TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 11198-1: 2015

Xuất bản lần 1

THẺ MẠCH TÍCH HỢP EMV CHO HỆ THỐNG THANH TOÁN – ĐẶC TẢ ỨNG DỤNG THANH TOÁN CHUNG – PHẦN 1: TỔNG QUÁT

EMV Integrated Circuit Card for Payment Systems – Common payment application specification Part 1: General

HÀ NỘI – 2015

Mục lục **Trang**

Lời nói đầu 5

Lời giới thiệu 6

1 Phạm vi áp dụng 11

2 Tài liệu viện dẫn 12

3 Thuật ngữ và định nghĩa 12

4 Thuật ngữ viết tắt, ký hiệu, quy ước và biểu tượng 28

4.1 Thuật ngữ viết tắt 28

4.2 Ký hiệu 32

4.3 Quy ước định dạng phần tử dữ liệu 33

4.4 Biểu tượng 34

5 Giải thích thuật ngữ 36

6 Các quy trình xử lý chức năng 37

Thư mục tài liệu tham khảo 38

·i nói đầu

VN 11198-1:2015 được xây dựng trên cơ sở tham khảo EMV CPA ɔmmon Payment Application Specification) Version 1.0, 2005.

VN 11198-1:2015 do Ban Kỹ thuật tiêu chuẩn quốc gia :VN/JTC1/SC 17 *Thẻ nhận dạng* biên soạn, Tổng cục Tiêu chuẩn lường Chất lượng đề nghị,Bộ Khoa học và Công nghệ công bố.

tiêu chuẩn TCVN 11198 *Thẻ mạch tích hợp EMV cho hệ thống ɜnh toán – Đặc tả ứng dụng thanh toán chung* gồm các tiêu chuẩn ɔ:

TCVN 11198-1:2015, Phần 1: Tổng quát;

TCVN 11198-2:2015, Phần 2: Giới thiệu về quy trình xử lý;

TCVN 11198-3:2015, Phần 3: Quy trình xử lý chức năng;

TCVN 11198-4:2015, Phần 4: Phân tích hành động thẻ;

TCVN 11198-5:2015, Phần 5: Quy trình xử lý tập lệnh bên phát hành đến thẻ;

TCVN 11198-6:2015, Phần 6: Quản lý khóa và an ninh;

TCVN 11198-7:2015, Phần 7: Mô tả về chức năng;

TCVN 11198-8:2015, Phần 8: Thư mục phần tử dữ liệu;

Lời giới thiệu

Bộ tiêu chuẩn TCVN 11198 này được phân chia tương ứng với các quy định trong EMV CPA như sau và phân vào các tiêu chuẩn:

TCVN 11198-1 bao gồm các điều sau:

- **Điều 1** (Điều 1, EMV CPA), **Phạm vi**
- **Điều 2** (Điều 2, EMV CPA), **Tài liệu viện dẫn** – Danh sách các tiêu chuẩn và tài liệu đặc tả được viện dẫn trong tiêu chuẩn này.
- **Điều 3** (Điều 3, EMV CPA), **Định nghĩa** – Cung cấp một bộ thuật ngữ được sử dụng trong tiêu chuẩn này.
- **Điều 4** (Điều 4, EMV CPA), **Từ viết tắt, ký hiệu, quy ước, thuật ngữ, và biểu tượng** – Danh sách các từ viết tắt và mô tả cho từng phần được sử dụng trong tiêu chuẩn này.

TCVN 11198-2 bao gồm các điều sau:

- **Điều 5** (Điều 5, EMV CPA), **Tổng quan** – Điều này cung cấp một cách tổng quát về từng chức năng trong quy trình giao dịch;

  Tổng quan Quy trình được cấu trúc thành các quy trình chức năng được mô tả trong EMV như các điều nhỏ sau:

  - Điều 5.1, Bộ thực thi – các tùy chọn – chức năng nhận diện là tùy chọn cho bên cung cấp ứng dụng để thực thi;
  - Điều 5.2, Tổng quan chức năng
    - Mô tả chung – Cung cấp một cách tổng quan mức cao về chức năng trong quy trình giao dịch;
    - Điều kiện thực hiện – Định nghĩa các điều kiện theo đó quy trình được thực hiện;
  - Điều 5.3, Luồng giao dịch mẫu – Minh họa một luồng mẫu về việc giao dịch CPA tại thiết bị đầu cuối tương thích EMV;
  - Điều 5.4, Chức năng tối thiểu – Cung cấp một cách tổng quan mức cao về các chức năng là bắt buộc đối với tất cả các triển khai thẻ phải hỗ trợ;
- **Điều 6** (Điều 6, EMV CPA), **Thông tin chung về Lệnh** – Cung cấp các yêu cầu chung về các lệnh xử lý trong một giao dịch EMV. Các quy trình xử lý lệnh chung bao gồm máy trạng thái ứng dụng, kiểm tra lệnh và xử lý ngoại lệ.

TCVN 11198-3 bao gồm các điều sau

- **Điều 5** (Điều 7, EMV CPA), **Lựa chọn ứng dụng** – Chức năng này xác định các ứng dụng, được hỗ trợ bởi cả thẻ và thiết bị đầu cuối, được sử dụng để tiến hành xây dựng cuộc giao dịch.
- **Điều 6** (Điều 8, EMV CPA), **Quy trình Khởi tạo ứng dụng** – Trong khi thực hiện chức năng này, thẻ thu nhận bất kỳ dữ liệu thiết bị đầu cuối nào mà thẻ được yêu cầu trong Lựa chọn Ứng dụng và gửi cho thiết bị đầu cuối đó một danh sách dữ liệu có thể đọc và các chức năng cần hỗ trợ cho cuộc giao dịch.

- **Điều 7** (Điều 9, EMV CPA), **Đọc Dữ liệu Ứng dụng** – Trong khi thực hiện chức năng này, thiết bị đầu cuối đọc các bản ghi dữ liệu thẻ cần thiết cho cuộc giao dịch.
- **Điều 8** (Điều 10, EMV CPA), **Xác thực Dữ liệu Ngoại tuyến** – Trong khi thực hiện chức năng này, thiết bị đầu cuối thực hiện xác thực dữ liệu có trong thẻ bằng cách sử dụng công nghệ khóa công khai RSA;
- **Điều 9** (Điều 11, EMV CPA), **Ràng buộc quy trình xử lý** – Trong khi thực hiện chức năng này, kiểm tra phiên bản ứng dụng, kiểm tra ngày hiệu lực và ngày hết hạn, và các kiểm tra khác được thực hiện bởi thiết bị đầu cuối;
- **Điều 10** (Điều 12, EMV CPA), **Xác minh Chủ thẻ** - Trong khi thực hiện chức năng này, thiết bị đầu cuối xác định phương thức xác minh chủ thẻ CVM được sử dụng và thực hiện việc CVM đã chọn.
- **Điều 11** (Điều 13, EMV CPA), **Quản lý Rủi ro Thiết bị đầu cuối** – Trong khi thực hiện chức năng này, thiết bị đầu cuối đảm bảo rằng các giao dịch giá trị lớn được gửi trực tuyến và như thế các giao dịch mức chip được tiến hành trực tuyến định kỳ.
- **Điều 12** (Điều 14, EMV CPA), **Phân tích Hành động Thiết bị đầu cuối** – Trong khi thực hiện chức năng này, thiết bị đầu cuối áp dụng các quy tắc thiết lập bởi bên phát hành thẻ và bởi bên cung ứng thiết bị đầu cuối đối với quy trình xử lý ngoại tuyến. Việc phân tích này xác định khi nào việc giao dịch phải tiến hành ngoại tuyến, ràng buộc ngoại tuyến, và gửi trực tuyến cho bên được ủy quyền;

TCVN 11198-4 bao gồm các điều sau:

- **Điều 5** (Điều 15, EMV CPA), **Phân tích Hành động Thẻ lần đầu** – Trong khi thực hiện chức năng này, tiến hành kiểm tra tần suất giao dịch và các quản lý rủi ro khác, được thực hiện trong nội tại của thẻ. Ứng dụng sau đó xác định khi nào gửi giao dịch trực tuyến cho bên được ủy quyền hoặc chấp thuận hoặc từ chối giao dịch ngoại tuyến, và sinh ra mã hồi đáp;
- **Điều 6** (Điều 16, EMV CPA), **Quy trình xử lý Trực tuyến** – Trong khi thực hiện chức năng này, máy chủ của bên phát hành (hoặc một đại diện bên phát hành) soát xét và xác thực hoặc từ chối giao dịch bằng cách sử dụng các tham số rủi ro trên máy chủ của bên phát hành;
- **Điều 7** (Điều 17, EMV CPA), **Phân tích Hành động Thẻ lần hai** – Trong khi thực hiện chức năng này,thực hiện các quản lý rủi ro thẻ bổ sung, và thẻ xử lý các kết quả của lần thử gửi giao dịch trực tuyến. Ứng dụng sau đó sinh ra mã hồi đáp lần hai;

TCVN 11198-5 bao gồm các điều sau:

- **Điều 5** (Điều 18, EMV CPA), **Quy trình xử lý Tập lệnh từ bên Phát hành đến Thẻ** - Trong khi thực hiện chức năng này, thẻ áp dụng các thay đổi so với lần phát hành trước được gửi từ bên phát hành;

TCVN 11198-6 bao gồm các điều sau

- **Điều 5** (Điều 19, EMV CPA), **Các chức năng bổ sung** – Mô tả các mở rộng tùy chọn cho ứng dụng, bao gồm các ví dụ về cách thức để hỗ trợ bộ đếm bổ sung hoặc kết hợp các chức năng bổ sung bằng cách sử dụng các bit do bên phát hành quy định trong các phần tử dữ liệu ứng dụng.

- **Điều 6** (Điều 20, EMV CPA), **Quản lý an ninh và khóa** - Cung cấp các yêu cầu liên quan đến quản lý khóa và an ninh cho việc triển khai CPA trong đó bổ sung các đặc tả về ứng dụng tương thích CCD, như đã mô tả tại EMV 4.1;
- **Điều 7** (Điều 21, EMV CPA), **Cá thể hóa** – Mô tả các yêu cầu cá thể hóa đối với việc triển khai CPA.

TCVN 11198-7 bao gồm các điều sau

- **Điều 5** (Phụ lục A, EMV CPA), **Quy trình xử lý Tệp tin Lựa chọn Hồ sơ** – Mô tả cách thức mà Tệp tin Lựa chọn Hồ sơ có thể được sử dụng trong khi Khởi động Ứng dụng để tùy chỉnh hành động ứng dụng dựa trên các đặc điểm của giao dịch như đã quy định bởi bên phát hành tại thời điểm cá thể hóa. Bao gồm một ví dụ minh họa cách thức phần tử dữ liệu có thể được cá thể hóa để cung cấp chức năng này.
- **Điều 6** (Phụ lục B, EMV CPA), **Chức năng Bảng kiểm tra bổ sung** - Mô tả cách thức mà các Bảng Kiểm tra Bổ sung có thể được sử dụng trong khi tiến hành Phân tích hành động thẻ để cung cấp một cách kiểm thử quản lý rủi ro thẻ từ đó có thể được tùy chỉnh bởi bên phát hành tại thời điểm cá thể hóa. Bao gồm một ví dụ minh họa cách thức mà phần tử dữ liệu có thể được cá thể hóa để cung cấp chức năng này.
- **Điều 7** (Phụ lục C, EMV CPA), **Chức năng Quy đổi Tiền tệ** - Mô tả cách thức mà Bảng Quy đổi Tiền tệ có thể được sử dụng để ước lượng giá trị đồng tiền nội tệ cho giao dịch tiền ngoại tệ bằng cách sử dụng các Tham số Quy đổi Tiền tệ được quy định bởi bên phát hành tại thời điểm cá thể hóa. Bao gồm một ví dụ minh họa cách thức phần tử dữ liệu có thể được cá thể hóa để cung cấp chức năng này.
- **Điều 8** (Phụ lục D, EMV CPA), **Ghi Log Giao dịch** – Mô tả cách thức mà thẻ có thể được cấu hình để hỗ trợ việc ghi chép giao dịch linh hoạt được quy định tại thời điểm cá thể hóa. Bao gồm một ví dụ minh họa cách thức phần tử dữ liệu có thể được cá thể hóa để cung cấp chức năng này.
- **Điều 9** (Phụ lục E, EMV CPA), **Quản lý Ngày tháng theo Ngày** – Mô tả cách thức mà ngày tháng theo định dạng YYMMDD có thể được chuyển đổi để tính số ngày từ ngày tham chiếu, sao cho ứng dụng có thể thực hiện quản lý rủi ro thẻ dựa trên số lượng ngày đã trôi qua;
- **Điều 10** (Phụ lục F, EMV CPA), **Bộ đếm An ninh** – Mô tả một việc thực thi cho bộ đếm an ninh đối với CPA nếu bộ đếm an ninh được mô tả tại Điều 20 được thực hiện trong ứng dụng.
- **Điều 11** (Phụ lục G, EMV CPA), **Quản lý Dữ liệu Hồ sơ** – Mô tả việc quản lý dữ liệu nguồn tài nguyên ứng dụng cho các lệnh PUT DATA và GET DATA sử dụng thẻ tag bản mẫu đơn cho từng kiểu tài nguyên.
- **Điều 12** (Phụ lục H, EMV CPA), **Đặc tả Tùy chọn Hồ sơ bên Phát hành và quy trình xử lý** – Mô tả cách thức mà ứng dụng tiến hành xử lý các tùy chọn Hồ sơ được quy định bởi bên phát hành và cấu hình hành động thẻ dựa theo các tùy chọn đó;
- **Điều 13** (Phụ lục I, EMV CPA), **Hiểu rõ Thanh tổng Chu kỳ**–Giải thích các hành động và quản lý Thanh tổng Chu kỳ bên trong ứng dụng.

TCVN 11198-8 bao gồm các điều sau

- **Điều 5** (Phụ lục J, EMV CPA), **các Phần tử Dữ liệu GET DATA và PUT DATA** – Liệt kê các phần tử dữ liệu hỗ trợ cho các lệnh GET DATA và PUT DATA;
- **Điều 6** (Phụ lục K, EMV CPA), **các thẻ Tag Phần tử Dữ liệu** - Liệt kê các thẻ phần tử dữ liệu và các thẻ khuôn mẫu được sử dụng trong ứng dụng và thiết bị đầu cuối;
- **Điều 7** (Phụ lục L, EMV CPA), **Từ điển Dữ liệu** - Xác định các phần tử dữ liệu được sử dụng trong quy trình xử lý ứng dụng từ thẻ và quan điểm của bên phát hành.

Thẻ mạch tích hợp EMV cho Hệ thống Thanh toán - Đặc tả ứng dụng thanh toán chung - Phần 1: Tổng quát

EMV Integrated Circuit Card for Payment Systems – Common payment application specification – Part 1: General

1 Phạm vi áp dụng

Bộ TCVN 11198 cung cấp các đặc tả kỹ thuật về phần Ứng dụng Thanh toán Chung (CPA), định nghĩa các phần tử dữ liệu và các chức năng cho ứng dụng tương thích với Định nghĩa Lõi Chung (CCD) EMV. Tiêu chuẩn này hướng đến các chức năng được thực hiện bởi thẻ mạch tích hợp (ICC) và việc tương tác giữa ICC và thiết bị đầu cuối tại điểm giao dịch.

Mục đích của bộ tiêu chuẩn này là:

- Mô tả chức năng của việc thực thi phù hợp với CCD của EMV để giảm bớt sự ảnh hưởng của bên cung cấp phát triển;
- Quy định về tập các chức năng lõi mà các bên phát hành có thể dựa vào những thứ có sẵn trong mọi thực thi CPA;
- Quy định việc thực thi có thể cá thể hóa với cùng các phần tử dữ liệu để đạt được các yêu cầu kinh doanh trong nhiều hệ thống thanh toán.

Bởi vì CPA dựa trên EMV và CCD, do đó các đặc tả kỹ thuật nên được sử dụng cùng nhau cho các mục đích tham khảo và phát triển.

Bộ TCVN 11198 được xây dựng dựa trên các tiêu chuẩn EMV và nên được sử dụng kết hợp với các tiêu chuẩn đó. Tuy nhiên, nếu có bất kỳ điều khoản hoặc định nghĩa nào trong bộ TCVN 11198 khác với trong các tiêu chuẩn đó thì các điều khoản tại đây phải được ưu tiên hơn

Bộ TCVN 11198 được dành cho việc sử dụng bởi các bên phát triển ứng dụng ICC, các nhà sản xuất ICC, các nhà thiết kế hệ thống trong các hệ thống thanh toán, và các chuyên viên tổ chức tài chính chịu trách nhiệm về việc thực thi các ứng dụng tài chính trong các ICC.

2 Tài liệu viện dẫn

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

EMV Book 3, EMV Integrated Circuit Card Specifications for Payment Systems, version 4.1, Book 3, Application Specification, May 2004. (*EMV Quyển 3*).

EMV Book 4, EMV Integrated Circuit Card Specifications for Payment Systems, version 4.1, Book 4, Cardholder, Attendant, and Acquirer Interface Requirements, May 2004. (*EMV Quyển 4*).

3 Thuật ngữ và định nghĩa

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

3.1

bên chấp nhận thẻ (Acquirer)

Thành viên Hệ thống Thanh toán mà có quan hệ hợp đồng với bên bán hàng hoặc thực hiện xuất tiền cho chủ thẻ trong một hệ thống rút tiền mặt, và trực tiếp hoặc gián tiếp tham gia giao dịch trong quá trình trao đổi.

3.2

ứng dụng (Application)

Một chương trình và dữ liệu có liên quan mà tại đó hiện có một chip mạch tích hợp và đáp ứng một chức năng nghiệp vụ. Ví dụ ứng dụng bao gồm việc thanh toán, giá trị lưu giữ và độ trung thực.

3.3

mã lệnh xác thực ứng dụng (Application Authentication Cryptogram)

AAC

Một mã ứng dụng được sinh ra bởi thẻ khi từ chối giao dịch trực tuyến và ngoại tuyến.

3.4

khóa ứng dụng (Application Block)

Chỉ lệnh gửi đến thẻ bởi bên phát hành, để tắt ứng dụng đã chọn trên thẻ để ngăn chặn việc tiếp tục sử dụng ứng dụng. Quy trình này không ngăn cản việc sử dụng các ứng dụng khác trên thẻ. Một ứng dụng bị chặn có thể được mở lại bởi bên phát hành.

3.5

mã lệnh ứng dụng (Application Cryptogram)

Một mã lệnh được sinh ra bởi thẻ để đáp ứng một lệnh GENERATE AC. Có ba loại mã lệnh ứng dụng bao gồm:

- Mã lệnh xác thực ứng dụng AAC;

- Mã lệnh yêu cầu chuẩn chi ARQC;
- Chứng chỉ giao dịch TC;

3.6

kỹ thuật mã hóa bất đối xứng (Asymmetric Cryptographic Technique)

Một kỹ thuật mã hóa được sử dụng hai phép biến đổi có liên quan là: một biến đổi công khai (được xác định bởi khóa công khai) và một biến đổi riêng (được xác định bởi khóa riêng). Hai phép biến đổi này có thể có tính chất là với phép biến đổi công khai đã biết thì không thể tính toán ra được phép biến đổi riêng.

3.7

ATM

Một thiết bị đầu cuối không cần giám sát, có khả năng chạy bằng điện, chấp nhận mã PIN và chi trả tiền tệ hoặc séc.

3.8

xác thực (Authentication)

Một quy trình mã hóa để xác minh tính hợp lệ về nguồn gốc đang có của dữ liệu hoặc định danh của một thực thể.

3.9

chuẩn chi (Authorisation)

Một quy trình tại đó một bên phát hành hoặc bên đại diện của bên phát hành phê duyệt một giao dịch.

3.10

yêu cầu chuẩn chi (Authorisation Request)

Một yêu cầu của bên chấp nhận thẻ hoặc bên bán hàng về việc chuẩn chi cho một giao dịch.

3.11

mã lệnh yêu cầu chuẩn chi (Authorisation Request Cryptogram)

ARQC

Một mã ứng dụng được sinh ra bởi thẻ khi yêu cầu chuẩn chi trực tuyến cho một giao dịch. Mã này được gửi cho bên phát hành bên trong một yêu cầu chuẩn chi. Bên phát hành có thể xác minh mã ARQC trong khi thực hiện chức năng Quy trình xử lý Trực tuyến để đảm bảo rằng thẻ được chuẩn chi.

3.12

hồi đáp chuẩn chi (Authorisation Response)

Trả lời của bên phát hành đối với yêu cầu chuẩn chi.

3.12

Mã lệnh hồi đáp chuẩn chi (Authorisation Response Cryptogram)

ARPC

Một mã lệnh được sinh ra bởi bên phát hành và có thể được gửi đến thẻ trong một hồi đáp chuẩn chi. Mã lệnh này là kết quả của mã yêu cầu chuẩn chi ARQC và mã Cập nhật Trạng thái Thẻ được mã hóa với một khóa phiên. Mã ARPC này được xác minh hợp lệ bởi thẻ trong khi Xác thực bên phát hành để đảm bảo rằng hồi đáp đến từ bên phát hành hợp lệ.

3.13

byte

dữ liệu 8 bit.

3.14

thẻ (card)

Một thẻ thanh toán được xác định bởi một hệ thống thanh toán.

3.15

khóa thẻ (Card Block)

Chỉ lệnh được gửi đến thẻ bởi bên phát hành để tắt tất cả các ứng dụng hợp lệ hay không hợp lệ có trên thẻ nhằm ngăn chặn việc tiếp tục sử dụng thẻ.

Một thẻ khi bị khóa thì không thể được mở lại.

3.16

chủ thẻ (Cardholder)

Một cá nhân sở hữu một thẻ đã phát hành hoặc là người được chuẩn chi sử dụng thẻ.

3.17

xác nhận của chủ thẻ (Cardholder Confirmation)

Việc xác nhận bởi chủ thẻ khi ứng dụng đã chọn bởi thiết bị đầu cuối đang được sử dụng trong quá trình xử lý giao dịch.

3.18

lựa chọn của chủ thẻ (Cardholder Selection)

Quy trình tại đó một chủ thẻ có thể lựa chọn một trong nhiều ứng dụng cùng được hỗ trợ bởi thẻ và thiết bị đầu cuối để xử dụng trong quá trình xử lý giao dịch.

3.19

xác minh chủ thẻ (Cardholder Verification)

Quy trình xác định rằng sự hiện diện của thẻ là chủ thẻ hợp lệ.

3.20

phương thức xác minh chủ thẻ (Cardholder Verification Method)

CVM

Một phương thức được sử dụng để xác nhận định danh của một chủ thẻ.

3.21

chi trả tiền mặt (Cash Disbursement)

Tiền (bao gồm cả séc du lịch) được chi trả đến chủ thẻ đang sử dụng thẻ.

3.22

hoàn tiền (Cashback)

Tiền mặt nhận được khi thực hiện một giao dịch mua.

3.23

chứng chỉ (Certificate)

Khóa công khai và định danh của một thực thể cùng với một số thông tin khác tạo sự ký kết không thể giả mạo với khóa riêng của tổ chức chứng nhận đã phát hành chứng nhận đó.

3.24

tổ chức chứng nhận (Certification Authority)

CA

Một bên thứ ba tin cậy có thể thiết lập một bằng chứng cho biết các liên kết khóa công khai và các thông tin có liên quan khác là họ sở hữu.

3.25

bản mã hóa (Ciphertext)

Thông tin đã được mã hóa.

3.26

sinh mã lệnh ứng dụng kết hợp DDA (Combined DDA/Application Cryptogram Generation)

CDA

Một hình thức xác thực dữ liệu động ngoại tuyến kết hợp với quy trình xử lý lệnh GENERATE AC.

3.27

lệnh (command)

Một thông điệp được gửi bởi thiết bị đầu cuối đến ICC để khởi động một hành động và yêu cầu một hồi đáp từ ICC.

3.28

định nghĩa tập lõi chung (Common Core Definitions)

CCD

Một tập chung tối thiểu các tùy chọn thực thi ứng dụng thẻ, các hành động ứng dụng thẻ và các định nghĩa phần tử dữ liệu đủ để triển khai một giao dịch EMV như quy định trong *EMV Quyển 3*.

3.29

ghép nối (Concatenation)

Hai phần tử được ghép nối bằng cách thêm các byte từ phần tử thứ hai tại vị trí cuối cùng của phần tử thứ nhất. Các byte của từng phần tử được biểu diễn trong chuỗi (kiểu string) thể hiện trong cùng một chuỗi (dạng sequence) tại đó chúng được thể hiện tại thiết bị đầu cuối bởi ICC, trong đó là hầu hết các byte quan trọng đầu tiên. Bên trong từng byte, các bit được xếp thứ tự từ bit quan trọng nhất đến bit ít quan trọng nhất. Danh sách các phần tử hoặc đối tượng có thể được kết nối bằng cách kết nối cặp đầu tiên để tạo thành phần tử mới, bằng cách phần tử đầu tiên kết hợp với phần tử tiếp theo trong danh sách, tiếp tục như vậy cho đến hết.

3.30

mã lệnh (Cryptogram)

Kết quả của một hành động mã hóa.

3.31

thuật toán mã hóa (Cryptographic Algorithm)

Một thuật toán hoạt động với sự kiểm soát của khóa mã hóa và được sử dụng để bảo vệ tính bí mật và/hoặc tính toàn vẹn cảu dữ liệu đầu vào.

3.32

khóa mã hóa (Cryptographic Key)

Một chuỗi các bit được sử dụng bởi một thuật toán mã hóa.

3.33

mã hóa (Cryptography)

Nghệ thuật hoặc kỹ thuật giữ cho thông điệp bí mật và/hoặc bảo mật.

3.34

danh sách CVM (CVM List)

Danh sách được xác định bởi bên phát hành bao gồm bên trong một ứng dụng của chip đang thiết lập hệ phương thức cho việc xác minh tính xác thực của chủ thẻ.

3.35

xác thực dữ liệu (Data Authentication)

Xác minh tính hợp lệ của dữ liệu được lưu giữ trong thẻ mạch tích hợp không bị cảnh báo từ khi phát hành thẻ. Xem thêm Xác thực Dữ liệu Ngoại tuyến.

3.36

chuẩn mã hóa dữ liệu (Data Encryption Standard)

DES

Thuật toán mã hóa khóa đối xứng công khai của tổ chức Viện Tiêu chuẩn và Công nghệ quốc gia NIST.

3.37

tính toán vẹn dữ liệu (Data Integrity)

Một thuộc tính của dữ liệu mà khi đó không bị cảnh báo hoặc bị phá hủy theo một cách thức không hợp lệ.

3.38

giải mã (Decipherment)

Trái ngược với hành động mã hóa tương ứng.

3.39

khóa DES (DES key)

một tham số bí mật 64 bit của thuật toán DES, bao gồm 56 bit có thể là độc lập và ngẫu nhiên, và 8 bit xác định lỗi để tạo tương đương với từng 8 bit byte của khóa lẻ.

3.40

chữ ký số (Digital Signature)

Một biến đổi mã hóa không đối xứng của dữ liệu tại đó cho phép bên nhận dữ liệu chứng minh nguồn gốc và tính toàn vẹn của dữ liệu, và như thế bảo vệ bên gửi và bên nhận dữ liệu khỏi sự giả mạo bởi bên thứ ba, và bên gửi tránh sự giả mạo của bên nhận.

3.41

xác thực dữ liệu động (Dynamic Data Authentication)

DDA

Một hình thức xác thực dữ liệu ngoại tuyến tại đó thẻ sinh ra một chữ ký số bằng cách sử dụng các phần tử dữ liệu đặc tả giao dịch để xác minh tính hợp lệ bởi thiết bị đầu cuối nhằm ngăn chặn tấn công vớt (skimming).

3.42

đặc tả EMV (EMV Specifications)

Tài liệu đặc tả kỹ thuật được duy trì bởi tổ chức quốc tế JCB, MasterCard và Visa để tạo ra các tiêu chuẩn và đảm bảo khả năng tương tác toàn cầu về việc sử dụng công nghệ thẻ chip trong ngành công nghiệp thanh toán.

3.43

sự mã hóa (Encipherment)

Việc biến đổi khả nghịch của dữ liệu bằng một thuật toán mã hóa để tạo ra bản mã.

3.44

tuyển loại trừ (Exclusive-OR)

Phép cộng nhị phân không hoán vị tuân theo luật:

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

3.45

thẻ hết hạn (Expired Card)

Một thẻ trong đó hạn sử dụng được dập nổi, được mã hóa hoặc được in đã hết.

3.46

giao dịch tài chính (Financial Transaction)

Hành động giữa một chủ thẻ và một bên bán hàng hoặc bên chấp nhận thẻ mà kết quả là việc trao đổi hàng hóa hoặc dịch vụ cho thanh toán hoặc chi trả tiền mặt.

3.47

hạn mức sàn (Floor Limit)

Lượng tiền tệ mà Hệ thống Thanh toán đã thiết lập cho một lần giao dịch tại các kiểu bên bán hàng cụ thể, nếu cao hơn thì cần có xác thực trực tuyến.

3.48

chức năng (Function)

Một quy trình xử lý được hoàn thành bằng một hoặc nhiều lệnh và kết quả là các hành động được sử dụng để thực hiện tất cả hoặc một phần cuộc giao dịch.

3.49

môđun an ninh phần cứng (Hardware Security Module)

thiết bị an ninh

HSM

Một môđun bảo mật được sử dụng để lưu giữ các khóa mã hóa và thực hiện các hàm mã hóa.

3.50

hàm băm (Hash Function)

Một hàm ánh xạ các chuỗi (string) bit thành các chuỗi bit có chiều dài cố định, tuân theo hai thuộc tính sau:

- Không thể tính toán với đầu ra cho trước để tìm đầu vào có ánh xạ tới đầu ra này;
- Không thể tính toán với đầu vào cho trước để tìm ra đầu vào thứ hai cùng ánh xạ tới đầu ra

3.51

kết quả băm (Hash Result)

Chuỗi (string) bit là đầu ra của một hàm băm.

3.52

khóa chính ICC (ICC Master Key)

MK

Một khóa đơn nhất cho thẻ, được sử dụng để thu một khóa phiên.

3.53

mạch tích hợp (integrated circuit)

Thành phần điện tử được thiết kế để thực hiện quy trình xử lý và/hoặc chức năng nhớ.

3.54

thẻ mạch tích hợp (Integrated Circuit Card)

ICC

Một thẻ trên đó có một hoặc nhiều mạch tích hợp được ghép vào để thực hiện quy trình xử lý và chức năng nhớ.

3.55

khả năng tương tác (interoperability)

Khả năng của tất cả các thiết bị và thiết bị đầu cuối có thể chấp nhận thẻ để chấp nhận và đọc tất cả các thẻ chip mà đã được lập trình hợp lệ và hỗ trợ một trong các ứng dụng được hỗ trợ bởi thiết bị đầu cuối.

3.56

bên phát hành (issuer)

Thành viên của Hệ thống Thanh toán thực hiện phát hành thẻ.

3.57

mã hành động bên phát hành (Issuer Action Code)

IAC

Các điều lệ được cấu hình bởi bên phát hành tại đó thiết bị đầu cuối sử dụng để xác định khi nào một giao dịch phải bị từ chối ngoại tuyến, gửi trực tuyến để xác thực, hoặc từ chối nếu không có trực tuyến. EMV định nghĩa như bên dưới, ánh xạ các hành động được chọn bởi bên phát hành sẽ được thực hiện khi phân tích các phần tử dữ liệu TVR:

- IAC – Mặc định: các điều lệ xác định khi một giao dịch phải bị từ chối ngoại tuyến nếu nó không thể thực hiện trực tuyến;
- IAC – Từ chối: các điều lệ xác định khi một giao dịch phải bị từ chối ngoại tuyến;
- IAC – Trực tuyến: các điều lệ xác định khi một giao dịch phải được gửi trực tuyến để xác thực;

3.58

xác thực bên phát hành (Issuer Authentication)

Xác minh tính hợp lệ của bên phát hành bởi thẻ để đảm bảo tính toàn vẹn của hồi đáp chuẩn chi.

CHÚ THÍCH Xem thêm mã hồi đáp chuẩn chi ARPC.

3.59

khóa (key)

Một chuỗi (sequence) bit điều khiển một hành động trong biến đổi mã hóa.

3.60

ngày hết hạn khóa (key expiry date)

Ngày mà sau đó giá trị được tạo cho từng khóa riêng là không còn hợp lệ. Ví dụ: chứng chỉ bên phát hành được ký bởi khóa CA phải có thời hạn trong hoặc trước ngày Hiệu lực Khóa CA. Khóa CA có thể bị loại bỏ khỏi thiết bị đầu cuối sau khi hết hạn.

3.61

sinh khóa (key generation)

Việc tạo ra một khóa mới cho sự kiện tiếp theo sử dụng.

3.62

bàn phím số (keypad)

Một mảng bao gồm các số, lệnh, và (khi có yêu cầu) phím chức năng và/hoặc phím chữ số được sắp xếp theo một phương thức cụ thể.

3.63

thông điệp (message)

tin điện

Một chuỗi (string) byte được gửi bởi thiết bị đầu cuối đến thẻ hoặc ngược lại, không bao gồm các ký tự kiểm soát giao dịch.

CHÚ THÍCH Thuật ngữ "tin điện" hiện nay vẫn được sử dụng trong một số trường hợp cụ thể.

3.64

mã xác thực thông điệp (Message Authentication Code)

MAC

Một mã điện tử được sinh ra bởi một thuật toán mã hóa đối xứng sao cho có thể bảo vệ dữ liệu người gửi và người nhận khỏi sự giả mạo của bên thứ ba.

3.65

nibble (nibble)

Bốn bit quan trọng nhất hoặc ít quan trọng nhất của một byte dữ liệu.

3.66

chấp thuận ngoại tuyến (offline approval)

Một giao dịch được chấp thuận (được chấp nhận) tại điểm giao dịch giữa thẻ và thiết bị đầu cuối mà không có hồi đáp chuẩn chi từ bên phát hành hoặc từ một đại diện của bên phát hành.

3.67

xác thực dữ liệu ngoại tuyến (offline data authentication)

Một quy trình tại đó thẻ được xác minh hợp lệ tại điểm giao dịch bằng cách sử dụng công nghệ khóa công khái RSA để chống lại các tấn công tráo hàng (counterfeit) hoặc tấn công vớt (skimming). Bao gồm ba dạng:

- Xác thực Dữ liệu Tĩnh (SDA);
- Xác thực Dữ liệu Động (DDA);
- Sinh mã DDA/AC kết hợp (CDA);

3.68

từ chối ngoại tuyến (offline decline)

Một giao dịch bị từ chối (không được chấp nhận) tại điểm giao dịch giữa thẻ và thiết bị đầu cuối mà không có hồi đáp chuẩn chi từ bên phát hành hoặc bên đại diện của bên phát hành.

3.69

mã PIN ngoại tuyến (Offline PIN)

Giá trị mã PIN được lưu trên thẻ dùng để xác minh tính hợp lệ tại điểm giao dịch giữa thẻ và thiết bị đầu cuối.

3.70

xác minh mã PIN ngoại tuyến (Offline PIN Verification)

Quy trình tại đó mã PIN được nhập bởi chủ thẻ được so sánh với giá trị mã PIN được lưu bảo mật trên thẻ.

3.71

thiết bị đầu cuối thuần ngoại tuyến (Offline-only Terminal)

Thiết bị chấp nhận thẻ không có khả năng tiến hành gửi giao dịch trực tuyến để bên phát hành chuẩn chi.

3.72

chuẩn chi trực tuyến (online authorisation)

Một phương thức yêu cầu việc chuẩn chi thông qua mạng truyền thông khác mạng thoại đến bên phát hành hoặc bên đại diện của bên phát hành.

3.73

xác thực thẻ trực tuyến (online card authentication)

Một quy trình được thực hiện bởi bên phát hành để xác minh tính hợp lệ của thẻ là được phép và ngăn chặn sự lặp dữ liệu.

3.74

mã PIN trực tuyến (Online PIN)

Một phương thức xác minh mã PIN tại đó mã PIN được nhập bởi chủ thẻ vào bảng mã PIN của thiết bị đầu cuối được mã hóa và kèm vào trong thông điệp yêu cầu chuẩn chi trực tuyến được gửi tới bên phát hành.

3.75

thiết bị đầu cuối có khả năng trực tuyến (Online-capable Terminal)

Một thiết bị chấp nhận thẻ có khả năng gửi trực tuyến giao dịch đến bên phát hành để chuẩn chi. EMV mô tả rằng thiết bị này "có khả năng hoạt động trực tuyến và ngoại tuyến".

3.76

bộ đệm (padding)

Các bit hoặc byte phụ thêm vào cả hai bên chuỗi (string) dữ liệu.

3.77

môi trường hệ thống thanh toán (payment system environment)

Tập hợp cá điều kiện lôgic được thiết lập bên trong ICC khi một ứng dụng hệ thống thanh toán phù hợp với bộ TCVN 11198 này được lựa chọn sử dụng, hoặc khi một Tệp tin Định nghĩa Từ điển DDF được sử dụng trong ứng dụng hệ thống thanh toán.

3.78

cá thể hóa (personalisation)

cá nhân hóa

Quy trình gắn liền trên thẻ với dữ liệu ứng dụng được tạo để sẵn sàng sử dụng.

3.79

bàn nhập mã PIN (PIN Pad)

Mảng bao gồm các phím số và phím lệnh dùng để nhập mã nhận diện cá nhân mã PIN.

3.80

bản rõ (plaintext)

Dữ liệu ở dạng gốc chưa mã hóa.

3.81

điểm giao dịch (point of transaction)

Vị trí vật lý tại đó bên bán hàng hoặc bên chấp nhận thẻ (trong môi trường trao đổi trực tiếp) hoặc một thiết bị đầu cuối không cần giám sát (trong môi trường không giám sát).

3.82

cập nhật sau phát hành (post-issuance update)

Một lệnh được gửi bởi bên phát hành thông qua thiết bị đầu cuối trên một hồi đáp chuẩn chi để cập nhật nội dung lưu trữ điện tử trên thẻ chip.

3.83

khóa riêng (private key)

khóa bí mật

Một trong cặp khóa không đồng bộ của một thực thể được giữ bí mật và chỉ được sử dụng bởi thực thể đó. Trong trường hợp sử dụng lược đồ chữ ký số, khóa riêng xác định chức năng ký.

3.84

khóa công khai (public key)

khóa chung

Một trong cặp khóa không đồng bộ cảu một thực thể được sử dụng công khai. Trong trường hợp sử dụng lược đồ chữ ký số, khóa công khai xác định chức năng xác minh tính hợp lệ.

CHÚ THÍCH Trong một số trường hợp cụ thể, thuật ngữ "khóa công cộng" được sử dụng tương đương.

3.85

chứng chỉ khóa công khai (public key certificate)

Thông tin khóa công khai của một thực thể được ký (xác nhận) bởi cơ quan chức nhận CA và do đó không thể làm giả.

3.86

thuật toán mã hóa khóa công khai (public key cryptographic algorithm)

Thuật toán mã hóa cho phép bảo mật thông tin trao đổi, nhưng không yêu cầu khóa riêng đã chia sẻ, thông qua việc sử dụng hai loại khóa có liên quan: một khóa công khai được phân phối công khai và một khóa riêng được giữ bí mật.

3.87

cặp khóa công khai (public key pair)

Hai khóa có liên quan toán học với nhau: một khóa riêng và một khóa công khai, tại đó khi được sử dụng với một thuật toán mã hóa khóa công khai thích hợp, có thể cho phép giữ bảo mật thông tin trao đổi mà không cần bảo mật việc trao đổi bí mật.

3.88

giao dịch mua (purchase transaction)

Việc mua lẻ hàng hóa hoặc dịch vụ; điểm bán hàng giao dịch.

3.89

lựa chọn ngẫu nhiên (random selection)

Chức năng của thiết bị đầu cuối có khả năng trực tuyến theo EMV cho phép thực hiện lựa chọn các giao dịch để xử lý trực tuyến. Đây là một phần chức năng Quản lý Rủi ro Thiết bị đầu cuối.

3.90

biên lai (receipt)

Một hồ sơ trên giấy về cuộc giao dịch được tạo cho chủ thẻ tại điểm giao dịch.

3.91

hồi đáp (response)

Một thông điệp được trả về bởi ICC đến thiết bị đầu cuối sau khi quy trình xử lý thông điệp lệnh được nhận bởi ICC.

3.92

RSA

Hệ thống mã hóa khóa công khai được phát triển bởi Rivest, Shamir, Adleman, được sử dụng để mã hóa dữ liệu và xác thực dữ liệu.

3.93

tập lệnh (script)

Một lệnh hoặc một chuỗi (string) lệnh được truyền bởi bên phát hành đến thiết bị đầu cuối cho mục đích gửi đến ICC một dãy các lệnh. Việc này thường được sử dụng để cung cấp việc cập nhật sau khi phát hành đến dữ liệu ứng dụng.

3.94

khóa bí mật (secret key)

Một khóa được sử dụng trong các kỹ thuật mã hóa đối xứng và chỉ có thể sử dụng bởi một số các thực thể đã xác định. Khóa bí mật này không thể bị tiết lộ công khai mà không có sự cho phép của hệ thống an ninh.

CHÚ THÍCH 1 Thuật ngữ này không giống như khóa riêng (Điều 3.83) trong cặp khóa riêng/công khai.

CHÚ THÍCH 2 Thuật ngữ này chỉ được sử dụng trong kỹ thuật mã hóa đối xứng.

3.95

gửi thông điệp bí mật (Secure Messaging)

xử lý tin điện an toàn

Một quy trình cho phép các thông điệp dùng để gửi từ thực thể này đến thực thể khác và ngăn chặn việc chỉnh sửa hoặc xem trái phép.

3.96

khóa phiên (session key)

Một khóa mã hóa tạm thời được tính toán trong bộ nhớ biến động và không còn giá trị sau khi phiên đó kết thúc.

3.97

xác thực dữ liệu tĩnh (Static Data Authentication)

SDA

Một kiểu Xác thực Dữ liệu Ngoại tuyến tại đó thiết bị đầu cuối xác minh tính hợp lệ của giá trị mã hóa có trên thẻ trong khi cá nhân hóa. Việc xác minh tính hợp lệ ngăn chặn một số kiểu tấn công tráo hàng (counterfeit) nhưng không ngăn chặn việc sao chép và chạy lại.

3.98

kỹ thuật mã hóa đối xứng (symmetric cryptographic technique)

Một kỹ thuật mã hóa có sử dụng cùng khóa bí mật cho cả hai bên khởi tạo và bên nhận khi trao đổi thông tin. Không có khóa bí mật rõ ràng thì không thể có khả năng tính toán ra được thông tin trao đổi của bên khởi tạo hoặc của bên nhận.

CHÚ THÍCH Thuật ngữ "khóa bí mật" được sử dụng tại đây được định nghĩa tại Điều 3.94.

3.99

bản mẫu (template)

Trường giá trị của một đối tượng dữ liệu có cấu trúc, định nghĩa một nhóm logic các đối tượng dữ liệu.

3.100

thiết bị đầu cuối (terminal)

Thiết bị được sử dụng kết hợp với ICC tại điểm giao dịch để thực hiện cuộc giao dịch tài chính. Thiết bị đầu cuối kết hợp thiết bị giao diện và có thể bao gồm các thành phần khác và các giao diện khác như máy chủ truyền thông.

3.101

mã hành động thiết bị đầu cuối (Terminal Action Code)

TAC

Các điều lệ tại đó thiết bị đầu cuối sử dụng để xác định khi nào cuộc giao dịch phải bị từ chối ngoại tuyến, gửi trực tuyến để chuẩn chi, hoặc từ chối nếu không thể trực tuyến. Bộ tiêu chuẩn này định nghĩa như sau (tại đó bao gồm hành động được lựa chọn bởi bên chấp nhận thẻ để thực hiện phân tích dựa trên phần tử dữ liệu TVR):

- TAC – Mặc định: các điều lệ xác định khi nào một giao dịch phải bị từ chối ngoại tuyến nếu nó không thể thực hiện trực tuyến;
- TAC – Từ chối: các điều lệ xác định khi nào một giao dịch phải bị từ chối ngoại tuyến;
- TAC – Trực tuyến: các điều lệ xác định khi nào một giao dịch phải được gửi trực tuyến để xin chuẩn chi.

3.102

chấm dứt giao dịch (Terminate Transaction)

Dừng quy trình xử lý ứng dụng đối với cuộc giao dịch hiện thời và hủy kích hoạt thẻ.

3.103

xác thực bằng token (Token Authentication)

Một chức năng không trong thanh toán được hỗ trợ trong ứng dụng để cho phép thẻ sinh ra một token để có thể được sử dụng để xác thực rằng thẻ và chủ thẻ là hợp lệ.

3.104

giao dịch (Transaction)

Một hành động thực hiện bởi thiết bị đầu cuối theo yêu cầu của người sử dụng. Đối với một thiết bị đầu cuối POS, một cuộc giao dịch phải là thanh toán hàng hóa,..v..v.. Một giao dịch lựa chọn trong số một hoặc nhiều ứng dụng như là một phần luồng quy trình xử lý.

3.105

chứng chỉ giao dịch (Transaction Certificate)

TC

Một mã lệnh ứng dụng được sinh ra khi chấp nhận một cuộc giao dịch.

3.106

dữ liệu chuyển tiếp (Transient Data)

dữ liệu nhất thời

Dữ liệu được quy định cho giao dịch hiện thời. Dữ liệu này sẽ được đặt lại tại thời điểm bắt đầu một giao dịch mới.

3.107

kiểm tra tần suất giao dịch (velocity checking)

kiểm tra nhanh

Một chức năng quản lý rủi ro thẻ được sử dụng để kiểm soát việc thực hiện ngoại tuyến diễn ra bao lâu hoặc có bao nhiêu cuộc giao dịch diễn ra trực tuyến.

3.108

thanh toán giá trị thấp Visa (Visa Low-Value Payment)

VLP

Cho phép thực hiện nhanh các giao dịch giá trị thấp tại các thiết bị đầu cuối có hỗ trợ chức năng này.

4 Thuật ngữ viết tắt, ký hiệu, quy ước và biểu tượng

4.1 Thuật ngữ viết tắt

a	Alphabetic	chữ cái
AAC	Application Authentication Cryptogram	Mã xác thực ứng dụng
AC	Application Cryptogram	Mã lệnh ứng dụng
ADR	Application Decisional Results	Kết quả Quyết định Ứng dụng
AEF	Application Elementary File	Tệp tin phần tử ứng dụng
AFL	Application File Locator	Định vị tệp tin ứng dụng
AID	Application Identifier	Định danh ứng dụng
AIP	Application Interchange Profile	Hồ sơ hoán đổi ứng dụng
an	Alphanumeric	chữ và số
ans	Alphanumeric Special	Chữ và số đặc biệt
App.	Application	Ứng dụng
ARC	Authorisation Response Code	Mã hồi đáp chuẩn chi
ARPC	Authorisation Response Cryptogram	Mã lệnh hồi đáp chuẩn chi
ARQC	Authorisation Request Cryptogram	Mã lệnh yêu cầu chuẩn chi
ATC	Application Transaction Counter	Bộ đếm giao dịch ứng dụng
ATM	Automated Teller Machine	Máy thanh toán tự động
AUC	Application Usage Control	Kiểm soát việc sử dụng ứng dụng
auth.	Authentication	chuẩn chi
b	Binary	nhị phân
BER	Basic Encoding Rules (defined in ISO/IEC 8825-1)	điều lệ mã hóa cơ bản (theo ISO/IEC 8825-1)
C	Conditional	điều kiện
CA	Certification Authority	tổ chức chứng nhận
CCD	Common Core Definitions	định nghĩa lõi chung
CCI	Common Core Identifier	định danh lõi chung
CDA	Combined DDA/Application Cryptogram Generation	sinh mã lệnh ứng dụng kết hợp DDA
CDOL	Card Risk Management Data Object List	Danh sách Đối tượng Dữ liệu Quản lý rủi ro thẻ
Cert.	Certificate	chứng nhận
CIAC	Card Issuer Action Code	Mã hành động bên phát hành thẻ
CID	Cryptogram Information Data	Dữ liệu thông tin mã lệnh
CLA	Class Byte of the Command Message	Byte theo lớp của thông điệp lệnh

CPA	Common Payment Application	Ứng dụng Thanh toán Chung
CPS	EMVCo Common Personalisation Specification	Đặc tả Cá thể hóa Chung của EMV
CRM	Card Risk Management	Quản lý Rủi ro Thẻ
CSU	Card Status Update	Cập nhật Trạng thái Thẻ
CV	Cryptogram Version	Phiên bản mã lệnh
CV Rule	Cardholder Verification Rule	Điều lệ xác minh chủ thẻ
CVM	Cardholder Verification Method	Phương thức xác minh chủ thẻ
CVR	Card Verification Results	Kết quả xác minh thẻ
DDA	Dynamic Data Authentication	Chứng thực Dữ liệu Động
DDF	Directory Definition File	Tệp tin Định nghĩa Thư mục
DDOL	Dynamic Data Authentication Data Object List	Danh sách Đối tượng Dữ liệu Chứng thực Dữ liệu Động
DES	Data Encryption Standard	Chuẩn mã hóa dữ liệu
DKI	Derivation Key Index	Chỉ mục khóa phân phối
DOL	Data Object List	Danh sách Đối tượng Dữ liệu
EMV	Europay, MasterCard, Visa	Europay, MasterCard, Visa
FC	Format Code	Mã định dạng
FCI	File Control Information	Thông tin kiểm soát tệp tin
FIPS	Federal Information Processing Standard	Chuẩn xử lý thông tin liên bang
GEN AC	GENERATE APPLICATION CRYPTOGRAM	Sinh Mã lệnh ứng dụng
GPO	GET PROCESSING OPTIONS	Tùy chọn xử lý lệnh Get
hex.	Hexadecimal	hệ thập lục phân
HSM	Hardware Security Module	Mô đun an ninh phần cứng
IA	Issuer Authentication	Chứng thực bên phát hành
IAC	Issuer Action Code (Denial, Default, Online)	Mã hành động bên phát hành (Từ chối, Mặc định, Trực tuyến)
IAD	Issuer Application Data	Dữ liệu Ứng dụng bên phát hành
ICC	Integrated Circuit Card	Thẻ mạch tích hợp
IDN	ICC Dynamic Number	số hiệu động ICC
INS	Instruction Byte of the Command Message	Byte theo chỉ lệnh của thông điệp lệnh
Int'l	International	Quốc tế
ISO	International Organization for Standardization	Tổ chức tiêu chuẩn hóa quốc tế

L	Length	Chiều dài
Lc	Length of the Command Data Field	Chiều dài của trường dữ liệu lệnh
L_D	Length of the Plaintext Data in the Command Data Field	Chiều dài của dữ liệu bản rõ trong trường dữ liệu lệnh
Le	Maximum Expected Length of the Response Data Field	Chiều dài dự kiến tối đa của trường dữ liệu hồi đáp
LEN	Length	Chiều dài
M	Mandatory	Bắt buộc
MAC	Message Authentication Code	Mã xác thực thông điệp
MK	ICC Master Key for Session Key Generation	Khóa chính ICC để sinh khóa phiên
MKAC	Master Key for Application Cryptogram Generation	Khóa chính để sinh mã lệnh ứng dụng
MKSMC	Master Key for Secure Messaging for Confidentiality	Khóa chính để gửi thông điệp bảo đảm cho tính bí mật
MKSMI	Master Key for Secure Messaging for Integrity	Khóa chính đẻ gửi thông điệp bảo đảm cho tính toàn vẹn
MTA	Maximum Transaction Amount	Lượng giao dịch tối đa
n	Numeric	số
N	No	Không
N/A	Not Applicable	Không thể áp dụng
NCA	Length of the Certification Authority Public Key Modulus	Chiều dài của mô đun khóa công khai cơ quan chứng nhận
NI	Length of the Issuer Public Key Modulus	Chiều dài mô đun khóa công khai bên phát hành
NIC	Length of the ICC Public Key Modulus	Chiều dài mô đun khóa công khai ICC
NPE	Length of the ICC PIN Encipherment Public Key Modulus	Chiều dài mô đun khóa công khai bản mã hóa PIN ICC
New Lc	Length of Command Data including Secure Messaging Components	Chiều dài dữ liệu lệnh gồm cả các thành phần thông điệp bảo mật
P1	Parameter 1	Tham số 1
P2	Parameter 2	Tham số 2
PAN	Primary Account Number	Số cá nhân chính
PDOL	Processing Options Data Object List	Danh sách đối tượng dữ liệu tùy chọn quy trình xử lý
PIN	Personal Identification Number	số nhận dạng cá nhan
PK	Public Key	Khóa công khai
POS	Point Of Service	Điểm cung cấp dịch vụ

PTH	Previous Transaction History	Lịch sử giao dịch trước đây
Req	Requirement	Yêu cầu
RFU	Reserved for Future Use	để dành sử dụng trong tương lai
RID	Registered Application Provider Identifier	Định danh bên cung cấp ứng dụng đã đăng ký
RSA	Rivest, Shamir, Adleman	Rivest, Shamir, Adleman
SDA	Static Data Authentication	Xác thực dữ liệu tĩnh
SFI	Short File Identifier	định danh tệp tin ngắn
SMC	Secure Messaging for Confidentiality	Gửi thông điệp bảo đảm cho tính bí mật
SMI	Secure Messaging for Integrity	Gửi thông điệp bảo đảm cho tính toàn vẹn
SSAD	Signed Static Application Data	Dữ liệu ứng dụng tĩnh có dấu
SW1	Status Byte One	Byte trạng thái 1
SW2	Status Byte Two	Byte trạng thái 2
TAC	Terminal Action Code(s) (Default, Denial, Online)	Mã hành động thiết bị đầu cuối (Mặc định, Từ chối, Trực tuyến)
TC	Transaction Certificate	Chứng chỉ giao dịch
TLV	Tag-Length-Value	Tag-Length-Value
TSI	Transaction Status Information	Thông tin tình trạng giao dịch
TVR	Terminal Verification Results	Kết quả xác minh thiết bị đầu cuối
Txn	Transaction	Giao dịch
var.	Variable	Giá trị
VLP	Visa Low-Value Payment	Thanh toán giá trị thấp Visa
Y	Yes	Có
YYMM	year, month	năm, tháng
YYMMDD	year, month, day	năm, tháng, ngày

4.2 Ký hiệu

'0' đến '9' và 'A' đến 'F'	16 ký tự thập lục phân
'Tên bit'	bit được xác định bởi "tên bit" trong phần tử dữ liệu
xb, xxb	giá trị nhị phân
xx	bất kỳ giá trị nào
A := B	A được gán giá trị của B
A = B	Giá trị của A tương đương với giá trị của B
AND	lệnh logic AND
OR	lệnh logic OR
X ⊕ Y	Ký hiệu '⊕' cho biết so sánh từng bit tuyển loại trừ (exclusive-OR, Điều 3.44) và được định nghĩa như sau: X ⊕ Y so sánh từng bit ngoại trừ lệnh OR về khối dữ liệu X và Y. Nếu một khối dữ liệu ngắn hơn cái còn lại thì đầu tiên phải thêm vào bên trái một số bit 0 nhị phân thích hợp làm các đoạn có chiều dài giống nhau
[bx]	Bit x của phần tử dữ liệu đã tham chiếu
[x]	Byte x của phần tử dữ liệu đã tham chiếu
[x][by]	Bit y của byte x của phần tử dữ liệu đã tham chiếu
A / n	phép chia số nguyên của A với n, tại đó số nguyên đơn nhất d thì sẽ tồn tại một số nguyên r, $0 \le r < n$, sao cho: $A = dn + r$
x*y	phép nhân x với y
C := (A || B)	Phép nối n bit A với m bit B tại đó có C = 2m A + B.
Phần tử x	biểu diễn phần tử x của phần tử dữ liệu (ví dụ Thanh tổng X có thể là Thanh tổng 1 hoặc Thanh tổng 2)
trái nhất	Áp dụng cho một chuỗi (sequence) bit, byte hoặc số được sử dụng trong trao đổi với thuật ngữ "nhiều ý nghĩa nhất". Nếu C = (A || B) như bên trên, thì A là n bit trái nhất của C.
phải nhất	Áp dụng cho một chuỗi (sequence) bit, byte hoặc số được sử dụng trong trao đổi với thuật ngữ "ít ý nghĩa nhất". Nếu C = (A || B) như bên trên, thì B là m bit phải nhất của C.
Y/N	Có/Không
Req. x.x:	Các yêu cầu đối với CPA được chỉ ra và đánh số hiệu in đậm và các hành động được yêu cầu sẽ viết nghiêng để phân biệt với phần giải thích của hành động ứng dụng. Ví dụ: **Req x.x:** *Nếu thử nghiệm thành công, thiết lập giá trị bit là 1b.*

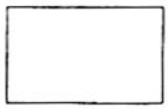
4.3 Quy ước định dạng phần tử dữ liệu

Bộ tiêu chuẩn TCVN 11198 sử dụng các định dạng phần tử dữ liệu như sau:

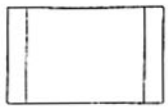
a	các phần tử dữ liệu chữ cái có chứa một ký tự đơn theo byte. Các ký tự được phép chỉ là chữ cái (từ a đến z và A đến Z, viết hoa và viết thường)
an	các phần tử dữ liệu chữ và số bao gồm một ký tự đơn theo byte. Các ký tự được phép là các chữ cái (từ a đến z và A đến Z, viết hoa và viết thường) và số (từ 0 đến 9)
ans	phần tử dữ liệu chữ cái đặc biệt bao gồm một ký tự đơn theo byte. Các ký tự được phép và chúng mã hóa như trong bảng Tập Ký tự Chung trong EMV Quyển 4, phụ lục B. Có một ngoại lệ: các ký tự được phép cho Tên Ưu tiên Ứng dụng không phải là các ký tự kiểm soát được định nghĩa trong ISO/IEC 8859 đã thiết kế trong Bảng chỉ mục Mã Bên phát hành tuân theo Tên Ưu tiên Ứng dụng
b	Các phần tử dữ liệu bao gồm hoặc các chữ số nhị phân không dấu hoặc tổ hợp bit mà được xác định trong bộ tiêu chuẩn TCVN 11198 này. Ví dụ nhị phân: Bộ đếm Giao dịch Ứng dụng (ATC) được định nghĩa là "b" với chiều dài là hai byte. Một giá trị ATC là 19 được lưu dạng Hex là "00 13". Ví dụ tổ hợp bit: Danh sách đối tượng dữ liệu tùy chọn quy trình xử lý (PDOL) được định nghĩa là "b" với định dạng như trong EMV Quyển 3, điều 5.4.
cn	Các phần tử dữ liệu dạng số đã nén bao gồm hai chữ số (có giá trị trong giải "0-9" dạng HEX) theo byte. Các phần tử dữ liệu này được căn trái và bù thêm một dãy thập lục phần "F". VÍ DỤ: Số Tài khoản Chính (PAN) cho ứng dụng được định nghĩa là "cn" với chiều dài lên tới 10 byte. Một giá trị trong 1234567890123 có thể được lưu trữ trong PAN cho ứng dụng dưới dạng HEX là "12 34 56 78 90 12 3F FF" với chiều dài là 8
n	Các phần tử dữ liệu dạng số bao gồm hai chữ số (có giá trị nằm trong dải "0-9" dạng HEX) theo byte. Các chữ số này được căn phải và bù thêm với các số 0 thập lục phân. Các tài liệu đặc tả khác thỉnh thoảng tham chiếu tới định dạng dữ liệu này như là kiểu Thập phân mã hóa nhị phân ("BCD") hoặc gói không dấu. VÍ DỤ: Số lượng, đã chuẩn chi (số) được định nghĩa là "n 12" với chiều dài là sáu byte. Một giá trị là 12345 được lưu tại Số lượng, đã chuẩn chi (số) dạng HEX là "00 00 00 01 23 45"
var	Các phần tử dữ liệu biến thiên với chiều dài biến thiên và có thể chứa bất kỳ tổ hợp bit nào. Thông tin bổ sung trong các dạng phần tử dữ liệu biến thiên cụ thể có thể tồn tại ở bất cứ đâu

4.4 Biểu tượng

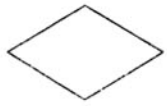
Bộ tiêu chuẩn TCVN 11198 này sử dụng các biểu tượng sau trong các biểu đồ luồng và trong các sơ đồ.



bước (quy trình) xử lý



bước (quy trình) xử lý con



quyết định

Kết nối hết trang
(từ N đến N)

Gửi hồi đáp đến thiết bị đầu cuối

Ngoài phạm vi

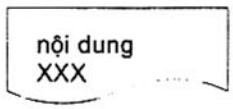
Quy trình xử lý đã định trước
(tiếp tục /kết nối hết trang)

tham chiếu đến số điều của tài liệu

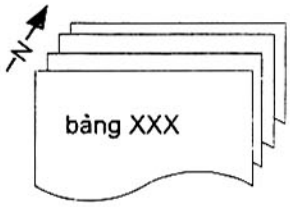
Dữ liệu thông tin mã lệnh
Bộ đếm giao dịch ứng dụng
Mã lệnh ứng dụng
Dữ liệu ứng dụng

các phần tử con của Dữ liệu

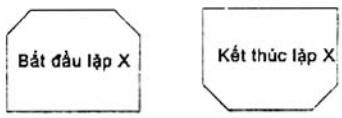
Phần tử dữ liệu



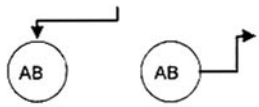
Phần tử dữ liệu lôgic



Tập các phần tử dữ liệu logic



Bắt đầu và Kết thúc của một Vòng lặp Mã Vòng



Kết nối trang trên

Thiết bị đầu cuối biểu đồ luồng

5 Giải thích thuật ngữ

Trong bộ tiêu chuẩn TCVN 11198 này sử dụng một số thuật ngữ mang ý nghĩa dành riêng trong phạm vi áp dụng.

Độc quyền

"Độc quyền" chỉ ra các khái niệm không được định nghĩa trong bộ tiêu chuẩn này và/hoặc nằm ngoài phạm vi của bộ tiêu chuẩn này.

Bắt buộc/Yêu cầu/Khuyến nghị/Tùy chọn

Một mục tiêu của CPA là định nghĩa một tập lõi các chức năng mà phải có đối với bên phát hành trong mọi công việc triển khai CPA. Các yêu cầu tối thiểu và tùy chọn của bên phát hành liên quan đến các hạng mục bắt buộc của EMV và CCD trong phần bổ sung yêu cầu xác định các hệ thống thanh toán phải có đối với tất cả bên phát hành.

Tất cả các chức năng khác là tùy chọn và không được yêu cầu.

Nhiều tính năng được yêu cầu có hỗ trợ bởi việc triển khai CPA không là bắt buộc sử dụng bởi bên phát hành. Tiêu chuẩn này đặc tả các yêu cầu đối với việc triển khai đặc tả CPA.

- Các chức năng này là tùy chọn với bên cung cấp ứng dụng để triển khai được gọi là *tùy chọn-triển khai*, và chức này có đặc tính là *tính tùy chọn-triển khai*. Nếu đã triển khai, việc bên phát hành lựa chọn khi nào sử dụng chức năng đó;
- Các năng năng là tùy chọn đối với bên Phát hành được gọi là *tùy chọn-bên phát hành* và chức năng này có đặc tính là *tính tùy chọn-bên phát hành*.

Các thuật ngữ sau đây được sử dụng để chỉ ra các khác biệt này.

Bảng 1 – Thuật ngữ cho chức năng được yêu cầu và tùy chọn

bắt buộc được yêu cầu phải tùy chọn-bên phát hành	yêu cầu tối thiểu đối với CPA
nên	chức năng được khuyến nghị
tùy chọn có thể tùy chọn-triển khai	các chức năng và phần tử dữ liệu chọn lọc

Các thị trường có thể tùy chỉnh các ứng dụng thẻ của họ cao hơn các nhu cầu tối thiểu thông qua chấp nhận các chức năng tùy chọn và thông qua quy trình xử lý độc quyền. Quy trình xử lý độc quyền, tuy nhiên, không được đối lập với khả năng tương tác toàn cầu.

Thẻ/Mạch tích hợp

Theo thông thường, thuật ngữ "thẻ" được sử dụng để mô tả các chức năng được thực hiện bởi ứng dụng CPA trên thẻ. Khi cần thiết phân biệt bản thân thẻ chip đó và các tính năng thẻ khác như dải từ, thì thuật ngữ "mạch tích hợp" được sử dụng.

6 Các quy trình xử lý chức năng

Phần này cung cấp một cách tổng quát về từng điều có trong bộ tiêu chuẩn TCVN 11198. Để cung cấp một cách rõ ràng các yêu cầu từ EMV (bao gồm cả CCD) có thể được thể hiện hoặc tái tạo lại trong bộ tiêu chuẩn TCVN 11198 này nhằm cung cấp một đặc tả ứng dụng toàn diện.

Để dễ dàng sử dụng, từng điều quy trình xử lý chức năng được cấu trúc như sau:

- Mục đích – Định nghĩa chức năng của quy trình;
- Trình tự thực hiện – Vạch ra quy trình ưu tiên cần thêm vào trong các hành động đã biết trước đó liên quan đến chức năng này, và các chuỗi xử lý nhỏ cần thêm vào trong các hành động đã biết tại tương lai có liên quan đến chức năng này;
- Dữ liệu thẻ - Cung cấp một mô tả ngắn gọn về dữ liệu trong thẻ hỗ trợ chức năng;
- Quy trình xử lý lệnh – Cung cấp một mô tả ngắn gọn về các lệnh được sử dụng để hỗ trợ chức năng và chức năng của quy trình chức năng. Nếu có một số lệnh hoặc chức năng này bên trong một quy trình, thì chúng phải được liệt kê riêng rẽ;
- Biểu đồ luồng chức năng – Tại đây cung cấp một luồng mẫu để minh họa cách thức mà một chức năng được triển khai;

CHÚ THÍCH Các biểu đồ luồng thể hiện quy trình xử lý và có thể không bao gồm tất cả các bước phải thực hiện. Cho phép cả các luồng xử lý khác nhưng có cùng kết quả;

Thư mục tài liệu tham khảo

[1] EMV Book 1, EMV Integrated Circuit Card Specifications for Payment Systems, version 4.1, Book 1, Application Independent ICC to Terminal Interface Requirements, May 2004 (EMV Quyển 1).

[2] EMV Book 2, EMV Integrated Circuit Card Specifications for Payment Systems, version 4.1, Book 2, Security and Key Management, May 2004 (EMV Quyển 2).

[3] EMV CPS, EMV Card Personalization Specification, version 1.0, June 2003.;