lệnh LOAD APPLICATION có thể được yêu cầu để truyền một Load Object tới thẻ.

Bảng B.4 - Cặp lệnh-hồi đáp LOAD APPLICATION

CLA INS P1 P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4). 'EA' Byte có ý nghĩa nhất số chuỗi khối Load Block, xem Bảng B.5 Byte có ít nghĩa nhất số chuỗi khối Load Block, xem Bảng B.6
Trường L_c	Số byte trong trường dữ liệu lệnh.
Trường dữ liệu	Load Block
Trường L_e	Rỗng đối với mã hóa $N_e = 0$, có giá trị đối với mã hóa Ne > 0
Trường dữ liệu	Rỗng hoặc thông tin xác nhận tạo ứng dụng
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 6 và 7 liên quan, ví dụ: '6581', '6484'.

Thông số P1 và P2 của lệnh LOAD APPLICATION mô tả chuỗi Load Block và được mã hoá trong Bảng B.5 và B.6.

Bảng B.5 - Byte có ý nghĩa nhất số chuỗi trong P1

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	1	X	X	X	X	X	X	Nhiều khối, byte có nghĩa nhất số chuỗi
1	1	X	X	X	X	X	X	Khối cuối, byte có nghĩa nhất số chuỗi

b8 = 0 chỉ ra có nhiều Load Block hơn mong đợi

b8 = 1 chỉ ra Load Block cuối cùng trong một chuỗi.

b7 = 1 chỉ ra một số thứ tự Load Block được mã hóa trên 14 bit, từ 0 đến 16383.

Bảng B.6 - Byte có ít ý nghĩa nhất số chuỗi trong P2

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
X	X	X	X	X	X	X	X	Byte có nghĩa nhất số chuỗi

Lệnh LOAD APPLICATION đầu tiên được bắt đầu bằng một lệnh APPLICATION MANAGEMENTREQUEST với lệnh tạo (b2 của P1 đặt là 1).

Số chuỗi của Load Block (ít hơn 14 bit của P1-P2) bắt đầu từ 0. Việc đánh số Load Block là theo đúng trình tự và gia tăng +1. Thẻ được thông báo về khối cuối cùng của Load Object (b8 của P1 của lệnh LOAD APPLICATION đặt là 1).

Một trường dữ liệu hồi đáp có thể được trả về theo thông điệp hồi đáp. Nội dung của trường dữ liệu hồi đáp bao gồm độ dài (được mã hóa theo quy tắc ASN.1 được quy định trong ISO/IEC

8825-1) và giá trị việc xác nhận tạo ứng dụng. Giá trị này chỉ xuất hiện trong trường dữ liệu hồi đáp của lệnh LOAD APPLICATION truyền khối Load Block cuối cùng (b8 của P1 đặt là 1).

Đối với lệnh LOAD APPLICATION khác với lệnh LOAD APPLICATION cuối cùng truyền Load Block cuối cùng (b8 của P1 đặt là 1), không có trường dữ liệu hồi đáp.

B.3 Chuỗi quản lý ứng dụng

Chuỗi quản lý ứng dụng điển hình đối với việc tạo và kích hoạt một ứng dụng trong mô hình này được tuân theo:

a) SELECT ứng dụng với AID 'E8 28 BD 08 0D'.
b) GET DATA lấy mẫu dịch vụ quản lý thẻ (thẻ '7F64')
c) SELECT ứng dụng quản lý thẻ với AID (thẻ '4F') chỉ ra trong mẫu dịch vụ quản lý thẻ
d) APPLICATION MANAGEMENT REQUEST cho việc khởi tạo với P1='02' và P2='01'.
e) LOAD APPLICATION đầu tiên với P1='40' và P2='00'.
f) Các lệnh LOAD APPLICATION theo trình tự gia tăng của P1-P2.
g) LOAD APPLICATION cuối cùng với P1='Cx' và P2='yz' khi 'xyz' là chuỗi số của Load Block cuối cùng (giả định 'xy' nhỏ hơn 4 095).
h) APPLICATION MANAGEMENT REQUEST đối với việc khởi tạo và kích hoạt với P1='0C' và P2='03'.

Phụ lục C

(tham khảo)

Ví dụ thực hành bổ sung của quản lý ứng dụng thẻ

C.1 Giới thiệu

Ví dụ này trình bày mô hình ba-bước đối với việc tạo và kích hoạt ứng dụng: ấn định tài nguyên thẻ, tải mã ứng dụng và dữ liệu và tạo ra kích hoạt vận hành.

CHÚ THÍCH MULTOS dùng mô hình này.

Lệnh APPLICATION MANAGEMENT REQUEST ban đầu đảm bảo tính sẵn có của tài nguyên thẻ và chuẩn bị sẵn sàng cho thẻ đối với các yêu cầu quản lý nội dung thẻ kế tiếp. Ứng dụng sau đó được tải tới thẻ với lệnh LOAD APPLICATION. Một ứng dụng gồm mã ứng dụng và dữ liệu ứng dụng, thông tin điều khiển tệp tin mặc định, mục vào tệp tin thư mục, chữ ký số và đơn vị chuyển đổi khóa. Tất cả được tải vào thẻ như một đơn vị tải ứng dụng. Lệnh APPLICATION MANAGEMENT REQUEST thứ hai và cuối cùng kết thúc quy trình tạo và kích hoạt ứng dụng, bao gồm việc kiểm tra quyền bên phát hành thẻ và chữ ký số của bên cung cấp dịch vụ ứng dụng của đơn vị tải ứng dụng.

C.2 Lệnh đối với quản lý ứng dụng

C.2.1 Lệnh APPLICATION MANAGEMENT REQUEST

Lệnh APPLICATION MANAGEMENT REQUEST được phát hành nhằm khởi tạo và hoàn thiện quy trình tải ứng dụng.

Bảng C.1 - Cặp lệnh-hồi đáp APPLICATION MANAGEMENT REQUEST

CLA INS P1 P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4). '40' Mục đích của APPLICATION MANAGEMENT REQUEST, xem Bảng C.2 Mục đích của APPLICATION MANAGEMENT REQUEST, xem Bảng C.3
Trường Lc	Số byte trong trường dữ liệu lệnh.
Trường dữ liệu	Chứng nhận tải ứng dụng
Trường Lc	Rỗng đối với mã hóa Ne = 0, có giá trị đối với mã hóa Ne > 0
Trường dữ liệu	Rỗng hoặc Chứng nhận khóa phổ thông
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 6 và 7 liên quan, ví dụ: '6982', '6985'.

Tham số P1 của lệnh APPLICATION MANAGEMENT REQUEST mô tả mục đích của lệnh và được mã hóa theo Bảng C.2.

Bảng C.2 - Mã hóa P1 của lệnh APPLICATION MANAGEMENT REQUEST

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	0	0	0	1	1	1	0	Chuyển đổi từ trạng thái Không tồn tại thành Kích hoạt Vận hành

Tham số P2 của lệnh APPLICATION MANAGEMENT REQUEST mô tả mục đích của lệnh và được mã hóa theo Bảng C.2.

Bảng C.3 - Mã hóa P2 của lệnh APPLICATION MANAGEMENT REQUEST

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	0	0	0	0	0	0	1	Xác minh yêu cầu quản lý ứng dụng
0	0	0	0	0	0	1	1	Xác minh và gửi yêu cầu quản lý ứng dụng

C.2.2 Lệnh LOAD APPLICATION

Đơn vị tải ứng dụng được chia thành các thành phần nhỏ hơn để truyền tới thẻ. Lệnh LOAD APPLICATION khởi tạo việc truyền các thành phần vào thẻ. Nhiều lệnh LOAD APPLICATION có thể được dùng để truyền một đơn vị tải ứng dụng tới thẻ.

Bảng C.4 - Cặp lệnh-hồi đáp LOAD APPLICATION

CLA INS P1 P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4). 'EA' Tải byte có nghĩa nhất số chuỗi, xem Bảng C.5 Tải byte có ít nghĩa nhất số chuỗi, xem Bảng C.6
Trường Lc	Số byte trong trường dữ liệu lệnh.
Trường dữ liệu	Load Block
Trường Lc	Rỗng đối với mã hóa Ne = 0, có giá trị đối với mã hóa Ne > 0
Trường dữ liệu	Rỗng
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 6 và 7 liên quan, ví dụ: '6981', '6984'.

Thông số P1 và P2 của lệnh LOAD APPLICATION mô tả chuỗi số của các thành phần và được mã hóa trong Bảng C.5 và C.6.

Bảng C.5 - Mã hóa P1 của lệnh LOAD APPLICATION

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
0	1	x	x	x	x	x	x	Nhiều khối hơn, byte có nghĩa nhất số chuỗi
1	1	x	x	x	x	x	x	Khối cuối, byte có nghĩa nhất số chuỗi

b8 = 0 chỉ ra nhiều Load Block như mong đợi.

b8 = 1 chỉ ra Load Block cuối cùng trong chuỗi.

b7 = 1 chỉ ra một chuỗi số của Load Block được mã hóa theo 14 bit, từ 0 tới 16383.

Bảng C.6 - Mã hóa P2 của lệnh LOAD APPLICATION

b8	b7	b6	b5	b4	b3	b2	b1	Ý nghĩa
x	x	x	x	x	x	x	x	Byte có ít nghĩa ít nhất số chuỗi

Lệnh LOAD APPLICATION đầu tiên được bắt đầu bằng lệnh APPLICATION MANAGEMENT REQUEST.

Số chuỗi Load Block (ít hơn 14 bit của P1-P2) bắt đầu từ 0. Việc đánh số Load Block là đúng theo tuần tự và gia tăng +1. Thẻ được thông báo về khối cuối cùng của Load Object (b8 của P1 đặt là 1).

C.3 Chuỗi quản lý ứng dụng

Chuỗi quản lý ứng dụng điển hình cho việc tạo và kích hoạt một ứng dụng của mô hình này như sau:

a) SELECT ứng dụng với AID 'E8 28 BD 08 0D'.

b) GET DATA để thu hồi khuôn mẫu dịch vụ quản lý thẻ (thẻ '7F64').

c) SELECT quản lý ứng dụng thẻ.

d) APPLICATION MANAGEMENT REQUEST cho xác minh yêu cầu kích hoạt vận hành với P1 = '0E' và P2 = '01'.

e) LOAD APPLICATION đầu tiên với P1 = '40' và P2 = '00'.

f) Nhiều lệnh LOAD APPLICATION với tuần tự tăng dần của P1-P2.

g) LOAD APPLICATION với P1 = 'Cx' và P2 = 'yz' khi 'xyz' là số chuỗi Load Block cuối cùng.

h) APPLICATION MANAGEMENT REQUEST cho kích hoạt vận hành với P1 = '0E' và P2 = '03'.

Phụ lục D

(tham khảo)

V dụ thực hành bổ sung của quản lý ứng dụng thẻ

Ví dụ sau trình bày việc sử dụng lệnh LOAD APPLICATION như một trình bao bọc các lệnh cho việc cài đặt ứng dụng. Việc sử dụng này cho phép kiểm soát toàn bộ chuỗi tải bởi một quy tắc truy cập đơn lẻ đối với lệnh LOAD APPLICATION, ví dụ: việc chứng thực bên ngoài với thỏa thuận khóa thông điệp an ninh được yêu cầu. Thủ tục chứng thực này được thực hiện bởi một hệ thống quản lý ứng dụng thẻ (CAMS).

CHÚ THÍCH 1 Chuỗi lệnh có thể được gửi với thông điệp an ninh.

CHÚ THÍCH 2 Lệnh-thực thi trong trường dữ liệu lệnh được mã hóa mà không có thông điệp an ninh.

Bảng D.1 - Cặp lệnh-hồi đáp LOAD APPLICATION

CLA INS P1-P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4), bit 5 đặt là 1 chỉ ra rằng lệnh này không phải là lệnh cuối trong chuỗi 'EB' '0000'
Trường Lc	Số byte trong trường dữ liệu lệnh.
Trường dữ liệu	Lệnh-thực thi (Thẻ '52'): '52'-L-.... (Lệnh CREATE FILE (DF))
Trường Lc	Rỗng
Trường dữ liệu	Rỗng
SW1-SW2	'9000' hoặc các byte trạng thái cụ thể

Bảng D.2 - Cặp lệnh-hồi đáp LOAD APPLICATION

CLA INS P1-P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4), bit 5 đặt là 1 chỉ ra rằng lệnh này không phải là lệnh cuối trong chuỗi 'EB' '0000'
Trường L_c	Số byte trong trường dữ liệu lệnh.
Trường dữ liệu	Số byte theo trường dữ liệu lệnh
Trường Lc	Rỗng
Trường dữ liệu	Rỗng
SW1-SW2	'9000' hoặc các byte trạng thái cụ thể

Bảng D.3 - Cặp lệnh-hồi đáp LOAD APPLICATION

CLA	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4), bit 5 đặt là 1 chỉ ra rằng lệnh này không phải là lệnh cuối trong chuỗi
INS	'EB'
P1-P2	'0000'
Trường L_c	Số byte trong trường dữ liệu lệnh.
Trường dữ liệu	Lệnh thực thi (Thẻ đánh dấu '52'): '52'-L-.... (Lệnh CREATE FILE (DF))
Trường L_e	Rỗng
Trường dữ liệu	Rỗng
SW1-SW2	'9000' hoặc các byte trạng thái cụ thể

Bảng D.4 - Cặp lệnh-hồi đáp LOAD APPLICATION

CLA	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4), bit 5 đặtt là 1 chỉ ra rằng lệnh này không phải là lệnh cuối trong chuỗi
INS	'EB'
P1-P2	'0000'
Trường Lc	Số byte trong trường dữ liệu lệnh.
Trường dữ liệu	Lệnh thực thi (Thẻ '52'): '52'-L-.... (Lệnh CREATE FILE (DF))
Trường Lc	Rỗng
Trường dữ liệu	Rỗng
SW1-SW2	'9000' hoặc các byte trạng thái cụ thể

Thư mục tài liệu tham khảo

[1] TCVN 11167 (ISO/IEC 7816) Thẻ định danh - Thẻ mạch tích hợp (tất cả các phần).

[2] Đặc tả thẻ GlobalPlatform, phiên bản 2.1.1 hoặc cao hơn, http://www.globalplatform.org/

[3] NICSS Prerequisites Version 1.20, The Next generation IC Card System Study group: http://www.nicss.or.jp/

[4] Guide to Loading and Deleting Applications, MAO-DOC-REF-008, MAOSCO: http://www.multos.com/

[5] Guide to Generating Application Load Units, MAO-DOC-REF-009, MAOSCO: http://www.multos.com/