TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 11167-9:2015
ISO/IEC 7816-9:2004

Xuất bản lần 1

THẺ DANH ĐỊNH - THẺ MẠCH TÍCH HỢP - PHẦN 9: LỆNH ĐỐI VỚI QUẢN LÝ THẺ

Identification cards - Integrated circuit cards - Part 9: Commands for card management

HÀ NỘI - 2015

Mục lục

Trang

Lời nói đầu

TCVN 11167-9:2015 hoàn toàn tương đương với ISO/IEC 7816-9:2004.

TCVN 11167-9:2015 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 9: Lệnh đối với quản lý thẻ

Identification cards - Integrated circuit cards - Part 9: Commands for card management

1 Phạm vi áp dụng

Tiêu chuẩn này quy định nghĩa các lệnh đối với quản lý thẻ và tệp tin liên ngành. Các lệnh này được đề cập trong toàn bộ vòng đời của thẻ cho nên một vài lệnh có thể được sử dụng trước khi thẻ được đưa ra đối với chủ thẻ hay sau khi thẻ hết hạn.

Tiêu chuẩn này không đề cập đến việc thiết lập trong thẻ và/hoặc thế giới bên ngoài.

2 Tài liệu viện dẫn

Các tài liệu tham khảo dưới đây không thể thiếu đối với việc áp dụng tài liệu này. Đối với các tham khảo ghi năm, chỉ áp dụng bản được nêu. Đối với các tham khảo không ghi năm, bản mới nhất của tài liệu tham khảo (bao gồm cả sửa đổi) được áp dụng (nếu có).

TCVN 11167-4:2015 (ISO/IEC 7816-4) Thẻ định danh - Thẻ mạch tích hợp - Phần 4: Tổ chức, an ninh và lệnh trao đổi.

3 Thuật ngữ và định nghĩa

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

3.1.

Thông điệp an ninh (secure messaging)

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

Tập phương thức bảo vệ bằng mã hóa của (hay một phần) của các cặp lệnh-hồi đáp.

4 Thuật ngữ viết tắt và ký hiệu

Tiêu chuẩn này áp dụng các thuật ngữ viết tắt sau.

Thuật ngữ	Tên tiếng Anh	Tên tiếng Việt
APDU	application protocol data unit	Đơn vị dữ liệu giao thức ứng dụng
FCP	file control parameters	Tham số kiểm soát tệp tin
LCS	life cycle status	Trạng thái vòng đời

5 Vòng đời

Một trạng thái vòng đời có thể liên quan tới bất kỳ đối tượng nào trong thẻ và với chính thẻ đó. Thẻ phải được sử dụng trong trạng thái vòng đời kết hợp với các thuộc tính an ninh bổ sung, nhằm xác định một thao tác trên một đối tượng là phụ thuộc vào một chính sách an ninh hay không. Trạng thái vòng đời thể hiện việc sử dụng các đối tượng theo các quy tắc sau:

- Nếu một đối tượng đặt trong trạng thái khởi tạo, thì không có thuộc tính an ninh nào đối với đối tượng đó bắt buộc áp dụng.
- Nếu một đối tượng đặt trong trạng thái không kích hoạt, thì bất kỳ thuộc tính an ninh nào quy định cho trạng thái này có thể áp dụng.
- Nếu một đối tượng đặt trong trạng thái vận hành, thì mỗi trạng thái an ninh liên quan bắt buộc áp dụng.
- Nếu một đối tượng đặt trong trạng thái kết thúc, thì giá trị của đối tượng đó không được thay đổi nhưng đối tượng này có thể được dùng như đã quy định bởi các thuộc tính an ninh liên quan của nó, ví dụ: nó có thể bị xóa.

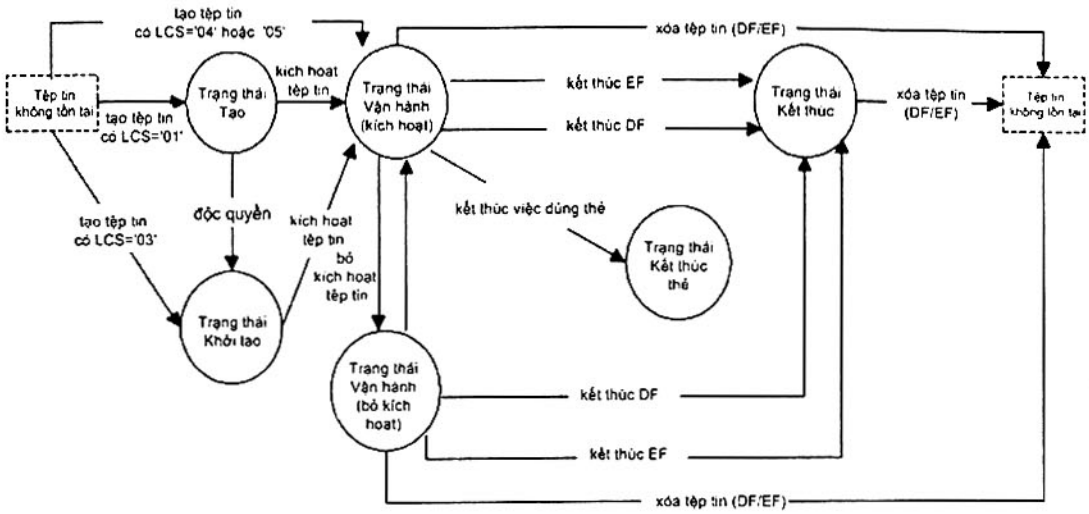
Các chuyển đổi giữa các trạng thái vòng đời không thể thay đổi và chỉ diễn ra từ khi khởi tạo tới khi kết thúc. Hơn nữa, ứng dụng có thể định nghĩa các trạng thái vòng đời thứ cấp: mỗi trạng thái sơ cấp có thể có các trạng thái thứ cấp có thể đảo nghịch. Các thay đổi được kiểm soát bởi thẻ và có thể được thực hiện theo một trình tự được quy định trước, thể hiện các thay đổi có thể hay không thể đảo nghịch về trạng thái. Các lệnh sau đối với quản lý thẻ và tệp tin có thể được sử dụng nhằm khởi tạo một chuyển đổi trạng thái vòng đời.

CREATE FILE	ACTIVATE FILE	TERMINATE EF
DELETE FILE	DEACTIVATE FILE	TERMINATE DF
	TERMINATE CARD USAGE	

Các lệnh có thể nhóm các giá trị của các trạng thái vòng đời khi chúng thực thi. Tuy nhiên, thẻ phải duy trì tính toàn vẹn của giá trị này theo tiêu chuẩn này.

5.1 Vòng đời tệp tin

Hình 1 là một biểu diễn khái niệm của các trạng thái vòng đời và các lệnh nhằm gọi một chuyển đổi giữa một hoàn thiện thành công. Hình 1 không thể hiện các điều kiện của việc xử lý các lệnh này (xem TCVN 11167-4 (ISO/IEC 7816-4)).



Hình 1 - Mô hình vòng đời tệp tin

6 Lệnh đối với quản lý thẻ

Tiêu chuẩn này không bắt buộc đối với các thẻ tuân thủ theo tiêu chuẩn này nhằm hỗ trợ tất cả các lệnh đó hoặc tất cả các tùy chọn của một lệnh hỗ trợ.

Các lệnh có thể thực hiện chỉ khi trạng thái an ninh thỏa mãn các thuộc tính an ninh đối với các lệnh này.

Đối với các lệnh này, các bit 4 và 3 không có nghĩa và phải được bỏ qua.

Đối với mỗi lệnh, một danh sách các điều kiện trạng thái không đầy đủ được đưa ra (xem TCVN 11167-4 (ISO/IEC 7816-4)).

6.1 Lệnh CREATE FILE

Lệnh CREATE FILE khởi tạo việc khởi tạo một tệp tin (DF hay EF) đặt trực tiếp dưới dạng DF hiện tại. Lệnh này có thể phân bổ bộ nhớ với tệp tin mà tệp tin đó tạo ra. Tệp tin được tạo ra phải được thiết lập như các tệp tin hiện tại, ngoại trừ các quy định khác.

Khi có nhiều hơn một EF với một bộ định danh EF ngắn tồn tại với cùng DF, hoạt động của thẻ không được quy định trong tiêu chuẩn này.

Lệnh này có thể chỉ thực hiện chỉ khi nếu trạng thái an ninh thỏa mãn các thuộc tính an ninh đối với DF hiện tại.

Các byte của bộ mã hóa tệp tin là bắt buộc. Tệp tin này chỉ ra khi một DF hay EF được tạo ra hay không.

- Nếu một DF được tạo ra, thì một tên DF và/hoặc một bộ định danh tệp tin phải được quy định.
- Nếu một EF được tạo ra, thì một bộ định danh tệp tin và/hoặc một bộ định danh EF ngắn phải được quy định.

Bảng 1 - Cặp lệnh-hồi đáp CREATE FILE

CLA INS P1-P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4) "E0" "0000" Mã định danh tệp tin và tham số tệp tin được mã hóa theo trường dữ liệu lệnh P1 không bằng "00": byte bộ mã hóa tệp tin P2 Mã định danh EF ngắn chỉ nằm từ bit 8 tới bit 4; từ bit 3 tới bit 1
Trường L_c	Rỗng đối với mã hóa Nc = 0, có giá trị đối với mã hóa Nc > 0
Trường dữ liệu	Khuôn mẫu FCP (gắn nhãn "62") và các khuôn mẫu khác có thể hoặc Rỗng
Trường L_e	Rỗng đối với mã hóa Ne = 0
Trường dữ liệu	Rỗng
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 5 và 6 liên quan, ví dụ: 6982, 6A84, 6A89, 6A8A

CHÚ THÍCH Nếu số N_e bằng 0, thì tệp tin được tạo ra có các thông số kiểm soát tệp tin mặc định.

6.2 Lệnh DELETE FILE

Lệnh DELETE FILE khởi tạo việc xóa tức thời một EF tham chiếu ở dạng DF hiện tại, hoặc một DF với cây phụ hoàn thiện của nó. Sau khi thực thi thành công lệnh này, tệp tin bị xóa không được chọn. Tệp tin hiện tại sau khi xóa một EF là DF hiện tại. DF hiện tại sau khi xóa một DF là DF cha, nếu không thì các tệp tin khác được quy định. Tài nguyên của các tệp tin phải được giải phóng và bộ nhớ được sử dụng bởi tệp tin này phải được thiết lập với trạng thái bị xóa một cách logic.

Việc xóa tệp tin có thể phụ thuộc và trạng thái hiện tại của tệp tin bổ sung. MF không được xóa.

Nếu P1-P2 = "0000" và trường dữ liệu lệnh được Rỗng, thì lệnh này áp dụng với một tệp tin được chọn lựa bởi các lệnh thực thi trực tiếp trước đó. Hơn nữa, nếu các tệp tin được chọn lựa theo kênh logic khác thì việc thực thi các lệnh bị bỏ qua và một lỗi tương ứng được báo lại.

Các ý nghĩa khác của P1-P2, bao gồm việc quy định các quy tắc về sự duy nhất của mã định danh tệp tin, được quy định trong lệnh SELECT.

Bảng 2 - Cặp lệnh-hồi đáp DELETE FILE

CLA INS P1-P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4) "E4" "0000" Xóa tệp tin hiện tại Các giá trị khác được quy định đối với lệnh SELECT (xem TCVN 11167-4 (ISO/IEC 7816-4))
Trường L_c	Rỗng đối với mã hóa Nc = 0, có giá trị đối với mã hóa Nc > 0
Trường dữ liệu	Quy định đối với lệnh SELECT (xem TCVN 11167-4 (ISO/IEC 7816-4))
Trường L_e	Rỗng đối với mã hóa Ne = 0
Trường dữ liệu	Rỗng
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 5 và 6 liên quan, ví dụ: 6982, 6985

6.3 Lệnh DEACTIVATE FILE

Lệnh DEACTIVATE FILE khởi tạo việc bỏ kích hoạt dành riêng cho một tệp tin. Sau khi một hoàn thiện của các lệnh thành công, nhằm bổ sung cho lệnh SELECT, chỉ các lệnh: ACTIVATE FILE, DELETE FILE, TERMINATE EF và trong trường hợp của một DF, lệnh TERMINATE DF phải được phép.

Khi áp dụng cho một tệp tin bị bỏ kích hoạt, lệnh SELECT chọn lựa các tệp tin và trả lại giá trị SW1-SW2 = '6283' như một trạng thái cảnh báo: tệp tin lựa chọn không hiệu lực, ví dụ: bị bỏ kích hoạt.

Nếu một EF được chọn lựa thì các lệnh chỉ bắt buộc áp dụng cho các EF và không được áp dụng cho các DF cha.

Nếu P1-P2 = '0000' và nếu trường dữ liệu lệnh bị thiếu thì các lệnh áp dụng cho tệp tin này được lựa chọn bởi các lệnh thực thi trực tiếp trước đó. Ý nghĩa khác của P1-P2 bao gồm các quy tắc định nghĩa sự duy nhất của mã định danh tệp tin được quy định trong lệnh SELECT.

Thông điệp an ninh phải được sử dụng. Nếu APDU hồi đáp không được bảo vệ thì cách thức kiểm tra chức năng được thực thi thông thường không được quy định trong phạm vi của bộ tiêu chuẩn này.

Vì lí do an ninh, các chức năng tương tự có thể thực hiện theo phương thức độc quyền.

Bảng 3 - Cặp lệnh-hồi đáp DEACTIVATE FILE

CLA INS P1-P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4) "04" "0000" Dừng kích hoạt tệp tin hiện tại Các giá trị khác được quy định đối với lệnh SELECT (xem TCVN 11167-4 (ISO/IEC 7816-4))
Trường L_c	Rỗng đối với mã hóa Nc = 0, có giá trị đối với mã hóa Nc > 0
Trường dữ liệu	Quy định đối với lệnh SELECT (xem TCVN 11167-4 (ISO/IEC 7816-4))
Trường L_e	Rỗng đối với mã hóa Ne = 0
Trường dữ liệu	Rỗng
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 5 và 6 liên quan, ví dụ: 6982, 6A80

6.4 Lệnh ACTIVATE FILE

Lệnh ACTIVE FILE nhằm chuyển đổi một trạng thái tệp tin từ bất kỳ trạng thái khởi tạo hay từ bất kỳ trạng thái khởi tạo nào hoặc từ trạng thái vận hành (không kích hoạt) sang trạng thái vận hành khác (kích hoạt).

Việc kích hoạt một tệp tin chính xác luôn được phép. Việc kích hoạt một tệp tin không kích hoạt có thể chỉ được thực hiện nếu trạng thái an ninh thỏa mãn các thuộc tính an ninh được quy định đối với tệp tin này đối với chức năng kích hoạt.

Nếu APDU hồi đáp không được bảo vệ bởi thông điệp an ninh, thì cách thức để kiểm tra chức năng được thực thi thông thường không được quy định trong phạm vi của bộ tiêu chuẩn này.

Nếu P1-P2 = '0000' và nếu trường dữ liệu lệnh bị thiếu, thì các lệnh áp dụng cho tệp tin được lựa chọn bởi các lệnh được thực thi trực tiếp trước đó. Ý nghĩa khác của P1-P2 bao gồm các quy tắc định nghĩa sự duy nhất của các bộ định danh tệp tin, được quy định trong lệnh SELECT.

Bảng 4 - Cặp lệnh-hồi đáp ACTIVATE FILE

CLA INS P1-P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4) '44' '0000' Kích hoạt tệp tin hiện tại Các giá trị khác được quy định đối với lệnh SELECT (xem TCVN 11167-4 (ISO/IEC 7816-4))
Trường L_c	Rỗng đối với mã hóa Nc = 0, có giá trị đối với mã hóa Nc > 0
Trường dữ liệu	Quy định đối với lệnh SELECT (xem TCVN 11167-4 (ISO/IEC 7816-4))
Trường L_e	Rỗng đối với mã hóa Ne = 0
Trường dữ liệu	Rỗng
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 5 và 6 liên quan, ví dụ: 6400, 6982

6.5 Lệnh TERMINATE FILE

Lệnh TERMINATE DF khởi tạo việc chuyển đổi một DF không thể đảo ngược thành trạng thái kết thúc. Sau khi thực thi thành công lệnh này, DF ở trạng thái kết thúc và chức năng sẵn có từ DF và nhánh phụ của nó bị suy giảm. DF phải được chọn lựa và trạng thái cảnh báo SW1-SW2 = '6285' (tệp tin được chọn lựa ở trạng thái kết thúc) phải được trả về. Các hành động sau đó không được quy định trong bộ tiêu chuẩn này.

CHÚ THÍCH Mục tiêu của việc kết thúc DF thường được tạo ra cho ứng dụng không được sử dụng bởi chủ thẻ.

Nếu P1-P2 = '0000' và nếu trường dữ liệu bị bỏ Rỗng, thì các lệnh áp dụng cho tệp tin này được lựa chọn bởi các lệnh thực thi trực tiếp trước đó. Ý nghĩa khác của P1-P2, bao gồm các quy tắc định nghĩa sự duy nhất của các bộ định danh tệp tin, được quy định trong lệnh SELECT.

Thông điệp an ninh phải được sử dụng. Nếu APDU hồi đáp không được bảo vệ bởi thông điệp an ninh thì cách thức kiểm tra chức năng phải được thực thi nhưng không được quy định trong phạm vi của bộ tiêu chuẩn này.

Bảng 5 - Cặp lệnh-hồi đáp TERMINATE DF

CLA INS P1-P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4) 'E6' '0000' Kết thúc DF hiện tại Các giá trị khác được quy định đối với lệnh SELECT (xem TCVN 11167-4 (ISO/IEC 7816-4))
Trường L_c	Rỗng đối với mã hóa Nc = 0, có giá trị đối với mã hóa Nc > 0
Trường dữ liệu	Quy định đối với lệnh SELECT (xem TCVN 11167-4 (ISO/IEC 7816-4))
Trường L_e	Rỗng đối với mã hóa Ne = 0
Trường dữ liệu	Rỗng
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 5 và 6 liên quan, ví dụ: 6982, 6985

CHÚ THÍCH Trong các lệnh, khi P1-P2 được mã hóa theo lệnh SELECT (xem TCVN ISO/IEC 67816-4), các bit 3 và 4 của P2 không có nghĩa và phải được Rỗng.

6.6 Lệnh TERMINATE EF

Lệnh TERMINATE EF khởi tạo việc chuyển đổi không thể đảo ngược của EF cụ thể thành trạng thái kết thúc.

EF kết thúc phải ở trạng thái kích hoạt hay không kích hoạt.

Vì lí do an ninh, các chức năng tương tự có thể thực hiện theo phương thức độc quyền.

Nếu P1-P2 = '0000' và nếu trường dữ liệu lệnh bị bỏ Rỗng thì các lệnh áp dụng cho các tệp tin được lựa chọn bởi các lệnh thực thi trực tiếp trước đó. Ý nghĩa khác của P1-P2 bao gồm các quy tắc định nghĩa sự duy nhất của các bộ định danh tệp tin, được quy định trong lệnh SELECT.

Bảng 6 - Cặp lệnh-hồi đáp TERMINATE EF

CLA INS P1-P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4) 'E8' '0000' Kết thúc EF hiện tại Các giá trị khác được quy định đối với lệnh SELECT (xem TCVN 11167-4 (ISO/IEC 7816-4))
Trường L_c	Rỗng đối với mã hóa Nc = 0, có giá trị đối với mã hóa Nc > 0
Trường dữ liệu	Quy định đối với lệnh SELECT (xem TCVN 11167-4 (ISO/IEC 7816-4))
Trường L_e	Rỗng đối với mã hóa Ne = 0
Trường dữ liệu	Rỗng
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 5 và 6 liên quan, ví dụ: 6982, 6985

6.7 Lệnh TERMINATE CARD USAGE

Lệnh TERMINATE CARD USAGE khởi tạo việc chuyển đổi không thể đảo ngược của thẻ thành trạng thái kết thúc. Việc sử dụng lệnh này đưa ra một chọn lựa hàm ý của MF.

Đối với các thẻ hỗ trợ lệnh này, trạng thái kết thúc cần được chỉ ra trong Answer-to-Reset.

Sau khi thực thi thành công một lệnh, thẻ không được hỗ trợ lệnh SELECT nữa.

Vì lí do an ninh, các chức năng tương tự có thể thực hiện theo phương thức độc quyền.

CHÚ THÍCH Mục đích của việc chấm dứt sử dụng thẻ là làm cho thẻ không sử dụng được bởi chủ thẻ.

Thông điệp an ninh cần được sử dụng. Nếu APDU phản hồi không được bảo vệ bởi thông điệp an ninh thì cách thức kiểm tra chức năng được thực thi thông thường không được quy định trong phạm vi của bộ tiêu chuẩn này.

Bảng 7 - Cặp lệnh-hồi đáp TERMINATE CARD USAGE

CLA INS P1-P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4) 'FE' '0000'
Trường L_c	Rỗng đối với mã hóa N_c = 0
Trường dữ liệu	Rỗng
Trường L_e	Rỗng đối với mã hóa Ne = 0
Trường dữ liệu	Rỗng
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 5 và 6 liên quan, ví dụ: 6982, 6985

Phụ lục A

(tham khảo)

Ví dụ về thuộc tính an ninh được sử dụng cho việc tải xuống

A.1 Giới thiệu

Ví dụ này trình bày cách thức kiểm soát việc tải dữ liệu (tải xuống an toàn) trong các thẻ, theo cách thức xác minh quyền truy cập của việc tải thực thể và việc bảo vệ dữ liệu truyền tải với thông điệp an ninh. Dữ liệu được tải có thể bao gồm, ví dụ: mã, các khóa và các applet.

Các giả định sau được đưa ra:

- Hệ thống tệp tin phụ thuộc vào tiêu chuẩn này;
- Cấu trúc lệnh, vòng đời và kiểm soát truy cập phụ thuộc vào tiêu chuẩn này;
- DF hiện tại sẵn sàng ở trạng thái vận hành (LCS = 4);
- Dữ liệu được tải vào một tệp tin chuyển đổi không thể đảo ngược số 1 (DF/EF ở trạng thái không đối xứng (LCS = 3));
- SEID = 2 đối với LCS = 3, trạng thái không đối xứng và kết nối trực tuyến, thể hiện trong DF hiện tại;
- SEID = 3 đối với LCS = 3, trạng thái không đối xứng và kết nối ngoại tuyến, thể hiện trong DF hiện tại;
- SEID = 4 đối với LCS = 4, trạng thái vận hành, thể hiện trong DF hiện tại;
- Dữ liệu được bảo vệ đối với sự truy vấn (và được tùy chọn mã hóa) bởi các đối tượng dữ liệu thông điệp an ninh;
- Trong một kết nối trực tuyến (SEID = 2), một quy trình sở hữu không đối xứng đã được thực thi thành công trước đó, ví dụ: với việc trao đổi khóa phiên nhằm bảo vệ việc tải thông điệp an ninh. Dữ liệu tải được bảo vệ bởi một đối tượng dữ liệu bộ kiểm tra lỗi mã hóa và được tùy chọn bởi đối tượng dữ liệu mã hóa;
- Trong một kết nối ngoại tuyến (SEID = 3), dữ liệu tải được bảo vệ bởi một đối tượng dữ liệu chữ kí số và được tùy chọn mã hóa bởi một đối tượng dữ liệu mã hóa;
- Thông tin chứng thực (chứng thực người chứng nhận) có thể đang nằm trong một chứng nhận thẻ xác minh liên kết việc tải thực thể cho khóa chứng thực (SEID = 2, kết nối trực tuyến) hoặc cho khóa chữ kí số (SEID = 3, kết nối ngoại tuyến) và cho các quyền truy cập của chính nó.

A.2 Tải xuống an toàn

Việc tải xuống an toàn được mô tả bên dưới, theo các kết nối trực tuyến và ngoại tuyến.

Kết nối trực tuyến

1. Lựa chọn DF hiện tại (SELECT (tên DF = AID))
2. Thiết lập trạng thái khởi tạo đối với kết nối trực tuyến (MSE: RESTORE SEID = 2)
3. Chứng thực bên ngoài (xác minh chứng nhận, chứng thực bên ngoài)
4. Lựa chọn tệp tin 1 (SELECT (bộ định danh tệp tin))
5. Tải dữ liệu vào tệp tin (ví dụ: WRITE BINARY) với SM, được bảo vệ bởi đối tượng dữ liệu bộ kiểm tra mã hóa.
6. Kích hoạt tệp tin (ACTIVATE FILE)
7. Thiết lập trạng thái vận hành (MSE: RESOTE SEID = 4)
8. Xác minh chứng thực người dùng (VERiFY (mật khẩu))
9. Lựa chọn tệp tin 1 (SELECT (bộ định danh tệp tin))
10. Đọc thông tin (READ BINARY)

Kết nối ngoại tuyến

1. Lựa chọn DF hiện tại (SELECT (tên DF = AID))
2. Thiết lập trạng thái khởi tạo đối với kết nối ngoại tuyến (MSE: RESTORE SEID = 3)
3. Xác minh chứng nhận (VERIFY CERTIFICATE)
4. Lựa chọn tệp tin (SELECT (bộ định danh tệp tin))
5. Tải dữ liệu thành tệp tin với SM (ví dụ: WRITE BINARY) được bảo vệ bởi đối tượng dữ liệu chữ kí số
6. Kích hoạt tệp tin (ACTIVATE FILE)
7. Thiết lập trạng thái vận hành (MSE: RESTORE SEID = 4)
8. Xác minh chứng thực người dùng (VERIFY (mật khẩu))
9. Lựa chọn tệp tin 1 (SELECT (bộ định danh tệp tin))
10. Đọc thông tin (READ BINARY)

A.3 Mã hóa định dạng thu gọn đối với các thuộc tính an ninh

Việc mã hóa sau mô tả truy cập theo các trạng thái vận hành có thể khác nhau từ các truy cập theo trạng thái khởi tạo.

Kết nối trực tuyến

Nếu một WRITE BINARY và (sau khi thực thi thành công) một ACTIVATE FILE được phép ở trạng thái khởi tạo và một READ BINARY ở trạng thái vận hành đối với một trạng thái an ninh hiện tại thì việc mã hóa các byte AM và SC tuân theo các quy tắc sau:

- **Trạng thái khởi tạo**
  - Byte AM (ACTIVATE FILE (bit 5 = 1), WRITE BINARY (bit 3 = 1))
  - Byte 1 SC (Tất cả các điều kiện (bit 8 = 1), thông điệp an ninh đối với ACTIVATE FILE (bit 7 = 1))
  - Byte 2 SC (Tất cả các điều kiện (bit 8 = 1), chứng thực bên ngoài và thông điệp an ninh đối với WRITE BINARY (bits 7 to 6 = 11))
- **Trạng thái vận hành**
  - Byte AM (READ BINARY (bit 1 = 1))
  - Byte SC (Thẩm quyền người dùng (bit 5 = 1))

Hoặc là:

- Từ bit 4 tới bit 1 mã hóa một bộ định danh SE (2 như 0010, 4 như 0100) trong các byte SC
- hoặc SE liên quan được định danh như SE hiện tại (0000); trong trường hợp này thì các thuộc tính an ninh được mã hóa theo định dạng mở rộng.

Kết nối ngoại tuyến

Nếu một WRITE BINARY và (sau khi hoàn thiện thành công) một ACTIVATE FILE được phép ở trạng thái khởi tạo và một READ BINARY ở trạng thái vận hành đối với một trạng thái an ninh hiện tại thì việc mã hóa các byte AM và SC tuân theo các quy tắc sau:

- **Trạng thái khởi tạo**
  - Byte AM (ACTIVATE FILE (bit 5 = 1), WRITE BINARY (bit 3 = 1))
  - Byte 1 SC (Tất cả các điều kiện (bit 8 = 1), thông điệp an ninh đối với ACTIVATE FILE (bit 7 = 1))
  - Byte 2 SC (Tất cả các điều kiện (bit 8 = 1), thông điệp an ninh đối với WRITE BINARY (bit 7 = 1))
- **Trạng thái vận hành**
  - Byte AM (READ BINARY (bit 1 = 1))
  - Byte SC (Thẩm quyền người dùng (bit 5 = 1))

Hoặc là:

- Từ bit 4 tới bit 1 mã hóa một bộ định danh SE (3 như 0011, 4 như 0100) trong các byte SC
- hoặc SE liên quan được định danh như SE hiện tại (0000); trong trường hợp này thì các thuộc tính an ninh được mã hóa theo định dạng mở rộng

A.4 Mã hóa định dạng mở rộng đối với các thuộc tính an ninh

Kết nối trực tuyến

Nếu một WRITE BINARY và (sau khi hoàn thiện thành công) một ACTIVATE FILE được phép ở trạng thái khởi tạo và một READ BINARY ở trạng thái vận hành đối với một trạng thái an ninh hiện tại thì việc mã hóa các đối tượng dữ liệu AM và dữ liệu SC tuân theo các quy tắc sau:

- **Trạng thái khởi tạo**
  - Đối tượng dữ liệu 1 AM truyền một byte AM (WRITE BINARY (bit 3 = 1))
  - Đối tượng dữ liệu 1 SC truyền một AT bao gồm một đối tượng dữ liệu tham chiếu khóa và một đối tượng dữ liệu bộ định tính sử dụng đối với thẩm quyền bên ngoài (bit 8 = 1)
  - Đối tượng dữ liệu 2 SC truyền một CTT bao gồm một đối tượng dữ liệu tham chiếu khóa và một đối tượng dữ liệu bộ định tính sử dụng đối với thông báo an ninh (từ bit 5 tới bit 6 = 11)
  - Đối tượng dữ liệu 2 AM truyền một byte AM (ACTIVATE FILE (bit 5 = 1))
  - Đối tượng dữ liệu 3 SC truyền một CCT bao gồm một đối tượng dữ liệu tham chiếu khóa và một đối tượng dữ liệu sử dụng CRT đối với thông báo an ninh (từ bit 5 tới bit 6 = 11)
- **Trạng thái vận hành**
  - Đối tượng dữ liệu AM truyền một byte AM (READ BINARY (bit 1 = 1))
  - Đối tượng dữ liệu SC truyền một AT bao gồm một đối tượng dữ liệu tham chiếu khóa và một đối tượng dữ liệu bộ định tính sử dụng CRT chỉ báo thẩm quyền người dùng (bit 4 = 1).

SE liên quan được định danh như SE hiện tại (từ bit 4 tới bit 1 = 0000). Trong trường hợp này các thuộc tính an ninh được mã hóa dưới định dạng mở rộng.

Kết nối ngoại tuyến

Nếu một WRITE BINARY và (sau khi hoàn thiện thành công) một ACTIVATE FILE được phép ở trạng thái khởi tạo và một READ BINARY ở trạng thái vận hành đối với một trạng thái an ninh hiện tại thì việc mã hóa các đối tượng dữ liệu AM và SC tuân theo các quy tắc sau:

- **Trạng thái khởi tạo**
  - Đối tượng dữ liệu 1 AM truyền một byte AM (WRITE BINARY (bit 3 = 1), ACTIVATE FILE (bit 5 = 1))
  - Đối tượng dữ liệu 1 SC truyền một DST bao gồm một đối tượng dữ liệu tham chiếu khóa và một đối tượng dữ liệu bộ định tính sử dụng đối với thông báo an ninh (từ bit 5 tới bit 6 = 11)
- **Trạng thái vận hành**
  - Đối tượng dữ liệu AM truyền một byte AM (READ BINARY (bit 1 = 1))

- Đối tượng dữ liệu SC truyền một AT bao gồm một đối tượng dữ liệu tham chiếu khóa và một đối tượng dữ liệu bộ định tính sử dụng CRT chỉ báo thẩm quyền người dùng (bit 4 = 1).

SE liên quan được định danh như SE hiện tại. Trong trường hợp này các thuộc tính an ninh được mã hóa theo định dạng mở rộng.

A.5 Mã hóa đối với các môi trường an ninh liên quan

SEID = 2 bên trong khuôn mẫu ('7B')

{'80' - L - '02'} - {'8A' - L - '03'} - {'A4' - L - {'83' - L - Key reference} - {'95' - 01 - 80} - {'5F4B' - L - Giấy phép người chứng nhận}} - - {'B4' - L - {'83' - L - Tham chiếu khóa} - {'95' - '01' – '30'}}

SEID = 3 bên trong khuôn mẫu ('7B')

{'80' - L - '03'} - {'8A' - L - '03'} - {'B6' - L - {'83' - L - Tham chiếu khóa} - {'95' - '01' – '30'}}

SEID = 4 bên trong khuôn mẫu ('7B')

{'80' - L - '04'} - {'8C' - L - '04'} - {'A4' - L - {'83' - L - Tham chiếu khóa} - {'95' - '01' - '08'}}

Thư mục tài liệu tham khảo

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

[2] ISO/IEC 10536 Identification cards - Contactless intergrated circuit(s) cards - Close-coupled cards (tất cả các phần).

[3] ISO/IEC 14443 Identification cards - Contactless intergrated circuit(s) cards - Proximity cards (tất cả các phần).

[4] ISO/IEC 15693 Identification cards - Contactless intergrated circuit(s) cards - Vicinity cards (tất cả các phần).