TCVN TIÊU CHUẨN QUỐC GIA

TCVN 11167-8:2015
ISO/IEC 7816-8:2004

Xuất bản lần 1

THẺ DANH ĐỊNH - THẺ MẠCH TÍCH HỢP - PHẦN 8: LỆNH ĐỐI VỚI THAO TÁC AN NINH

Identification cards - Integrated circuit cards - Part 8: Commands for security operations

HÀ NỘI - 2015

Mục lục **Trang**

Lời nói đầu

TCVN 11167-8:2015 hoàn toàn tương đương với ISO/IEC 7816-8:2004.

TCVN 11167-8:2015 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 8: Lệnh đối với hoạt động an ninh

Identification cards - Integrated circuit cards - Part 8: Commands for security operations

1 Phạm vi áp dụng

Tiêu chuẩn này quy định lệnh liên ngành có thể được sử dụng cho hoạt động mã hóa.

Việc chọn lựa và điều kiện sử dụng phương thức mã hóa có thể ảnh hưởng tới khả năng xuất khẩu thẻ. Việc đánh giá sự phù hợp của thuật toán và giao thức không được đề cập trong phạm vi của tiêu chuẩn. Tiêu chuẩn này không đề cập đến việc thiết lập bên 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 (ISO/IEC 7816-4) Thẻ định danh - Thẻ vi mạch - Phần 4: Tổ chức, an ninh và lệnh trao đổi.

3 Định nghĩa

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

3.1

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

Kỹ thuật mã hóa sử dụng hai thao tác liên quan: một thao tác công khai được quy định bởi số công khai hay bởi một khóa công khai và một thao tác cá nhân được quy định bởi số cá nhân hoặc bởi một khóa riêng.

CHÚ THÍCH Hai thao tác này có tính chất: đưa ra thao tác công khai được tính toán cho thao tác cá nhân.

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

3.2

Chứng nhận (certificate)

Chữ ký số ràng buộc một cá nhân hay đối tượng cụ thể và tương ứng với một khóa công khai của nó.

CHÚ THÍCH Đơn vị cấp giấy chứng nhận cũng hoạt động như cơ quan phân bổ thẻ liên quan tới thành phần dữ liệu trong chứng nhận.

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

3.3

Chữ ký số (digital signature)

Dữ liệu nối thêm hay việc chuyển đổi mã hóa của một chuỗi dữ liệu nhằm chứng minh nguồn gốc và tính toàn vẹn của chuỗi dữ liệu và bảo vệ chống lại sự giả mạo, ví dụ: bằng cách nhận các chuỗi dữ liệu.

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

3.4

Khóa (key)

Chuỗi ký hiệu kiểm soát một thao tác mã hóa (ví dụ: mã hóa, giải mã một thao tác cá nhân hay công khai theo một chứng thực động, cung cấp chữ ký và xác nhận chữ ký).

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

3.5

Thông điệp an ninh (secure messaging)

Tập cách thức cho việc bảo vệ mã hóa của một hay (một phần của) của cặp lệnh-hồi đáp.

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

4 Thuật ngữ viết tắt và ký hiệu

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

Thuật ngữ	Tiếng Anh	Tiếng Việt
CCT	control reference template for cryptographic checksum	Khuôn mẫu tham chiếu kiểm soát checksum mã hóa
CRT	control reference template	Khuôn mẫu tham chiếu kiểm soát
CT	control reference template for confidentiality	Khuôn mẫu tham chiếu kiểm soát bảo mật
DSA	digital signature algorithm	Thuật toán chữ ký số
DST	control reference template for digital	Khuôn mẫu tham chiếu kiểm soát

Thuật ngữ	Tiếng Anh	Tiếng Việt
	signature	chữ ký số
ECDSA	elliptic curve digital signature algorithm	Thuật toán chữ ký số vòng e-líp
HT	control reference template for hash-code	Khuôn mẫu tham chiếu kiểm soát hàm băm
MSE	MANAGE SECURITY ENVIRONMENT command	Lệnh MANAGE SECURITY ENVIRONMENT
PK	public key	Khóa công khai
PSO	PERFORM SECURITY OPERATION command	Lệnh PERFORM SECURITY OPERATION
GQ	Guillou and Quisquater	Guillou và Quisquater
RFU	reserved for future use	Dành riêng để sử dụng sau này
RSA	Rivest, Shamir, Adleman	Rivest, Shamir, Adleman
SE	security environment	Môi trường an ninh
SEID	security environment identifier	Mã định danh môi trường an ninh

5 Lệnh liên ngành đối với thao tác mã hóa

Tiêu chuẩn này không bắt buộc tất cả lệnh phải phù hợp với tiêu chuẩn này nhằm hỗ trợ tất cả các lệnh này hay tùy chọn của một lệnh được hỗ trợ.

5.1 Lệnh GENERATE ASYMMETRIC KEY PAIR

Lệnh GENERATE ASYMMETRIC PAIR không những chỉ báo việc tạo và lưu trữ một cặp khóa không đối xứng, ví dụ: một khóa công khai và một khóa riêng trong thẻ, hay truy cập một cặp khóa không đối xứng được tạo ra trước đó trong thẻ.

Lệnh này có thể được bắt đầu bởi một lệnh MANAGE SECURITY ENVIRONMENT để thiết lập việc tạo khóa liên quan với các thông số (ví dụ: tham chiếu thuật toán). Lệnh này có thể thực thi trong một hay nhiều bước, thường sử dụng trong xâu chuỗi lệnh (Xem TCVN 11167-4 (ISO/IEC 7816-4)).

Bảng 1 - Cặp lệnh-hồi đáp GENERATE ASYMMETRIC PAIR

CLA INS P1 P2	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4) '46' hoặc '47' Việc khởi tạo được kiểm soát trong Bảng 2 '00' (không có thông tin) hay tham chiếu khóa được tạo ra
Trường L_c	Trống đối với mã hóa Nc = 0, có giá trị đối với mã hóa Nc > 0
Trường dữ liệu	Trống, hoặc Dữ liệu độc quyền nếu P1-P2 = '0000', hoặc Một hay nhiều CRT liên quan tới việc tạo khóa nếu P1-P2 khác '0000' (xem CHÚ THÍCH)
Trường L_e	Trống đối với mã hóa Ne = 0, có giá trị đối với Ne > 0
Trường dữ liệu	Trống, hoặc Khóa công khai như một chuỗi phần tử hay đối tượng dữ liệu, hoặc Chuỗi đối tượng dữ liệu liên quan tới một danh sách tiêu đề mở rộng
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 5 và 6 liên quan, ví dụ: 6985

CHÚ THÍCH Một vài CRT được thể hiện khi cặp khóa được tạo ra cho một vài mục đích. Trong một trường dữ liệu, một CRT có thể có chiều dài bằng 0.

Bảng 2 - Kiểm soát khởi tạo trong P1

b8	b7	b6	b5	b4	b3	b2	b1	Giá trị
0	0	0	0	0	0	0	0	Không có thông tin nào được đưa ra
1	0	0	0	0	x	x	x	Thông tin bổ sung được đưa ra
1	0	0	0	0	-	-	x	**Tạo khóa**
-	-	-	-	-	x	x	0	– Tạo ra cặp khóa không đối xứng
-	-	-	-	-	x	x	1	– Truy cập một khóa công khai có sẵn
1	0	0	0	0	-	x	-	**Định dạng của dữ liệu khóa công khai được trả về**
-	-	-	-	-	x	0	x	– Định dạng độc quyền của dữ liệu khóa công khai
-	-	-	-	-	x	1	x	– Định dạng xuất của dữ liệu khóa công khai liên quan tới một danh sách tiêu đề mở rộng
1	0	0	0	0	x	-	-	**Bộ định danh đầu ra**
-	-	-	-	-	0	x	x	– Dữ liệu khóa công khai trong trường dữ liệu hồi đáp
-	-	-	-	-	1	x	x	– Không có dữ liệu hồi đáp nếu trường L_e trống hoặc độc quyền nếu trường Le có giá trị
Bất kỳ giá trị khác nào được dành riêng cho việc sử dụng sau này bởi cơ quan có thẩm quyền.								

Đối với việc tạo ra một cặp khóa, khi thiếu trường L_e thì cặp khóa được lưu trữ trong thẻ, nhất là trong một EF tham chiếu đã biết trước khi sử dụng lệnh này.

Để truy cập một cặp khóa (không tạo ra), trường dữ liệu lệnh có thể Trống.

Dựa trên tính chẵn lẻ của mã INS (Xem TCVN 11167-4 (ISO/IEC 7816-4)), một khóa công khai trong trường dữ liệu hồi đáp vừa là một chuỗi phần tử dữ liệu ('46') hay một chuỗi đối tượng dữ liệu ('47')

Nếu một danh sách tiêu đề mở rộng mô tả trường dữ liệu hồi đáp, được biết trước khi phát lệnh này. Danh sách này bao gồm các đối tượng dữ liệu khóa công khai và đối tượng dữ liệu được yêu cầu khác.

Khi bit 1 được đặt với một giá trị trong INS, ví dụ: INS đặt là '47' và khi một khóa công khai trả lại trong trường dữ liệu hồi đáp, một mẫu liên ngành được dùng để lồng ghép một tập đối tượng dữ liệu khóa công khai tương ứng theo Bảng 3. Nếu thuật toán này không chỉ ra trong lệnh thì thuật toán này được biết tới trước khi phát lệnh. Trong khuôn mẫu khóa công khai, lớp ngữ cảnh cụ thể (byte đầu tiên từ '80' tới 'BF') được dành cho các đối tượng dữ liệu khóa công khai.

Bảng 3 - Đối tượng dữ liệu khóa công khai

Thẻ		Giá trị
'7F49'		Khuôn mẫu liên ngành cho việc lồng ghép một tập đối tượng dữ liệu khóa công khai với các thẻ sau:
	'06'	Mã định danh đối tượng của thuật toán, tùy chọn
	'80'	Tham chiếu thuật toán được dùng trong các đối tượng dữ liệu tham chiếu đối với thông điệp an ninh, tùy chọn
		Tập đối tượng dữ liệu khóa công khai đối với RSA
	'81'	Các mô-đun (một số được ký hiệu là n được mã hóa theo x byte)
	'82'	Mũ công khai (một số được ký hiệu là v, ví dụ: 65537)
		Tập đối tượng dữ liệu khóa công khai đối với DSA
	'81'	Số nguyên tố đầu tiên (một số được ký hiệu là p được mã hóa theo y byte)
	'82'	Số nguyên tố thứ hai (một số được ký hiệu là p chia thành p-1, ví dụ: 20 byte)
	'83'	Số cơ bản (một số được ký hiệu là g của trình tự q được mã hóa theo y byte)
	'84'	Khóa công khai (một số được ký hiệu là y tương đương với g với lũy thừa x mô đun p khi x là khóa riêng được mã hóa theo y byte)
		Tập đối tượng dữ liệu khóa công khai đối với ECDSA
	'81'	Số nguyên tố (một số được ký hiệu là p được mã hóa theo z byte)
	'82'	Hệ số đầu tiên (một số được ký hiệu là a được mã hóa theo z byte)
	'83'	Hệ số thứ hai (một số được ký hiệu là b được mã hóa theo z byte)
	'84'	Bộ khởi tạo (một điểm được ký hiệu là PB trên đường cong, được mã hóa theo 2z hay z+1 byte)
	'85'	Trình tự (một số nguyên tố được ký hiệu là q, theo trình tự của bộ khởi tạo PB, được mã hóa theo z byte)
	'86'	Khóa công khai (một điểm được ký hiệu là PP trên đường cong, tương đương với x lần PB khi x là khóa riêng, được mã hóa theo 2z hay z+1 byte)
	'87'	Phần phụ đại số
		Tập đối tượng dữ liệu khóa công khai đối với GQ2
		Các mô-đun (một số được ký hiệu là n, được mã hóa theo x byte)
	'81'	Số lượng các số cơ bản (một số được ký hiệu là m, được mã hóa theo 1 byte. Nếu thẻ
	'83'	'83' được thể hiện, thì thẻ 'A3' phải trống và các số cơ bản m được ký hiệu là g, g_2,...,g_m là các số nguyên tố m đầu tiên: 2, 3, 5, 7, 11,...)
		Tham số xác minh (một số được ký hiệu là k, được mã hóa theo 1 byte)
	'84'	Tập m số cơ bản được ký hiệu là g, g_2,... g_m mà mỗi số được mã hóa theo 1 byte với
	'A3'	thẻ '80' (nếu thẻ 'A3' được thể hiện thì thẻ '83' phải trống)

– Trong ngữ cảnh này, cơ quan có thẩm quyền dành riêng bất kỳ đối tượng dữ liệu nào cho lớp ngữ cảnh cụ thể (byte đầu tiên trong dải từ '80' tới 'BF')

5.2 Lệnh PERFORM SECURITY OPERATION

Lệnh này khởi tạo các thao tác an ninh sau, theo các đối tượng dữ liệu được quy định trong P1-P2.

- Tính toán một checksum mã hóa;
- Tính toán một chữ ký số;
- Phép tính của một mã băm;
- Xác thực một checksum mã hóa;
- Xác thực một chữ ký số;
- Xác thực một chứng nhận;
- Mã hóa;
- Giải mã.

Nếu thao tác an ninh yêu cầu một vài lệnh sau để hoàn thành thì việc xâu chuỗi lệnh phải được áp dụng (Xem TCVN 11167-4 (ISO/IEC 7816-4)).

Lệnh này có thể được bắt đầu bằng một lệnh MANAGE SECURITY ENVIRONMENT.

Ví dụ: tham chiếu khóa cũng như tham chiếu thuật toán không những phải được biết tới hoặc được quy định trong một CRT trong lệnh MANAGE SECURITY ENVIRONMENT.

Lệnh này có thể được thực thi chỉ khi nếu trạng thái an ninh thỏa mãn các thuộc tính an ninh cho các thao tác. Việc thực thi thành công các lệnh có thể được hoàn thiện thành công các lệnh trước đó (ví dụ: VERIFY trước khi tính toán một chữ ký số)

Nếu có, một danh sách tiêu đề hay danh sách tiêu đề mở rộng quy định trình tự và các mục dữ liệu tạo nên đầu vào đối với thao tác an ninh.

Bảng 4 - Cặp lệnh-hồi đáp PERFORM SECURITY OPERATION

CLA	Quy định trong TCVN 11167-4 (ISO/IEC 7816-4)
INS	'A2'
P1	Thẻ (trường dữ liệu hồi đáp là phần tử dữ liệu, nếu có) hoặc '00' (trường dữ liệu hồi đáp luôn Trống); 'FF' là RFU
P2	Thẻ (trường dữ liệu hồi đáp là phần tử dữ liệu, nếu có) hoặc '00' (trường dữ liệu hồi đáp luôn Trống); 'FF' là RFU đối với cơ quan có thẩm quyền
Trường L_c	Trống đối với mã hóa Nc = 0, có giá trị đối với mã hóa Nc > 0
Trường dữ liệu	Trống hoặc giá trị của đối tượng dữ liệu nằm trong P2
Trường L_e	Trống đối với mã hóa Ne = 0, có giá trị đối với Ne > 0
Trường dữ liệu	Trống hoặc giá trị của đối tượng dữ liệu nằm trong P1
SW1-SW2	Xem TCVN 11167-4 (ISO/IEC 7816-4), Bảng 5 và 6 liên quan, ví dụ: 6985

Lệnh này dùng các khuôn mẫu được liệt kê trong Bảng 5. Các khuôn mẫu này là đối tượng dữ liệu cơ bản cho thông điệp an ninh (Xem TCVN 11167-4 (ISO/IEC 7816-4)).

Bảng 5 - Khuôn mẫu

Thẻ	Giá trị
'A0'	Khuôn mẫu đối với việc tính toán mã băm (khuôn mẫu bị băm)
'A2'	Khuôn mẫu đối với việc xác thực một checksum mã hóa (mẫu được tích hợp)
'AB'	Khuôn mẫu đối với việc xác thực một chữ ký số (khuôn mẫu được ấn định)
'AC'	Khuôn mẫu đối với việc tính toán chữ ký số (trường giá trị nối được ấn định)
'AE'	Khuôn mẫu đối với việc xác thực một chứng nhận (trường giá trị nối được chứng nhận)
'BC'	Khuôn mẫu đối với việc tính toán một chữ ký số (khuôn mẫu được ấn định)
'BE'	Khuôn mẫu đối với việc xác thực một chứng nhận (khuôn mẫu được chứng nhận)

Trong khuôn mẫu, lớp ngữ cảnh cụ thể (byte đầu tiên trong dải '80' tới 'BF') được dành riêng cho đối tượng dữ liệu nhập. Bảng 6 liệt kê các đối tượng dữ liệu trong khuôn mẫu.

Bảng 6 - Đối tượng dữ liệu nhập

Thẻ	Giá trị	'A0'	'A2'	'AB'	'AC', 'BC'	'AE', 'BE'
'80'	Giá trị thường	x	x	x	x	x
'8E'	Checksum mã hóa		x			x
'90'	Hàm băm	x		x	x	x
'92'	Chứng nhận					x
'9C'	Khóa công khai			x		x
'9E'	Chữ ký số			x		x

5.3 Thao tác COMPUTE CRYPTOGRAPHIC CHECKSUM

Thao tác này khởi tạo việc tính toán một checksum mã hóa.

Bảng 7 - Thông số và trường dữ liệu cho thao tác COMPUTE CRYPTOGRAPHIC CHECKSUM

P1 P2	'8E' '80'
Trường dữ liệu lệnh	Dữ liệu cho checksum mã hóa phải được tính toán
Trường dữ liệu hồi đáp	Checksum mã hóa

5.4 Thao tác COMPUTE DIGITAL SIGNATURE

Thao tác này khởi tạo việc tính toán một chữ ký số. Thuật toán vừa có thể là một thuật toán chữ ký số hay một kết hợp của một thuật toán băm và một thuật toán chữ ký số. Phụ lục A đưa ra các ví dụ về thao tác chữ ký số.

Đối với việc tính toán một chữ ký số, dữ liệu được ấn định hay tích hợp vào trong quy trình gán được chuyển đổi thành trường dữ liệu lệnh hay được khai báo trong một lệnh trước đó, ví dụ: PSO: HASH. Trong P2, chữ ký số được quy định với các thẻ: '9A', 'AC' hay 'BC' theo cấu trúc nhập (Xem TCVN 11167-4 (ISO/IEC 7816-4)).

Nếu dữ liệu bắt buộc bao gồm việc nhập chữ ký số thì một tham chiếu phải được thể hiện trong CRT (Xem TCVN 11167-4 (ISO/IEC 7816-4)). Nếu một đối tượng dữ liệu tham chiếu Trống đối với dữ liệu bắt buộc được thể hiện thì thẻ phải chèn dữ liệu bắt buộc vào. Dữ liệu bắt buộc được tham chiếu trong trường dữ liệu lệnh được ưu tiên hơn bất kì danh sách tiêu đề nào.

Thẻ phải trả lại một chữ ký số (P1 = '9E')

Bảng 8 - Thông số và trường dữ liệu cho thao tác COMPUTE DIGITAL SIGNATURE

P1 P2	'9E' '9A', 'AC' hay 'BC'
Trường dữ liệu lệnh	Trống (dữ liệu sẵn sàng trong thẻ) hoặc Nếu P2 = '9A', dữ liệu được ấn định hay tích hợp trong quy trình ấn định, hoặc Nếu P2 = 'AC', đối tượng dữ liệu, trường giá trị được ấn định hay tích hợp trong quy trình ấn định, hoặc Nếu P2 = 'BC', đối tượng dữ liệu được ấn định hay tích hợp trong quy trình ấn định
Trường dữ liệu hồi đáp	Chữ ký số

CHÚ THÍCH Thẻ 'AC' và 'BC' không được tích hợp trong việc nhập chữ ký số.

5.5 Thao tác HASH

Thao tác này khởi tạo việc tính toán một hàm băm bằng cách thực hiện:

- Việc tính toán toàn bộ trong thẻ hoặc
- Một tính toán một phần trong thẻ (ví dụ: vòng cuối của việc băm)

HT ('AA', 'AB') chỉ ra tham chiếu thuật toán đối với việc tính toán một hàm băm (Xem TCVN 11167-4 (ISO/IEC 7816-4))

Dữ liệu nhập phải được thể hiện với thẻ theo khối nhập hoàn chỉnh (một hay nhiều trong một thời điểm), chiều dài mà thuật toán phụ thuộc, Dựa vào thuật toán băm, dữ liệu nhập cuối có chiều dài tương đương hoặc ngắn hơn chiều dài của khối. Thuật toán đệm, nếu thích hợp là một phần của việc quy định thuật toán băm.

Đối với kết quả của hàm băm, hai trường hợp sau có nhiều khác biệt:

- Khi thẻ lưu trữ cả hàm băm đối với lệnh chuỗi phụ; thì trường L_e không được thể hiện hoặc
- Thẻ phân phối hàm băm theo cách hồi đáp thì trường L_e được thiết lập với chiều dài tương ứng.

Bảng 9 - Thông số và trường dữ liệu của thao tác HASH

P1 P2	'90' '80 hay 'A0'
Trường dữ liệu lệnh	Nếu P2 = '80', dữ liệu được băm, hoặc Nếu P2 = 'A0', đối tượng dữ liệu liên quan tới việc băm (ví dụ: '90' đối với hàm băm trung gian, '80' đối với khối cuối cùng)
Trường dữ liệu hồi đáp	Hàm băm hoặc Trống

5.6 Thao tác VERIFY CRYTOGRAPHIC CHECKSUM

Thao tác này khởi tạo việc xác thực một bộ kiểm tra mã hóa.

Bảng 10 - Thông số và trường dữ liệu của thao tác VERIFY CRYPTOGRAPHIC CHECKSUM

P1 P2	'00' 'A2'
Trường dữ liệu lệnh	Đối tượng dữ liệu liên quan tới thao tác (ví dụ: '80', '8E')
Trường dữ liệu hồi đáp	Trống

CHÚ THÍCH Trường giá trị của đối tượng dữ liệu giá trị thường (thẻ '80') bao gồm dữ liệu (các phần tử dữ liệu hay đối tượng dữ liệu) bao trùm bộ kiểm tra mã hóa.

5.7 Thao tác VERIFY DIGITAL SIGNATURE

Thao tác này khởi tạo việc xác minh một chữ ký số được phân phát như một đối tượng dữ liệu trong trường dữ liệu lệnh. Các xác minh dữ liệu liên quan được chuyển đổi cả trong quy trình xâu chuỗi lệnh hoặc được thể hiện trong thẻ. Thuật toán có thể là một thuật toán chữ ký số hay một kết hợp của thuật toán băm và thuật toán chữ ký số. Phụ lục A đưa ra các ví dụ về thao tác chữ ký số.

Khóa công khai cũng như thuật toán có thể được:

- Cũng được biết đến, hay
- Được tham chiếu trong một DST ('B6') của lệnh MANAGE SECURITY ENVIRONMENT hay
- Sẵn có như một kết quả từ thao tác VERIFY CERTIFICATION trước đó.

Nếu tham chiếu thuật toán trong thẻ mô tả một chữ ký số mà chỉ có thuật toán thì dữ liệu bao gồm một hàm băm, hoặc chữ ký của loại phục hồi thông điệp (xem ISO/IEC 9796). Nếu không thì việc tính toán hàm băm được thực hiện trong thẻ và tham chiếu thuật toán bổ sung bao gồm một tham chiếu đối với thuật toán băm.

Bảng 11 - Thông số và trường dữ liệu của thao tác VERIFY DIGITAL SIGNATURE

P1 P2	'00' 'AB'
Trường dữ liệu lệnh	Đối tượng dữ liệu liên quan tới thao tác (ví dụ: cả '9A', 'AC', hay 'BC' và '9E')
Trường dữ liệu hồi đáp	Trống

Nếu trường dữ liệu lệnh bao gồm một đối tượng dữ liệu Trống thì thẻ cần biết giá trị sử dụng theo cách xác minh của nó.

5.8 Thao tác VERIFY CERTIFICATE

Đối với việc xác minh một chứng nhận trong một thẻ (xem Phụ lục B), chữ ký số của một chứng nhận được xác minh được phân phối như một đối tượng dữ liệu trong trường dữ liệu lệnh. Khóa công khai của thẩm quyền chứng nhận được dùng trong quy trình xác minh phải được thể hiện trong thẻ và được chọn lựa hàm ý hay có thể được tham chiếu trong một DST sử dụng lệnh MANAGE SECURITY ENVIRONMENT. Thuật toán áp dụng được biết tới hoặc có thể được tham chiếu trong một DST. Nếu các đối tượng dữ liệu khác được sử dụng trong quy trình xác minh (ví dụ: hàm băm) thì các đối tượng dữ liệu này phải được thể hiện trong thẻ hoặc phải được truyền sử dụng quy trình xâu chuỗi lệnh.

Hai trường hợp sau có các khác biệt:

- Nếu chứng nhận là tự mô tả (P2 = 'BE') thì thẻ nhận một khóa công khai được nhận dạng bởi thẻ của nó trong nội dung chứng nhận (được phục hồi).
- Nếu chứng nhận là không tự mô tả (P2 = 'AE') thì thẻ nhận một khóa công khai trong chứng nhận cả hàm ý hay tường minh bằng cách sử dụng thẻ khóa công khai trong một danh sách tiêu đề mô tả nội dung của chứng nhận.

Nếu khóa công khai được lưu trữ, nó là khóa mặc định đối với thao tác phụ VERIFY DIGITAL SIGNATURE.

Bảng 12 - Thông số và trường dữ liệu của thao tác VERIFY CERTIFICATE

P1 P2	'00' '92', 'AE' hay 'BE'
Trường dữ liệu lệnh	Đối tượng dữ liệu liên quan tới thao tác
Trường dữ liệu hồi đáp	Trống

CHÚ THÍCH Nếu một lược đồ phục hồi thông điệp một phần được dùng và một phần thông tin được lưu trữ trên thẻ thì đối tượng dữ liệu của dữ liệu phụ trợ phải được gửi trắng, với dữ liệu được chèn vào sau đó bởi thẻ.

5.9 Thao tác ENCIPHER

Thao tác này mã hóa dữ liệu được truyền trong trường dữ liệu lệnh. Sử dụng thao tác này có thể bị hạn chế.

Bảng 13 - Thông số và trường dữ liệu của thao tác ENCIPHER

P1 P2	'82', '84', '86' (giản đồ mã hóa) '80 (giá trị thường)
Trường dữ liệu lệnh	Trống (dữ liệu nằm sẵn trong thẻ) hoặc Dữ liệu được mã hóa
Trường dữ liệu hồi đáp	Dữ liệu được mã hóa

5.10 Thao tác DECIPHER

Thao tác này giải mã dữ liệu được truyền trong trường dữ liệu lệnh. Sử dụng thao tác này có thể bị hạn chế.

Bảng 14 - Thông số và trường dữ liệu của thao tác DECIPHER

P1 P2	'80' (giá trị thường) '82, '84', '86 (giản đồ mã hóa)
Trường dữ liệu lệnh	Dữ liệu được giải mã
Trường dữ liệu hồi đáp	Trống (dữ liệu giải mã còn nằm trong thẻ) hoặc dữ liệu được giải mã

Phụ lục A

(tham khảo)

Ví dụ về thao tác liên quan tới chữ ký số

A.1 Chuỗi lệnh quản lý môi trường an ninh

Bảng A.1 trình bày một chuỗi lệnh của MANAGE SECURITY ENVIRONMENT từ các thành phần: SET DST, CCT và CT của SE hiện tại và SE cuối cùng với lệnh STORE SE hiện tại theo một SEID được chỉ ra trong P2.

Bảng A.1 - Thiết lập các thành phần của môi trường an ninh

Lệnh	Thao tác	P1-P2	Trường dữ liệu lệnh
MSE	SET DST	'41' - 'B6'	{'84' - L - Tham chiếu khóa} - {'91' - L = 0}
MSE	SET CCT	'41' - 'B4'	{'83' - L - Tham chiếu khóa} - {'87' - L - Giá trị khởi tạo}
MSE	SET CT	'41' - 'B8'	{'83' - L - Tham chiếu khóa}
MSE	STORE (SEID = 1)	'F2' - '01'	-

Thao tác SET DST tham chiếu khóa riêng dùng trong tính toán chữ ký và quy định việc tương tác một số ngẫu nhiên khi nhập chữ ký số. Thao tác SET CCT tham chiếu một khóa bí mật và một giá trị khởi tạo với việc tính toán một bộ kiểm tra mã hóa. Thao tác SET CT tham chiếu một khóa phiên bí mật đáng tin cậy.

A.2 Chuỗi lệnh của việc tính toán chữ ký số

Bảng A.2 trình bày cấu trúc đối với việc cung cấp một chữ ký số bằng cách dùng một lược đồ chữ ký có phụ lục. Phần nhập là một hàm băm hoàn chỉnh có các byte đệm. Ví dụ này mô tả việc tính toán một chữ ký số với thuật toán kết hợp bao gồm một thao tác băm. Trong ví dụ này, việc nhập băm được phân phối cho thẻ.

Bảng A.2 - Ví dụ đầu tiên của lược đồ chữ ký số có phụ lục

Lệnh	Thao tác	P1-P2	Trường dữ liệu lệnh	Trường dữ liệu hồi đáp
MSE	RESTORE	'41' - 'B6'		
PSO	COMPUTE DIGITAL SIGNATURE	'41' - 'B4'	Hàm băm với các byte đệm	Chữ ký số

CHÚ THÍCH Ví dụ này được minh họa hoàn chỉnh và giá trị của nó bị giới hạn theo việc thiết lập như một hệ quả của các kiểm soát đầu ra có thể mà có thể áp dụng và thực sự dùng cho các lý do an ninh chung (tránh các chữ ký lặp lại trong một vài trường hợp).

Bảng A.3 trình bày cấu trúc đối việc việc cung cấp một chữ ký số bằng cách dùng một lược đồ chữ ký có phụ lục. Việc nhập chữ ký số bao gồm của hàm băm mà không cần các byte đệm.

Bảng A.3 - Ví dụ thứ hai của lược đồ chữ ký số có phụ lục

Lệnh	Thao tác	P1-P2	Trường dữ liệu lệnh	Trường dữ liệu hồi đáp
MSE	RESTORE	'F3' - '01'	-	-
PSO	COMPUTE DIGITAL SIGNATURE	'9E' - '9A'	Hàm băm với các byte đệm	Chữ ký số

CHÚ THÍCH 1 Nhằm tránh các hạn chế đầu ra, một chữ ký kết hợp và thuật toán băm có thể được sử dụng.

CHÚ THÍCH 2 Trong một vài trường hợp, việc trách lặp lại chữ ký mặc dù mong muốn có thể không đạt được.

Bảng A.4 trình bày một lược đồ chữ ký có phụ lục. Việc nhập chữ ký số bao gồm một hàm băm mà không có các byte đệm được phân phối tới thẻ và thẻ được yêu cầu tạo ta một số ngẫu nhiên được yêu cầu trong danh sách tiêu đề mở rộng của DST trong trường dữ liệu lệnh của lệnh MSE. Được quy định bởi thẻ 'BC' trong P2, một kết hợp đối tượng dữ liệu (hàm băm được cấp cho thẻ và số ngẫu nhiên được cấp bởi thẻ) được ấn định.

Bảng A.4 - Ví dụ thứ ba của lược đồ chữ ký số có phụ lục

Lệnh	Thao tác	P1-P2	Trường dữ liệu lệnh	Trường dữ liệu hồi đáp
MSE	SET	'41' - 'B6'	{'4D' - L - {'90' - L - '91' - L = 0}} - {'84' - L - Tham chiếu khóa}	-
PSO	COMPUTE DIGITAL SIGNATURE	'9E' - 'BC'	{'90' - L - Hàm băm}	Chữ ký số

Bảng A.5 trình bày cấu trúc chữ ký số với việc phục hồi thông điệp hạn chế. Dữ liệu ấn định được cấu hình phụ thuộc vào lược đồ chữ ký chỉ ra việc phục hồi thông điệp hạn chế dùng các đối tượng dữ liệu được trình bày trong trường dữ liệu lệnh, theo đó bộ đếm chữ ký số được dùng như thông điệp nội bộ được cấp bởi thẻ.

Bảng A.5 - Ví dụ thứ tư của lược đồ chữ ký số có phụ lục

Lệnh	Thao tác	P1-P2	Trường dữ liệu lệnh	Trường dữ liệu hồi đáp
MSE	RESTORE	'F3' - '02'	-	-
PSO	COMPUTE DIGITAL SIGNATURE	'9E' - 'AC'	{'90' - L - Hàm băm}	Chữ ký số

Trong Bảng A.6, thẻ thực thi việc băm (hay vòng cuối của việc tính toán băm). Việc nhập chữ ký số là trống trong thao tác COMPUTE DIGITAL SIGNATURE, khi tất cả dữ liệu nhập nằm trên thẻ.

Bảng A.6 - Ví dụ thứ năm của lược đồ chữ ký số có phụ lục

Lệnh	Thao tác	P1-P2	Trường dữ liệu lệnh	Trường dữ liệu hồi đáp
MSE	RESTORE	'F3' - '01'	-	-
PSO	HASH	'90' - '80'	Dữ liệu để băm	-
PSO	COMPUTE DIGITAL SIGNATURE	'9E' - '9A'	-	Chữ ký số

A.3 Chuỗi lệnh của việc xác minh chữ ký số

Trong bảng A.7, một danh sách tiêu đề mở rộng quy định cấu trúc của một chứng nhận không tự mô tả (xem Phụ lục B): đầu vào chữ ký số bao gồm các phần tử dữ liệu. Thao tác VERIFY CERTIFICATE sử dụng xâu chuỗi lệnh.

Bảng A.7 - Ví dụ đầu tiên của việc xác minh chữ ký số

Lệnh	Thao tác	P1-P2	Trường dữ liệu lệnh
MSE	SET DST	'41' - 'B6'	{'4D' - L - {'42' - L - '5F20' - L - '5F49' - L}} - {'83' - L - Tham chiếu khóa}
PSO	VERIFY CERTIFICATE (CLA='1X')	'00' - 'AE'	{'5F4E' - L - Nội dung chứng nhận}
PSO	VERIFY CERTIFICATE (CLA='0X')	'00' - 'AE'	{'5F37' - L - Chữ ký số của chứng nhận}
PSO	HASH	'90' - '80'	Nhập băm
PSO	VERIFY DIGITAL SIGNATURE	'00' - 'AB'	{'9E' - L - Chữ ký số}

- Bước đầu tiên: đối tượng dữ liệu chứng nhận được trình bày (kết hợp các phần tử dữ liệu): mã định danh bên cung cấp (thẻ '42'), tên chủ thẻ (thẻ '5F20') và khóa công khai chủ thẻ (thẻ '5F49'). Thẻ thực hiện việc băm sử dụng nội dung chứng nhận như đầu vào băm.
- Bước thứ hai: chữ ký số phụ thuộc vào chứng nhận được tái biến hình và kết quả được so sánh với hàm băm tạo ra trước đó. Sau đó thì thao tác HASH được thực hiện. Đối với việc xác minh chữ ký số, khóa công khai được nhận và được xác thực bởi thao tác VERIFY CERTIFICATE trước đó. Đầu vào băm là độc lập với thuật toán băm, cả với giá trị thường, có thể được thể hiện theo các lệnh xâu chuỗi hoặc hàm băm tiền xử lý nếu thẻ chỉ thực hiện vòng cuối của việc tính toán băm.
- Bước cuối cùng: Thao tác VERIFY DIGITA SIGNATURE được thực hiện.

Bảng A.8 trình bày việc xác minh một chứng nhận tự mô tả (xem Phụ lục B): đầu vào chữ ký số bao gồm các đối tượng dữ liệu. Thao tác VERIFY CERTIFICATE sử dụng xâu chuỗi lệnh. Trong bước đầu tiên, đối tượng dữ liệu tương tác với chứng nhận được thể hiện (ví dụ: kết hợp các đối

tượng dữ liệu: tham chiếu thẩm quyền chứng nhận, tên chủ thẻ và khóa phổ thông chủ thẻ). Thẻ sử dụng kết hợp này như đầu vào băm. Các bước sau được chỉ định với ví dụ bên trên.

Bảng A.8 - Ví dụ thứ hai của việc xác minh chữ ký số

Lệnh	Thao tác	P1-P2	Trường dữ liệu lệnh
MSE	SET DST	'41' - 'B6'	{'83' - L - Tham chiếu khóa}
PSO	VERIFY CERTIFICATE (CLA='1X')	'00' - 'BE'	{'42' - L - Số định danh bên phát hành} - {'5F20' - L - Tên chủ thẻ} - {'5F49' - L - Khóa công khai chủ thẻ}
PSO	VERIFY CERTIFICATE (CLA='0X')	'00' - 'AE'	{'5F37' - L - Chữ ký số của chứng nhận}
PSO	HASH	'90' - '80'	Nhập băm
PSO	VERIFY DIGITAL SIGNATURE	'00' - 'AB'	{'9E' - L - Chữ ký số}

Bảng A.9 trình bày việc dùng một khóa công khai trước khi cài đặt trên thẻ.

Bảng A.9 - Ví dụ thứ ba của việc xác minh chữ ký số

Lệnh	Thao tác	P1-P2	Trường dữ liệu lệnh
MSE	SET DST	'41' - 'B6'	{'83' - L - Tham chiếu khóa}
PSO	HASH	'90' - 'A8'	Nhập băm
PSO	VERIFY DIGITAL SIGNATURE	'00' - 'AB'	{'9E' - L - Chữ ký số}

Phụ lục B

(tham khảo)

Ví dụ về chứng nhận được biên dịch bởi thẻ

B.1 Đối tượng dữ liệu của chứng nhận thẻ xác minh được

Bảng B.1 trình bày các đối tượng dữ liệu liên quan của chứng nhận thẻ xác minh được.

Bảng B.1 - Ví dụ đối tượng dữ liệu liên ngành liên quan tới chứng nhận thẻ xác minh được

Thẻ	Phần tử dữ liệu
'42'	Số định danh bên phát hành
'5F20'	Tên chủ thẻ
'5F37'	Thẩm quyền nội bộ tĩnh (chữ ký của một chứng nhận, được tạo bởi bên phát hành)
'5F49'	Khóa công khai chủ thẻ
'5F4C'	Thẩm quyền người giữ chứng nhận
'5F4E'	Nội dung chứng nhận
'7F21'	Chứng nhận chủ thẻ

Bên phát hành có thể quy định các đối tượng dữ liệu sau, như: số se-ri chứng nhận, số phiên bản, ngày hết hạn,..v..v.

Hai cấu trúc khác nhau của chứng nhận thẻ xác minh được được phân biệt:

- Một chứng nhận thẻ xác minh được tự mô tả bao gồm một kết hợp của nhiều đối tượng dữ liệu BER-TLV;
- Một chứng nhận thẻ có thẻ xác nhận không tự mô tả bao gồm một kết hợp của nhiều phần tử dữ liệu.

B.2 Chứng nhận thẻ xác minh được tự mô tả

Đối với chữ ký của một chứng nhận, một lược đồ chữ ký số có hay không có phục hồi thông điệp có thể được sử dụng. Bảng B.2 trình bày ví dụ của một chứng nhận thẻ xác minh được tự mô tả với một lược đồ chữ ký số có phục hồi thông điệp.

Bảng B.2 - (Ví dụ) Chứng nhận thẻ xác minh được tự mô tả của một chủ thẻ

'7F21'	Độ dài	Giá trị của đối tượng dữ liệu độc quyền	
		{'42' - L - Số định danh bên phát hành} - {'5F20' - L - Tên chủ thẻ} - {'5F49' - L - Khóa công khai chủ thẻ}	{'5F37' - L - Chữ ký số}
Thẻ chứng nhận (được xây dựng)	Độ dài của chứng nhận	Giá trị của chứng nhận bao gồm các đối tượng dữ liệu tương tác với chữ ký số (xem xét chỉ trong việc thiếu phục hồi thông điệp)	Đối tượng dữ liệu được ấn định: {'42' - L - Số định danh bên phát hành} {'5F20' - L - Tên chủ thẻ} {'5F49' - L - Khóa công khai chủ thẻ}

CHÚ THÍCH 1 Dữ liệu định danh của thẩm quyền chứng nhận có thể tham chiếu khóa công khai.

CHÚ THÍCH 2 Dữ liệu định danh của chủ thẻ có thể dùng cho việc kiểm soát quyền truy cập dữ liệu được lưu trữ trên thẻ.

CHÚ THÍCH 3 Khóa công khai của chủ thẻ có thể được dùng trong thao tác VERIFY DIGITAL SIGNATURE phụ.

B.3 Chứng nhận thẻ xác minh không tự mô tả

Một đối tượng dữ liệu danh sách tiêu đề mở rộng có thể được thể hiện trong thẻ nhằm xác thực loại chứng nhận; mặt khác, nó cần được bảo vệ khi phân phối tới thẻ. Một đối tượng dữ liệu danh sách tiêu đề mở rộng (thẻ '4D', Xem TCVN 11167-4 (ISO/IEC 7816-4)) mô tả kết hợp các phần tử dữ liệu theo cặp thẻ/độ dài trong cùng trình tự như trong chữ ký số.

Bảng B.3 - (Ví dụ) Chứng nhận thẻ xác minh được không tự mô tả của một chủ thẻ

'7F21'	Độ dài	Giá trị của đối tượng dữ liệu độc quyền		
		{'4D' - L - {42' - L - {'5F20' - L - {'5F49' - L}}	{'5F4E' - L - Số định danh bên phát hành - Tên chủ thẻ – Khóa công khai chủ thẻ}	{'5F37' - L - Chữ ký số}
Thẻ chứng nhận (được xây dựng)	Độ dài chứng nhận	Danh sách tiêu đề mở rộng (chỉ thể hiện nếu cấu trúc chứng nhận không được biết tới)	Đối tượng dữ liệu nội dung chứng nhận liên kết chữ ký (chỉ thể hiện nếu thiếu phục hồi thông điệp, bao gồm các phần tử dữ liệu phụ thuộc danh sách tiêu đề mở rộng)	Các phần tử dữ liệu được chỉ định: - Số định danh bên phát hành - Tên chủ thẻ - Khóa công khai chủ thẻ

Phụ lục C

(tham khảo)

Ví dụ về xuất/nhập khóa không đối xứng

C.1 Sử dụng lệnh GET DATA đối với xuất khóa công khai

Giả định rằng các đối tượng dữ liệu mô tả một khóa công khai (PK) được trình bày trong thẻ, mã hóa theo dạng được trình bày trong Bảng C.1

Bảng C.1 - Mã hóa các đối tượng dữ liệu PK trên thẻ

'AB'	L	Cặp T-L chỉ ra một khuôn mẫu đối với xác minh chữ ký số				
		'B6'	L	DST		
				'83'	L	Tham chiếu khóa với PK.CH.DS
		'7F49'	L	Đối tượng dữ liệu khóa công khai		
				'81'	L	Các mô-đun
				'82'	L	Mũ công khai
		'9E'	L	Chữ ký số (tất cả các byte của khuôn mẫu xác minh chữ ký số trước thẻ '9E' được chỉ định		

Với lệnh MSE, PK đã nhận được chọn lựa. Sau đó lệnh GET DATA (INS lẻ, P1-P2='3FFF') được dùng trong 3 bước, do đó các trường dữ liệu được trình bày trong các Bảng từ C.2 đến C.7 diễn ra trên giao diện thẻ.

Bảng C.2 - Trường dữ liệu của lệnh GET DATA, bước 1 (3 bước)

'4D'	'0B'	Danh sách tiêu đề mở rộng						
		'AB'	09	Cặp T-L chỉ ra một mẫu đối với xác minh chữ ký số				
				'B2'	02	Cặp T-L chỉ ra một dối tượng dữ liệu DST		
						'83'	00	Cặp T-L chỉ ra một tham chiếu khóa công khai
		'7F49'	02	Cặp T-L chỉ ra đối tượng dữ liệu khóa công khai				
				'81'	00	Cặp T-L chỉ ra các mô-đun		

Bảng C.3 - Trường dữ liệu của hồi đáp GET DATA, bước 1 (3 bước)

'AB'	L					
	'B6'	L	DST			
			'83'	L	Tham chiếu khóa PK.CH.DS	
	'7F49'	L	khóa công khai			
			'81'	L	Các mô-đun	

Bảng C.4 - Trường dữ liệu của lệnh GET DATA, bước 2 (3 bước)

'4D'	07	Danh sách tiêu đề mở rộng					
	'AB'	07	Cặp T-L chỉ ra một mẫu xác thực chữ ký số				
			'7F49'	02	Cặp T-L chỉ ra đối tượng dữ liệu khóa công khai		
				'82'	00	Cặp T-L chỉ ra các mô-đun	

Bảng C.5 - Trường dữ liệu của hồi đáp GET DATA, bước 2 (3 bước)

'AB'	L				
	'7F49'	L	Khóa công khai		
			'82'	L	Mũ công khai

Bảng C.6 - Trường dữ liệu của lệnh GET DATA, bước 3 (3 bước)

'4D'	04	Danh sách tiêu đề mở rộng			
	'AB'	02	Cặp T-L chỉ ra một mẫu xác thực chữ ký số		
			'9E'	00	Cặp T-L chỉ ra đối tượng dữ liệu chữ ký số

Bảng C.7 - Trường dữ liệu của hồi đáp GET DATA, bước 3 (3 bước)

'AB'	L		
	'9E'	L	Chữ ký số

C.2 Sử dụng lệnh PUT DATA đối với nhập khóa riêng

Trước tiên, một lệnh MSE phải được gửi tới tham chiếu khóa riêng tương ứng (ví dụ: tham chiếu khóa được biết trên thẻ). Sau đó lệnh PUT DATA (IND lẻ, P1-P2= '3FFF') được dùng với trường dữ liệu lệnh được trình bày trong Bảng C.9.

Bảng C.8 - Danh sách tiêu đề mở rộng mô tả đối tượng khóa riêng

'4D'	L	Danh sách tiêu đề mở rộng					
		'AB'	L	Cặp T-L chỉ ra một mẫu xác thực chữ kí số			
			'B6'	L	Cặp T-L chỉ ra một DST		
					'84'	L	Cặp T-L chỉ ra một tham chiếu khóa cho SK.CH.DS
			'7F48'	L	Cặp T-L chỉ ra một đối tượng dữ liệu khóa riêng		
					'92'	L	Cặp T-L đối với tham số p
					'93'	L	Cặp T-L đối với tham số q
					'94'	L	Cặp T-L đối với tham số 1/q x p
					'95'	L	Cặp T-L đối với tham số d x (p-1)
					'96'	L	Cặp T-L đối với tham số d x (q-1)
				'9E'	L	Cặp T-L chỉ ra một chữ ký số	

Bảng C.9 - Trường dữ liệu của lệnh PUT DATA

'4D'	L	Danh sách tiêu đề mở rộng					
		'AB'	L	Cặp T-L chỉ ra một mẫu xác minh chữ ký số			
			'B6'	L	Cặp T-L chỉ ra một DST		
					'84'	L	Cặp T-L chỉ ra một tham chiếu khóa cho SK.CH.DS
			'7F48'	L	Cặp T-L chỉ ra một đối tượng dữ liệu khóa riêng		
					'92'	L	Cặp T-L đối với tham số p
					'93'	L	Cặp T-L đối với tham số q
					'94'	L	Cặp T-L đối với tham số 1/q x p
					'95'	L	Cặp T-L đối với tham số d x (p-1)
					'96'	L	Cặp T-L đối với tham số d x (q-1)
				'9E'	L	Cặp T-L chỉ ra một chữ ký số	
'5F48'	L	Kết hợp các phần tử tham số khóa phụ thuộc danh sách tiêu đề mở rộng. Các phần tử dữ liệu tương ứng với thẻ bộ lọc '00' trong danh sách tiêu đề mở rộng được đọc ra nhưng bị bỏ qua.					
'9E'	L	Chữ ký số					

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 9796 Information technology - Security techniques - Digital signature scheme giving message recovery (tất cả các phần).

[3] ISO/IEC 9798-5:1999[12] Information technology - Security techniques - Entity authentication - Part 5: Mechanisms using zero knowledge techniques.

[4] ISO/IEC 10536 Identification cards - Contactless integrated circuits cards - Close coupled cards (tất cả các phần).

[5] ISO/IEC 14443 Identification cards - Contactless integrated circuits cards - Proximity cards (tất cả các phần).

[6] ISO/IEC 15693 Identification cards - Contactless integrated circuits cards - Vicinity cards (tất cả các phần).

1 Đã phát hành