TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 11295:2016
ISO/IEC 19790:2012

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - YÊU CẦU AN TOÀN CHO MÔ-ĐUN MẬT MÃ

Information technology - Security techniques - Security requirements for cryptographic modules

HÀ NỘI - 2016

Mục lục

Lời nói đầu

TCVN 11295:2016 hoàn toàn tương đương với ISO/IEC 19790:2012.

TCVN 11295:2016 do Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã biên soạn, Ban Cơ yếu Chính phủ đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Trong lĩnh vực công nghệ thông tin, nhu cầu sử dụng các cơ chế mật mã như bảo vệ dữ liệu chống lại sự tiết lộ hoặc thao tác trái phép, đối với xác thực thực thể và chống chối bỏ liên tục gia tăng. Tính an toàn và tin cậy của các cơ chế như vậy phụ thuộc trực tiếp vào các mô-đun mật mã trong đó chúng được thực thi.

Tiêu chuẩn này cung cấp bốn mức định tính tăng dần của các yêu cầu an toàn nhằm bao quát một giải rộng các ứng dụng và các môi trường tiềm năng. Các kỹ thuật mật mã là như nhau cho cả bốn mức an toàn này. Các yêu cầu an toàn còn bao quát cả những lĩnh vực liên quan tới thiết kế và thực thi của mô-đun mật mã. Các lĩnh vực này bao gồm: đặc tả mô-đun mật mã; các giao diện của mô-đun mật mã; các vai trò, các dịch vụ và xác thực; an toàn phần mềm/phần sụn; môi trường hoạt động; an toàn vật lý; an toàn không xâm lấn; quản lý tham số an toàn nhạy cảm; các tự kiểm tra; đảm bảo vòng đời và giảm thiểu các tấn công khác.

Cần phân mức tổng thể an toàn của mô-đun mật mã để lựa chọn mức an toàn phù hợp cho các yêu cầu an toàn của ứng dụng và môi trường trong đó mô-đun sẽ được ứng dụng và cho những dịch vụ an toàn mà mô-đun sẽ cung cấp. Thẩm quyền chịu trách nhiệm trong mỗi tổ chức cần đảm bảo rằng các hệ thống viễn thông và máy tính của họ khi sử dụng các mô-đun mật mã phải cung cấp một mức an toàn chấp nhận được đối với môi trường và ứng dụng đã cho. Vì mỗi thẩm quyền chịu trách nhiệm cho việc lựa chọn các chức năng an toàn đã được phê duyệt nào là phù hợp với một ứng dụng đã cho, nên việc tuân thủ theo tiêu chuẩn này không hàm ý liên tác đầy đủ hoặc chấp nhận lẫn nhau của các sản phẩm tuân thủ theo tiêu chuẩn. Tầm quan trọng của nhận thức và của việc tạo ra một ưu tiên quản lý cho an toàn thông tin cần được truyền đạt cho tất cả những đối tượng quan tâm.

Các yêu cầu an toàn thông tin biến đổi đối với các ứng dụng khác nhau; các tổ chức cần phải nhận biết các tài nguyên thông tin của họ và xác định mức độ nhạy cảm và ảnh hưởng tiềm năng của việc thất thoát thông tin bằng cách thực thi các kiểm soát phù hợp. Các kiểm soát bao gồm nhưng không chỉ giới hạn ở các nội dung sau:

- Các kiểm soát vật lý và môi trường;
- Các kiểm soát truy cập;
- Phát triển phần mềm;
- Các kế hoạch dự phòng sao lưu và dự phòng bất trắc; và
- Các kiểm soát dữ liệu và thông tin.

Các kiểm soát này chỉ có hiệu quả nếu như có sự thi hành các chính sách an toàn và các thủ tục phù hợp bên trong môi trường hoạt động.

TIÊU CHUẨN QUỐC GIA TCVN 11295 : 2016

Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu an toàn cho các mô-đun mật mã

Information technology - Security techniques - Security Requirements For Cryptographic Modules

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu an toàn cho mô-đun mật mã được sử dụng bên trong một hệ thống an toàn bảo vệ thông tin nhạy cảm trong các hệ thống viễn thông và máy tính. Tiêu chuẩn này xác định bốn mức an toàn cho các mô-đun mật mã để cung cấp một phổ rộng của độ nhạy cảm dữ liệu (ví dụ: Dữ liệu quản lý có giá trị thấp, những sự chuyển vốn hàng triệu đô la, dữ liệu bảo vệ cuộc sống, thông tin định danh cá nhân, và thông tin nhạy cảm được sử dụng bởi chính phủ) và sự đa dạng của các môi trường ứng dụng (ví dụ: một phương tiện được bảo vệ, một văn phòng, phương tiện có thể tháo lắp, và một địa điểm hoàn toàn không được bảo vệ). Tiêu chuẩn này chỉ rõ bốn mức an toàn cho mỗi một lĩnh vực trong số 11 lĩnh vực yêu cầu với mỗi mức an toàn sau tăng thêm an toàn so với mức an toàn trước đó.

Tiêu chuẩn này quy định các yêu cầu an toàn được cụ thể hóa hướng đến duy trì độ an toàn được cung cấp bởi mô-đun mật mã và việc tuân thủ theo tiêu chuẩn này là chưa đủ để đảm bảo rằng mô-đun cụ thể là an toàn hoặc rằng độ an toàn cung cấp bởi mô-đun đó là đủ và chấp nhận được đối với chủ sở hữu thông của thông tin mà nó đang được bảo vệ.

2 Tài liệu viện dẫn

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

Các tài liệu được liệt kê ở các phụ lục C, D, E và F của Tiêu chuẩn này.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa sau:

3.1

Danh sách kiểm soát truy cập (access control list)

ACL (ACL)

Danh sách các cho phép để nhận truy cập tới một đối tượng.

3.2

Tài liệu hướng dẫn người quản trị (administrator guidance)

Tài liệu được viết ra được sử dụng bởi chuyên viên mật mã và/hoặc các vai trò quản trị khác để quản trị, duy trì và cấu hình chính xác mô-đun mật mã.

3.3

Tự động hóa (automated)

Không có sự can thiệp thủ công hoặc nhập dữ liệu thủ công (ví dụ: bằng phương tiện điện tử như việc thông qua một mạng máy tính).

3.4

Thẩm quyền phê duyệt (approval authority)

Bất kì tổ chức/thẩm quyền quốc tế hoặc quốc gia được ủy quyền để phê duyệt và/hoặc đánh giá các chức năng an toàn.

CHÚ THÍCH: Một thẩm quyền phê duyệt trong ngữ cảnh của định nghĩa này đánh giá và phê duyệt các chức năng an toàn dựa trên phẩm chất mật mã hoặc toán học của chúng, nhưng không phải là thực thể kiểm tra để kiểm tra tính tuân theo đối với tiêu chuẩn này

3.5

Kỹ thuật xác thực dữ liệu được phê duyệt (approved data authentication technique)

Phương thức được phê duyệt có thể bao gồm việc sử dụng chữ ký số, mã xác thực thông điệp hoặc hàm băm có khóa (ví dụ: HMAC).

3.6

Kỹ thuật toàn vẹn được phê duyệt (approved integrity technique)

Hàm băm, mã xác thực thông điệp hoặc thuật toán chữ ký số được phê duyệt.

3.7

Chế độ hoạt động được phê duyệt (approved mode of operation)

Tập hợp các dịch vụ bao gồm ít nhất một dịch vụ sử dụng một chức năng hoặc một tiến trình an toàn được phê duyệt và có thể bao gồm các dịch vụ không an toàn có liên quan.

CHÚ THÍCH 1: Không nhầm lẫn với một chế độ cụ thể của một chức năng an toàn được phê duyệt, ví dụ: chế độ móc xích khối mã CBC (Cipher Block Chaining).

CHÚ THÍCH 2: Các chức năng hoặc các tiến trình an toàn không được phê duyệt thì bị loại trừ.

3.8

Chức năng an toàn được phê duyệt (approved security function)

Chức năng an toàn (ví dụ: thuật toán mật mã) được tham chiếu đến trong Phụ lục C.

3.9

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

Kỹ thuật mật mã sử dụng hai phép biến đổi có liên quan đến nhau bao gồm một phép biến đổi công khai (được xác định bởi khóa công khai) và một phép biến đổi bí mật (được xác định bởi khóa riêng).

CHÚ THÍCH: Hai phép biến đổi có tính chất là cho phép biến đổi công khai, không thể về mặt tính toán nhận được phép biến đổi bí mật trong một thời gian hạn chế đã cho và với các tài nguyên tính toán đã cho.

3.10

Sinh trắc (biometric)

Đặc trưng vật lý hoặc đặc điểm hành vi cá nhân đo được, được sử dụng để nhận dạng định danh hoặc kiểm tra định danh được tuyên bố của một người vận hành.

3.11

Khả năng bỏ qua (bypass capability)

Khả năng của một dịch vụ bỏ qua một phần hoặc toàn bộ một chức năng mật mã

3.12

Chứng thư (certificate)

Dữ liệu của thực thể được làm cho không thể giả mạo thông qua khóa riêng hoặc khóa bí mật của một thẩm quyền chứng thực

CHÚ THÍCH: Không nên nhầm lẫn với chứng nhận kiểm tra hợp lệ của các mô-đun được cấp bởi một thẩm quyền kiểm tra hợp lệ.

3.13

Làm tổn hại (compromise)

Việc tiết lộ, sửa đổi, thay thế, hoặc sử dụng các tham số an toàn quan trọng trái phép hoặc sửa đổi hay thay thế trái phép các tham số an toàn công khai.

3.14

Tự kiểm tra có điều kiện (conditional self-test)

Việc kiểm tra được thực hiện bởi mô-đun mật mã khi các điều kiện được chỉ rõ đối với việc kiểm tra xảy ra.

3.15

Tính bí mật (confidentiality)

Tính chất mà thông tin không ở dạng sẵn sàng hoặc bị tiết lộ cho các thực thể không có thẩm quyền.

3.16

Hệ thống quản lý cấu hình (configuration management system)

CMS (CMS)

Quản lý các đặc tính và các đảm bảo an toàn thông qua việc kiểm soát những thay đổi được thực hiện đối với phần cứng, phần mềm và tài liệu của mô-đun mật mã.

3.17

Thông tin điều khiển (control information)

Là thông tin được đưa vào mô-đun mật mã với các mục đích điều khiển hoạt động của mô-đun đó.

3.18

Tham số an toàn quan trọng (critical security parameter)

CSP (CSP)

Thông tin liên quan tới tính an toàn mà việc tiết lộ hoặc sửa đổi có thể làm tổn hại đến tính an toàn của mô-đun mật mã.

VÍ DỤ: Các khóa mật và bí mật, dữ liệu xác thực như mật khẩu, PINs, các chứng thư số hay các mỏ neo tin cậy khác.

CHÚ THÍCH: Một CSP có thể ở dạng bản rõ hoặc được mã hóa (encrypt).

3.19

Chuyên viên mật mã (crypto officer)

Vai trò được đảm bảo bởi một cá nhân hoặc một tiến trình (ví dụ chủ thể) hành động nhân danh cho một cá nhân truy cập tới mô-đun mật mã để thực hiện các chức năng quản lý hoặc khởi hoạt mật mã của mô-đun mật mã.

3.20

Thuật toán mật mã (cryptographic algorithm)

Thủ tục tính toán được định nghĩa tốt, nhận các đầu vào biến thiên, các đầu vào này có thể bao gồm cả các khóa mật mã, và sinh ra một đầu ra.

3.21

Ranh giới mật mã (cryptographic boundary)

Đường bao khép kín liên tục được xác định ở dạng hiển, thiết lập các ranh giới lôgic và/hoặc vật lý của mô-đun mật mã và chứa tất cả các thành phần phần cứng, phần mềm và/hoặc phần sụn của mô-đun mật mã.

3.22

Hàm băm mật mã (cryptographic hash function)

Hàm hiệu quả về mặt tính toán ánh xạ các chuỗi nhị phân có độ dài bất kỳ thành các chuỗi nhị phân có độ dài cố định sao cho bằng tính toán không thể tìm được hai giá trị khác biệt mà chúng băm thành một giá trị chung.

3.23

Khóa mật mã (cryptographic key)

khóa (key)

Dãy các ký hiệu mà chúng kiểm soát thao tác của một biến đổi mật mã.

VÍ DỤ: Một biến đổi mật mã có thể bao gồm nhưng không giới hạn bởi việc mã mật, giải mã, tính toán hàm kiểm tra mật mã, sinh chữ ký, hoặc kiểm tra hợp lệ chữ ký.

3.24

Thành phần khóa mật mã (cryptographic key component)

thành phần khóa (key component)

Tham số được sử dụng kết hợp với các thành phần khóa khác trong một chức năng an toàn được phê duyệt để tạo thành một CSP bản rõ hoặc thực hiện một chức năng mật mã.

3.25

Mô-đun mật mã (cryptographic module)

mô-đun (module)

Tập hợp phần cứng, phần mềm, và/hoặc phần sụn thực thi các chức năng an toàn và được chứa bên trong ranh giới mật mã.

3.26

Chính sách an toàn của mô-đun mật mã (cryptographic module security policy)

chính sách an toàn (security policy)

Đặc tả chính xác các quy tắc an toàn, theo đó mô-đun mật mã hoạt động, bao gồm các quy tắc nhận được từ các yêu cầu của tiêu chuẩn này và các quy tắc bổ sung được áp đặt bởi mô-đun đó hoặc thẩm quyền xác nhận hợp lệ.

CHÚ THÍCH: Xem Phụ lục B.

3.27

Đường dẫn dữ liệu (data path)

Định tuyến lôgic hoặc vật lý mà dữ liệu đi qua.

CHÚ THÍCH: Một đường dẫn dữ liệu vật lý có thể được chia sẻ bởi nhiều đường dẫn dữ liệu lôgic.

3.28

Hoạt động bị xuống cấp (degraded operation)

Hoạt động mà tại đó một tập con của tập toàn bộ của các thuật toán, các hàm, các dịch vụ hoặc các tiến trình an toàn là sẵn sàng và/hoặc có thể được cấu hình như là kết quả của việc cấu hình lại từ trạng thái lỗi.

3.29

Phân tích vi sai điện năng (Differential power analysis)

DPA (DPA)

Phân tích các biến thiên về việc tiêu thụ điện năng của mô-đun mật mã nhằm mục đích trích rút ra thông tin có tương quan với phép toán mật mã.

3.30

Chữ ký số (digital signature)

Dữ liệu được nối vào, hoặc một biến đổi mật mã của một đơn vị dữ liệu cho phép người nhận đơn vị dữ liệu chứng minh nguồn gốc và tính toàn vẹn của đơn vị dữ liệu và bảo vệ chống lại sự giả mạo (ví dụ. bởi người nhận).

3.31

Đầu vào trực tiếp (direct entry)

Đầu vào của một SSP hoặc thành phần khóa vào trong mô-đun mật mã, sử dụng thiết bị, chẳng hạn như bàn phím.

3.32

Chữ ký tách rời (disjoint signature)

Một hoặc nhiều chữ ký cùng biểu diễn một tập mã đầy đủ.

3.33

Phát xạ điện từ (electromagnetic emanations)

EME (EME)

Tín hiệu mang thông tin, nếu bị chặn bắt và phân tích, có khả năng làm lộ thông tin được phát đi, được thu về, được điều khiển hoặc không thì được xử lý bởi thiết bị xử lý thông tin bất kì.

3.34

Đầu vào điện tử (electronic entry)

Đầu vào các SSP hoặc các thành phần khóa vào mô-đun mật mã sử dụng các phương pháp điện tử.

CHÚ THÍCH: Người vận hành của khóa có thể không có hiểu biết về giá trị của khóa được nhập vào.

3.35

Chữ ký hoàn chỉnh (encompassing signature)

Chỉ một chữ ký cho một tập mã đầy đủ.

3.36

Khóa được mã hóa (encrypt) (encrypted key)

Khóa mật mã mà nó được mã hóa (encrypt) bằng cách sử dụng một hàm an toàn đã được phê duyệt với một khóa mã hóa (encrypt) khóa.

CHÚ THÍCH: Nó được cho là đã được bảo vệ.

3.37

Thực thể (entity)

Người, nhóm, thiết bị, hoặc tiến trình.

3.38

Entropy (Entropy)

Độ đo tính hỗn độn, tính ngẫu nhiên hay tính biến thiên trong một hệ thống đóng.

CHÚ THÍCH: Entropy của một biến số ngẫu nhiên X là một độ đo toán học của lượng thông tin được cung cấp bởi một sự quan sát của X.

3.39

Bảo vệ chống lỗi do môi trường (environment failure protection)

EFP (EFP)

Việc sử dụng các đặc tính để bảo vệ chống lại tổn hại về an toàn của mô-đun mật mã do các điều kiện môi trường bên ngoài dải hoạt động bình thường của mô-đun đó.

3.40

Kiểm tra lỗi do môi trường (environment failure testing)

EFT (EFT)

Sử dụng các phương pháp cụ thể để cung cấp sự bảo đảm hợp lý rằng tính an toàn của mô-đun mật mã sẽ không bị tổn hại bởi các điều kiện môi trường bên ngoài dải hoạt động bình thường của mô-đun đó.

3.41

Mã phát hiện sai (error detection code)

EDC (EDC)

Giá trị được tính toán từ dữ liệu và bao gồm các bit dư thừa của thông tin được thiết kế để phát hiện, nhưng không hiệu chỉnh, những thay đổi không cố ý trong dữ liệu.

3.42

Dạng có thể thực hiện (executable form)

Dạng mã trong đó phần mềm hoặc phần sụn được quản lý và điều khiển hoàn toàn bởi môi trường hoạt động của mô-đun và không yêu cầu phải biên dịch (chẳng hạn: không có mã nguồn, mã đối tượng, hoặc mã chỉ biên dịch khi thực thi).

3.43

Cảm ứng lỗi (fault induction)

Kỹ thuật để cảm sinh các thay đổi về hành vi hoạt động trong phần cứng bằng việc áp dụng các điện áp tức thời, bức xạ, laser hoặc các kỹ thuật xiên lệch thời gian.

3.44

Mô hình trạng thái hữu hạn (finite state model)

FSM (FSM)

Mô hình toán học của một máy tuần tự bao gồm một tập hữu hạn các sự kiện đầu vào, một tập hữu hạn các sự kiện đầu ra, một tập hữu hạn các trạng thái, một hàm ánh xạ các trạng thái và đầu vào tới đầu ra, một hàm ánh xạ các trạng thái và các đầu vào tới các trạng thái (một hàm chuyển đổi trạng thái) và một đặc tả mô tả trạng thái khởi đầu.

3.45

Phần sụn (firmware)

Mã thực thi của mô-đun mật mã được lưu trữ trong phần cứng bên trong ranh giới mật mã và không thể được ghi hoặc sửa đổi động trong suốt quá trình thực hiện trong khi hoạt động trong một môi trường không thể sửa đổi hoặc bị giới hạn.

Ví dụ: Phần cứng lưu trữ có thể bao gồm nhưng không bị giới hạn như PROM, EEPROM, FLASH, bộ nhớ trạng thái cứng, ổ cứng, v.v...

3.46

Mô-đun phần sụn (firmware module)

Mô-đun mà nó được bao gồm duy nhất phần sụn.

3.47

Đặc tả chức năng (functional specification)

Mô tả mức cao các cổng và các giao diện có thể nhìn thấy được đối với người vận hành và mô tả mức cao hành vi của mô-đun mật mã đó.

3.48

Kiểm tra chức năng (functional testing)

Kiểm tra chức năng của mô-đun mật mã được xác định bởi đặc tả chức năng.

3.49

Độ cứng/cứng (hard/hardness)

Độ kháng tương đối của một kim loại hoặc vật liệu khác chống lại việc tạo ra vết lõm, trầy xước hoặc bẻ cong; bền chặt; bền chắc và bền lâu về mặt vật lý.

CHÚ THÍCH: Những độ kháng tương đối của vật liệu sẽ có thể bị xuyên thấu bởi một đối tượng khác.

3.50

Phần cứng (hardware)

Thiết bị/các thành phần vật lý nằm bên trong ranh giới mật mã được sử dụng để xử lý các chương trình và dữ liệu.

3.51

Mô-đun phần cứng (hardware module)

Mô-đun bao gồm chủ yếu là phần cứng, có thể cũng chứa cả phần sụn.

3.52

Giao diện mô-đun phần cứng (hardware module interface)

HMI (HMI)

Toàn bộ tập các lệnh được sử dụng để yêu cầu các dịch vụ của mô-đun phần cứng, bao gồm các tham số đi vào hoặc đi ra khỏi ranh giới mật mã của mô-đun như là một phần của dịch vụ được yêu cầu.

3.53

Giá trị băm (hash value)

Đầu ra của một hàm băm mật mã.

3.54

Mô-đun lai ghép (hybrid module)

Mô-đun mà có ranh giới mật mã phân giới hỗn hợp của một phần mềm hoặc phần sụn, thành phần và một thành phần phần cứng tách rời.

3.55

Giao diện mô-đun phần sụn lai ghép (hybrid firmware module interface)

HFMI (HFMI)

Toàn bộ tập các lệnh được sử dụng để yêu cầu các dịch vụ của mô-đun phần sụn lai ghép, bao gồm các tham số đi vào hoặc đi ra khỏi ranh giới mật mã của mô-đun như là một phần dịch vụ được yêu cầu.

3.56

Giao diện mô-đun phần mềm lai ghép (hybrid software module interface)

HSMI (HSMI)

Toàn bộ tập các lệnh được sử dụng để yêu cầu các dịch vụ của mô-đun phần mềm lai ghép, bao gồm các tham số đi vào hoặc đi ra khỏi ranh giới mật mã của mô-đun như là một phần dịch vụ được yêu cầu.

3.57

Dữ liệu đầu vào (input data)

Thông tin được nhập vào mô-đun mật mã và có thể được sử dụng nhằm các mục đích biến đổi hoặc tính toán bằng cách sử dụng một chức năng an toàn đã được phê duyệt.

3.58

Tính toàn vẹn (integrity)

Tính chất mà dữ liệu không bị sửa đổi hoặc bị xóa được một cách trái phép và không bị phát hiện.

3.59

Giao diện (interface)

Điểm đầu vào hoặc đầu ra lôgic của mô-đun mật mã cung cấp truy cập đến mô-đun cho các luồng thông tin lôgic.

3.60

Chấp nhận của ISO/IEC (ISO/IEC adopted)

Chức năng an toàn hoặc là:

- Được chỉ rõ trong một tiêu chuẩn của ISO/IEC, hoặc
- Được chấp thuận được khuyến cáo trong một tiêu chuẩn ISO/IEC và được chỉ rõ hoặc trong một phụ lục của tiêu chuẩn ISO/IEC hoặc trong một tài liệu được tham chiếu bởi tiêu chuẩn ISO/IEC.

3.61

Thỏa thuận khóa (key agreement)

Thủ tục thiết lập SSP nơi mà khóa có được là một hàm của thông tin bởi hai hay nhiều hơn các bên tham gia sao cho không có bên nào xác định trước được giá trị của khóa một cách độc lập mà không cần sự phối hợp của bên khác, sử dụng các phương pháp tự động.

3.62

Khóa mã hóa (encrypt) khóa (key encryption key)

KEK (KEK)

Khóa mật mã được sử dụng để mã hóa (encrypt) hoặc giải mã các khóa khác.

3.63

Bộ nạp khóa (key loader)

Thiết bị độc lập khép kín có khả năng lưu trữ ít nhất một SSP ở dạng rõ hoặc được mã hóa (encrypt) hoặc thành phần khóa có thể được truyền vào trong mô-đun mật mã khi có yêu cầu.

CHÚ THÍCH: Việc sử dụng một bộ nạp khóa yêu cầu thao tác của con người.

3.64

Quản lý khóa (key management)

Quản trị và sử dụng việc khởi tạo, đăng ký, chứng nhận, hủy đăng ký, phân phối, cài đặt, lưu giữ, lưu trữ, thu hồi, thu nhận và hủy bỏ nguyên liệu khóa tuân theo một chính sách an toàn.

3.65

Vận chuyển khóa (key transport)

Tiến trình chuyển một khóa từ một thực thể tới một thực thể khác sử dụng các phương pháp tự động.

3.66

Môi trường hoạt động hạn chế (limited operational environment)

Môi trường hoạt động được thiết kế để chỉ chấp nhận những thay đổi phần sụn được kiểm soát mà chúng vượt qua thành công kiểm tra nạp của phần sụn/phần mềm.

3.67

Kiểm tra mức thấp (low-level testing)

Kiểm tra các thành phần riêng lẻ hoặc nhóm các thành phần của mô-đun mật mã và các cổng vật lý và các giao diện lôgic của chúng.

3.68

Vai trò duy trì (maintenance role)

Vai trò được cho là thực hiện các dịch vụ duy trì lôgic và/hoặc vật lý.

VÍ DỤ: Các dịch vụ duy trì có thể bao gồm nhưng không giới hạn đối với các chẩn đoán phần mềm và/hoặc phần cứng.

3.69

Thủ công (manual)

Yêu cầu thao tác vận hành của con người.

3.70

Mã xác thực thông điệp (message authentication code)

MAC (MAC)

Giá trị tổng kiểm tra mật mã trên dữ liệu sử dụng một khóa đối xứng để phát hiện cả những sửa đổi tình cờ lẫn có chủ đích của dữ liệu.

VÍ DỤ: Một mã xác thực thông điệp dựa trên hàm băm.

3.71

Vi mã (microcode)

Các lệnh của bộ xử lý tương ứng với một lệnh chương trình thực thi.

VÍ DỤ: mã Assembler.

3.72

Entropy tối thiểu (minimum entropy)

Cận dưới của entropy là hữu ích trong việc xác định ước lượng trường hợp tồi nhất của entropy mẫu.

3.73

Môi trường hoạt động có thể sửa đổi (modifiable operational environment)

Môi trường hoạt động được thiết kế để chấp nhận các thay đổi chức năng có thể chứa phần mềm không được kiểm soát (tức là không đáng tin cậy).

3.74

Xác thực đa yếu tố (multi-factor authentication)

Xác thực với ít nhất hai yếu tố xác thực độc lập.

CHÚ THÍCH 1: Một yếu tố xác thực là một mẩu thông tin và tiến trình được sử dụng để xác thực hoặc kiểm tra định danh của một thực thể.

CHÚ THÍCH 2: Các phân loại yếu tố xác thực độc lập là: thứ gì đó bạn biết, thứ gì đó bạn có và thứ gì đó là bạn.

3.75

Mô-đun mật mã nhúng đa chíp (multiple-chip embedded cryptographic module)

Dạng thể hiện vật lý mà trong đó hai hay nhiều chíp mạch tích hợp (IC) được liên kết với nhau và được nhúng vào trong một vỏ bọc hoặc một sản phẩm có thể không được bảo vệ vật lý.

VÍ DỤ: Các adapter hoặc các bo mạch mở rộng.

3.76

Mô-đun mật mã đứng độc lập đa chíp (multiple-chip standalone cryptographic module)

Dạng thể hiện vật lý tại đó hai hay nhiều chip mạch tích hợp (IC) được liên kết với nhau và toàn bộ vỏ bọc được bảo vệ vật lý.

VÍ DỤ: Các bộ định tuyến mã hóa (encrypt) hoặc các máy phát vô tuyến an toàn.

3.77

Tài liệu hướng dẫn không dành cho người quản trị (non-administrator guidance)

Tài liệu viết ra được sử dụng bởi người sử dụng và/hoặc các vai trò không phải quản trị để vận hành mô-đun mật mã trong một chế độ hoạt động đã được phê duyệt.

CHÚ THÍCH: Tài liệu hướng dẫn phi người quản trị mô tả các chức năng an toàn của mô-đun mật mã và chứa thông tin và các thủ tục cho việc sử dụng an toàn mô-đun mật mã, bao gồm: các chỉ lệnh, các chỉ dẫn và các cảnh báo.

3.78

Tấn công không xâm lấn (non-invasive attack)

Tấn công mà có thể thực hiện trên mô-đun mật mã mà không cần tiếp xúc vật lý trực tiếp tới các thành phần bên trong ranh giới mật mã của mô-đun đó.

CHÚ THÍCH: Một tấn công mà nó không sửa đổi hoặc làm thay đổi trạng thái của mô-đun mật mã.

3.79

Môi trường hoạt động không thể sửa đổi (non-modifiable operational environment)

Môi trường hoạt động được thiết kế để không chấp nhận các thay đổi phần sụn.

3.80

Không liên quan đến an toàn (non-security relevant)

Các yêu cầu không được đề cập bên trong phạm vi của tiêu chuẩn này và không bao gồm các tham chiếu đến các tiến trình hoặc các chức năng an toàn không được phê duyệt hoặc đã được phê duyệt.

3.81

Hoạt động bình thường (normal operation)

Hoạt động mà tại đó toàn bộ tập các thuật toán, các chức năng, các dịch vụ hoặc các tiến trình an toàn là sẵn sàng và/hoặc có khả năng cấu hình được.

3.82

Chắn sáng (opaque)

Có thể chắn ánh sáng (tức là ánh sáng bên trong phổ nhìn thấy được có dải bước sóng từ 400nm đến 750nm); không trong suốt và cũng không mờ bên trong phổ nhìn thấy được.

3.83

Môi trường hoạt động (operational environment)

Tập hợp tất cả phần mềm và phần cứng gồm cả một hệ điều hành và nền phần cứng được yêu cầu để cho mô-đun hoạt động an toàn.

3.84

Trạng thái hoạt động (operational state)

Trạng thái mà tại đó các dịch vụ hoặc các chức năng có thể được yêu cầu bởi một người vận hành và dữ liệu tạo ra đầu ra từ giao diện đầu ra dữ liệu của mô-đun mật mã.

3.85

Người vận hành (operator)

Cá nhân hoặc một tiến trình (chủ thể) vận hành thay mặt cho cá nhân, được phép đảm nhận một hay nhiều vai trò.

3.86

Dữ liệu đầu ra (output data)

Thông tin hoặc các kết quả được tính toán được sinh ra từ mô-đun mật mã.

3.87

Ô xy hóa chống gỉ (passivation)

Hiệu ứng của một quá trình phản ứng trong các mối nối bán dẫn, các bề mặt hoặc các thành phần và các mạch tích hợp được xây dựng để bao gồm phương tiện bảo vệ và phát hiện.

VÍ DỤ: Dioxide silicon hoặc kính photpho

CHÚ THÍCH: Sự chống oxy hóa có thể làm thay đổi hành vi của mạch. Vật liệu chống oxy hóa là phụ thuộc vào công nghệ.

3.88

Mật khẩu (password)

Một xâu ký tự được sử dụng để xác thực một định danh hoặc để kiểm tra phân quyền truy cập.

VÍ DỤ: các chữ cái, các chữ số, và các ký hiệu khác

3.89

Số định danh cá nhân (personal identification number)

PIN (PIN)

Mã dạng số được sử dụng để xác thực một định danh.

3.90

Bảo vệ vật lý (physical protection)

Việc bảo vệ mô-đun mật mã, các CSP và các PSP, sử dụng phương thức vật lý.

3.91

Khóa dạng rõ (plaintext key)

Khóa mật mã chưa được mã hóa (encrypt) hoặc một khóa mật mã được làm cho mờ đi bằng các phương pháp chưa được phê duyệt được coi là khóa chưa được bảo vệ.

3.92

Cổng (port)

Điểm đầu vào hoặc đầu ra vật lý/lôgic của mô-đun mật mã cung cấp truy cập vào mô-đun đó.

3.93

Tự kiểm tra tiền hoạt động (pre-operational self-test)

Sự kiểm tra được thực hiện bởi mô-đun mật mã giữa thời điểm mô-đun mật mã được bật nguồn hoặc được khởi phiên (sau khi bị tắt nguồn, thiết lập lại, khởi động lại, khởi động nguội, bị ngắt nguồn điện,v.v...) và những chuyển tiếp đến trạng thái vận hành.

3.94

Khóa riêng (private key)

Khóa thuộc một cặp khóa phi đối xứng của một thực thể, thứ mà chỉ nên được sử dụng bởi thực thể đó.

CHÚ THÍCH: Trong trường hợp của một hệ thống chữ ký phi đối xứng thì khóa riêng xác định phép biến đổi chữ ký. Trong trường hợp của một hệ thống mã hóa (encrypt) phi đối xứng thì khóa riêng xác định phép biến đổi giải mã.

3.95

Sản phẩm đã được kiểm tra (production-grade)

Sản phẩm, thành phần, hoặc phần mềm đã được kiểm tra đáp ứng với các đặc tả hoạt động.

3.96

Khóa công khai (public key)

Khóa của một cặp khóa phi đối xứng của một thực thể mà nó có thể được công bố công khai.

CHÚ THÍCH 1: Trong trường hợp của một hệ thống ký số phi đối xứng thì khóa công khai xác định phép biến đổi kiểm tra. Trong trường hợp của một hệ thống mã hóa (encrypt) phi đối xứng thì khóa công khai xác định phép biến đổi mã hóa (encrypt). Một khóa "được biết một cách công khai" không nhất thiết phải luôn công bố toàn cầu. Khóa đó có thể chỉ được công bố cho tất cả các thành viên thuộc một nhóm chỉ định trước.

CHÚ THÍCH 2: Đối với các mục đích của tiêu chuẩn này, các khóa công khai không được cho là các CSP.

3.97

Chứng thư khóa công khai (public key certificate)

Thông tin khóa công khai của một thực thể được ký số bởi một thẩm quyền chứng thực phù hợp và vì thế được làm cho không thể bị giả mạo.

3.98

Thuật toán mật mã khóa công khai (phi đối xứng) (public key (asymmetric) cryptographic algorithm)

Thuật toán mật mã sử dụng hai khóa liên quan với nhau, khóa công khai và khóa riêng.

CHÚ THÍCH: Hai khóa này có tính chất là nhận được khóa riêng từ khóa công khai là không thể được về mặt tính toán.

3.99

Tham số an toàn công khai (public security parameter)

PSP (PSP)

Thông tin công khai liên quan đến tính an toàn mà sự sửa đổi nó có thể làm tổn hại đến sự an toàn của mô-đun mật mã.

VÍ DỤ: Các khóa mật mã công khai, các chứng thư khóa công khai, các chứng thư được tự ký, các mỏ neo tin cậy, các mật khẩu một lần liên kết với một bộ đếm và ngày tháng và thời gian được lưu giữ bên trong.

CHÚ THÍCH: Một PSP được cho là được bảo vệ nếu nó không thể bị sửa đổi hoặc nếu việc sửa đổi nó có thể được xác định bởi mô-đun đó.

3.100

Bộ sinh bit ngẫu nhiên (random bit generator)

RBG (RBG)

Thiết bị hoặc thuật toán đưa ra một dãy các bít xuất hiện độc lập về mặt thống kê và không bị thiên lệch.

3.101

Vỏ có thể tháo rời (removeable cover)

Phương cách vật lý cho phép một truy cập không làm hư hại được thiết kế có chủ đích tới các nội dung vật lý của mô-đun mật mã.

3.102

Vai trò (role)

Thuộc tính an toàn gắn kết với một người sử dụng, xác định các quyền truy cập hoặc những hạn chế của người sử dụng đến các dịch vụ của mô-đun mật mã.

CHÚ THÍCH: Một hoặc nhiều dịch vụ có thể được gắn kết với một vai trò. Một vai trò có thể được gắn kết với một hoặc nhiều người sử dụng và một người sử dụng có thể đảm nhiệm một hoặc nhiều vai trò.

3.103

Kiểm soát truy cập dựa trên vai trò (role-based access control)

RBAC (RBAC)

Các cho phép được gán cho một vai trò cho phép truy cập tới một đối tượng.

3.104

Môi trường thời gian chạy (runtime environment)

Trạng thái máy ảo cung cấp các dịch vụ phần mềm cho các tiến trình hoặc các chương trình trong khi máy tính đang chạy.

CHÚ THÍCH: Nó đi đôi với chính hệ điều hành hoặc phần mềm chạy bên dưới nó. Mục đích đầu tiên là thực hiện mục đích của lập trình "độc lập nền"

3.105

Khóa bí mật (secret key)

Khóa mật mã, được sử dụng với thuật toán mật mã khóa bí mật được gắn kết duy nhất với một hoặc nhiều thực thể và không được công khai.

3.106

Chức năng an toàn (security function)

Các thuật toán mật mã cùng với các chế độ hoạt động, như mã khối, mã dòng, thuật toán khóa đối xứng, phi đối xứng, mã xác thực thông điệp, hàm băm, hoặc các chức năng an toàn khác, bộ tạo bit ngẫu nhiên, xác thực thực thể và sinh và thiết lập SSP tất cả được phê duyệt hoặc là bởi ISO/IEC hoặc là bởi một thẩm quyền phê duyệt.

CHÚ THÍCH: Xem phụ lục C.

3.107

Khóa mầm (seed key)

Giá trị bí mật được sử dụng để khởi hoạt một bộ sinh bít ngẫu nhiên.

3.108

Các tự kiểm tra (self-tests)

Bộ các tự kiểm tra có điều kiện và tiền hoạt động được thực hiện dựa trên yêu cầu của người vận hành hoặc định kỳ sau một thời gian hoạt động tối đa và trong các điều kiện được chỉ ra trong chính sách an toàn.

3.109

Dữ liệu nhạy cảm (sensitive data)

Dữ liệu theo cách nhìn của người sử dụng, yêu cầu sự bảo vệ.

3.110

Các tham số an toàn nhạy cảm (sensitive security parameters)

SSP (SSP)

Các tham số an toàn quan trọng (CSP) và các tham số an toàn công khai (PSP).

3.111

Dịch vụ (service)

Chức năng hoặc/và hoạt động được viện đến của người vận hành bên ngoài bất kỳ có thể được thực hiện bởi mô-đun mật mã.

3.112

Đầu vào dịch vụ (service input)

Tất cả các dữ liệu hoặc thông tin điều khiển được sử dụng bởi mô-đun mật mã khởi động hoặc đạt được các hoạt động hay các chức năng cụ thể.

3.113

Đầu ra dịch vụ (service output)

Tất cả dữ liệu và thông tin các trạng thái là kết quả của các hoạt động hay các chức năng được khởi động hoặc đạt được bởi đầu vào dịch vụ.

3.114

Phân tích điện năng đơn giản (simple power analysis)

SPA (SPA)

Sự phân tích trực tiếp (chủ yếu bằng trực quan) các mẫu thực hiện chỉ lệnh (hoặc việc thực hiện các chỉ lệnh riêng lẻ) liên quan đến việc tiêu thụ điện năng của mô-đun mật mã, nhằm mục đích trích rút ra thông tin có tương quan với một hoạt động mật mã.

3.115

Mô-đun mật mã đơn chip (single-chip cryptographic module)

Dạng thể hiện vật lý mà ở đó chỉ có một chip mạch tích hợp (IC) có thể được sử dụng như một thiết bị đứng độc lập hoặc có thể được nhúng vào bên trong một vỏ bọc hoặc một sản phẩm có thể chưa được bảo vệ về mặt vật lý.

VÍ DỤ: Các chip mạch tích hợp IC đơn hoặc các thẻ thông minh có chỉ một chip mạch tích hợp IC.

3.116

Phần mềm (software)

Mã thực hiện của mô-đun mật mã được lưu trữ trong đa phương tiện có khả năng xóa, có thể được ghi và được sửa đổi động trong quá trình thực hiện trong khi đang hoạt động trong một môi trường vận hành có thể sửa đổi.

VÍ DỤ: Đa phương tiện có thể xóa có thể bao gồm nhưng không giới hạn đối với các bộ nhớ trạng thái cứng, ổ đĩa cứng, v.v...

3.117

Mô-đun phần mềm (software module)

Mô-đun mà chỉ bao gồm duy nhất phần mềm.

3.118

Kiểm tra việc nạp phần mềm/ phần sụn (software/firmware load test)

Tập các kiểm tra được thực hiện trên phần mềm hoặc phần sụn mà nó buộc phải vượt qua một cách thành công trước khi nó có thể được thực hiện bởi mô-đun mật mã.

CHÚ THÍCH: Không áp dụng được nếu phần mềm hoặc phần sụn là một sự thay thế hình ảnh toàn bộ và được thực hiện chỉ sau một vòng cấp nguồn điện cho mô-đun.

3.119

Giao diện mô-đun phần mềm/phần sụn (software/firmware module interface)

SFMI (SFMI)

Tập các lệnh được sử dụng để yêu cầu các dịch vụ của mô-đun phần sụn hoặc phần mềm, bao gồm các tham số đi vào hoặc đi ra khỏi ranh giới mật mã của mô-đun như là một phần của dịch vụ đã được yêu cầu.

3.120

Phân chia thông tin (split knowledge)

Quá trình mà bởi nó khóa mật mã được phân chia thành nhiều thành phần khóa, chia sẻ riêng rẽ không mang thông tin về khóa ban đầu mà nó có thể sau đó là đầu vào hoặc đầu ra của mô-đun mật mã bởi các thực thể tách biệt và được kết hợp lại để tái tạo ra khóa mật mã ban đầu.

CHÚ THÍCH: Tất cả hoặc một tập con các thành phần có thể được yêu cầu để thực hiện việc kết hợp.

3.121

Thiết lập SSP (SSP establishment)

Quá trình làm cho một SSP được chia sẻ trở thành sẵn sàng cho một hoặc nhiều thực thể

CHÚ THÍCH: Thiết lập SSP bao gồm thỏa thuận SSP, vận chuyển SSP và nhập vào hoặc xuất ra SSP

3.122

Thông tin trạng thái (status information)

Thông tin là đầu ra từ mô-đun mật mã với các mục đích chỉ ra các đặc tính hoặc các trạng thái hoạt động nhất định của mô-đun đó.

3.123

Bền (strong)

Không dễ dàng bị đánh bại, có sức mạnh hay năng lực lớn hơn so với trung bình hoặc kỳ vọng, có khả năng chịu đựng tấn công hoặc được xây dựng vững chắc.

3.124

Kỹ thuật mật mã đối xứng (symmetric cryptographic technique)

Kỹ thuật mật mã sử dụng cùng một khóa mật cho cả phép biến đổi mã hóa (encrypt) và giải mã.

3.125

Phát hiện xâm phạm (tamper detection)

Xác định tự động bởi mô-đun mật mã rằng có một nỗ lực đã được thực hiện nhằm làm tổn hại đến an toàn của mô-đun đó.

3.126

Bằng chứng xâm phạm (tamper evidence)

Dấu hiệu quan sát được rằng có một nỗ lực đã được thực hiện nhằm làm tổn hại đến sự an toàn của mô-đun.

3.127

Đáp trả xâm phạm (tamper response)

Hành động tự động được thực hiện bởi mô-đun mật mã khi sự phát hiện xâm phạm đã xảy ra.

3.128

Mỏ neo tin cậy (trust anchor)

Thông tin được tin cậy bao gồm thuật toán khóa công khai, một giá trị khóa công khai, tên người phát hành, và các tham số tùy chọn khác.

VÍ DỤ: Các tham số khác có thể bao gồm nhưng không bị giới hạn trong thời kỳ hợp lệ.

CHÚ THÍCH: Một mỏ neo tin cậy có thể được cung cấp dưới dạng một chứng thư tự ký.

3.129

Kênh tin cậy (trusted channel)

Đường truyền an toàn và tin cậy được thiết lập giữa mô-đun mật mã và một người gửi hoặc người nhận để truyền an toàn các CSP dạng rõ chưa được bảo vệ, các thành phần khóa và dữ liệu xác thực.

CHÚ THÍCH: Một kênh tin cậy bảo vệ chống lại việc nghe trộm cũng như xâm phạm vật lý hoặc lôgic bởi các thực thể/người vận hành không mong muốn, các tiến trình hoặc các thiết bị khác giữa các cổng vào hoặc ra được xác định của mô-đun và dọc theo đường truyền với điểm cuối có chủ đích.

3.130

Người dùng (user)

Vai trò được thực hiện bởi một cá nhân hoặc một tiến trình (tức là chủ thể) hành động nhân danh một cá nhân truy cập vào mô-đun mật mã để đạt được các dịch vụ mật mã.

3.131

Được kiểm tra hợp lệ (validated)

Đảm bảo sự đáp ứng đã được kiểm tra bởi một thẩm quyền kiểm tra hợp lệ.

3.132

Thẩm quyền kiểm tra hợp lệ (validation authority)

Thực thể sẽ kiểm tra hợp lệ các kết quả kiểm tra đối với việc đáp ứng đối với tiêu chuẩn này.

3.133

Nhà cung cấp (vendor)

Thực thể, nhóm hoặc hiệp hội đệ trình mô-đun mật mã để kiểm tra và kiểm tra hợp lệ.

CHÚ THÍCH: Nhà cung cấp có quyền truy cập đến tất cả các bằng chứng thiết kế và tài liệu có liên quan, không quan trọng là họ có thiết kế hay phát triển mô-đun mật mã hay không.

3.134

Xóa trắng (zeroisation)

Phương thức phá hủy dữ liệu đã lưu trữ và các SSP không được bảo vệ để ngăn chặn khả năng khôi phục và tái sử dụng.

4 Từ viết tắt

Đối với các mục đích của tài liệu này, các thuật ngữ được viết tắt sau đây được áp dụng.

CHÚ THÍCH: Các thuật ngữ viết tắt đưa ra ở phần này được lấy từ thuật ngữ tiếng Anh. Phần giải nghĩa tiếng Việt được đưa vào cho mục đích tham chiếu.

Từ viết tắt	Tiếng Anh	Tiếng Việt
API	Application Program Interface	Giao diện lập trình ứng dụng
CBC	Cipher Block Chaining	Chế độ móc xích khối mã
CCM	Counter with Cipher block chaining-Message authentication code	Bộ đếm với chế độ móc xích khối mã – Mã xác thực thông điệp
ECB	Electronic Code Book	Chế độ sách mã điện tử
HDL	Hardware Description Language	Ngôn ngữ mô tả phần cứng
IC	Integrated Circuit	Mạch tích hợp
PROM	Programmable Read-Only Memory	Bộ nhớ chỉ đọc lập trình được
RAM	Random Access Memory	Bộ nhớ truy cập ngẫu nhiên

URL	Uniform Resource Locator	Bộ định vị tài nguyên thống nhất

5 Các mức an toàn của mô-đun mật mã

Các điều nhỏ sau đây cung cấp một cái nhìn tổng quan về bốn mức an toàn. Các ví dụ chung được đưa ra để minh họa cho việc các yêu cầu được đáp ứng như thế nào, mà không có mục đích chỉ giới hạn ở đó hoặc bao quát toàn bộ. Trong tài liệu này, tham chiếu đến mô-đun sẽ được hiểu là tham chiếu tới mô-đun *mật mã*. Các kỹ thuật mật mã là như nhau cho cả bốn mức an toàn. Mỗi mức an toàn áp đặt các mức yêu cầu an toàn tăng dần của các yêu cầu an toàn đối với việc bảo vệ chính mô-đun đó (chẳng hạn như truy cập và thông tin về các thành phần và hoạt động bên trong) và các SSP được chứa và được kiểm soát bên trong mô-đun. Mỗi yêu cầu an toàn được nhận biết bằng ký hiệu **shall [xx.yy]** trong đó **xx** cho biết điều và **yy** là chỉ mục bằng số bên trong điều.

5.1 Mức an toàn 1

Mức an toàn 1 cung cấp một mức cơ sở về an toàn. Các yêu cầu an toàn cơ bản được chỉ rõ đối với mô-đun mật mã (chẳng hạn, ít nhất một chức năng an toàn đã được phê duyệt hoặc một phương pháp thiết lập tham số an toàn nhạy cảm đã được phê duyệt sẽ được sử dụng). Các mô-đun phần mềm hoặc phần sụn có thể hoạt động trong một môi trường hoạt động không thể sửa đổi, bị hạn chế hoặc có thể sửa đổi. Không có các cơ chế an toàn vật lý cụ thể nào được yêu cầu trong mô-đun mật mã phần cứng ở Mức an toàn 1 ngoài yêu cầu cơ bản cho các thành phần sản phẩm đã được kiểm tra. Các phương pháp giảm thiểu không xâm lấn hoặc sự giảm thiểu các tấn công khác mà chúng được thực thi được tài liệu hóa. Các ví dụ về mô-đun mật mã ở Mức an toàn 1 là một bo mạch phần cứng được mã hóa (encrypt) được tìm thấy trong một máy tính cá nhân (PC) hoặc một bộ công cụ mật mã thực thi trong một thiết bị cầm tay hoặc một máy tính mục đích thông thường.

Các thực thi như vậy là phù hợp một cách lý tưởng đối với các ứng dụng an toàn nơi mà các kiểm soát như an toàn vật lý, an toàn mạng, và các thủ tục quản lý được cung cấp bên ngoài mô-đun chứ không phải bên trong môi trường tại đó mô-đun được triển khai. Ví dụ, thực thi mô-đun mật mã Mức an toàn 1 có thể có lợi hơn trong các môi trường như vậy so với các mô-đun tương ứng tại các mức đảm bảo cao hơn mà chúng cung cấp độ an toàn lớn hơn cho các mô-đun SSP làm cho các tổ chức phải lựa chọn các giải pháp mật mã khác nhau để đáp ứng các yêu cầu an toàn nơi mà sự chú ý đến môi trường tại đó mô-đun đang hoạt động là cốt yếu trong việc cung cấp độ an toàn tổng thể.

5.2 Mức an toàn 2

Mức an toàn 2 tăng cường các cơ chế an toàn vật lý của Mức an toàn 1 bằng cách bổ sung thêm yêu cầu đối với bằng chứng xâm phạm bao gồm việc sử dụng các lớp phủ phát hiện bằng chứng xâm phạm hoặc các dấu niêm phong hoặc các khóa chống trộm cấp trên các vỏ ngoài hoặc các cửa tháo rời được.

Các lớp phủ ngoài hoặc các dấu niêm phong bằng chứng xâm phạm được đặt lên mô-đun sao cho việc phủ ngoài hoặc niêm phong phải bị phá vỡ mới đạt được truy cập vật lý đến các SSP bên trong mô-đun đó. Các dấu niêm phong hoặc các khóa chống trộm cấp làm bằng chứng xâm phạm được đặt lên các vỏ ngoài hay các cửa để bảo vệ chống lại truy cập vật lý trái phép.

Mức an toàn 2 đòi hỏi xác thực dựa trên vai trò mà trong đó, mô-đun mật mã xác thực quyền được phép của người vận hành để đảm nhận một vai trò cụ thể và thực thi một tập tương ứng các dịch vụ.

Mức an toàn 2 cho phép mô-đun mật mã phần mềm được thực thi trong môi trường có thể sửa đổi để thực thi các kiểm soát truy cập dựa trên vai trò hoặc tối thiểu là quyền kiểm soát truy cập tùy chọn theo

thực tế với cơ chế tin cậy xác định các nhóm mới và gán các quyền cho phép hạn chế thông qua các danh sách kiểm soát truy cập (chẳng hạn các ACL), và với khả năng gán mỗi người sử dụng vào nhiều hơn một nhóm và nó bảo vệ chống lại việc thực thi, sửa đổi, và đọc phần mềm mật mã trái phép.

5.3 Mức an toàn 3

Thêm vào các cơ chế an toàn vật lý bằng chứng xâm phạm được yêu cầu tại Mức an toàn 2, Mức an toàn 3 còn cung cấp các yêu cầu bổ sung để giảm thiểu truy cập trái phép tới các SSP bên trong mô-đun mật mã. Các cơ chế an toàn vật lý được yêu cầu tại Mức an toàn 3 nhằm phát hiện với xác suất cao để phát hiện và đáp trả các nỗ lực truy cập vật lý trực tiếp, sử dụng hoặc sửa đổi mô-đun mật mã và thăm dò thông qua các lỗ hổng hoặc các khe hở thông gió. Các cơ chế an toàn vật lý có thể bao gồm việc sử dụng các vỏ bọc chắc chắn và kết cấu mạch phát hiện/đáp trả xâm phạm, chúng xóa trắng tất cả các CSP khi các cửa/các vỏ bọc tháo rời được của mô-đun mật mã bị mở ra.

Mức an toàn 3 đòi hỏi các cơ chế xác thực dựa trên định danh, tăng cường an toàn được cung cấp bởi các cơ chế xác thực dựa trên vai trò được chỉ rõ đối với Mức an toàn 2. Mô-đun mật mã xác thực định danh của một người vận hành và kiểm tra rằng người vận hành được định danh được trao quyền đảm nhiệm một vai trò cụ thể và thực hiện một tập tương ứng các dịch vụ.

Mức an toàn 3 yêu cầu các CSP dạng rõ được thiết lập thủ công sẽ phải được mã hóa (encrypt), sử dụng một kênh tin cậy hoặc sử dụng một thủ tục phân chia thông tin đối với đầu vào và đầu ra.

Mức an toàn 3 cũng bảo vệ mô-đun mật mã chống lại việc xâm hại an toàn do các điều kiện môi trường nằm ngoài các dải hoạt động bình thường của mô-đun đối với điện áp và nhiệt độ, những dịch chuyển có chủ đích nằm ngoài các dải hoạt động bình thường có thể được sử dụng bởi một kẻ tấn công để cản trở những bảo vệ của mô-đun mật mã. Mô-đun mật mã được yêu cầu để hoặc bao gồm các đặc tính bảo vệ môi trường đặc biệt được thiết kế để phát hiện khi nào các giới hạn nhiệt độ và điện thế bị vượt quá và xóa trắng các CSP hoặc trải qua việc kiểm tra sai sót môi trường nghiêm ngặt để cung cấp một sự đảm bảo hợp lý rằng mô-đun sẽ không bị ảnh hưởng khi nằm bên ngoài dải hoạt động bình thường theo cách mà nó có thể xâm hại an toàn của mô-đun đó.

Các phương pháp giảm thiểu tấn công không xâm lấn được chỉ rõ trong 7.8 mà chúng được thực thi trong mô-đun và được kiểm tra theo các thước đo tại Mức an toàn 3.

Mức an toàn 3 không được đề xuất trong tất cả điều khoản của tiêu chuẩn này đối với các mô-đun mật mã phần mềm, vì vậy mức an toàn cao nhất tổng thể có thể đạt được bởi mô-đun mật mã phần mềm bị giới hạn ở Mức an toàn 2.

Các mô-đun ở Mức an toàn 3 yêu cầu những bảo đảm vòng đời bổ sung như: quản lý cấu hình tự động, thiết kế chi tiết, kiểm tra mức thấp, và xác thực người vận hành sử dụng thông tin xác thực được cung cấp bởi nhà cung cấp.

5.4 Mức an toàn 4

Mức an toàn 4 cung cấp mức an toàn cao nhất được xác định trong tiêu chuẩn này. Mức an toàn này bao gồm tất cả các đặc tính an toàn thích hợp của các mức thấp hơn cũng như các đặc tính an toàn mở rộng.

Tại Mức an toàn 4, các cơ chế an toàn vật lý cung cấp một gói bọc bảo vệ đầy đủ xung quanh mô-đun mật mã với chủ đích phát hiện và đáp trả tất cả các nỗ lực truy cập vật lý trái phép khi các SSP được chứa trong mô-đun cho dù việc cấp điện ngoài có được áp dụng hay không. Việc xâm nhập lớp vỏ mô-đun mật mã từ bất kỳ hướng nào có một xác suất rất cao để bị phát hiện, dẫn đến việc xóa trắng ngay lập tức tất cả các SSP không được bảo vệ. Các mô-đun mật mã tại Mức an toàn 4 là hữu ích đối với hoạt động trong các môi trường không được bảo vệ về mặt vật lý.

Mức an toàn 4 đưa ra yêu cầu xác thực đa yếu tố để xác thực người vận hành. Ít nhất điều này yêu cầu hai trong số 3 thuộc tính sau:

- Một thứ gì đó được biết, chẳng hạn như một mật khẩu bí mật,
- Một thứ gì đó được sở hữu, chẳng hạn như một thẻ hoặc khóa vật lý,
- Một tính chất vật lý, chẳng hạn như sinh trắc.

Tại Mức an toàn 4, mô-đun mật mã được yêu cầu phải bao gồm các đặc tính bảo vệ môi trường đặc biệt được thiết kế để phát hiện các giới hạn điện áp và nhiệt độ và xóa trắng các CSP để cung cấp đảm bảo hợp lý rằng mô-đun sẽ không bị ảnh hưởng khi nằm ngoài dải hoạt động bình thường theo cách mà nó có thể gây tổn hại cho an toàn của mô-đun đó.

Các phương pháp giảm thiểu tấn công không xâm lấn được chỉ rõ trong 7.8 mà nó được thực thi trong mô-đun, được kiểm tra theo các thước đo tại Mức an toàn 4.

Mức an toàn 4 không được đề xuất trong tất cả các điều khoản của tiêu chuẩn này đối với các mô-đun mật mã phần mềm, vì vậy mức an toàn cao nhất tổng thể có thể đạt được bởi các mô-đun mật mã phần mềm bị giới hạn ở Mức an toàn 2.

Thiết kế mô-đun ở Mức an toàn 4 được kiểm tra bởi sự tương ứng giữa cả các điều kiện tiền trạng thái và hậu trạng thái và đặc tả chức năng.

6. Các mục tiêu an toàn chức năng

Các yêu cầu an toàn được chỉ rõ trong tiêu chuẩn này liên quan đến thiết kế và thực thi mô-đun mật mã. Các yêu cầu an toàn bắt đầu từ mức cơ sở và tăng dần theo mức các mục tiêu an toàn. Các yêu cầu này nhận được từ các mục tiêu an toàn chức năng mức cao sau đây đối với mô-đun mật mã để:

- Sử dụng và thực thi đúng các chức năng an toàn đã được phê duyệt để bảo vệ thông tin nhạy cảm;
- Bảo vệ mô-đun mật mã khỏi việc sử dụng hoặc vận hành trái phép;
- Ngăn chặn sự tiết lộ trái phép các nội dung của mô-đun mật mã, bao gồm các CSP;
- Ngăn chặn việc sửa đổi trái phép và không bị phát hiện đối với mô-đun mật mã và các thuật toán mật mã, bao gồm việc sửa đổi, thay thế, chèn thêm và xóa bỏ trái phép các SSP;
- Cung cấp các chỉ dẫn về trạng thái hoạt động của mô-đun mật mã;
- Đảm bảo rằng mô-đun mật mã thực hiện đúng đắn khi vận hành trong chế độ hoạt động đã được phê duyệt;
- Phát hiện các lỗi trong quá trình hoạt động của mô-đun và ngăn chặn các tổn hại đến các SSP gây ra từ các lỗi này; và
- Đảm bảo thiết kế, phân phối và thực thi đúng đắn mô-đun mật mã.

7 Các yêu cầu an toàn

7.1 Yêu cầu chung

Điều khoản này chỉ rõ các yêu cầu an toàn mà **shall [01.01]** cần được thỏa mãn bằng việc tuân thủ chuẩn này của mô-đun mật mã. Các yêu cầu an toàn bao quát hết các lĩnh vực liên quan đến thiết kế và sự thực thi mô-đun mật mã. Các lĩnh vực này bao gồm đặc tả mô-đun mật mã; các giao diện mô-đun mật mã; các vai trò, các dịch vụ và xác thực; an toàn phần mềm/phần sụn; môi trường hoạt động; an toàn vật lý; an toàn không xâm lấn; quản lý tham số an toàn nhạy cảm; các tự kiểm tra; đảm bảo vòng đời; và giảm thiểu các tấn công khác.

Bảng 1 tổng kết các yêu cầu an toàn trong mỗi lĩnh vực trong các lĩnh vực này.

Mô-đun mật mã **shall [01.02]** được kiểm tra theo các yêu cầu của từng lĩnh vực được đề cập trong điều khoản này. Mô-đun mật mã **shall [01.03]** được xếp loại một cách độc lập trong từng lĩnh vực. Một số lĩnh vực cung cấp các mức an toàn tăng dần bằng cách tích lũy các yêu cầu an toàn cho từng mức. Trong các lĩnh vực này, mô-đun mật mã sẽ nhận được một sự xếp loại mà nó phản ánh mức an toàn cao nhất mà đối với nó mô-đun sẽ đáp ứng tất cả các yêu cầu của lĩnh vực đó. Trong các lĩnh vực mà chúng không cung cấp đối với các mức an toàn khác nhau (tức là một tập chuẩn các yêu cầu), thì mô-đun mật mã sẽ nhận được một xếp loại tương xứng với xếp loại tổng thể.

Ngoài việc nhận được các xếp loại độc lập đối với mỗi lĩnh vực an toàn, mô-đun mật mã cũng sẽ nhận được một sự xếp loại an toàn tổng thể. Xếp loại an toàn tổng thể sẽ chỉ ra mức tối thiểu của các xếp loại độc lập nhận được trong các lĩnh vực.

Nhiều yêu cầu an toàn của tiêu chuẩn này bao gồm các yêu cầu về tài liệu mà chúng được tổng kết lại trong các Phụ lục A và B. Tất cả tài liệu, bao gồm các bản sách hướng dẫn thực thi và người sử dụng, các đặc tả thiết kế, tài liệu vòng đời **shall [01.04]** được cung cấp đối với mô-đun mật mã, mà nó sẽ phải trải qua một kiểm tra độc lập hoặc một lược đồ kiểm.

Các Phụ lục C, D, E và F cung cấp các tham chiếu đến các chức năng an toàn được phê duyệt, các phương pháp thiết lập tham số an toàn nhạy cảm được phê duyệt, các cơ chế xác thực đã được phê duyệt và các phương pháp kiểm tra giảm thiểu tấn công không xâm lấn.

Bảng 1 – Tóm tắt các yêu cầu an toàn

	Mức an toàn 1	**Mức an toàn 2**	**Mức an toàn 3**	**Mức an toàn 4**
Đặc tả mô-đun mật mã	Đặc tả mô-đun mật mã, ranh giới mật mã, các chức năng an toàn đã được phê duyệt và các chế độ hoạt động bình thường và xuống cấp. Mô tả về mô-đun mật mã bao gồm tất cả thành phần phần cứng, phần mềm và phần sụn. Tất cả các dịch vụ cung cấp thông tin trạng thái để chỉ ra khi nào dịch vụ sử dụng thuật toán mật mã, chức năng hoặc tiến trình an toàn đã được phê duyệt theo cách thức được phê duyệt.			
Các giao diện của mô-đun mật mã	Các giao diện yêu cầu và tùy chọn. Đặc tả của tất cả các giao diện và tất cả các đường dẫn dữ liệu đầu vào và đầu ra.		Kênh tin cậy.	
Các vai trò, các dịch vụ và sự xác thực	Phân tách lôgic của các vai trò và các dịch vụ yêu cầu và tùy chọn.	Xác thực người vận hành dựa trên vai trò hoặc dựa trên định danh.	Xác thực người vận hành dựa trên định danh	Xác thực đa yếu tố.
An toàn phần mềm/ phần sụn	Kỹ thuật toàn vẹn đã được phê duyệt được xác định là SFMI, HFMI và HSMI. Mã thực thi.	Kiểm tra toàn vẹn dựa trên mã xác thực thông báo có khóa hoặc chữ ký số đã được phê duyệt.	Kiểm tra toàn vẹn dựa trên chữ ký số đã được phê duyệt.	
Môi trường hoạt	Có thể sửa đổi hoặc bị giới hạn,	Có thể sửa đổi.		

động	không thể sửa đổi. Kiểm soát các SSP.	Kiểm soát truy cập tùy theo thực tế hoặc dựa trên vai trò. Cơ chế kiểm toán.		
An toàn vật lý	Các thành phần bền chắc.	Bằng chứng xâm phạm. Che đậy hoặc bao bọc chắn sáng.	Phát hiện và đáp trả xâm phạm đối với các che đậy hoặc các cửa. Bảo vệ các lớp vỏ bọc hoặc bao bọc mạnh. chống lại thăm dò trực tiếp, EFP hoặc EFT.	Bọc gói phát hiện và đáp trả xâm phạm. EFP. Giảm thiểu tiêm chèn lỗi.
An toàn không xâm lấn	Mô-đun được thiết kế để làm giảm thiểu các tấn công không xâm lấn được chỉ rõ trong Phụ lục F.			
	Tài liệu và tính hiệu quả của các kỹ thuật giảm thiểu được chỉ rõ trong Phụ lục F.		Kiểm tra sự giảm thiểu.	Kiểm tra sự giảm thiểu.
Quản lý tham số an toàn nhạy cảm	Các bộ sinh bít ngẫu nhiên, sinh, thiết lập, đầu vào, đầu ra, lưu trữ và xóa trắng SSP.			
	Vận chuyển SSP tự động hoặc thỏa thuận SSP sử dụng các phương pháp đã được phê duyệt.			
	Các SSP được thiết lập thủ công có thể đưa vào hoặc xuất ra ở dạng rõ.		Các SSP được thiết lập thủ công có thể được nhập vào hoặc xuất ra hoặc ở dạng đã được mã hóa thông qua một kênh tin cậy, hoặc sử dụng các thủ tục phân tách thông tin.	
Các tự kiểm tra	Trước khi hoạt động: Kiểm tra các chức năng quan trọng và bỏ qua, tính toàn vẹn của phần mềm/phần sụn.			
	Có điều kiện: Kiểm tra các chức năng quan trọng và bỏ qua có điều kiện, đầu vào thủ công, nạp phần mềm/phần sụn, tính kiên định theo cặp, thuật toán mật.			
Đảm bảo vòng đời	Quản lý cấu hình	Hệ thống quản lý cấu hình đối với mô-đun mật mã, các thành phần và tài liệu. Mỗi hệ thống này được nhận biết duy nhất và được theo dõi trong suốt vòng đời.	Hệ thống quản lý cấu hình tự động.	
	Thiết kế	Mô-đun được thiết kế cho phép kiểm tra tất cả các dịch vụ liên quan đến an toàn được cung cấp.		

	FSM	Mô hình trạng thái hữu hạn.		
	Phát triển	Mã nguồn được chú giải, các sơ đồ hoặc HDL.	Ngôn ngữ bậc cao phần mềm. Ngôn ngữ mô tả bậc cao phần cứng.	Tài liệu được chú giải với các tiền điều kiện trên đầu vào vào các thành phần mô-đun và các hậu điều kiện được kỳ vọng là đúng khi các thành phần được hoàn thành.
	Kiểm tra	Kiểm tra chức năng.	Kiểm tra mức thấp.	
	Phân phối và hoạt động	Các thủ tục khởi hoạt.	Các thủ tục phân phối.	Xác thực người vận hành sử dụng thông tin xác thực được cung cấp bởi nhà cung cấp.
	Hướng dẫn	Tài liệu hướng dẫn cho người quản trị và không phải quản trị.		
Giảm thiểu các tấn công khác		Đặc tả việc giảm thiểu các tấn công mà đối với chúng, không có các yêu cầu có thể kiểm tra được hiện đang sẵn có.		Đặc tả việc giảm thiểu các tấn công với các yêu cầu có thể kiểm tra được.

7.2 Đặc tả mô-đun mật mã

7.2.1 Các yêu cầu chung đối với đặc tả mô-đun mật mã

Mô-đun mật mã **shall [02.01]** là một tập phần cứng, phần mềm, phần sụn, hoặc một tổ hợp nào đó trong số đó mà nó ít nhất thực thi một dịch vụ mật mã được xác định sử dụng một quá trình hoặc chức năng an toàn, thuật toán mật mã được phê duyệt và được chứa bên trong một ranh giới mật mã đã được xác định.

Các yêu cầu về mặt tài liệu được chỉ rõ trong A.2.2 **shall [02.02]** được cung cấp.

7.2.2 Các kiểu mô-đun mật mã

Mô-đun mật mã **shall [02.03]** được xác định là một trong số những kiểu mô-đun sau:

- ***Mô-đun phần cứng*** là mô-đun mà ranh giới mật mã của nó được chỉ rõ tại một đường biên vòng ngoài phần cứng. Phần sụn và/hoặc phần mềm cũng có thể bao gồm cả một hệ điều hành, cũng có thể nằm trong ranh giới mật mã phần cứng này.
- ***Mô-đun phần mềm*** là mô-đun mà ranh giới mật mã của nó phân định (các) thành phần dành riêng của phần mềm (có thể là một hoặc nhiều thành phần phần mềm) thành phần (những thành phần) thực thi trong môi trường hoạt động có thể sửa đổi. Nền tính toán và hệ điều hành

của môi trường hoạt động nơi mà phần mềm thực thi nằm ngoài ranh giới mô-đun phần mềm được xác định.

- ***Mô-đun phần sụn*** là mô-đun mà ranh giới mật mã của nó phân định (các) thành phần dành riêng của phần sụn, thành phần (các thành phần) mà thực thi trong một môi trường hoạt động bị giới hạn hoặc không thể sửa đổi. Nền tính toán và hệ điều hành của môi trường hoạt động nơi mà phần sụn thực thi nằm ngoài ranh giới mô-đun phần sụn đã được xác định nhưng bị ràng buộc rõ ràng đối với mô-đun phần sụn.
- ***Mô-đun phần mềm lai ghép*** là mô-đun mà ranh giới mật mã của nó phân định sự kết hợp của một thành phần phần mềm và một thành phần phần cứng tách rời (tức là, thành phần phần mềm không được chứa bên trong ranh giới mô-đun phần cứng). Nền tính toán và hệ điều hành của môi trường hoạt động nơi mà phần mềm thực thi là bên ngoài ranh giới mô-đun phần mềm lai ghép đã được xác định.
- ***Mô-đun phần sụn lai ghép*** là mô-đun mà ranh giới mật mã của nó phân định sự kết hợp một thành phần phần sụn và một thành phần phần cứng tách rời (tức là, thành phần phần sụn không được chứa bên trong ranh giới mô-đun phần cứng). Nền tính toán và hệ điều hành của môi trường hoạt động nơi mà phần sụn thực thi là bên ngoài ranh giới mô-đun phần sụn lai ghép đã được xác định nhưng bị ràng buộc rõ ràng đối với mô-đun phần sụn lai ghép.

Đối với các mô-đun phần mềm thực thi trong một môi trường sửa đổi được, các yêu cầu về an toàn vật lý và an toàn không xâm lấn được tìm thấy trong 7.7 và 7.8 là tùy chọn.

Đối với các mô-đun phần cứng và phần sụn, các yêu cầu về an toàn vật lý và an toàn không xâm lấn được tìm thấy trong 7.7 và 7.8 **shall [02.04]** được áp dụng.

Đối với các mô-đun lai ghép, (các) thành phần phần mềm và phần sụn **shall [02.05]** đáp ứng tất cả các yêu cầu áp dụng được của 7.5 và 7.6. (Các) thành phần phần cứng **shall [02.06]** đáp ứng tất cả các yêu cầu áp dụng được của 7.7 và 7.8.

7.2.3 Ranh giới mật mã

7.2.3.1 Các yêu cầu chung về ranh giới mật mã

Ranh giới mật mã **shall [02.07]** bao gồm một đường biên được xác định ở dạng hiển (tức là, một tập các thành phần phần cứng, phần mềm, hoặc phần sụn) thiết lập ranh giới của tất cả các thành phần của mô-đun mật mã. Các yêu cầu của tiêu chuẩn này **shall [02.08]** cần áp dụng cho tất cả các thuật toán, các chức năng an toàn, các tiến trình và các thành phần bên trong ranh giới mật mã của mô-đun. Mô-đun mật mã **shall [02.09]** cần tối thiểu bao gồm tất cả các thuật toán liên quan đến an toàn, các chức năng an toàn, các tiến trình và các bộ phận của mô-đun mật mã (tức là, liên quan an toàn bên trong phạm vi của tiêu chuẩn này). Các thuật toán không liên quan đến an toàn, các chức năng an toàn, các tiến trình hoặc các thành phần có thể được chứa bên trong ranh giới mật mã. Các thuật toán không liên quan đến an toàn, các chức năng an toàn, các tiến trình hoặc các thành phần cũng có thể được sử dụng trong một chế độ hoạt động đã được phê duyệt. Các thuật toán không liên quan đến an toàn, các chức năng an toàn, các tiến trình hoặc các thành phần mà chúng được sử dụng trong một chế độ hoạt động đã được phê duyệt **shall [02.10]** được thực thi theo cách thức để không can thiệp hay làm tổn hại đến hoạt động đã được phê duyệt của mô-đun mật mã.

Tên được xác định của mô-đun mật mã **shall [02.11]** là đại diện của tổ hợp các thành phần bên trong ranh giới mật mã và không là đại diện của một tổ hợp hay một sản phẩm lớn hơn. Mô-đun mật mã **shall [02.12],** tối thiểu, chứa thông tin đánh số phiên bản cụ thể đại diện cho các thành phần phần cứng, phần mềm và/hoặc phần sụn cá thể riêng biệt.

Các thành phần phần cứng, phần mềm và/hoặc phần sụn bên trong ranh giới có thể được loại trừ khỏi các yêu cầu của tiêu chuẩn này. Các thành phần phần cứng, phần mềm hoặc phần sụn được loại trừ **shall [02.13]** cần được thực thi theo cách không can thiệp hay làm tổn hại đến hoạt động an toàn đã được phê duyệt của mô-đun mật mã. Phần cứng, phần mềm hoặc phần sụn được loại trừ **shall [02.14]** được chỉ rõ (Phụ lục A).

7.2.3.2 Các định nghĩa của ranh giới mật mã.

Ranh giới mật mã của mô-đun mật mã phần cứng **shall [02.15]** phân định và nhận biết:

- Tập hợp các thành phần phần cứng có thể bao gồm:
  - Các cấu trúc vật lý, bao gồm: các bảng mạch, các lớp nền, hoặc các lớp bề mặt nâng lên khác, những thứ cung cấp dây dẫn điện kết nối vật lý với nhau,
  - Các thành phần điện tích cực như các mạch tích hợp bán dẫn, các mạch tích hợp tùy chỉnh hay các mạch tích hợp chung, các bộ xử lý, bộ nhớ, các nguồn cung cấp điện, các bộ chuyển đổi, v.v...
  - Các cấu trúc vật lý như các lớp bao quanh, các vật liệu vỏ bọc hoặc đóng bình, các bộ kết nối và các giao diện,
  - Phần sụn mà nó có thể bao gồm hệ điều hành,
  - Các loại thành phần khác không được liệt kê ở trên.

Ranh giới mật mã của mô-đun **mật mã phần mềm shall [02.16]** phân định và nhận biết:

- Một tập tệp hoặc các tệp mã thực thi cấu thành mô-đun mật mã; và
- Sự khởi phiên của mô-đun mật mã được lưu trong bộ nhớ và được thực hiện bởi một hoặc nhiều bộ xử lý.

Ranh giới mật mã của mô-đun **mật mã phần sụn shall [02.17]** phân định và nhận biết:

- Một tập tệp hoặc các tệp mã thực thi cấu thành mô-đun mật mã; và
- Sự khởi phiên của mô-đun mật mã được lưu trong bộ nhớ và được thực hiện bởi một hoặc nhiều bộ xử lý.

Ranh giới mật mã của mô-đun **mật mã** lai ghép **shall [02.18]**:

- Là kết hợp của ranh giới thành phần phần cứng của mô-đun và (các) ranh giới thành phần phần sụn hoặc phần mềm tách rời; và
- Bao gồm tập hợp tất cả các cổng và các giao diện từ mỗi một thành phần.

Ngoài (các) thành phần phần mềm hoặc phần sụn tách rời, thành phần phần cứng cũng có thể bao gồm phần sụn hoặc phần mềm nhúng.

7.2.4 Các chế độ hoạt động

7.2.4.1 Các yêu cầu chung của các chế độ hoạt động

Người vận hành **shall [02.19]** có khả năng vận hành mô-đun trong một chế độ hoạt động đã được phê duyệt. Chế độ hoạt động đã được phê duyệt **shall [02.20]** được xác định là một tập các dịch vụ mà nó chứa ít nhất một dịch vụ sử dụng thuật toán mật mã đã được phê duyệt, chức năng hoặc tiến trình an toàn và các dịch vụ hoặc các tiến trình đó được chỉ rõ trong 7.4.3.

Các thuật toán mật mã không được phê duyệt, các chức năng an toàn, và các tiến trình hoặc các dịch vụ khác không được chỉ rõ trong 7.4.3 **shall [02.21]** không được sử dụng bởi người vận hành trong

một chế độ hoạt động đã được phê duyệt trừ khi thuật toán mật mã hoặc chức năng an toàn không được phê duyệt là một phần của một tiến trình đã được phê duyệt và không liên quan về mặt an toàn đến hoạt động của các tiến trình đã được phê duyệt (chẳng hạn, thuật toán mật mã không được phê duyệt hoặc một khóa được tạo ra không được phê duyệt có thể được sử dụng để làm mờ dữ liệu hoặc các CSP nhưng kết quả được coi là bản rõ không được bảo vệ và không cung cấp chức năng liên quan đến an toàn cho đến khi được bảo vệ với thuật toán mật mã đã được phê duyệt).

7.2.4.2 Hoạt động bình thường

Hoạt động bình thường là nơi mà tập hợp đầy đủ các thuật toán, các chức năng an toàn, các dịch vụ hoặc các tiến trình là sẵn sàng và/hoặc cấu hình được.

Các CSP **shall [02.22]** phân biệt giữa các dịch vụ và các chế độ hoạt động đã được phê duyệt và không được phê duyệt (chẳng hạn, không được chia sẻ hoặc không được truy nhập). Đầu ra của một RBG đã được phê duyệt có thể được cung cấp cho thuật toán, chức năng hoặc tiến trình an toàn không được phê duyệt mà không có sự xóa trắng của mầm RBG chừng nào mầm đó không thể được truy cập trong chế độ không được phê duyệt.

Chính sách an toàn của mô-đun **shall [02.23]** xác định một tập hợp hoàn chỉnh các dịch vụ mà chúng được cung cấp đối với mỗi một chế độ hoạt động đã được xác định (cả chế độ đã được phê duyệt và không được phê duyệt).

Tất cả các dịch vụ **shall [02.24]** cung cấp một bộ chỉ báo khi dịch vụ sử dụng thuật toán mật mã, chức năng hoặc tiến trình an toàn đã được phê duyệt theo cách thức đã được phê duyệt và các dịch vụ hoặc các tiến trình đó được chỉ rõ trong 7.4.3.

7.2.4.3 Hoạt động bị xuống cấp

Mô-đun mật mã có thể được thiết kế để hỗ trợ chức năng bị xuống cấp nếu mô-đun đi vào trạng thái có lỗi. Đối với mô-đun mật mã để hoạt động trong chế độ bị xuống cấp, các điều sau đây **shall [02.25]** áp dụng:

- Hoạt động bị xuống cấp **shall [02.26]** xảy ra chỉ sau khi đi ra khỏi một trạng thái có lỗi;
- Mô-đun **shall [02.27]** cung cấp thông tin trạng thái khi hoạt động được tái cấu hình và bị xuống cấp xảy ra.
- Cơ chế hay chức năng thất bại **shall [02.28]** được cách ly;
- Tất cả các tự kiểm tra thuật toán có điều kiện **shall [02.29]** được thực hiện trước lần hoạt động đầu tiên của thuật toán mật mã sau khi đi vào hoạt động bị xuống cấp; và
- Các dịch vụ **shall [02.30]** cung cấp một bộ chỉ báo nếu những nỗ lực đang được tiến hành để sử dụng một tiến trình, chức năng an toàn hoặc thuật toán không hoạt động.

Mô-đun mật mã **shall [02.31]** giữ nguyên trong hoạt động bị xuống cấp cho đến lúc nào mà mô-đun mật mã vượt qua mà không thất bại tất cả các tự kiểm tra tiền hoạt động và có điều kiện một cách thành công. Nếu mô-đun mật mã thất bại đối với các tự kiểm tra tiền hoạt động thì mô-đun **shall not [02.32]** đi vào trạng thái hoạt động bị xuống cấp.

7.3 Các giao diện của mô-đun mật mã

7.3.1 Các yêu cầu chung về các giao diện của mô-đun mật mã

Mô-đun mật mã **shall [03.01]** hạn chế toàn bộ luồng thông tin logic, chỉ các điểm truy cập vật lý và các giao diện logic nào được nhận biết là các điểm vào và ra đến và đi khỏi ranh giới mật mã của mô-đun. Các giao diện lôgic của mô-đun mật mã **shall [03.02]** là tách biệt với nhau cho dù chúng có thể chia sẻ một cổng vật lý (chẳng hạn dữ liệu đầu vào có thể đi vào và dữ liệu đầu ra có thể đi ra thông qua cùng

một cổng vật lý), hoặc phải được phân phối trên một hoặc nhiều cổng vật lý (chẳng hạn, dữ liệu đầu vào có thể được đưa vào thông qua cả cổng tuần tự và cổng song song). Giao diện lập trình ứng dụng (API) của một thành phần phần mềm của mô-đun mật mã có thể được xác định là một hoặc nhiều giao diện lôgic.

Các yêu cầu về tài liệu được chỉ rõ trong A.2.3 **shall [03.03]** được cung cấp.

7.3.2 Các kiểu giao diện

- *Giao diện mô-đun phần cứng (HMI):* Toàn bộ tập hợp các giao diện sử dụng để yêu cầu các dịch vụ của mô-đun phần cứng, bao gồm các tham số đi vào hoặc đi ra khỏi ranh giới mật mã của mô-đun như là một phần của dịch vụ được yêu cầu.
- *Giao diện mô-đun phần mềm hoặc phần sụn (SFMI):* Toàn bộ tập hợp các giao diện được sử dụng để yêu cầu các dịch vụ của mô-đun phần mềm hoặc phần sụn, bao gồm các tham số đi vào vào hoặc đi ra khỏi ranh giới mật mã của mô-đun như là một phần của dịch vụ được yêu cầu.
- *Giao diện mô-đun phần mềm lai ghép hoặc phần sụn lai ghép (HSMI hoặc HFMI):* Toàn bộ tập hợp các giao diện được sử dụng để yêu cầu các dịch vụ của mô-đun phần mềm lai ghép hoặc phần sụn lai ghép gồm các tham số đi vào hoặc đi ra khỏi ranh giới mật mã của mô-đun như là một phần của dịch vụ được yêu cầu.

7.3.3 Định nghĩa các giao diện

Mô-đun mật mã **shall [03.04]** có năm giao diện sau ("đầu vào" và "đầu ra" được chỉ ra từ góc độ của mô-đun đó):

1. *Giao diện đầu vào dữ liệu.* Tất cả các dữ liệu (ngoại trừ dữ liệu điều khiển được nhập vào thông qua giao diện đầu vào điều khiển) được nhập vào và được xử lý bởi mô-đun mật mã (bao gồm dữ liệu dữ liệu bản rõ, dữ liệu bản mã, các SSP, và thông tin trạng thái từ mô-đun khác) **shall [03.05]** đi vào thông qua giao diện "đầu vào dữ liệu". Dữ liệu có thể được chấp nhận bởi mô-đun thông qua giao diện đầu vào dữ liệu trong khi mô-đun đang thực hiện các tự kiểm tra (7.10).
2. *Giao diện đầu ra dữ liệu.* Tất cả các dữ liệu (ngoại trừ đầu ra dữ liệu trạng thái thông qua giao diện đầu ra trạng thái và giao diện đầu ra điều khiển) mà nó được đưa ra khỏi mô-đun mật mã (bao gồm dữ liệu bản rõ, dữ liệu bản mã, và các SSP) **shall [03.06]** thoát ra thông qua giao diện "đầu ra dữ liệu". Tất cả đầu ra dữ liệu thông qua giao diện "đầu ra dữ liệu" **shall [03.07]** bị chặn lại trong khi thực hiện nhập vào, các tự kiểm tra tiền hoạt động, nạp và xóa trắng phần mềm/phần sụn bằng thủ công; hoặc khi mô-đun mật mã ở trong một trạng thái có lỗi.
3. *Giao diện đầu vào điều khiển.* Tất cả các lệnh, các tín hiệu đầu vào (ví dụ, đầu vào xung nhịp) và dữ liệu điều khiển đầu vào (bao gồm các lời gọi hàm và các điều khiển thủ công như các chuyển mạch, các nút bấm, và các bàn phím) được sử dụng để điều khiển hoạt động của mô-đun mật mã **shall [03.08]** đi vào thông qua giao diện "đầu vào điều khiển".
4. *Giao diện đầu ra điều khiển.* Tất cả các lệnh, các tín hiệu, và dữ liệu điều khiển đầu ra (ví dụ các lệnh điều khiển đối với mô-đun khác) được sử dụng để điều khiển hoặc chỉ ra trạng thái hoạt động của mô-đun mật mã **shall [03.09]** thoát ra thông qua giao diện "đầu ra điều khiển". Toàn bộ đầu ra điều khiển thông qua giao diện "đầu ra điều khiển" **shall [03.10]** bị chặn lại khi mô-đun mật mã ở trong trạng thái có lỗi trừ khi các ngoại lệ được chỉ rõ và được tài liệu hóa trong chính sách an toàn.

5. *Giao diện đầu ra trạng thái.* Tất cả các tín hiệu, các bộ chỉ báo (ví dụ, bộ chỉ báo lỗi) và dữ liệu trạng thái (bao gồm các mã trả về và các bộ chỉ báo vật lý trực quan (màn hình, các đèn chỉ báo) âm thanh (còi, âm, chuông) và cơ học (sự giao động)) đầu ra được sử dụng để chỉ ra trạng thái của mô-đun mật mã **shall [03.11]** thoát ra thông qua giao diện "đầu ra trạng thái". Đầu ra trạng thái có thể là hiển hoặc ẩn.

Ngoại trừ đối với các mô-đun mật mã phần mềm, tất cả các mô-đun **shall [03.12]** cũng có giao diện sau đây:

- *Giao diện nguồn điện.* Tất cả nguồn điện bên ngoài được đưa vào mô-đun mật mã **shall [03.13]** đi vào thông qua một giao diện nguồn điện. Giao diện nguồn điện không được yêu cầu khi tất cả nguồn điện được cung cấp hoặc duy trì bên trong ranh giới mật mã của mô-đun mật mã (chẳng hạn, một bộ pin bên trong).

Mô-đun mật mã **shall [03.14]** phân biệt giữa dữ liệu, thông tin điều khiển, và nguồn điện cho đầu vào và thông tin trạng thái và điều khiển, dữ liệu cho đầu ra.

Đặc tả mô-đun mật mã **shall [03.15]** theo một cách không nhập nhằng, chỉ rõ định dạng của dữ liệu đầu vào và thông tin điều khiển, bao gồm các hạn chế độ dài đối với tất cả các đầu vào có độ dài thay đổi.

7.3.4 Kênh tin cậy

Kênh tin cậy là đường kết nối được thiết lập giữa mô-đun mật mã và người gửi hoặc người nhận để trao đổi một cách an toàn các CSP dạng rõ, các thành phần khóa và dữ liệu xác thực chưa được bảo vệ. Kênh tin cậy bảo vệ chống lại nghe lén, cũng như các can thiệp vật lý hoặc lôgic bởi những người vận hành/các thực thể, các tiến trình hoặc các thiết bị khác không mong muốn, giữa các cổng đầu vào hoặc đầu ra được xác định của mô-đun và dọc theo đường kết nối liên lạc với điểm cuối người gửi hoặc người nhận được dự định.

MỨC AN TOÀN 1 VÀ 2

Đối với Mức an toàn 1 và 2, không có các yêu cầu đối với kênh tin cậy.

MỨC AN TOÀN 3

Đối với Mức an toàn 3,

- Đối với việc truyền các CSP bản rõ, các thành phần khóa mật mã, và dữ liệu xác thực chưa được bảo vệ giữa mô-đun mật mã và người gửi hoặc các người nhận đầu cuối, mô-đun mật mã **shall [03.16]** thực thi một kênh tin cậy;
- Kênh tin cậy **shall [03.17]** ngăn chặn sửa đổi, thay thế, và tiết lộ trái phép dọc theo đường kết nối liên lạc;
- Các cổng vật lý được sử dụng cho kênh tin cậy **shall [03.18]** được tách biệt về mặt vật lý khỏi tất cả các cổng hoặc các giao diện lôgic khác được sử dụng cho kênh tin cậy **shall [03.19]** được tách biệt về mặt lôgic khỏi tất cả các giao diện khác;
- Sự xác thực dựa trên định danh **shall [03.20]** được sử dụng cho tất cả các dịch vụ sử dụng kênh tin cậy; và
- Một bộ chỉ báo trạng thái **shall [03.21]** được cung cấp khi kênh tin cậy đang được sử dụng.

MỨC AN TOÀN 4

Ngoài các yêu cầu của mức an toàn 3, đối với Mức an toàn 4, xác thực dựa trên định danh đa yếu tố **shall [03.22]** được sử dụng cho tất cả các dịch vụ sử dụng kênh tin cậy.

7.4 Các vai trò, các dịch vụ và xác thực

7.4.1 Các yêu cầu chung về các vai trò, các dịch vụ và xác thực

Mô-đun mật mã **shall [04.01]** hỗ trợ các vai trò được cho phép đối với những người vận hành và các dịch vụ tương ứng bên trong mỗi vai trò. Một người vận hành đơn lẻ có thể đảm nhiệm nhiều vai trò. Nếu mô-đun mật mã hỗ trợ nhiều người vận hành cùng một lúc, khi đó mô-đun **shall [04.02]** duy trì nội tại sự phân tách của các vai trò được đảm nhiệm bởi mỗi người vận hành và các dịch vụ tương ứng. Người vận hành không được yêu cầu để đảm nhiệm cho một vài trò đã được cho phép để thực hiện các dịch vụ mà ở đó các CPS và các PSP không bị sửa đổi, tiết lộ hoặc thay thế (ví dụ, chỉ ra trạng thái, các tự kiểm tra, hoặc các dịch vụ khác mà chúng không làm ảnh hưởng đến sự an toàn của mô-đun).

Các cơ chế xác thực có thể được yêu cầu trong mô-đun mật mã để xác thực người vận hành truy cập tới mô-đun, và để kiểm tra rằng người vận hành đó được cho phép để đảm nhiệm vai trò đã được yêu cầu và thực thi các dịch vụ bên trong vai trò đó.

Các yêu cầu về tài liệu được chỉ rõ tại Phụ lục A.2.4 **shall [04.04]** được cung cấp.

7.4.2 Các vai trò

Mô-đun mật mã **shall [04.04],** tối thiểu, hỗ trợ một *Vai trò chuyên viên mật mã (Crypto Officer Role). Vai trò Chuyên viên mật mã* **shall [04.05]** được đảm nhiệm để thực hiện khởi hoạt mật mã hoặc các chức năng quản lý, và các dịch vụ an toàn chung (ví dụ khởi hoạt mô-đun, quản lý các CSP, các PSP và các chức năng kiểm toán).

Mô-đun mật mã có thể hỗ trợ *Vai trò Người sử dụng*. Nếu mô-đun mật mã hỗ trợ vai trò người sử dụng, thì *Vai trò Người sử dụng* **shall [04.06]** được đảm nhiệm để thực hiện các dịch vụ an toàn chung, bao gồm các hoạt động mật mã và các chức năng an toàn đã được phê duyệt khác.

Mô-đun mật mã có thể hỗ trợ một *Vai trò duy trì. Vai trò duy trì* là vai trò được đảm nhiệm trong suốt các dịch vụ duy trì vật lý và/hoặc lôgic (ví dụ như mở các vỏ bọc dịch vụ, thực hiện một số chuẩn đoán nhất định như tự kiểm tra được xây dựng sẵn (BIST)). Tất cả các SSP không được bảo vệ **shall [04.07]** được xóa trắng khi đi vào hoặc đi ra khỏi vai trò duy trì.

Mô-đun mật mã có thể hỗ trợ các vai trò khác hoặc ngoài các vai trò được chỉ rõ trên đây.

7.4.3 Các dịch vụ

7.4.3.1 Các yêu cầu chung về các dịch vụ

Các dịch vụ **shall [04.08]** tham chiếu đến tất cả dịch vụ, các hoạt động hoặc các chức năng mà chúng có thể được thực hiện bởi mô-đun. Các đầu vào dịch vụ **shall [04.09]** bao gồm tất cả các đầu vào dữ liệu hoặc điều khiển đến mô-đun khởi hoạt hoặc đạt được các dịch vụ, các hoạt động hoặc các chức năng cụ thể. Các đầu ra dịch vụ **shall [04.10]** bao gồm tất cả các đầu ra dữ liệu và trạng thái mà chúng là kết quả từ các dịch vụ, các hoạt động, hoặc các chức năng được khởi hoạt hay đạt được bởi các đầu vào dịch vụ. Mỗi đầu vào dịch vụ **shall [04.11]** tạo ra một đầu ra dịch vụ.

Mô-đun mật mã **shall [04.12]** cung cấp các dịch vụ sau tới những người vận hành:

1. *Chỉ ra thông tin đánh số phiên bản của mô-đun.* Mô-đun mật mã **shall [04.13]** xuất ra tên hoặc bộ định danh mô-đun và thông tin đánh số phiên bản mà chúng có thể là tương quan với một bộ dữ liệu kiểm tra hợp lệ (ví dụ: thông tin đánh số phiên bản phần cứng, phần mềm và/hoặc phần sụn).
2. *Chỉ ra trạng thái.* Mô-đun mật mã **shall [04.14]** xuất ra trạng thái hiện tại. Điều này có thể bao gồm đầu ra của các bộ chỉ trạng thái để đáp ứng với một yêu cầu dịch vụ.

3. *Thực hiện các tự kiểm tra.* Mô-đun mật mã **shall [04.15]** khởi hoạt và chạy các tự kiểm tra tiền hoạt động như được chỉ rõ trong 7.10.2.
4. *Thực hiện các chức năng an toàn đã được phê duyệt.* Mô-đun mật mã **shall [04.16]** thực hiện ít nhất một chức năng an toàn đã được phê duyệt được sử dụng trong một chế độ hoạt động đã được phê duyệt như đã được chỉ rõ trong 7.2.
5. *Thực hiện việc xóa trắng.* Mô-đun mật mã **shall [04.17]** thực hiện xóa trắng các tham số như được chỉ rõ trong 7.9.7.

Mô-đun mật mã có thể cung cấp các dịch vụ, các hoạt động, hoặc các chức năng khác, cả được phê duyệt, và không được phê duyệt, ngoài các dịch vụ được chỉ rõ trên đây. Các dịch vụ cụ thể có thể được cung cấp trong nhiều hơn một vai trò (ví dụ các dịch vụ nhập khóa có thể được cung cấp trong vai trò Người sử dụng và vai trò Chuyên viên mật mã).

7.4.3.2 Khả năng bỏ qua

Khả năng bỏ qua là khả năng của một dịch vụ bỏ qua một phần hoặc toàn bộ một chức năng hoặc một tiến trình mật mã. Nếu mô-đun có thể xuất ra một mục tin trạng thái hoặc dữ liệu đặc biệt trong một dạng được bảo vệ bằng mật mã, hay (như một kết quả của việc cấu hình mô-đun hoặc can thiệp người hoạt động) cũng có thể xuất ra mục tin ở một dạng không được bảo vệ, thì khả năng bỏ qua **shall [04.18]** được xác định.

Nếu mô-đun mật mã thực thi một *khả năng bỏ qua*, thì:

- Người vận hành **shall [04.19]** đảm nhiệm một vai trò được cho phép trước khi cấu hình khả năng bỏ qua;
- Hai hành động bên trong độc lập nhau **shall [04.20]** được yêu cầu để kích hoạt khả năng ngăn chặn sự bỏ qua không cố ý của dữ liệu bản rõ do một lỗi đơn lẻ. Hai hành động bên trong độc lập này **shall [04.21]** sửa đổi hành vi của phần mềm và/hoặc phần cứng mà nó được dành để dàn xếp khả năng bỏ qua (chẳng hạn hai cờ hiệu phần mềm hoặc phần cứng khác nhau được thiết lập, một trong hai cờ đó được khởi hoạt bởi người dùng), và
- Mô-đun **shall [04.22]** chỉ ra trạng thái để chỉ ra xem liệu có phải là khả năng bỏ qua không:
    1. Không được kích hoạt, và mô-đun đang dành riêng cung cấp các dịch vụ có xử lý mật mã (ví dụ dữ liệu bản rõ được mã hóa (encrypt)), hoặc
    2. Được kích hoạt và mô-đun đang dành riêng cung cấp các dịch vụ không có xử lý mật mã (ví dụ dữ liệu bản rõ không được mã hóa (encrypt)), hoặc
    3. Được kích hoạt và vô hiệu hóa chọn một trong hai và mô-đun đang cung cấp một số dịch vụ có xử lý mật mã và một số dịch vụ không có xử lý mật mã (ví dụ, đối với các mô-đun với nhiều kênh truyền thông, dữ liệu bản rõ có thể được mã hóa (encrypt) hoặc không được mã hóa (encrypt) tùy thuộc vào cấu hình của mỗi kênh).

7.4.3.3 Khả năng đầu ra mật mã tự khởi hoạt

Khả năng đầu ra mật mã tự khởi hoạt là khả năng của mô-đun thực hiện các thao tác mật mã và các chức năng an toàn được phê duyệt hoặc các kỹ thuật quản lý SSP khác mà không cần yêu cầu của người vận hành bên ngoài. Khả năng đầu ra mật mã tự khởi hoạt **shall [04.23]** được cấu hình bởi Chuyên viên mật mã và cấu hình này ta có thể được bảo toàn suốt chu kỳ cung cấp điện, khởi động lại hay tái thiết lập của mô-đun.

Nếu mô-đun mật mã thực thi *khả năng đầu ra mật mã tự khởi hoạt*, lúc đó:

- Hai hành động bên trong độc lập **shall [04.24]** được yêu cầu để kích hoạt khả năng này nhằm ngăn chặn đầu ra không cố ý gây ra bởi một lỗi đơn lẻ. Hai hành động bên trong độc lập **shall [04.25]** sẽ sửa đổi hành vi của phần mềm và/hoặc phần cứng mà nó được dành để dàn xếp khả năng này (chẳng hạn, hai cờ hiệu mềm hoặc cứng khác nhau được thiết lập, một trong chúng có thể được khởi hoạt bởi người dùng), và
- Mô-đun **shall [04.26]** chỉ ra trạng thái để cho biết xem *khả năng đầu ra mật mã tự khởi hoạt* có được kích hoạt hay không.

7.4.3.4 Sự nạp phần mềm/phần sụn

Nếu mô-đun mật mã có Khả năng nạp phần mềm/phần sụn từ một nguồn ngoài thì các yêu cầu sau **[04.27]** được áp dụng:

- Phần mềm hoặc phần sụn được nạp vào **shall [04.28]** được kiểm tra hợp lệ bởi một thẩm quyền kiểm tra hợp lệ trước khi nạp nhằm duy trì kiểm tra hợp lệ;
- Tất cả đầu ra dữ liệu thông qua giao diện đầu ra dữ liệu **shall [04.29]** bị chặn lại cho đến khi nạp và kiểm tra nạp phần mềm/phần sụn hoàn thành thành công;
- *Kiểm tra nạp phần mềm/phần sụn* được chỉ rõ tại 7.10.3.4 **shall [04.30]** được thực hiện trước khi mã được nạp có thể được thực hiện;
- Mô-đun mật mã **shall [04.31]** từ chối thực thi bất kì các chức năng an toàn được phê duyệt được nạp vào hoặc được sửa đổi cho đến sau khi các tự kiểm tra tiền hoạt động tại 7.10.2 được thực hiện thành công; và
- Thông tin đánh số phiên bản mô-đun **shall [04.32]** được sửa đổi để thể hiện bổ sung và/hoặc cập nhật của phần mềm hoặc phần sụn mới được nạp vào (7.4.3)

Nếu việc nạp phần mềm hoặc phần sụn là một sự thay thế hình ảnh hoàn toàn, thì việc này **shall [04.33]** thiết lập mô-đun mới hoàn toàn mô-đun này có thể yêu cầu kiểm tra hợp lệ bởi một thẩm quyền kiểm tra hợp lệ để duy trì kiểm tra hợp lệ. Hình ảnh phần mềm hoặc phần sụn mới **shall [04.34]** chỉ được thực thi sau khi chuyển đổi trạng thái của mô-đun thông qua việc bật lại nguồn điện. Tất cả các SSP bị xóa trắng trước khi thực hiện hình ảnh mới.

7.4.4 Xác thực

Các cơ chế xác thực có thể được yêu cầu bên trong mô-đun mật mã để xác thực người vận hành truy cập vào mô-đun và để kiểm tra rằng người vận hành được cho phép để đảm nhiệm vai trò được yêu cầu và thực hiện các dịch vụ bên trong vai trò đó. Các kiểu các cơ chế sau được sử dụng để kiểm soát truy cập vào mô-đun mật mã:

- *Xác thực dựa trên vai trò:* Nếu các cơ chế xác thực dựa trên vai trò được hỗ trợ bởi mô-đun mật mã, mô-đun **shall [04.36]** yêu cầu rằng một hoặc nhiều vai trò hoặc được lựa chọn ẩn hoặc được lựa chọn hiển bởi người vận hành, và **shall [04.37]** xác thực sự đảm nhiệm của vai trò được lựa chọn (hoặc tập hợp các vai trò). Mô-đun mật mã không được yêu cầu để xác thực theo định danh cá nhân của người vận hành. Việc lựa chọn các vai trò và việc xác thực sự đảm nhiệm của các vai trò được lựa chọn có thể được kết hợp với nhau. Nếu mô-đun mật mã cho phép một người vận hành thay đổi các vai trò, khi đó mô-đun **shall [04.38]** xác thực sự đảm nhiệm của bất kỳ vai trò nào mà nó đã không được xác thực trước đó đối với người vận hành đó.
- *Xác thực dựa trên định danh:* Nếu các cơ chế xác thực dựa trên định danh được hỗ trợ bởi mô-đun mật mã, mô-đun **shall [04.39]** yêu cầu rằng người vận hành sẽ được định danh một cách duy nhất và riêng biệt, **shall [04.40]** yêu cầu rằng một hoặc nhiều vai trò hoặc được lựa chọn

ẩn hoặc được lựa chọn hiển bởi người vận hành, và **shall [04.41]** xác thực sự định danh của người vận hành và phân quyền của người vận hành để đảm nhiệm vai trò hoặc tập hợp các vai trò đã lựa chọn. Việc xác thực định danh của người vận hành, lựa chọn các vai trò và phân quyền đảm nhiệm các vai trò được lựa chọn có thể được kết hợp. Nếu mô-đun mật mã cho phép một người vận hành thay đổi các vai trò, khi đó mô-đun này **shall [04.42]** kiểm tra phân quyền của người vận hành đã được định danh để đảm nhiệm bất kỳ vai trò nào mà nó đã không được phân quyền trước đó.

Mô-đun mật mã có thể cho phép người vận hành đã được xác thực thực hiện tất cả các dịch vụ được cho phép bên trong một vai trò đã được cho phép, hoặc có thể yêu cầu xác thực tách biệt cho mỗi dịch vụ hoặc cho các tập hợp các dịch vụ khác nhau. Khi mô-đun mật mã được tái thiết lập, khởi động lại, tắt nguồn và bật lại sau đó, mô-đun này **shall [04.43]** yêu cầu người vận hành phải được xác thực.

Các kiểu dữ liệu xác thực khác nhau có thể được yêu cầu bởi mô-đun mật mã để thực thi các cơ chế xác thực được hỗ trợ, bao gồm (nhưng không giới hạn) sự hiểu biết hay quyền sở hữu một mật khẩu, số PIN, khóa mật mã hoặc tương đương; quyền sở hữu một khóa vật lý, thẻ khóa hoặc tương đương; hoặc việc kiểm tra các đặc trưng cá nhân (ví dụ sinh trắc). Dữ liệu xác thực bên trong mô-đun mật mã **shall [04.44]** được bảo vệ tránh khỏi việc sử dụng, tiết lộ, sửa đổi và thay thế trái phép. Các chức năng an toàn được phê duyệt có thể được sử dụng như là một phần của cơ chế xác thực.

Sự khởi hoạt của các cơ chế xác thực có thể đảm bảo cách giải quyết đặc biệt. Nếu mô-đun mật mã không chứa dữ liệu xác thực được yêu cầu để xác thực người vận hành đối với lần đầu tiên mô-đun được truy cập, khi đó các phương pháp được phân quyền khác (chẳng hạn như các kiểm soát thủ tục, hoặc việc sử dụng dữ liệu xác thực thiết lập sẵn bởi nhà sản xuất hoặc sử dụng dữ liệu xác thực mặc định) **shall [04.45]** được sử dụng để kiểm soát truy cập đến mô-đun và khởi hoạt các cơ chế xác thực. Nếu dữ liệu xác thực mặc định được sử dụng để kiểm soát truy nhập tới mô-đun, khi đó dữ liệu xác thực mặc định **shall [04.46]** được thay thế vào lúc xác thực lần đầu tiên. Dữ liệu xác thực mặc định này không cần đáp ứng các yêu cầu xóa trắng (7.9.7).

Cơ chế xác thực có thể là một nhóm các cơ chế của các tính chất xác thực khác nhau mà chúng cùng nhau đáp ứng các yêu cầu của điều khoản này. Nếu mô-đun mật mã sử dụng các chức năng an toàn để xác thực người vận hành, thì các chức năng an toàn đó **shall [04.47]** là các chức năng an toàn đã được phê duyệt.

- Mô-đun **shall [04.48]** thực thi một cơ chế xác thực đã được phê duyệt như được tham chiếu trong Phụ lục E.
- Độ mạnh của cơ chế xác thực đã được phê duyệt **shall [04.49]** được cụ thể hóa trong chính sách an toàn (Phụ lục B)
- Đối với mỗi nỗ lực cố sử dụng cơ chế xác thực đã được phê duyệt, mô-đun **shall [04.50]** đáp ứng được độ mạnh của mục đích xác thực. Đối với nỗ lực nhiều lần cố sử dụng cơ chế xác thực đã được phê duyệt trong khoảng thời gian một phút, mô-đun **shall [04.51]** đáp ứng được độ mạnh của mục đích xác thực .
- Cơ chế xác thực đã được phê duyệt **shall [04.52]** được đáp ứng bởi việc thực thi của mô-đun đó và không dựa vào các sự kiểm soát thủ tục hoặc các quy tắc an toàn được tài liệu hóa (ví dụ, những hạn chế kích thước mật khẩu).
- Đối với mô-đun mật mã phần mềm ở Mức an toàn 2, hệ điều hành có thể thực thi cơ chế xác thực này. Nếu hệ điều hành thực thi cơ chế xác thực, khi đó cơ chế xác thực **shall [04.53]** đáp ứng các yêu cầu của điều khoản này.

- Phản hồi dữ liệu xác thực tới người vận hành **shall [04.54]** được làm mờ đi trong suốt quá trình xác thực (chẳng hạn không hiển thị nhìn thấy được các ký tự khi nhập vào mật khẩu). Các ký tự không có nghĩa có thể được hiển thị tại vị trí của dữ liệu xác thực thực tế.
- Phản hồi được cung cấp cho người vận hành trong quá trình một xác thực được cố nỗ lực **shall [04.55]** ngăn chặn việc làm suy yếu độ mạnh của cơ chế xác thực vượt ra ngoài độ mạnh xác thực được yêu cầu.

MỨC AN TOÀN 1

Đối với Mức an toàn 1, mô-đun mật mã không được yêu cầu sử dụng các cơ chế xác thực để kiểm soát truy cập đến mô-đun đó. Nếu mô-đun không hỗ trợ các cơ chế xác thực, mô-đun **shall [04.56]** yêu cầu rằng người vận hành hoặc có thể lựa chọn ẩn hoặc có thể lựa chọn hiển một hoặc nhiều vai trò.

MỨC AN TOÀN 2

Đối với Mức an toàn 2, mô-đun mật mã **shall [04.57]** sử dụng, tối thiểu, xác thực dựa trên vai trò để kiểm soát truy cập đến mô-đun đó.

MỨC AN TOÀN 3

Đối với Mức an toàn 3, mô-đun mật mã **shall [04.58]** sử dụng các cơ chế xác thực dựa trên định danh để kiểm soát truy cập đến mô-đun đó.

MỨC AN TOÀN 4

Đối với Mức an toàn 4, mô-đun mật mã **shall [04.59]** sử dụng các cơ chế xác thực dựa trên định danh đa yếu tố để kiểm soát truy cập đến mô-đun đó.

7.5 An toàn phần mềm/phần sụn

Mô-đun mật mã được xác định như hoặc là mô-đun phần cứng, mô-đun phần mềm, mô-đun phần sụn hoặc mô-đun lai ghép (7.2.2). Các yêu cầu của điều khoản này **shall [05.01]** áp dụng cho các thành phần phần mềm và phần sụn của mô-đun mật mã.

Mô-đun mật mã mà nó được thực thi hoàn toàn trong phần cứng không phải là chủ đề của các yêu cầu an toàn phần mềm/phần sụn của tiêu chuẩn này.

Khóa kiểm tra công khai hoặc khóa xác thực thông điệp có khóa có thể thường trú bên trong mã mô-đun và không được coi là một SSP.

Các yêu cầu về tài liệu được chỉ rõ trong A.2.5 **shall [05.02]** được cung cấp.

MỨC AN TOÀN 1

Các yêu cầu sau đây **shall [05.03]** áp dụng cho các thành phần phần mềm và phần sụn của mô-đun mật mã đối với Mức an toàn 1:

- Tất cả phần mềm và phần sụn **shall [05.04]** phải là dưới dạng mà nó thỏa mãn các yêu cầu của tiêu chuẩn này mà không cần sửa đổi trước khi cài đặt. (7.11.7).
- Một cơ chế mật mã sử dụng kỹ thuật toàn vẹn đã được phê duyệt **shall [05.05]** được áp dụng cho tất cả các thành phần phần mềm và phần sụn bên trong ranh giới mật mã đã được xác định của mô-đun theo một trong các cách sau:
  - Bởi chính mô-đun mật mã này; hoặc
  - Bởi mô-đun mật mã hợp lệ khác hoạt động trong một chế độ vận hành đã được phê duyệt.
- Nếu việc kiểm tra tính toàn vẹn thất bại, mô-đun **shall [05.06]** đi vào trạng thái có lỗi. Kỹ thuật toàn vẹn được phê duyệt có thể bao gồm một mã hoặc chữ ký xác thực thông điệp hoàn chỉnh

đơn, hoặc các mã hay các chữ ký đa xác thực tách rời mà trong chúng sự thất bại của bất kì mã hoặc chữ ký xác thực tách rời nào **shall [05.07]** gây ra cho mô-đun đi vào trạng thái có lỗi. Đầu ra được tham chiếu kỳ vọng của cơ chế kỹ thuật toàn vẹn có thể là dữ liệu được xem xét và chính nó không phải là chủ đề của kỹ thuật toàn vẹn. (Các) giá trị tạm thời được tạo ra trong quá trình kiểm tra toàn vẹn của phần mềm hoặc phần sụn của mô-đun **shall [05.08]** được xóa trắng khỏi mô-đun vào lúc hoàn thành kiểm tra tính toàn vẹn.

- Một người vận hành **shall [05.09]** có khả năng thực hiện kỹ thuật toàn vẹn đã được phê duyệt dựa trên yêu cầu thông qua dịch vụ HMI, SFMI, HSMI hoặc HFMI (7.3.2).
- Tất cả các đầu vào dữ liệu và điều khiển, và các đầu ra trạng thái và điều khiển, dữ liệu (được chỉ rõ tại 7.3.3) của mô-đun và các dịch vụ mật mã (7.4.3) **shall [05.10]** được chỉ dẫn qua một HMI, SFMI, HFMI hoặc HSMI đã được xác định; và
- Đối với mô-đun phần mềm hoặc phần sụn, nếu hình ảnh phần mềm hoặc phần sụn đã được nạp là một sự thay thế hoặc lớp phủ lên hoàn chỉnh của hình ảnh mô-đun hợp lệ, thì việc kiểm tra nạp phần mềm/phần sụn sẽ không áp dụng được (NA) như việc thay thế hoặc lớp phủ lên tạo thành mô-đun mới.

Nếu phần mềm hoặc phần sụn được nạp vào mà được liên kết, ràng buộc, sửa đổi hoặc là một điều kiện tất yếu thực thi được của mô-đun hợp lệ nhưng không phải là một sự thay thế hoặc lớp phủ ngoài hoàn chỉnh của mô-đun hợp lệ, khi đó việc kiểm tra nạp phần mềm/ phần sụn được áp dụng và **shall [05.11]** được thực hiện bởi mô-đun hợp lệ.

MỨC AN TOÀN 2

Ngoài các yêu cầu của Mức an toàn 1, các yêu cầu sau đây **shall [05.12]** áp dụng cho các thành phần phần mềm và phần sụn của mô-đun mật mã đối với Mức an toàn 2:

- Các thành phần phần mềm và phần sụn của mô-đun mật mã **shall [05.13]** chỉ bao gồm mã dưới dạng thực thi được (ví dụ, không phải mã nguồn, mã đối tượng hoặc mã biên dịch đúng thời điểm chạy).
- Ở đó **shall [05.14]** không có các dịch vụ hay các thiết lập kiểm soát thông qua giao diện HMI, SFMI, HFMI, hay HSMI để cho phép người vận hành khởi hoạt hoặc thực hiện các kỹ thuật gỡ rối.
- Chữ ký số hoặc mã xác thực thông điệp có khóa được phê duyệt **shall [05.15]** được áp dụng cho toàn bộ phần mềm và phần sụn bên trong ranh giới mật mã được xác định của mô-đun. Nếu kết quả được tính toán không bằng kết quả sinh ra trước đó, thì kiểm tra thất bại và mô-đun **shall [05.16]** đi vào trạng thái có lỗi.

MỨC AN TOÀN 3 VÀ 4

Ngoài các yêu cầu của Mức an toàn 1 và 2, các yêu cầu sau đây **shall [05.17]** áp dụng cho các thành phần phần mềm và phần sụn của mô-đun mật mã đối với các Mức an toàn 3 và 4:

Cơ chế mật mã sử dụng một chữ ký số được phê duyệt **shall [05.18]** được áp dụng cho tất cả các thành phần phần mềm và phần sụn bên trong ranh giới mật mã được xác định của mô-đun này. Nếu kết quả tính toán không bằng kết quả sinh ra trước đó, thì kiểm tra thất bại và mô-đun **shall [05.19]** đi vào trạng thái có lỗi.

Kỹ thuật chữ ký số có thể chứa một chữ ký hoàn chỉnh đơn lẻ hoặc nhiều chữ ký tách rời mà trong chúng sự thất bại của một chữ ký rời bất kỳ **shall [05.20]** gây ra cho mô-đun đi vào trạng thái có lỗi. Khóa ký bí mật **shall [05.21]** thường trú bên ngoài mô-đun.

7.6 Môi trường hoạt động

7.6.1 Các yêu cầu chung của môi trường hoạt động

Môi trường hoạt động của mô-đun mật mã tham chiếu đến quản lý phần mềm, phần sụn và/hoặc phần cứng được yêu cầu cho mô-đun hoạt động. Môi trường hoạt động của một phần mềm, phần sụn hoặc mô-đun lai ghép bao gồm, tối thiểu, các thành phần của mô-đun, nền tính toán, và hệ điều hành để điều khiển hoặc cho phép thực hiện phần mềm hoặc phần sụn trên nền tính toán. Mô-đun phần cứng có thể có một môi trường hoạt động bên trong mô-đun bao gồm một hệ điều hành cho phép thực hiện phần mềm hoặc phần sụn bên trong. Hệ điều hành được xem là, khi áp dụng, bao gồm (các) máy ảo (hệ thống và/hoặc tiến trình) và môi trường thời gian chạy (ví dụ Môi trường thời gian chạy Java – Java Runtime Environment JRE).

Một môi trường hoạt động cho mục đích chung (general-purpose operational environment) tham chiếu đến việc sử dụng một hệ điều hành thương mại mục đích chung sẵn có (tức là người quản lý tài nguyên) quản lý các thành phần phần mềm hoặc phần sụn và cũng quản lý hệ thống và (các) tiến trình/luồng của (những) người vận hành, bao gồm phần mềm ứng dụng mục đích chung như các bộ xử lý văn bản.

Môi trường hoạt động có thể là không thể sửa đổi, hạn chế hoặc có thể sửa đổi.

Các điều khoản sau đây chỉ rõ về ba loại môi trường hoạt động cụ thể.

1. ***Môi trường hoạt động không thể sửa đổi:*** được thiết kế hoặc cấu hình theo cách thức để ngăn chặn việc bị sửa đổi bởi một người vận hành hoặc một tiến trình tới các thành phần của mô-đun, nền tính toán, hoặc hệ điều hành. Môi trường này có thể gồm mô-đun phần sụn hoạt động trên nền tính toán không lập trình được hoặc mô-đun phần cứng ngăn chặn việc nạp bất kỳ phần mềm hoặc phần sụn bổ sung nào.
2. ***Môi trường hoạt động hạn chế:*** được thiết kế hoặc cấu hình theo cách thức để cho phép sửa đổi có kiểm soát bởi một người vận hành hoặc một tiến trình tới các thành phần của mô-đun, nền tính toán, hoặc hệ điều hành. Môi trường này có thể là phần sụn hoạt động trong mô-đun phần cứng có thể lập trình được mà ở đó việc nạp phần sụn bổ sung đáp ứng các yêu cầu nạp phần sụn được chỉ rõ trong 7.4.3.4.
3. ***Môi trường hoạt động có thể sửa đổi:*** tham chiếu đến một môi trường hoạt động mà nó có thể được cấu hình lại chức năng thêm/xóa/sửa đổi, và/hoặc có thể bao gồm các khả năng của hệ điều hành mục đích chung (ví dụ: sử dụng một hệ điều hành máy tính, hệ điều hành thẻ thông minh có thể cấu hình được, hoặc phần mềm có thể lập trình được). Các hệ điều hành được xem như là các môi trường hoạt động có thể sửa đổi được nếu các thành phần phần mềm có thể được sửa đổi bởi một người vận hành hoặc một tiến trình và/hoặc một người vận hành hoặc một tiến trình có thể nạp và thực thi phần mềm (ví dụ, một bộ xử lý văn bản) mà nó không phải là một phần của mô-đun phần mềm, phần sụn, hoặc mô-đun lai ghép đã được xác định.

   Môi trường hoạt động có thể sửa đổi có các đặc tính sau:

   Các chức năng có thể được bổ sung hoặc sửa đổi bên trong môi trường hoạt động. Các chức năng đó không cần thiết là tin cậy để không can thiệp hoạt động của mô-đun mật mã trừ phi sự can thiệp đó bị ngăn cấm bởi môi trường hoạt động.

   Trong một môi trường như vậy, cần yêu cầu rằng không có chức năng hoạt động trong cùng môi trường hoạt động mà nó không thuộc về phần tin cậy của môi trường hoạt động có truy cập đến các SSP khác với thông qua giao diện được xác định của mô-đun mật mã.

Vậy nên, cần yêu cầu rằng môi trường hoạt động cung cấp khả năng tách biệt mô-đun mật mã trong quá trình hoạt động khỏi các chức năng khác trong môi trường hoạt động, như các chức năng nào có thể chẳng thu được thông tin từ mô-đun mật mã liên quan tới các CSP cũng không có khả năng sửa đổi được các CSP, PSP hoặc luồng thực thi của mô-đun mật mã khác với thông qua các giao diện được cung cấp bởi chính mô-đun mật mã.

Một cấu hình cụ thể của môi trường hoạt động có thể được yêu cầu để đạt được sự bảo vệ đầy đủ của mô-đun mật mã với mã và dữ liệu của nó (ví dụ ngăn cấm loại hình cụ thể liên lạc giữa các tiến trình đối với mô-đun mật mã, gán các quyền truy cập hạn chế các tệp chứa các SSP hay mã của mô-đun mật mã).

Một số ví dụ về các môi trường hoạt động được cung cấp trong bảng sau:

Bảng 2 – Các ví dụ về các môi trường hoạt động

Ví dụ cấu hình	Môi trường hoạt động
Nền tính toán không cho phép nạp các mã và không cho phép những người vận hành sửa đổi cấu hình của nền tính toán, hệ điều hành hoặc mô-đun mật mã.	Không thể sửa đổi
Nền tính toán chứa một hệ điều hành cho phép việc nạp mã bổ sung đã được xác thực và đáp ứng tất cả các yêu cầu áp dụng được của Tiêu chuẩn này.	Hạn chế
Nền tính toán cho phép việc nạp mã mà không cần đáp ứng các yêu cầu nạp phần mềm hoặc phần sụn của Tiêu chuẩn này.	Có thể sửa đổi
Nền tính toán chứa mã mà hệ điều hành của nó là cấu hình lại được bởi người vận hành, cho phép loại bỏ các bảo vệ an toàn.	Có thể sửa đổi

Đối với môi trường không thể sửa đổi hoặc hạn chế, các thành phần điều khiển duy trì môi trường không thể sửa đổi hoặc hạn chế có thể bao gồm các thuộc tính của nền tính toán, hệ điều hành hoặc chính mô-đun mật mã hoặc tất cả các yếu tố trên.

Mã được thực thi trong môi trường không thể sửa đổi hoặc hạn chế được tham chiếu đến như là *phần sụn* bên trong Tiêu chuẩn này. Mã được thực thi trong môi trường có thể sửa đổi được tham chiếu đến như là *phần mềm bên* trong Tiêu chuẩn này.

Nếu môi trường hoạt động là một môi trường hoạt động không thể sửa đổi hoặc hạn chế thì chỉ các yêu cầu hệ điều hành trong 7.6.2 **shall [06.01]** được áp dụng.

Nếu môi trường hoạt động là môi trường hoạt động có thể sửa đổi, thì các yêu cầu hệ điều hành trong 7.6.3 **shall [06.02]** được áp dụng.

Các yêu cầu về tài liệu được chỉ rõ tại A.2.6 **shall [06.03]** được cung cấp.

7.6.2 Các yêu cầu hệ điều hành đối với các môi trường hoạt động không thể sửa đổi hoặc hạn chế

MỨC AN TOÀN 1

Các yêu cầu trong 7.6.3 Mức an toàn 1 **shall [06.04]** được áp dụng nếu mô-đun là Mức an toàn 1 trong 7.7.

MỨC AN TOÀN 2,3, VÀ 4

Không có các yêu cầu bổ sung.

7.6.3 Các yêu cầu hệ điều hành đối với các môi trường hoạt động có thể sửa đổi

MỨC AN TOÀN 1

Các yêu cầu sau áp dụng cho các hệ điều hành đối với Mức an toàn 1.

- Mỗi trường hợp của mô-đun mật mã **shall [06.05]** có kiểm soát trên chính các SSP của nó.
- Môi trường hoạt động **shall [06.06]** cung cấp khả năng tách biệt các tiến trình ứng dụng riêng lẻ với nhau bằng cách ngăn chặn các truy nhập không kiểm soát được tới các CSP và các sửa đổi không kiểm soát được của các SSP bất kể là dữ liệu này nằm trong bộ nhớ hoặc được lưu trong một ổ lưu bền vững bên trong môi trường hoạt động. Điều này đảm bảo rằng việc truy cập trực tiếp tới các CSP và SSP bị hạn chế đối với mô-đun mật mã và các phần tin cậy của môi trường hoạt động. Các hạn chế đối với việc cấu hình môi trường hoạt động **shall [06.07]** được tài liệu hóa trong chính sách an toàn của mô-đun mật mã.
- Các tiến trình được sinh ra bởi mô-đun mật mã **shall [06.08]** thuộc sở hữu bởi mô-đun và không được sở hữu bởi các tiến trình/người vận hành bên ngoài.

CHÚ THÍCH: Các yêu cầu này không có thể là bắt buộc tuân theo bởi tài liệu và các thủ tục quản lý, nhưng phải là bắt buộc tuân theo bởi chính mô-đun mật mã.

MỨC AN TOÀN 2

Ngoài các yêu cầu của Mức an toàn 1, đối với Mức an toàn 2 một môi trường hoạt động **shall [06.09]** áp ứng các yêu cầu sau hoặc như được cho phép bởi thẩm quyền kiểm tra hợp lệ.

- Tất cả các phần mềm mật mã, các SSP, và thông tin kiểm soát và trạng thái **shall [06.10]** nằm dưới quyền kiểm soát của một hệ điều hành thực thi hoặc các kiểm soát truy nhập dựa trên vai trò hoặc, ở mức thấp nhất, kiểm soát truy cập tùy theo thực tế với cơ chế vững chắc để xác định các nhóm mới và gán các quyền hạn chế, ví dụ thông qua các danh sách kiểm soát truy cập (ACL), và với khả năng gán mỗi người dùng tới nhiều hơn một nhóm. Hệ điều hành **shall [06.11]** được cấu hình để bảo vệ chống lại thực thi, sửa đổi, và đọc được các SSP, dữ liệu kiểm soát và trạng thái trái phép.
- Để bảo vệ các dữ liệu dạng rõ, phần mềm mật mã, các SSP, và dữ liệu xác thực, các cơ chế kiểm soát truy cập của hệ điều hành:
    - **Shall [06.12]** được cấu hình để xác định và buộc tuân theo một tập các vai trò hoặc các nhóm và các quyền hạn chế kết hợp của chúng mà chúng có các quyền dành riêng thực thi phần mềm mật mã được lưu trữ;
    - **Shall [06.13]** được cấu hình để xác định và buộc tuân theo một tập các vai trò hoặc các nhóm và các quyền hạn chế kết hợp của chúng mà chúng có các quyền dành riêng sửa đổi (tức là, ghi, thay thế và xóa) phần mềm mô-đun mật mã sau đây được lưu giữ bên trong ranh giới mật mã: các chương trình mật mã, dữ liệu mật mã (ví dụ dữ liệu kiểm toán mật mã), các SSP và dữ liệu bản rõ;
    - **Shall [06.14]** được cấu hình để xác định và buộc tuân theo một tập các vai trò hoặc các nhóm và các quyền hạn chế kết hợp của chúng mà chúng có các quyền dành riêng để đọc dữ liệu mật mã (ví dụ dữ liệu kiểm toán mật mã), các SSP và dữ liệu bản rõ; và
    - **Shall [06.15]** được cấu hình để xác định và buộc tuân theo một tập các vai trò hoặc các nhóm và các quyền hạn chế kết hợp của chúng mà chúng có các quyền dành riêng để đi vào các SSP.

và

- Các đặc tả sau đây **shall [06.16]** là phù hợp với các vai trò hoặc các quyền và các dịch vụ của các 'nhóm được chỉ định' như được xác định trong chính sách an toàn:
  - Khi không hỗ trợ một vai trò duy trì, hệ điều hành **shall [06.17]** ngăn chặn tất cả những người vận hành và các tiến trình đang chạy khỏi việc sửa đổi các tiến trình mật mã đang chạy (tức là, các hình ảnh chương trình mật mã được nạp và thực hiện). Trong trường hợp này, các tiến trình đang chạy tham chiếu đến tất cả các tiến trình, có là mật mã hoặc không, không thuộc sở hữu hoặc được khởi hoạt bởi hệ điều hành (nghĩa là được khởi hoạt bởi người vận hành);
  - Hệ điều hành **shall [06.18]** ngăn chặn các tiến trình người dùng khỏi việc có được truy cập đọc hoặc ghi tới các SSP được sở hữu bởi các tiến trình khác và tới các SSP hệ thống; và
  - Việc cấu hình hệ điều hành đáp ứng các yêu cầu trên **shall [06.19]** được chỉ rõ trong hướng dẫn người quản trị. Hướng dẫn người quản trị **shall [06.20]** phát biểu rằng hệ điều hành phải được cấu hình như được chỉ rõ trong các nội dung mô-đun để được xem là được bảo vệ.

Cơ chế định danh và xác thực đối với hệ điều hành **shall [06.21]** đáp ứng các yêu cầu của 7.4.3 và được chỉ rõ trong chính sách an toàn của các mô-đun.

Tất cả phần mềm mật mã, các SSP, thông tin điều khiển và trạng thái **shall [06.22]** dưới sự kiểm soát của:

- Một hệ điều hành **shall [06.23]** mà nó có tối thiểu các thuộc tính sau:
  - Một hệ điều hành **shall [06.24]** cung cấp một cơ chế kiểm toán với ngày tháng và thời gian của mỗi sự kiện kiểm toán. Mô-đun mật mã **shall [06.25]** không bao gồm các SSP như một phần của bất kì bản ghi kiểm toán nào;
  - Mô-đun mật mã **shall [06.26]** cung cấp các sự kiện sau để được ghi lại bởi cơ chế kiểm toán của hệ điều hành:
    - Các sửa đổi, các truy nhập, xóa, và thêm dữ liệu mật mã và các SSP;
    - Các nỗ lực cố cung cấp đầu vào không hợp lệ đối với các chức năng của Chuyên viên mật mã;
    - Thêm hoặc xóa người vận hành vào hoặc ra khỏi một vai trò Chuyên viên mật mã (nếu các vai trò này được quản lý bởi mô-đun mật mã);
    - Sử dụng một chức năng của Chuyên viên mật mã liên quan đến an toàn;
    - Các yêu cầu truy cập vào dữ liệu xác thực kết hợp với mô-đun mật mã;
    - Sử dụng một cơ chế xác thực (ví dụ, đăng nhập) kết hợp với mô-đun mật mã; và
    - Các yêu cầu hiển để đảm nhiệm một vai trò Chuyên viên mật mã.
  - Cơ chế kiểm toán của hệ điều hành **shall [06.27]** có khả năng kiểm toán các sự kiện liên quan hệ điều hành sau đây:
    - Tất cả các truy cập đọc hoặc ghi của người vận hành tới dữ liệu kiểm toán lưu trữ tại vệt kiểm toán;
    - Truy cập đến các tập tin được sử dụng bởi mô-đun mật mã để lưu trữ dữ liệu mật mã hoặc các SSP;

- Thêm hoặc xóa một người vận hành vào hoặc ra khỏi một vai trò Chuyên viên mật mã (nếu các vai trò đó được quản lý bởi môi trường hoạt động);
- Các yêu cầu sử dụng các cơ chế quản lý dữ liệu xác thực;
- Các nỗ lực cố sử dụng chức năng kênh tin cậy và liệu yêu cầu có được đảm bảo, khi nào kênh tin cậy được hỗ trợ tại mức an toàn này; và
- Nhận biết người khởi hoạt và mục đích của một kênh tin cậy, khi kênh tin cậy được hỗ trợ tại mức an toàn đó.

o Hệ điều hành **shall [06.28]** được cấu hình để ngăn chặn những người vận hành khác với những người có các đặc quyền đã được nhận biết trong chính sách an toàn khỏi việc sửa đổi phần mềm mô-đun mật mã và dữ liệu kiểm toán được lưu trữ trong môi trường hoạt động của mô-đun mật mã.

Chỉ những hệ điều hành mà chúng được cấu hình để đáp ứng các yêu cầu an toàn trên mới **shall [06.29]** được cho phép tại mức an toàn này, cho dù mô-đun mật mã có hoạt động trong chế độ hoạt động được phê duyệt hay không. Bản ghi kiểm toán cần được bảo vệ chống lại sửa đổi trái phép thông qua sử dụng một chức năng toàn đã được phê duyệt.

7.7 An toàn vật lý

7.7.1 Các thể hiện của an toàn vật lý

Mô-đun mật mã **shall [07.01]** sử dụng các cơ chế an toàn vật lý để hạn chế sự truy cập vật lý trái phép vào các nội dung của mô-đun và để ngăn cản việc sử dụng hoặc sửa đổi trái phép mô-đun (bao gồm cả việc thay thế toàn bộ mô-đun) khi được cài đặt. Tất cả các thành phần phần cứng, phần mềm, phần sụn, dữ liệu và các SSP bên trong ranh giới mật mã **shall [07.02]** được bảo vệ.

Mô-đun mật mã mà được thực thi hoàn toàn ở dạng phần mềm sao cho an toàn vật lý được cung cấp đơn lẻ bởi nền tính toán không phải là chủ đề đối với các yêu cầu an toàn vật lý của tiêu chuẩn này.

Các yêu cầu của điều khoản này **shall [07.03]** được áp dụng cho các mô-đun phần cứng và phần sụn, và các thành phần phần cứng và phần sụn của các mô-đun lai ghép.

Các yêu cầu của điều khoản này **shall [07.04]** được áp dụng tại ranh giới vật lý đã được xác định của mô-đun.

Các yêu cầu về an toàn vật lý được chỉ rõ đối với ba thể hiện vật lý đã được xác định của mô-đun mật mã.

1. ***Các mô-đun mật mã đơn chíp*** là các thể hiện vật lý, trong đó một chip mạch tích hợp đơn (IC) có thể được sử dụng như một thiết bị đứng độc lập hoặc có thể được nhúng bên trong một vỏ bọc hoặc một sản phẩm có thể không được bảo vệ về mặt vật lý. Các ví dụ về các mô-đun mật mã đơn chíp bao gồm các chip IC đơn hoặc các thẻ thông minh với một chip IC đơn.
2. ***Các mô-đun mật mã nhúng đa chíp*** là những thể hiện vật lý mà trong đó hai hay nhiều các chip IC được kết nối với nhau và được nhúng vào bên trong một vỏ bọc hoặc một sản phẩm có thể không được bảo vệ về mặt vật lý. Các ví dụ về các mô-đun mật mã nhúng đa chip bao gồm các adapter và các bảng mạch mở rộng.
3. ***Các mô-đun mật mã đa chíp đứng độc lập*** là những thể hiện vật lý mà trong chúng hai hay nhiều các chip IC được kết nối với nhau và toàn bộ vỏ bọc được bảo vệ về mặt vật lý. Các ví dụ về mô-đun mật mã đa chip, đứng độc lập bao gồm các bộ định tuyến mã hóa (encrypt) hoặc các thiết bị radio an toàn hoặc các thẻ USB token.

Phụ thuộc vào các cơ chế an toàn vật lý của mô-đun mật mã, những nỗ lực trái phép nhằm truy cập, sử dụng hoặc sửa đổi **shall [07.05]** có xác suất bị phát hiện cao:

- Để lại dấu vết nhìn thấy được ngay sau khi nỗ lực truy cập (tức là bằng chứng xâm phạm)

  và/hoặc

- Khi nỗ lực truy cập

và các hành động tức thời phù hợp **shall [07.06]** được thực thi bởi mô-đun mật mã để bảo vệ các CSP.

Bảng 3 tổng kết các yêu cầu an toàn vật lý cả ba thể hiện tổng quát chung và cụ thể đối với mỗi trong 4 mức an toàn. Các yêu cầu an toàn vật lý cụ thể theo thể hiện tại mỗi mức an toàn nâng cao các yêu cầu chung tại cùng mức và các yêu cầu cụ thể theo thể hiện của mức trước đó.

Bảng 3 – Tổng hợp về các yêu cầu an toàn vật lý đối với các mô-đun mật mã

	Các yêu cầu chung cho tất cả các thể hiện	**Đơn chíp**	**Đa chíp nhúng**	**Đa chíp đứng độc lập**
Mức an toàn 1	Các thành phần gia cố chắc chắn. Ô xy hóa chống rỉ theo tiêu chuẩn Xóa trắng tự động hoặc theo thủ tục khi truy cập vào giao diện truy cập duy trì.	Không có các yêu cầu bổ sung.	Vỏ bọc hoặc nắp đậy tháo lắp được gia cố chắc chắn.	Vỏ bọc hoặc nắp đậy tháo lắp được gia cố chắc chắn.
Mức an toàn 2	Bằng chứng xâm phạm chấn ánh sáng hoặc trong mờ bên trong phổ nhìn thấy được. Ngăn chặn việc quan sát trực tiếp thông qua các lỗ hổng hoặc các khe hở.	Lớp phủ bằng chứng chống xâm phạm trên chíp hoặc vỏ bọc.	Vật liệu đóng gói hoặc vỏ bọc bằng chứng chống xâm phạm với các dấu niêm phong bằng chứng chống xâm phạm hoặc các khóa chống trộm cấp đối với các cửa và các vỏ bọc tháo lắp được.	Vật liệu đóng gói hoặc vỏ bọc bằng chứng chống xâm phạm với các dấu niêm phong bằng chứng chống xâm phạm hoặc các khóa chống trộm cấp đối với các cửa và các vỏ bọc tháo lắp được.
Mức an toàn 3	Kết cấu mạch đáp trả xâm phạm và xóa trắng. Tự động xóa trắng khi truy cập vào giao diện truy cập duy trì. Ngăn chặn thăm dò qua các lỗ hổng	Lớp phủ bằng chứng chống xâm phạm cứng trên chip hoặc vỏ bọc chống xâm nhập và chống tháo rời mạnh.	Vật liệu đóng gói bằng chứng chống xâm phạm cứng hoặc vỏ bọc bền.	Vật liệu cứng đóng gói bằng chứng chống xâm phạm hoặc vỏ bọc bền.

	hoặc khe hở. EFP hoặc EFT đối với nhiệt độ và điện áp.			
Mức an toàn 4	Lớp bọc phát hiện và đáp trả xâm phạm. EFP đối với nhiệt độ và điện áp. Bảo vệ chống cảm ứng lỗi.	Lớp phủ chống tháo rời cứng trên chip.	Lớp bọc phát hiện và đáp trả xâm phạm với khả năng xóa trắng.	Lớp bọc phát hiện và đáp trả xâm phạm với khả năng xóa trắng.

Nhìn chung, Mức an toàn 1 cung cấp một tập hợp các yêu cầu cơ bản. Mức an toàn 2 yêu cầu thêm các cơ chế bằng chứng chống xâm phạm và không có khả năng thu thập thông tin về các hoạt động bên trong của các khu vực quan trọng của mô-đun (độ chắn sáng). Mức an toàn 3 thêm các yêu cầu đối với sử dụng các vỏ bọc bảo toàn hình dạng hoặc không bảo toàn hình dạng bền hoặc cứng với các cơ chế phát hiện và đáp trả xâm phạm đối với các vỏ bọc và các cửa tháo lắp được và chống lại việc thăm dò trực tiếp qua các chỗ mở hoặc các điểm đi vào. Bảo vệ chống lỗi do môi trường (EFP) hoặc kiểm tra chống lỗi do môi trường (EFT) được yêu cầu tại Mức an toàn 3. Mức an toàn 4 thêm các yêu cầu đối với sử dụng các vỏ bọc bảo toàn hình dạng hoặc không bảo toàn hình dạng cứng hoặc bền với các cơ chế phát hiện và đáp trả xâm phạm đối với toàn bộ vỏ bọc hoặc hư hỏng đáng kể. Bảo vệ chống lỗi do môi trường (EFP) và bảo vệ chống các tấn công cảm ứng lỗi được yêu cầu tại Mức an toàn 4.

Các yêu cầu an toàn được chỉ ra rõ đối với một giao diện truy cập duy trì khi mô-đun mật mã được thiết kế để cho phép truy cập vật lý (ví dụ bởi nhà cung cấp mô-đun hoặc các cá nhân được cho phép khác).

Phát hiện xâm phạm và đáp trả xâm phạm không phải là các thay thế đối với bằng chứng xâm phạm.

Các yêu cầu tài liệu được chỉ rõ trong A.2.7 **shall [07.07]** được cung cấp.

7.7.2. Các yêu cầu chung về an toàn vật lý

Các yêu cầu sau đây **shall [07.08]** được áp dụng cho tất cả các thể hiện vật lý:

- Tài liệu **shall [07.09]** đặc tả thể hiện vật lý và mức an toàn mà các cơ chế an toàn vật lý của mô-đun mật mã được thực thi.
- Bất kể khi nào xóa trắng được thực hiện đối với các mục đích an toàn vật lý, thì việc xóa trắng **shall [07.10]** xảy ra trong một khoảng thời gian đủ nhỏ để đủ ngăn chặn việc khôi phục dữ liệu nhạy cảm trong khoảng thời gian giữa phát hiện và xóa trắng thực tế;
- Nếu mô-đun bao gồm một vai trò duy trì mà nó yêu cầu truy cập vật lý vào các nội dung của mô-đun hoặc nếu mô-đun được thiết kế để cho phép truy cập vật lý (ví dụ bởi nhà cung cấp mô-đun hoặc cá nhân được cho phép khác) thì:
    - Một giao diện truy cập duy trì **shall [07.11]** được xác định;
    - Giao diện truy cập duy trì **shall [07.12]** bao gồm tất cả các đường dẫn truy cập vật lý vào các nội dung của mô-đun mật mã, bao gồm bất kỳ các vỏ bọc tháo lắp được hoặc các cửa mở nào; và

- Bất kỳ các vỏ bọc tháo lắp được hoặc các cửa mở được bao gồm bên trong giao diện truy cập duy trì **shall [07.13]** được bảo vệ sử dụng các cơ chế an toàn vật lý phù hợp.

MỨC AN TOÀN 1

Các yêu cầu sau **shall [07.14]** được áp dụng cho tất cả mô-đun mật mã đối với Mức an toàn 1:

- Mô-đun mật mã **shall [07.15]** gồm các thành phần gia cố bền vững mà chúng bao gồm các kỹ thuật ô xy hóa chống rỉ theo tiêu chuẩn (ví dụ, một lớp phủ bảo toàn hình dạng hoặc một lớp phủ niêm phong được áp dụng trên toàn bộ kết cấu mạch của mô-đun để bảo vệ chống lại phá hủy môi trường hoặc phá hủy vật lý khác); và
- Khi thực hiện duy trì vật lý, xóa trắng **shall [07.16]** hoặc được thực hiện theo thủ tục bởi người vận hành hoặc tự động bởi mô-đun mật mã.

MỨC AN TOÀN 2

Ngoài các yêu cầu chung đối với Mức an toàn 1 thì các yêu cầu sau **shall [07.17]** được áp dụng cho tất cả các mô-đun mật mã đối với Mức an toàn 2:

- Mô-đun mật mã **shall [07.18]** cung cấp bằng chứng về xâm phạm (chẳng hạn như trên vỏ nắp, vỏ bọc hoặc dấu niêm phong) khi nỗ lực truy cập vật lý vào mô-đun đang được thực hiện;
- Vật liệu, lớp phủ hoặc vỏ bọc bằng chứng xâm phạm **shall [07.19]** hoặc chắn sáng hoặc là trong mờ bên trong phổ ánh sáng nhìn thấy được (tức là dải ánh sáng của bước sóng từ 400nm đến 750nm) để ngăn chặn việc thu thập thông tin về các hoạt động bên trong của các khu vực quan trọng của mô-đun; và
- Nếu mô-đun mật mã chứa các lỗ hổng thông gió hoặc các khe hở, thì mô-đun đó **shall [07.20]** được xây dựng theo cách thức để ngăn chặn thu thập thông tin về cấu trúc bên trong hoặc các thành phần của mô-đun bằng sự quan sát nhìn thấy được trực tiếp sử dụng các nguồn sáng nhân tạo trong phổ nhìn thấy được của các thành phần hay cấu trúc bên trong của mô-đun.

MỨC AN TOÀN 3

Ngoài các yêu cầu chung đối với Mức an toàn 1 và 2, thì các yêu cầu sau **shall [07.21]** được áp dụng cho tất cả các mô-đun mật mã đối với Mức an toàn 3:

- Nếu mô-đun mật mã chứa các cửa mở nào đó hoặc nắp đậy tháo lắp được nào đó hoặc nếu một giao diện truy cập duy trì được xác định thì mô-đun **shall [07.22]** chứa khả năng đáp trả xâm phạm và xóa trắng. Khả năng xóa trắng và đáp trả xâm phạm **shall [07.23]** ngay lập tức xóa trắng tất cả các SSP không được bảo vệ khi một cửa bị mở, một nắp đậy bị tháo ra hoặc khi giao diện truy cập duy trì bị truy cập. Khả năng đáp trả xâm phạm và xóa trắng **shall [07.24]** được duy trì hoạt động khi các SSP không được bảo vệ còn được chứa bên trong mô-đun mật mã;
- Nếu mô-đun mật mã chứa các lỗ hổng thông gió hoặc các khe hở thì mô-đun **shall [07.25]** được xây dựng theo cách thức mà nó ngăn chặn được việc thăm dò vật lý không bị phát hiện ở bên trong vỏ bọc thiết bị (ví dụ như ngăn chặn việc thăm dò bằng một bộ thăm dò khớp xoay đơn lẻ);
- Các vỏ bọc, lớp phủ hoặc các vật liệu phủ bọc bảo toàn hình dạng bền hoặc cứng **shall [07.26]** duy trì các đặc tính bền và cứng trên dải nhiệt độ chỉ định cho mô-đun của hoạt động, lưu trữ và phân phối,

- Nếu các dấu niêm phong bằng chứng xâm phạm được sử dụng, thì chúng **shall [07.27]** được đánh số duy nhất hoặc nhận biết một cách độc lập (ví dụ băng bằng chứng được đánh số duy nhất hoặc các dấu niêm phong toàn ký ảnh nhận biết duy nhất); và
- Mô-đun **shall [07.28]** hoặc bao gồm các đặc tính EFP hoặc trải qua kiểm tra EFT.

MỨC AN TOÀN 4

Ngoài các yêu cầu chung đối với Mức an toàn 1, 2 và 3 thì yêu cầu sau **shall [07.29]** được áp dụng cho tất cả các mô-đun mật mã đối với Mức an toàn 4:

- Mô-đun mật mã **shall [07.30]** được bảo vệ hoặc bởi một lớp phủ ngoài chống bóc rời chắn sáng cứng, hoặc bởi một vỏ bọc phát hiện xâm phạm với khả năng xóa trắng và đáp trả xâm phạm;
- Mô-đun **shall [07.31]** bao gồm các đặc tính EFP; và
- Mô-đun mật mã **shall [07.32]** cung cấp bảo vệ chống lại cảm ứng lỗi. Các kỹ thuật giảm thiểu cảm ứng lỗi và độ đo giảm thiểu được sử dụng **shall [07.33]** được tài liệu hóa như được chỉ rõ trong Phụ lục B.

7.7.3 Các yêu cầu an toàn vật lý đối với mỗi thể hiện an toàn vật lý

7.7.3.1 Các mô-đun mật mã đơn chíp

Ngoài các yêu cầu an toàn vật lý chung được chỉ rõ trong 7.7.2, thì các yêu cầu sau được cụ thể cho các mô-đun mật mã đơn chíp.

MỨC AN TOÀN 1

Không có các yêu cầu bổ sung nào của Mức an toàn 1 đối với các mô-đun mật mã đơn chíp.

MỨC AN TOÀN 2

Ngoài các yêu cầu đối với Mức an toàn 1, thì các yêu cầu sau **shall [07.34]** được áp dụng cho các mô-đun mật mã đơn chíp đối với Mức an toàn 2:

- Mô-đun mật mã **shall [07.35]** được phủ với một lớp phủ bằng chứng xâm phạm (chẳng hạn một vật liệu ô xy hóa chống rỉ bằng chứng xâm phạm hoặc một vật liệu bằng chứng xâm phạm bao phủ lớp ô xy hóa chống rỉ) hoặc được chứa trong một vỏ bọc bằng chứng xâm phạm để ngăn cản quan sát, thăm dò hoặc thao tác trực tiếp vào mô-đun và cung cấp bằng chứng về các nỗ lực cố xâm phạm hoặc lấy ra mô-đun.

MỨC AN TOÀN 3

Ngoài các yêu cầu đưa ra đối với Mức an toàn 1 và 2, thì các yêu cầu sau **shall [07.36]** được áp dụng cho các mô-đun mật mã đơn chíp đối với Mức an toàn 3.

- Mô-đun **shall [07.37]** được bao phủ bằng một lớp phủ bằng chứng xâm phạm chắn sáng cứng (ví dụ như phủ một lớp nhựa epoxy chắn sáng cứng trên lớp ô xy hóa chống rỉ)

  hoặc

- Vỏ bọc **shall [07.38]** được thực thi sao cho các nỗ lực cố loại bỏ hoặc thâm nhập vào vỏ bọc **shall [07.39]** có một xác suất cao gây ra phá hủy nghiêm trọng cho mô-đun mật mã (nghĩa là mô-đun sẽ không hoạt động nữa).

MỨC AN TOÀN 4

Ngoài các yêu cầu đối với Mức an toàn 1, 2 và 3, thì các yêu cầu sau **shall [07.40]** được áp dụng cho các mô-đun mật mã đơn chíp đối với Mức an toàn 4:

- Mô-đun mật mã **shall [07.41]** được phủ bằng một lớp phủ chống bóc ra chắn sáng, cứng với các đặc tính cứng rắn và bám chặt sao cho nỗ lực cố bóc hoặc cậy lớp phủ khỏi mô-đun sẽ có một xác suất cao làm hư hại nghiêm trọng cho mô-đun (nghĩa là mô-đun sẽ không hoạt động nữa); và
- Lớp phủ chống bóc ra **shall [07.42]** phải có các đặc tính tiêu hủy là việc phân hủy vỏ bọc sẽ có một xác suất cao làm phân hủy hoặc làm hỏng nghiêm trọng mô-đun (tức mô-đun không hoạt động nữa)

7.7.3.2 Các mô-đun mật mã nhúng đa chíp

Ngoài các yêu cầu an toàn chung được chỉ rõ trong 7.7.2, thì các yêu cầu sau được cụ thể cho các mô-đun mật mã nhúng đa chíp.

MỨC AN TOÀN 1

Nếu mô-đun mật mã được chứa bên trong một vỏ bọc hoặc nắp tháo mở được thì nắp tháo mở được hoặc vỏ bọc gia cố chắc chắn **shall [07.43]** được sử dụng.

MỨC AN TOÀN 2

Ngoài yêu cầu đối với Mức an toàn 1, thì các yêu cầu sau **shall [07.44]** được áp dụng cho các mô-đun mật mã nhúng đa chíp đối với Mức an toàn 2:

- Các thành phần mô-đun **shall [07.45]** được bao phủ với một lớp bao phủ bằng chứng xâm phạm hoặc vật liệu phủ bọc (chẳng hạn như lớp bao phủ chống khắc a xít hoặc lớp sơn chống hoen rỉ) để ngăn cản quan sát trực tiếp và cung cấp bằng chứng về các nỗ lực cố xâm phạm hoặc gỡ bỏ các thành phần mô-đun,

  hoặc

- Mô-đun **shall [07.46]** được chứa hoàn toàn bên trong một vỏ bọc gia cố chắc chắn bằng kim loại hoặc nhựa cứng mà nó có thể bao gồm các cửa hoặc các nắp tháo được.

và

- Vỏ bọc bao gồm bất kỳ cửa mở hoặc các nắp tháo được thì các cửa và các nắp tháo được **shall [07.47]** được khóa bằng các khóa cơ học chống trộm cắp sử dụng các khóa vật lý hoặc logic hoặc **shall [07.48]** được bảo vệ với các dấu niêm phong chống xâm phạm (ví dụ băng bằng chứng hoặc các dấu niêm phong toàn ký ảnh).

MỨC AN TOÀN 3

Ngoài các yêu cầu đối với các Mức an toàn 1 và 2, thì các yêu cầu sau **shall [07.49]** được áp dụng cho các mô-đun mật mã nhúng đa chíp đối với Mức an toàn 3:

- Đa chíp của kết cấu mạch bên trong mô-đun mật mã **shall [07.50]** được bao phủ với một lớp phủ cứng hoặc vật liệu phủ bọc (ví dụ bằng vật liệu nhựa epoxy cứng).

  hoặc

- Mô-đun **shall [07.51]** được chứa bên trong một lớp vỏ bền

sao cho các nỗ lực cố tháo bỏ hoặc xâm nhập vào vỏ bọc sẽ có một xác suất cao gây ra tổn hại nghiêm trọng cho mô-đun (nghĩa là mô-đun sẽ không hoạt động nữa).

MỨC AN TOÀN 4

Ngoài các yêu cầu đối với các Mức an toàn 1, 2 và 3, thì các yêu cầu sau **shall** [07.52] được áp dụng cho các mô-đun mật mã nhúng đa chíp đối với Mức an toàn 4:

- Các thành phần mô-đun **shall [07.53]** ở bên trong một vỏ bọc cứng hoặc bền, không bảo toàn hình dạng hoặc bảo toàn hình dạng. Vỏ bọc **shall [07.54]** được đóng gói bởi một vỏ bọc phát hiện xâm phạm (ví dụ như một mạch in mylar mềm dẻo với một mẫu hình học dạng xoắn của các chất dẫn hoặc một gói quấn dây hoặc một mạch giòn, không mềm dẻo hoặc một vỏ bọc bền) mà nó **shall [07.55]** phát hiện xâm phạm bằng cách như cắt, khoan, xay, nghiền, đốt, hòa tan hoặc phân hủy vật liệu phủ bọc hoặc vỏ bọc đến mức độ đủ để truy cập các SSP; và
- Mô-đun **shall [07.56]** chứa kết cấu mạch đáp trả xâm phạm và xóa trắng mà nó **shall [07.57]** liên tục giám sát vỏ bọc phát hiện xâm phạm và vào lúc phát hiện xâm phạm **shall [07.58]** ngay lập tức xóa trắng tất cả các SSP không được bảo vệ. Kết cấu mạch đáp trả xâm phạm **shall [07.59]** duy trì hoạt động khi các SSP không được bảo vệ được chứa bên trong mô-đun mật mã.

7.7.3.3 Các mô-đun mật mã đa chíp đứng độc lập

Ngoài các yêu cầu an toàn chung được chỉ rõ trong 7.7.2 thì các yêu cầu sau là cụ thể cho các mô-đun mật mã đa chíp đứng độc lập.

MỨC AN TOÀN 1

Mô-đun mật mã **shall [07.60]** được chứa hoàn toàn bên trong vỏ bọc đã được kiểm tra chất lượng bằng nhựa cứng hoặc kim loại mà nó có thể bao gồm các cửa hoặc các nắp tháo lắp được.

MỨC AN TOÀN 2

Ngoài các yêu cầu đối với Mức an toàn 1, thì các yêu cầu sau **shall [07.61]** được áp dụng cho các mô-đun mật mã đa chíp đứng độc lập đối với Mức an toàn 2:

- Nếu vỏ bọc của mô-đun mật mã bao gồm các cửa hoặc các nắp tháo lắp được nào đó thì các cửa hoặc các nắp tháo lắp **shall [07.62]** được khóa bằng các khóa cơ học chống cậy mở, sử dụng các chìa khóa dạng vật lý hoặc lôgic hoặc **shall [07.63]** được bảo vệ bằng các dấu niêm phong bằng chứng xâm phạm (ví dụ băng bằng chứng hoặc các dấu niêm phong toàn ký ảnh).

MỨC AN TOÀN 3

Ngoài các yêu cầu đối với các Mức an toàn 1 và 2, thì các yêu cầu sau **shall [07.64]** được áp dụng cho các mô-đun mật mã đa chíp đứng độc lập đối với Mức an toàn 3:

- Mô-đun **shall [07.65]** được chứa bên trong vỏ bọc bền sao cho các nỗ lực cố tháo mở hoặc xâm nhập vào vỏ bọc sẽ có một xác suất cao gây ra phá hủy nghiêm trọng đối với mô-đun (nghĩa là mô-đun sẽ không hoạt động nữa).

MỨC AN TOÀN 4

Ngoài các yêu cầu đối với các Mức an toàn 1, 2 và 3, thì các yêu cầu sau **shall [07.66]** được áp dụng cho các mô-đun mật mã đa chíp đứng độc lập đối với Mức an toàn 4:

- Vỏ bọc của mô-đun mật mã **shall [07.67]** chứa một lớp vỏ phát hiện xâm phạm sử dụng các cơ chế phát hiện xâm phạm như các bộ chuyển mạch nắp đậy (ví dụ như các vi chuyển mạch, các chuyển mạch hiệu ứng phòng từ tính, bộ trợ động từ tính vĩnh cửu, v.v...) các bộ phát hiện chuyển động (ví dụ siêu âm, hồng ngoại hoặc sóng cực ngắn) hoặc các cơ chế phát hiện xâm phạm khác như được mô tả trong 7.7.3.2 Mức an toàn 4. Các cơ chế phát hiện xâm phạm **shall [07.68]** phản ứng với các tấn công như là cắt, khoan, xay, nghiền, đốt, tan chảy, hoặc phân hủy đến một mức độ đủ để truy cập các SSP; và
- Mô-đun mật mã **shall [07.69]** chứa khả năng xóa trắng và đáp trả xâm phạm mà nó **shall [07.70]** liên tục giám sát lớp vỏ phát hiện xâm phạm và vào lúc phát hiện xâm phạm, **shall**

[07.71] ngay lập tức xóa trắng tất cả các SSP không được bảo vệ. Khả năng xóa trắng và đáp trả xâm phạm **shall [07.72]** duy trì hoạt động khi các SSP không được bảo vệ được chứa bên trong mô-đun mật mã.

7.7.4. Kiểm tra/bảo vệ chống lỗi do môi trường

7.7.4.1 Các yêu cầu chung về kiểm tra/bảo vệ chống lỗi do môi trường

Các thiết bị điện tử và kết cấu mạch được thiết kế để hoạt động bên trong một dải đặc biệt của các điều kiện môi trường. Các di chuyển có chủ ý hay vô ý ra ngoài các dải hoạt động thông thường đã được chỉ rõ về điện áp và nhiệt độ có thể gây ra sự hoạt động thất thường hoặc thất bại của các thiết bị hoặc kết cấu mạch điện tử có thể làm tổn hại đến tính an toàn của mô-đun mật mã. Sự đảm bảo hợp lý rằng tính an toàn của mô-đun mật mã sẽ không thể bị tổn hại bởi các điều kiện môi trường khắc nghiệt có thể được cung cấp bằng việc cho mô-đun sử dụng các đặc tính bảo vệ chống lỗi do môi trường (EFP) hoặc trải qua việc kiểm tra lỗi do môi trường (EFT).

Đối với các Mức an toàn 1 và 2 mô-đun là không được yêu cầu phải sử dụng các đặc tính bảo vệ chống lỗi do môi trường (EFP) hoặc phải trải qua kiểm tra lỗi do môi trường (EFP). Tại Mức an toàn 3, mô-đun **shall [07.73]** hoặc sẽ phải sử dụng các đặc tính bảo vệ chống lỗi do môi trường (EFP) hoặc phải trải qua kiểm tra lỗi do môi trường (EFT). Tại Mức an toàn 4, mô-đun **shall [07.74]** sử dụng các đặc tính bảo vệ chống lỗi do môi trường (EFP).

7.7.4.2. Các đặc tính bảo vệ chống lỗi do môi trường

Các đặc tính bảo vệ chống lỗi do môi trường (EFP) **shall [07.75]** bảo vệ mô-đun mật mã chống lại các điều kiện môi trường bất thường (ngẫu nhiên hoặc cảm ứng) khi nằm ngoài dải hoạt động bình thường của mô-đun mà chúng có thể làm tổn hại đến tính an toàn của mô-đun.

Mô-đun mật mã **shall [07.76]** giám sát và phản ứng đúng đắn khi nhiệt độ và điện áp hoạt động nằm ngoài các dải hoạt động bình thường đã được chỉ rõ.

Nếu nhiệt độ hoặc điện áp vượt ra ngoài dải hoạt động bình thường của mô-đun mật mã thì khả năng bảo vệ **shall [07.77]** hoặc là:

- Tắt mô-đun để ngăn chặn hoạt động tiếp,

  hoặc

- Ngay lập tức xóa trắng tất cả các SSP không được bảo vệ.

7.7.4.3. Các thủ tục kiểm tra lỗi do môi trường

Việc kiểm tra lỗi do môi trường (EFT) **shall [07.78]** bao hàm một sự kết hợp của phân tích, mô phỏng và kiểm tra mô-đun mật mã để cung cấp đảm bảo hợp lý rằng các điều kiện môi trường (ngẫu nhiên hoặc cảm ứng) khi vượt ra ngoài các dải hoạt động bình thường của mô-đun đối với nhiệt độ và điện áp, sẽ không tổn hại đến tính an toàn của mô-đun.

EFT **shall [07.79]** chứng tỏ rằng nếu nhiệt độ và điện áp hoạt động vượt ra khỏi dải hoạt động bình thường của mô-đun tạo ra thất bại, thì không bao giờ **shall [07.80]** gây tổn hại đến tính an toàn của mô-đun mật mã.

Dải nhiệt độ sẽ được kiểm tra **shall [07.81]** là từ một nhiệt độ bên trong dải nhiệt độ hoạt động bình thường tới nhiệt độ thấp nhất (nghĩa là lạnh nhất), mà chúng hoặc là (1) tắt mô-đun để ngăn chặn hoạt động tiếp hoặc (2) xóa trắng ngay lập tức tất cả các SSP không được bảo vệ; và từ một nhiệt độ bên trong dải nhiệt độ hoạt động bình thường tới nhiệt độ cao nhất (nghĩa là nóng nhất), mà nó hoặc là (1) tắt và chuyển sang một trạng thái có lỗi hoặc (2) xóa trắng tất cả các SSP không được bảo vệ. Dải nhiệt độ sẽ được kiểm tra **shall [07.82]** là từ -100°C đến +200°C (tương ứng từ -150°F đến +400°F),

tuy nhiên kiểm tra **shall 07.83]** được ngắt ngay khi hoặc (1) mô-đun bị tắt để ngăn chặn hoạt động tiếp, (2) tất cả các SSP không được bảo vệ sẽ bị xóa trắng ngay lập tức hoặc (3) mô-đun đi vào một trạng thái có lỗi. Nhiệt độ **shall [07.84]** được giám sát nội bộ tại các thành phần nhạy cảm và tại các thiết bị quan trọng và không chỉ tại ranh giới vật lý của mô-đun.

Dải điện áp được kiểm tra **shall [07.85]** phải giảm dần từ điện áp nằm bên trong dải điện áp hoạt động bình thường tới điện áp thấp hơn, hoặc là (1) tắt mô-đun để ngăn chặn hoạt động tiếp, hoặc là (2) ngay lập tức xóa trắng tất cả các SSP không được bảo vệ; và **shall [07.86]** tăng dần từ một điện áp bên trong dải điện áp hoạt động bình thường đến một điện áp cao hơn, hoặc (1) tắt mô-đun để ngăn chặn hoạt động tiếp, hoặc (2) ngay lập tức xóa trắng tất cả các SSP không được bảo vệ.

7.8 An toàn không xâm lấn

Các tấn công không xâm lấn nỗ lực gây tổn hại mô-đun mật mã bằng cách thu được thông tin hiểu biết về các CSP của mô-đun mà không cần sửa đổi hay xâm lấn về mặt vật lý đối với mô-đun. Các mô-đun có thể thực thi rất nhiều kỹ thuật khác nhau để giảm thiểu chống lại các kiểu tấn công này. Các độ đo kiểm tra đối với giảm thiểu tấn công không xâm lấn đối với mỗi một chức năng an toàn kết hợp được đề cập bởi Tiêu chuẩn này được tham chiếu đến trong Phụ lục F.

Điều khoản con này sẽ không được áp dụng nếu mô-đun mật mã không thực thi các kỹ thuật giảm thiểu tấn công không xâm lấn để bảo vệ các SSP không được bảo vệ của mô-đun khỏi các tấn công không xâm lấn được tham chiếu trong Phụ lục F.

Các kỹ thuật giảm thiểu tấn công không xâm lấn được thực thi bởi mô-đun mật mã để bảo vệ các SSP của mô-đun không được tham chiếu trong Phụ lục F **shall [08.01]** đáp ứng các yêu cầu trong 7.12.

Các kỹ thuật giảm thiểu tấn công không xâm lấn được thực thi bởi mô-đun mật mã để bảo vệ các SSP của mô-đun được tham chiếu trong Phụ lục F **shall [08.02]** đáp ứng các yêu cầu sau.

Các yêu cầu tài liệu được chỉ rõ trong A.2.8 **shall [08.03]** được cung cấp.

MỨC AN TOÀN 1 VÀ 2

Đối với các Mức an toàn 1 và 2, tài liệu **shall [08.04]** chỉ rõ tất cả các kỹ thuật giảm thiểu tấn công được sử dụng để bảo vệ các CSP của mô-đun từ các kỹ thuật giảm thiểu tấn công không xâm lấn được tham chiếu trong Phụ lục F. Tài liệu **shall [08.05]** bao gồm bằng chứng về tính hiệu quả của mỗi kỹ thuật giảm thiểu tấn công.

MỨC AN TOÀN 3

Ngoài các yêu cầu đối với mức an toàn 1 và 2, đối với Mức an toàn 3, mô-đun mật mã **shall [08.06]** được kiểm tra để đáp ứng các độ đo kiểm tra giảm thiểu tấn công không xâm lấn đã được phê duyệt đối với Mức an toàn 3 như được tham chiếu trong Phụ lục F.

MỨC AN TOÀN 4

Ngoài các yêu cầu an toàn đối với các Mức an toàn 1 và 2, đối với Mức an toàn 4, mô-đun mật mã **shall [08.07]** được kiểm tra để đáp ứng các độ đo kiểm tra giảm thiểu tấn công không xâm lấn đã được phê duyệt đối với Mức an toàn 4 như được tham chiếu trong Phụ lục F.

7.9 Quản lý tham số an toàn nhạy cảm

7.9.1 Các yêu cầu chung về quản lý tham số an toàn nhạy cảm

Các tham số an toàn nhạy cảm (SSP) bao gồm: Các tham số an toàn quan trọng (CSP) và Các tham số an toàn công khai (PSP). Các yêu cầu an toàn cho việc quản lý SSP bao gồm toàn bộ vòng đời của các SSP được sử dụng bởi mô-đun. Quản lý SSP bao gồm các bộ sinh bít ngẫu nhiên (RBG), tạo SSP, thiết lập SSP, vào/ra SSP, lưu trữ SSP và xóa trắng SSP không được bảo vệ.

Các CSP được mã hóa (encrypted) tham chiếu tới các CSP mà chúng được mã hóa (encrypted) sử dụng một chức năng an toàn được phê duyệt. Các CSP được mã hóa (encrypted) hoặc được làm khó hiểu, sử dụng các chức năng an toàn không được phê duyệt được coi như là bản rõ không được bảo vệ nằm bên trong phạm vi của Tiêu chuẩn này.

Các CSP **shall [09.01]** được bảo vệ bên trong mô-đun để chống lại truy cập, sử dụng, tiết lộ, sửa đổi và thay thế trái phép.

Các PSP **shall [09.02]** được bảo vệ bên trong mô-đun chống lại chỉnh sửa và thay thế trái phép.

Mô-đun **shall [09.03]** kết hợp một SSP được tạo ra, được nhập vào hoặc xuất ra khỏi mô-đun cùng với thực thể (có nghĩa con người, nhóm, vai trò hoặc tiến trình) mà SSP được gán cho họ.

Các giá trị băm của mật khẩu, thông tin trạng thái RBG và các giá trị tạo khóa trung gian **shall [09.04]** được coi là các CSP được bảo vệ.

Các yêu cầu tài liệu được chỉ rõ trong A.2.9 **shall** [09.05] được cung cấp.

7.9.2 Các bộ sinh bít ngẫu nhiên (RBG)

Mô-đun mật mã có thể chứa các RBG, một móc xích các RBG, hoặc có thể là chỉ là một RBG đơn lẻ. Các RBG đã được phê duyệt được liệt kê trong Phụ lục C.

Nếu một chức năng an toàn được phê duyệt, phương pháp sinh SSP hoặc thiết lập SSP yêu cầu các giá trị ngẫu nhiên, thì một RBG được phê duyệt **shall [09.06]** được sử dụng để cung cấp các giá trị này.

Nếu entropy được thu thập từ bên ngoài ranh giới mật mã của mô-đun, thì luồng dữ liệu được tạo ra sử dụng đầu vào entropy **shall [09.07]** được coi là một CSP.

7.9.3 Sinh tham số an toàn nhạy cảm

Mô-đun có thể sinh các SSP từ bên trong hoặc chúng có thể được nhận được từ các SSP được đưa vào mô-đun.

Việc gây tổn hại đến tính an toàn của phương pháp tạo SSP sử dụng đầu ra của một RBG đã được phê duyệt (chẳng hạn đoán giá trị mầm để khởi hoạt RBG tất định) **shall [09.08]** ít nhất đòi hỏi nhiều phép toán như việc xác định giá trị của SSP được sinh ra.

Các SSP được sinh ra bởi mô-đun từ hoặc là đầu ra của một RBG đã được phê duyệt hoặc nhận được từ một SSP nhập vào mô-đun và được sử dụng bởi một chức năng an toàn đã được phê duyệt hoặc phương pháp thiết lập SSP **shall [09.09]** được sinh ra sử dụng một phương pháp sinh SSP đã được phê duyệt được liệt kê trong Phụ lục D.

7.9.4 Thiết lập tham số an toàn nhạy cảm

Thiết lập SSP có thể bao gồm:

- Các phương pháp vận chuyển SSP *tự động* hoặc thỏa thuận SSP hoặc
- Nhập vào hay xuất ra SSP *thủ công* thông qua phương pháp trực tiếp hoặc điện tử.

Thiết lập SSP tự động **shall [09.10]** sử dụng một phương pháp đã được phê duyệt được liệt kê trong Phụ lục D. Thiết lập SSP thủ công **shall [09.11]** đáp ứng các yêu cầu của 7.9.5.

7.9.5 Nhập vào và xuất ra tham số an toàn nhạy cảm

Các SSP có thể được nhập vào hoặc xuất ra một cách thủ công từ mô-đun hoặc là trực tiếp (chẳng hạn được nhập vào thông qua một bàn phím hoặc bàn số hoặc được xuất ra thông qua một màn hiển thị trực quan) hoặc là bằng điện tử (chẳng hạn thông qua các thẻ thông minh/token, cạc PC, thiết bị

nạp khóa điện tử khác, hoặc hệ điều hành mô-đun). Nếu các SSP được nhập vào, xuất ra ra một cách thủ công từ mô-đun, thì đầu vào hoặc đầu ra **shall [09.12]** là thông qua các giao diện HMI, SFMI, HFMI hoặc HSMI (7.3.2) đã được xác định.

Tất cả các SSP được bảo vệ bằng mật mã, được nhập vào hoặc xuất ra khỏi mô-đun **shall [09.13]** được mã hóa (encrypted) sử dụng một chức năng an toàn đã được phê duyệt.

Đối với các SSP được nhập vào trực tiếp, thì các giá trị nhập vào có thể tạm thời được hiển thị để cho phép kiểm tra trực quan và cải thiện độ chính xác. Nếu các SSP được mã hóa (encrypted) được nhập trực tiếp vào mô-đun thì các giá trị bản rõ của các SSP **shall [09.14]** sẽ không cần được hiển thị. Các SSP được nhập vào trực tiếp (dạng rõ hoặc đã được mã hóa (encrypted)) **shall [09.15]** được kiểm tra trong quá trình nhập vào mô-đun để đảm bảo chính xác, sử dụng kiểm tra nhập vào thủ công có điều kiện được chỉ rõ trong 7.10.3.5.

Để ngăn chặn việc xuất ra vô ý của thông tin nhạy cảm, hai hành động bên trong độc lập **shall [09.16]** được yêu cầu để xuất ra bất kỳ CSP ở dạng rõ nào. Hai hành bên trong động độc lập **shall [09.17]** được chuyên biệt để dàn xếp việc xuất ra các CSP.

Đối với việc nhập vào hay xuất ra dạng điện tử thông qua một kết nối không dây; các CSP, các thành phần khóa và dữ liệu xác thực **shall [09.18]** được mã hóa (encrypted).

Các PSP được nhập vào thủ công không cần được xác thực bằng mật mã.

CÁC MỨC AN TOÀN 1 VÀ 2

Các CSP bản rõ, các thành phần khóa và dữ liệu xác thực có thể được nhập vào và xuất ra thông qua (các) cổng vật lý và (các) giao diện lôgic được chia sẻ với các cổng vật lý và các giao diện lôgic khác của mô-đun mật mã.

Đối với các mô-đun phần mềm hoặc các thành phần phần mềm của mô-đun phần mềm lai ghép, các CSP, các thành phần khóa và dữ liệu xác thực có thể được nhập vào hoặc xuất ra hoặc là dưới dạng rõ hoặc là dưới dạng đã được mã hóa (encrypted) với điều kiện là các CSP, các thành phần khóa và dữ liệu xác thực **shall [09.19]** được duy trì bên trong môi trường hoạt động và đáp ứng được các yêu cầu của 7.6.3.

MỨC AN TOÀN 3

Ngoài các Mức an toàn 1 và 2, đối với Mức an toàn 3, các CPS, các thành phần khóa và dữ liệu xác thực **shall [09.20]** được nhập vào hoặc xuất ra khỏi mô-đun hoặc là đã được mã hóa (encrypted) hoặc bằng một kênh tin cậy.

Các CSP mà là các khóa mật mã bí mật và khóa mật dạng rõ **shall [09.21]** được nhập vào hoặc xuất ra khỏi mô-đun sử dụng các thủ tục phân chia thông tin sư dụng một kênh tin cậy.

Nếu mô-đun sử dụng các thủ tục phân chia thông tin, thì mô-đun **shall [09.22]** sử dụng xác thực người vận hành dựa trên định danh tách biệt đối với việc nhập vào hoặc xuất ra mỗi thành phần khóa, và ít nhất hai thành phần khóa **shall [09.23]** được yêu cầu để khôi phục lại khóa mật mã gốc.

MỨC AN TOÀN 4

Ngoài Mức an toàn 3, đối với Mức an toàn 4, mô-đun **shall [09.24]** sử dụng xác thực người vận hành dựa trên định danh tách biệt đa yếu tố để nhập vào hoặc xuất ra mỗi thành phần khóa.

7.9.6 Lưu trữ tham số an toàn nhạy cảm

Các SSP được lưu trữ bên trong mô-đun có thể được lưu trữ hoặc là dưới dạng rõ hoặc được mã hóa (encrypted). Mô-đun **shall [09.25]** kết hợp mỗi SSP được lưu trữ bên trong mô-đun với thực thể (chẳng hạn người vận hành, vai trò, hoặc tiến trình) mà SSP được gán cho họ.

Truy cập vào các CSP dạng rõ bởi những người vận hành không được phân quyền **shall [09.26]** bị cấm. Việc sửa đổi các PSP bởi những người vận hành không được phân quyền **shall [09.27]** bị cấm.

7.9.7 Xóa trắng tham số an toàn nhạy cảm

Mô-đun **shall [09.28]** cung cấp các phương pháp để xóa trắng tất cả các SSP không được bảo vệ và các thành phần khóa bên trong mô-đun. Các SSP được lưu trữ tạm thời và các giá trị được lưu trữ khác được sở hữu bởi mô-đun cần được xóa trắng khi chúng không cần cho sử dụng tiếp nữa.

Một SSP bị xóa trắng **shall [09.29]** không thể được khôi phục hoặc tái sử dụng.

Việc xóa trắng các PSP đã được bảo vệ, các CSP đã được mã hóa (encrypted) hoặc các CSP mặt khác được bảo vệ bằng vật lý hoặc lôgic bên trong mô-đun hợp lệ nhúng bổ sung (đáp ứng được các yêu cầu của tiêu chuẩn này) là không được yêu cầu.

Các SSP không cần đáp ứng các yêu cầu xóa trắng này nếu chúng được sử dụng dành riêng để làm lộ dữ liệu bản rõ cho các tiến trình mà chúng là các bộ ủy nhiệm xác thực (chẳng hạn một CSP là một khóa khởi hoạt mô-đun).

Các tham số được sử dụng đơn lẻ cho các mục đích tự kiểm tra trong 7.10 không cần đáp ứng các yêu cầu xóa trắng.

MỨC AN TOÀN 1

Xóa trắng các SSP không được bảo vệ có thể được thực hiện bằng thủ tục bởi người vận hành mô-đun, và độc lập với điều khiển của mô-đun (chẳng hạn định dạng lại một ổ cứng, sự phá hủy của môi trường của mô-đun trong quá trình nhập lại).

CÁC MỨC AN TOÀN 2 VÀ 3

Mô-đun mật mã **shall [09.30]** thực hiện xóa trắng các SSP chưa được bảo vệ (chẳng hạn ghi đè, sử dụng tất cả các bít 0 hay 1 hay với dữ liệu ngẫu nhiên). Xóa trắng **shall [09.31]** loại trừ việc ghi đè của một SSP chưa được bảo vệ với một SSP chưa được bảo vệ khác. Các SSP tạm thời **shall [09.32]** bị xóa trắng khi chúng không còn cần thiết nữa. Mô-đun **shall [09.33]** cung cấp một chỉ báo trạng thái đầu ra khi xóa trắng được hoàn thành.

MỨC AN TOÀN 4

Ngoài các yêu cầu của các Mức an toàn 2 và 3, các yêu cầu sau **shall [09.34]** phải được đáp ứng:

- Xóa trắng **shall [09.35]** là ngay lập tức và không bị ngắt và **shall [09.36]** xảy ra trong một khoảng thời gian đủ nhỏ để cho ngăn chặn được việc khôi phục dữ liệu nhạy cảm giữa thời gian mà xóa trắng được khởi hoạt và xóa trắng thực tế được hoàn tất; và
- Tất cả các SSP chưa được bảo vệ **shall [09.37]** bị xóa trắng cho dù được bảo vệ ở dạng rõ hoặc được bảo vệ bằng mật mã, sao cho mô-đun được trả về trạng thái của nhà sản xuất.

7.10 Tự kiểm tra

7.10.1 Yêu cầu chung về tự kiểm tra

Tự kiểm tra có điều kiện và tiền hoạt động của mô-đun mật mã cung cấp cho người vận hành đảm bảo rằng các lỗi đã chưa đưa ra được mà chúng có thể ngăn cản hoạt động đúng đắn của mô-đun.Tất cả các tự kiểm tra **shall [10.01]** được thực hiện và sự xác định qua được hay không qua được **shall [10.02],** được thực hiện bởi mô-đun mà không có các điều khiển bên ngoài, các véc-tơ văn bản đầu vào được cung cấp bên ngoài, các kết quả đầu ra được kỳ vọng, hoặc sự can thiệp của người vận hành hoặc mô-đun sẽ hoạt động trong một chế độ đã được phê duyệt hay không được phê duyệt hay không.

Tự kiểm tra tiền hoạt động **shall [10.03]** được thực hiện và qua được thành công trước khi mô-đun đưa ra bất kì đầu ra dữ liệu qua giao diện đầu ra dữ liệu.

Tự kiểm tra có điều kiện **shall [10.04]** được thực hiện khi một chức năng hoặc một tiến trình an toàn áp dụng được gọi đến (tức là các chức năng an toàn mà đối với chúng các tự kiểm tra được yêu cầu).

Tất cả tự kiểm tra được nhận biết trong các chuẩn thuật toán nằm phía dưới (các Phụ lục C đến E) **shall [10.05]** được thực thi giống như khi được áp dụng được bên trong mô-đun mật mã. Tất cả các tự kiểm tra nhận biết được bổ sung hoặc thay thế những tự kiểm tra đã được chỉ rõ trong các chuẩn thuật toán nằm phía dưới (các Phụ lục C đến E) **shall [10.06]** được thực thi như được tham chiếu trong các Phụ lục từ C đến E đối với mỗi chức năng an toàn, phương pháp thiết lập SSP và cơ chế xác thực đã được phê duyệt.

Mô-đun mật mã có thể thực hiện kiểmm tra các chức năng quan trọng tiền hoạt động hoặc có điều kiện khác, ngoài các kiểm tra đã được chỉ rõ trong Tiêu chuẩn này.

Nếu mô-đun mật mã không qua được một tự kiểm tra, thì mô-đun **shall [10.07]** đi vào một trạng thái có lỗi và **shall [10.08]** đưa ra một chỉ báo lỗi như đã chỉ rõ trong 7.3.3. Mô-đun mật mã **shall not [10.09]** sẽ không cần thực hiện các phép toán mật mã bất kỳ hay đưa ra điều khiển và dữ liệu thông qua giao diện đầu ra điều khiển và dữ liệu trong khi ở trạng thái có lỗi. Mô-đun mật mã **shall [10.10]** sẽ không cần sử dụng bất kì chức năng nào mà nó dựa trên một hàm hoặc thuật toán mà nó không qua được một tự kiểm tra cho đến khi tự kiểm tra liên quan được lặp lại và qua được thành công. Nếu mô-đun không đưa ra một trạng thái lỗi trong lúc thất bại của tự kiểm tra của mô-đun, thì người vận hành mô-đun **shall [10.11]** có khả năng xác định xem nếu mô-đun đi vào được một trạng thái có lỗi một cách ẩn, thông qua một thủ tục không nhập nhằng đã được tài liệu hóa trong chính sách an toàn (Phụ lục B).

Tại các Mức an toàn 3 và 4, mô-đun **shall [10.12]** duy trì một nhật ký lỗi mà nó là truy cập được bởi một người vận hành mô-đun được phân quyền. Nhật ký lỗi đó **shall [10.13]** cung cấp thông tin, một cách tối thiểu, về sự kiện có lỗi hiện thời nhất (tức là, sự kiện mà tự kiểm tra đã thất bại).

Các yêu cầu tài liệu được chỉ rõ trong A.2.10 **shall [10.14]** được cung cấp.

7.10.2 Các tự kiểm tra tiền hoạt động

7.10.2.1 Các yêu cầu chung tự kiểm tra tiền hoạt động

Các kiểm tra tiền hoạt động **shall [10.15]** được thực hiện và qua được thành công bởi mô-đun mật mã giữa thời điểm mô-đun được bật nguồn hoặc được khởi hoạt (sau khi tắt nguồn, thiết lập lại, khởi động lại, khởi động nguội, ngắt nguồn điện,v.v...) và trước khi mô-đun chuyển đổi sang trạng thái hoạt động.

Mô-đun mật mã **shall [10.16]** thực hiện các kiểm tra tiền hoạt động sau, khi được áp dụng:

- Kiểm tra tính toàn vẹn phần mềm/phần sụn tiền hoạt động;
- Kiểm tra bỏ qua tiền hoạt động; và
- Kiểm tra các chức năng quan trọng tiền hoạt động.

7.10.2.2 Kiểm tra tính toàn vẹn phần mềm/ phần sụn tiền hoạt động

Tất cả các thành phần phần mềm và phần sụn bên trong ranh giới mật mã **shall [10.17]** được kiểm tra sử dụng một kỹ thuật toàn vẹn đã được phê duyệt thỏa mãn các yêu cầu đã được xác định trong 7.5. Nếu việc kiểm tra thất bại, thì kiểm tra tính toàn vẹn phần mềm/phần sụn tiền hoạt động **shall [10.18]** thất bại. Kiểm tra tính toàn vẹn phần mềm/phần sụn tiền hoạt động không được yêu cầu đối với phần mềm hoặc phần sụn bất kỳ đã được loại bỏ khỏi các yêu cầu an toàn của Tiêu chuẩn này hoặc đối với mã thực thi bất kì được lưu trữ trong bộ nhớ không cấu hình lại được.

Nếu mô-đun phần cứng không chứa hoặc phần mềm hoặc phần sụn, thì mô-đun **shall [10.19]**, ít nhất, thực thi một tự kiểm tra thuật toán mật mã như đã được chỉ rõ trong 7.10.3.2 như là một tự kiểm tra tiền hoạt động.

Thuật toán mật mã mà nó được sử dụng để thực hiện kỹ thuật toàn vẹn được phê duyệt đối với kiểm tra phần mềm/phần sụn tiền hoạt động **shall [10.20]** đầu tiên qua được tự kiểm tra thuật toán mật mã được chỉ rõ trong 7.10.3.2.

7.10.2.3 Kiểm tra bỏ qua tiền hoạt động

Nếu mô-đun mật mã thực thi một khả năng bỏ qua thì mô-đun **shall [10.21]** đảm bảo hoạt động chính xác việc kích hoạt khống chế lôgic khả năng cho qua bằng việc sử dụng lôgic đó. Mô-đun **shall [10.22]** cũng kiểm tra đường dẫn dữ liệu bằng cách:

- Thiết lập chuyển mạch bỏ qua để cung cấp xử lý mật mã và kiểm tra rằng dữ liệu được truyền qua cơ chế bỏ qua là được xử lý mật mã, và
- Thiết lập chuyển mạch bỏ qua để không cung cấp xử lý mật mã và kiểm tra rằng dữ liệu được truyền qua cơ chế bỏ qua là không được xử lý mật mã.

7.10.2.4 Kiểm tra các chức năng quan trọng tiền hoạt động

Có thể có các chức năng an toàn khác quan trọng đối với hoạt động an toàn của mô-đun mật mã mà **shall [10.23]** được kiểm tra như là một kiểm tra tiền hoạt động. Tài liệu **shall [10.24]** chỉ rõ các chức năng quan trọng tiền hoạt động đã được kiểm tra.

7.10.3 Các tự kiểm tra có điều kiện

7.10.3.1 Các yêu cầu chung tự kiểm tra có điều kiện

Các tự kiểm tra có điều kiện **shall [10.25]** được thực hiện bởi mô-đun mật mã khi các điều kiện được chỉ rõ để các kiểm tra sau xảy ra: Tự kiểm tra thuật toán mật mã, kiểm tra tính phù hợp theo cặp đôi, kiểm tra nạp phần mềm/phần sụn, kiểm tra nhập vào thủ công, kiểm tra bỏ qua có điều kiện và kiểm tra các chức năng quan trọng có điều kiện.

7.10.3.2 Tự kiểm tra thuật toán mật mã có điều kiện

Tự kiểm tra thuật toán mật mã. Một kiểm tra thuật toán mật mã **shall [10.26]** được tiến hành đối với tất cả các chức năng mật mã (ví dụ các chức năng an toàn, các phương pháp thiết lập SSP và xác thực) của mỗi thuật toán mật mã được phê duyệt được thực thi trong mô-đun mật mã như được tham chiếu trong các Phụ lục C đến E. Kiểm tra có điều kiện **shall [10.27]** được thực hiện trước lần sử dụng hoạt động đầu tiên của thuật toán mật mã.

Tự kiểm tra thuật toán mật mã có thể là một kiểm tra câu trả lời đã biết, một kiểm tra so sánh hoặc một kiểm tra phát hiện có lỗi.

Một kiểm tra câu trả lời đã biết gồm một tập các véc-tơ đầu vào đã biết (chẳng hạn: dữ liệu, nguyên liệu khóa hoặc các hằng số thay cho các bít ngẫu nhiên) mà chúng được vận hành bởi thuật toán mật mã để sinh ra một kết quả. Kết quả được so sánh với kết quả đầu ra kỳ vọng đã biết. Nếu đầu ra được tính toán không bằng câu trả lời đã biết, thì tự kiểm tra câu trả lời đã biết thuật toán mật mã **shall [10.28]** thất bại.

Tự kiểm tra thuật toán **shall [10.29]** sử dụng tối thiểu độ dài khóa đã được phê duyệt nhỏ nhất, kích thước mô-đun, số nguyên tố DSA, hoặc các đường cong tương ứng được hỗ trợ bởi mô-đun.

Nếu thuật toán đặc tả đa chế độ hoạt động (chẳng hạn ECB, CBC, v.v...), thì tối thiểu, một chế độ **shall [10.30]** được lựa chọn đối với tự kiểm tra được hỗ trợ bởi mô-đun hoặc như được chỉ rõ bởi thẩm quyền kiểm tra hợp lệ.

Các ví dụ về các kiểm tra câu trả lời đã biết:

- Các hàm một chiều: (Các) véc-tơ kiểm tra đầu vào sinh ra đầu ra mà nó **shall [10.31]** là đồng nhất với đầu ra kỳ vọng (chẳng hạn băm, các giá trị băm có khóa, xác thực thông điệp, RBG(véc-tơ entropy cố định), thỏa thuận SSP).
- Các hàm khả nghịch: Cả hàm chiều thuận và chiều nghịch **shall [10.32]** được tự kiểm tra (chẳng hạn: Mã hóa (encrypt) và giải mã khóa đối xứng, mã hóa (encrypt) và giải mã vận chuyển SSP, sinh và kiểm tra chữ ký số)

Kiểm tra so sánh so sánh đầu ra của hai hoặc nhiều thực thi thuật toán mật mã độc lập, nếu các đầu ra không bằng nhau, thì tự kiểm tra so sánh thuật toán mật mã **shall [10.33]** thất bại.

Kiểm tra phát hiện lỗi bao gồm việc thực thi các cơ chế phát hiện lỗi được tích hợp bên trong thuật toán mật mã, nếu một lỗi được phát hiện, thì tự kiểm tra phát hiện lỗi thuật toán mật mã **shall [10.34]** thất bại.

7.10.3.3 Kiểm tra tính phù hợp theo cặp đôi có điều kiện

Nếu mô-đun mật mã sinh ra các cặp khóa công khai hoặc bí mật, thì kiểm tra tính phù hợp theo cặp đôi **shall [10.35]** được thực hiện đối với mỗi cặp khóa riêng và công khai như được tham chiếu trong các Phụ lục từ C đến E đối với thuật toán mật mã áp dụng được.

7.10.3.4 Kiểm tra nạp phần sụn/ phần mềm có điều kiện

Nếu mô-đun mật mã có khả năng nạp phần mềm hoặc phần sụn từ một nguồn bên ngoài, thì các yêu cầu sau bổ sung cho các yêu cầu trong 7.4.3.4 **shall [10.36]** được thực hiện:

- Mô-đun mật mã **shall [10.37]** thực thi một kỹ thuật xác thực đã được phê duyệt để kiểm tra tính hợp lệ của phần mềm hay phần sụn được nạp vào;
- Khóa xác thực tham chiếu **shall [10.38]** được nạp một cách độc lập trong mô-đun trước thời điểm nạp phần mềm hay phần sụn; và
- Kỹ thuật xác thực đã được phê duyệt được áp dụng **shall [10.39]** được kiểm tra thành công hoặc kiểm tra nạp phần mềm/phần sụn **shall [10.40]** thất bại. Phần mềm hay phần sụn được nạp **shall [10.41]** không được sử dụng nếu kiểm tra nạp phần mềm/phần sụn thất bại.

7.10.3.5 Kiểm tra nhập vào thủ công có điều kiện

Nếu các SSP hoặc các thành phần khóa được nhập vào mô-đun mật mã trực tiếp bằng thủ công hoặc nếu lỗi thuộc về phần của người vận hành có thể tạo ra kết quả nhập vào không đúng của giá trị chủ định, thì các kiểm tra nhập vào thủ công sau **shall [10.42]** được thực hiện:

- SSP và các thành phần khóa **shall [10.43]** có mã phát hiện lỗi (EDC) được áp dụng hoặc **shall [10.44]** được nhập vào sử dụng các nhập vào lặp lại.

Nếu một EDC được sử dụng, thì EDC **shall [10.45]** ít nhất có chiều dài 16 bít. Nếu EDC không có thể được kiểm tra hoặc các nhập vào lặp lại không trùng nhau thì kiểm tra **shall [10.46]** thất bại.

7.10.3.6 Kiểm tra bỏ qua có điều kiện

Nếu mô-đun mật mã thực thi một khả năng bỏ qua, mà ở đó các dịch vụ có thể được cung cấp mà không xử lý mật mã (chẳng hạn vận chuyển bản rõ qua mô-đun) thì bộ các kiểm tra bỏ qua sau **shall [10.47]** được thực hiện để đảm bảo rằng một điểm thất bại đơn của các thành phần mô-đun sẽ không tạo ra đầu ra không chủ định của bản rõ.

Mô-đun mật mã **shall [10.48]** kiểm tra đối với hoạt động đúng đắn của các dịch vụ cung cấp xử lý mật mã khi một chuyển mạch xảy ra vào giữa một dịch vụ bỏ qua dành riêng và một dịch vụ mật mã dành riêng.

Nếu mô-đun mật mã có thể luân phiên một cách tự động giữa một dịch vụ bỏ qua và một dịch vụ mật mã, cung cấp một số dịch vụ có xử lý mật mã và một số dịch vụ không có xử lý mật mã, thì mô-đun **shall [10.49]** kiểm tra đối với hoạt động đúng đắn của các dịch vụ cung cấp xử lý mật mã khi cơ chế kiểm chế thủ tục chuyển mạch được sửa đổi (chẳng hạn một bảng địa chỉ IP nguồn/đích).

Nếu mô-đun mật mã duy trì thông tin nội bộ quản lý khả năng bỏ qua thì mô-đun **shall [10.50]** kiểm tra tính toàn vẹn của thông tin quản lý thông qua kỹ thuật toàn vẹn đã phê duyệt trực tiếp ngay trước khi việc sửa đổi thông tin quản lý, và **shall [10.51]** tạo ra một giá trị kiểm tra tính toàn vẹn mới, sử dụng kỹ thuật toàn vẹn đã được phê duyệt ngay lập tức theo sau việc sửa đổi.

7.10.3.7 Kiểm tra các chức năng quan trọng có điều kiện

Có thể là các chức năng an toàn khác quan trọng cho hoạt động an toàn của mô-đun mật mã mà nó **shall [10.52]** được kiểm tra như một tự kiểm tra có điều kiện.

7.10.3.8 Các tự kiểm tra định kỳ

CÁC MỨC AN TOÀN 1 VÀ 2

Mô-đun mật mã **shall [10.53]** cho phép những người vận hành khởi hoạt các tự kiểm tra tiền hoạt động hoặc có điều kiện theo yêu cầu đối với việc kiểm tra định kỳ của mô-đun. Cách chấp nhận được đối với việc khởi động theo yêu cầu của các tự kiểm tra định kỳ là: dịch vụ được cung cấp, tái thiết lập, tái khởi động hoặc chu trình bật nguồn.

CÁC MỨC AN TOÀN 3 VÀ 4

Ngoài các yêu cầu tại các Mức an toàn 1 và 2, mô-đun mật **shall [10.54]** lặp lại vào một khoảng thời gian được xác định một cách tự động, không có đầu vào hay điều khiển từ bên ngoài, thực hiện các tự kiểm tra tiền hoạt động hoặc có điều kiện. Khoảng thời gian và các điều kiện bất kỳ mà chúng có thể tạo ra ngắt các hoạt động của mô-đun trong suốt thời gian để lặp lại các tự kiểm tra có điều kiện hoặc tiền hoạt động **shall [10.55]** được chỉ rõ trong chính sách an toàn (Phụ lục B) (Ví dụ, nếu một mô-đun đang thực hiện các dịch vụ quan trọng không thể dừng lại và khoảng thời gian cần trôi qua để khởi động các tự kiểm tra tiền hoạt động; các tự kiểm tra có thể bị trì hoãn lại sau khoảng thời trôi qua lần nữa).

7.11 Đảm bảo vòng đời

7.11.1 Các yêu cầu chung đảm bảo vòng đời

Đảm bảo vòng đời tham chiếu đến việc sử dụng các thực hành tốt nhất bởi nhà cung cấp mô-đun mật mã trong suốt quá trình thiết kế, phát triển, vận hành và kết thúc đời sống của mô-đun mật mã, cung cấp đảm bảo rằng mô-đun được thiết kế, được phát triển, được kiểm tra, được cấu hình, được phân phối, được cài đặt và được loại bỏ đúng đắn và rằng tài liệu hướng dẫn người vận hành thích hợp được cung cấp. Các yêu cầu an toàn được chỉ rõ đối với quản lý cấu hình, thiết kế, mô hình trạng thái hữu hạn, phát triển, kiểm tra, phân phối và vận hành, và tài liệu hướng dẫn.

Các yêu cầu tài liệu được chỉ rõ trong A.2.11 **shall [11.01]** được cung cấp.

7.11.2 Quản lý cấu hình

Quản lý cấu hình chỉ rõ các yêu cầu đối với một hệ thống quản lý cấu hình được thực thi bởi nhà một nhà cung cấp mô-đun mật mã, cung cấp sự đảm bảo rằng tính toàn vẹn của mô-đun mật mã được bảo

toàn bằng việc yêu cầu nguyên tắc và kiểm soát trong các quá trình cải tiến và sửa đổi mô-đun mật mã và tài liệu liên quan. Một hệ thống quản lý cấu hình được thực thi để ngăn chặn các sửa đổi vô ý hoặc trái phép và cung cấp sự truy tìm nguồn gốc thay đổi đối với mô-đun mật mã và tài liệu liên quan.

CÁC MỨC AN TOÀN 1 VÀ 2

Các yêu cầu an toàn sau **shall [11.02]** được áp dụng cho các mô-đun mật mã đối với các Mức an toàn 1 và 2:

- Một hệ thống quản lý cấu hình **shall [11.03]** được sử dụng cho việc phát triển mô-đun mật mã và các thành phần mô-đun bên trong ranh giới mật mã và của các tài liệu kết hợp với mô-đun.
- Mỗi phiên bản của mỗi mục cấu hình (chẳng hạn mô-đun mật mã, các phần phần cứng của mô-đun, các thành phần phần mềm của mô-đun, HDL mô-đun, hướng dẫn người sử dụng, chính sách an toàn,v.v...) bao gồm mô-đun và tài liệu kèm theo **shall [11.04]** được gán và dán nhãn với một định danh duy nhất; và
- Hệ thống quản lý cấu hình **shall [11.05]** theo dõi và duy trì các thay đổi đối với việc định danh và phiên bản hoặc phiên bản chỉnh sửa lại của mỗi khoản cấu hình trong suốt vòng đời của mô-đun mật mã đã được kiểm tra hợp lệ.

CÁC MỨC AN TOÀN 3 VÀ 4

Ngoài các yêu cầu đối với các Mức an toàn 1 và 2, các khoản cấu hình **shall [11.06]** được quản lý sử dụng một hệ thống quản lý cấu hình tự động.

7.11.3 Thiết kế

Một thiết kế là một giải pháp kỹ thuật mà nó đề cập đến đặc tả chức năng cho mô-đun mật mã. Thiết kế được chủ định để cung cấp đảm bảo rằng đặc tả chức năng của mô-đun mật mã tương ứng với chức năng chủ định được mô tả trong chính sách an toàn.

Các mô-đun mật mã **shall [11.07]** được thiết kế để cho phép kiểm tra tất cả các dịch vụ liên quan đến an toàn được cung cấp.

7.11.4 Mô hình trạng thái hữu hạn

Hoạt động của mô-đun mật mã **shall [11.08]** được đặc tả sử dụng một mô hình trạng thái hữu hạn (hoặc tương đương) được biểu diễn bởi một sơ đồ chuyển dịch trạng thái và một bảng chuyển dịch trạng thái và các mô tả trạng thái. FSM **shall [11.09]** được chi tiết hóa đủ để chứng tỏ rằng mô-đun mật mã tuân thủ với tất cả các yêu cầu của Tiêu chuẩn này.

FSM của mô-đun mật mã **shall [11.10]** tối thiểu bao gồm các trạng thái hoạt động và có lỗi sau:

- *Trạng thái bật/tắt nguồn.* Một trạng thái mà tại đó mô-đun được tắt nguồn, đặt ở chế độ chờ (bộ nhớ không ổn định được duy trì), hoặc trạng thái hoạt động được bảo toàn trong bộ nhớ ổn định (chẳng hạn chế ngừng hoạt động) và tại đó, nguồn sơ cấp, thứ cấp hoặc nguồn dự phòng được áp dụng cho mô-đun. Trạng thái này có thể là phân biệt giữa các nguồn điện được áp dụng cho mô-đun mật mã. Đối với mô-đun phần mềm, bật nguồn là một hành động sinh ra một ảnh thực hiện (executable image) của mô-đun mật mã đó.
- *Trạng thái khởi hoạt chung:* Một trạng thái mà tại đó mô-đun mật mã trải qua quá trình khởi hoạt trước khi mô-đun chuyển dịch sang trạng thái đã được phê duyệt.

- *Trạng thái chuyên viên mật mã:* Một trạng thái mà tại đó các dịch vụ của chuyên viên mật mã được thực hiện (chẳng hạn như khởi hoạt mật mã, quản trị an toàn, và quản lý khóa).
- *Trạng thái nhập vào CSP:* Một trạng thái để nhập các CSP vào mô-đun mật mã.
- *Trạng thái người sử dụng:* (nếu một vai trò người sử dụng được thực thi): Một trạng thái tại đó những người sử dụng được phép đạt được các dịch vụ an toàn, thực hiện các hoạt động mật mã hoặc thực hiện các chức năng đã phê duyệt khác.
- *Trạng thái được phê duyệt:* Một trạng thái mà tại đó các chức năng an toàn được phê duyệt được thực hiện.
- *Trạng thái tự kiểm tra:* Một trạng thái tại đó mô-đun mật mã thực hiện các tự kiểm tra.
- *Trạng thái có lỗi:* Một trạng thái khi mô-đun mật mã gặp phải điều kiện có lỗi (chẳng hạn một tự kiểm tra thất bại). Có thể có một hoặc nhiều điều kiện có lỗi gây ra trong mỗi mô-đun đơn lẻ một trạng thái lỗi. Các trạng thái có lỗi có thể bao gồm các lỗi "cứng" chỉ ra một trục trặc thiết bị và có thể yêu cầu bảo trì, bảo dưỡng hoặc sửa chữa mô-đun mật mã, hoặc các lỗi "mềm" có thể khôi phục được có thể yêu cầu khởi hoạt hoặc thiết lập lại mô-đun. Khôi phục từ các trạng thái có lỗi **shall [11.11]** là có thể được, ngoại trừ đối với các trạng thái có lỗi được gây ra bởi các lỗi "cứng" mà chúng yêu cầu bảo trì, bảo dưỡng hoặc sửa chữa mô-đun mật mã.

Mỗi dịch vụ mô-đun mật mã khác biệt, sử dụng chức năng an toàn, trạng thái có lỗi, tự kiểm tra hoặc xác thực người vận hành **shall [11.12]** được mô tả như một trạng thái tách biệt.

Chuyển đổi sang trạng thái Chuyên viên mật mã từ vai trò nào đó khác với vai trò Chuyên viên mật mã **shall [11.13]** bị cấm.

Mô-đun mật mã có thể chứa các trạng thái khác bao gồm, nhưng không hạn chế các trạng thái sau đây:

Trạng thái cho qua: Một trạng thái mà tại đó một dịch vụ như là một kết quả của cấu hình mô-đun hoặc can thiệp của người vận hành, gây ra đầu ra ở dạng rõ của một dữ liệu đặc biệt hoặc mục trạng thái (status item) mà nó bình thường được xuất ra dưới dạng được mã hóa (encrypt).

Trạng thái không hoạt động: Một trạng thái mà tại đó mô-đun mật mã không hoạt động (ví dụ: nguồn thấp, bị treo hoặc không hoạt động).

7.11.5 Phát triển

Một quá trình *phát triển* đúng đắn cung cấp đảm bảo rằng việc thực thi của mô-đun mật mã tương ứng với đặc tả chức năng và chính sách an toàn mô-đun, rằng mô-đun mật mã được bảo trì và rằng mô-đun mật mã đã hợp lệ là có thể được tái sản xuất. Điều khoản này chỉ rõ các yêu cầu an toàn để thể hiện chức năng an toàn của mô-đun mật mã tại các mức trừu tượng khác nhau từ đặc tả chức năng đến thể hiện thực thi.

MỨC AN TOÀN 1

Các yêu cầu sau **shall [11.14]** áp dụng cho các mô-đun mật mã đối với Mức an toàn 1:

- Nếu mô-đun mật mã chứa phần mềm hoặc phần sụn, mã nguồn, tham chiếu ngôn ngữ, các trình biên dịch, các phiên bản trình biên dịch và các tùy chọn trình biên dịch, các trình liên kết và các tùy chọn trình liên kết, các thư viện thời gian chạy và các thiết lập thư viện thời gian chạy, các thiết lập cấu hình, các tiến trình và các phương thức được xây dựng, các tùy chọn được

xây dựng, các biến môi trường và tất cả các tài nguyên khác được sử dụng để biên dịch và liên kết mã nguồn thành dạng thực thi **shall [11.15]** được dõi vết sử dụng hệ thống quản lý cấu hình;

- Nếu mô-đun mật mã chứa phần mềm hoặc phần sụn, các mã nguồn **shall [11.16]** được chú giải với các lời giải thích mà chúng mô tả sự tương ứng của phần mềm hoặc phần sụn với thiết kế của mô-đun;
- Nếu mô-đun mật mã chứa phần cứng, tài liệu **shall [11.17]** chỉ rõ các sơ đồ mạch và/hoặc ngôn ngữ mô tả phần cứng (HDL), như có thể áp dụng được;
- Nếu mô-đun mật mã chứa phần cứng, HDL **shall [11.18]** được chú giải với các lời giải thích mà chúng mô tả sự tương ứng của phần cứng với thiết kế của mô-đun;
- Đối với các mô-đun mật mã phần mềm và phần sụn và thành phần phần mềm hoặc phần sụn của mô-đun lai ghép:
    - Kết quả của các cơ chế kỹ thuật xác thực và toàn vẹn được chỉ rõ trong 7.5 và 7.10 **shall [11.19]** được tính toán và tích hợp vào trong mô-đun phần mềm hoặc phần sụn bởi nhà cung cấp trong quá trình phát triển mô-đun;
    - Tài liệu mô-đun mật mã **shall [11.20]** chỉ rõ trình biên dịch, các thiết lập cấu hình và các phương pháp để biên dịch mã nguồn thành một dạng thực hiện; và
    - Mô-đun mật mã **shall [11.21]** được phát triển sử dụng các công cụ phát triển sản phẩm đã được kiểm tra chất lượng (ví dụ các trình biên dịch).

CÁC MỨC AN TOÀN 2 VÀ 3

Ngoài các yêu cầu đối với các Mức an toàn 1, các yêu cầu sau **shall [11.22]** áp dụng cho các mô-đun mật mã đối với các Mức an toàn 2 và 3:

- Tất cả phần mềm hoặc phần sụn **shall [11.23]** được thực thi sử dụng ngôn ngữ bậc cao không đăng ký bản quyền (non-proprietary) sở hữu hoặc cơ sở hợp lý **shall [11.24]** được cung cấp để sử dụng một ngôn ngữ bậc thấp (chẳng hạn ngôn ngữ assembly hoặc vi mã) nếu là thiết yếu đối với năng suất hoạt động của mô-đun hoặc khi một ngôn ngữ bậc cao là không có sẵn.
- Các mạch tích hợp tùy chỉnh bên trong mô-đun mật mã **shall [11.25]** được thực thi, sử dụng một ngôn ngữ mô tả phần cứng bậc cao (HDL) (chẳng hạn như VHDL hoặc Verilog); và
- Các mô-đun mật mã phần mềm hoặc phần sụn **shall [11.26]** được thiết kế và thực thi theo cách để tránh sử dụng mã, các tham số hoặc các ký hiệu không cần thiết đối với chức năng và thực hiện của mô-đun.

MỨC AN TOÀN 4

Ngoài các yêu cầu đối với các Mức an toàn 1, 2 và 3, yêu cầu sau **shall [11.27]** được áp dụng cho các mô-đun mật mã đối với Mức an toàn 4:

- Đối với mỗi thành phần phần cứng và phần mềm mô-đun mật mã, tài liệu **shall [11.28]** được chú giải với các giải thích chỉ rõ:(1) các tiền điều kiện được yêu cầu dựa trên việc nhập vào mỗi thành phần mô-đun, chức năng và thủ tục để thực hiện đúng đắn và (2) các hậu điều kiện được kỳ vọng là đúng khi việc thực hiện mỗi thành phần mô-đun, chức năng và thủ tục được hoàn thành. Các tiền điều kiện và hậu điều kiện có thể được chỉ rõ sử dụng ký hiệu bất kì mà nó

được chi tiết hóa vừa đủ để giải thích một cách đầy đủ và không nhập nhằng hành vi của thành phần, chức năng và thủ tục của mô-đun mật mã.

7.11.6 Kiểm tra nhà cung cấp

Điều khoản này sẽ chỉ rõ các yêu cầu đối với *việc kiểm tra nhà cung cấp* mô-đun mật mã, bao gồm kiểm tra chức năng an toàn được thực thi trong mô-đun mật mã, cung cấp bảo đảm rằng mô-đun mật mã cư xử tuân theo chính sách an toàn và các đặc tả chức năng của mô-đun.

CÁC MỨC AN TOÀN 1 VÀ 2

Đối với các Mức an toàn 1 và 2, tài liệu **shall [11.29]** đặc tả việc kiểm tra chức năng được thực hiện trên mô-đun mật mã.

Đối với các mô-đun mật mã phần mềm hoặc phần sụn và thành phần phần mềm hoặc phần sụn của mô-đun lai ghép, nhà cung cấp **shall [11.30]** sử dụng các công cụ chuẩn đoán an toàn tự động (ví dụ phát hiện tràn bộ đệm).

CÁC MỨC AN TOÀN 3 VÀ 4

Ngoài các yêu cầu đối với các Mức an toàn 1 và 2, tài liệu **shall [11.31]** chỉ rõ các thủ tục và các kết quả kiểm tra và các kết quả của việc kiểm tra mức thấp được thực hiện trên mô-đun mật mã.

7.11.7 Phân phối và vận hành

Điều khoản này chỉ rõ các yêu cầu an toàn đối với việc phân phối, cài đặt, và khởi động an toàn của mô-đun mật mã, cung cấp sự đảm bảo rằng mô-đun được phân phối một cách an toàn tới những người vận hành được phân quyền và được cài đặt và khởi hoạt theo một cách an toàn và đúng đắn.

MỨC AN TOÀN 1

Đối với Mức an toàn 1, tài liệu **shall [11.32]** chỉ rõ các thủ tục cài đặt, khởi hoạt và khởi động an toàn của mô-đun mật mã.

MỨC AN TOÀN 2 VÀ 3

Ngoài yêu cầu của Mức an toàn 1, tài liệu **shall [11.33]** chỉ rõ các thủ tục được yêu cầu để duy trì sự ar toàn trong khi phân phối, cài đặt và khởi hoạt các phiên bản của mô-đun mật mã đối với những người vận hành được phân quyền. Các thủ tục **shall [11.34]** chỉ rõ xem làm thế nào phát hiện được xâm phạm trong quá trình phân phối, cài đặt và khởi hoạt mô-đun đối với những người vận hành được phân quyền.

MỨC AN TOÀN 4

Ngoài các yêu cầu của các Mức an toàn 1, 2 và 3, các thủ tục **shall [11.35]** yêu cầu người vận hành được phân quyền xác thực mô-đun sử dụng dữ liệu xác thực được cung cấp bởi nhà cung cấp.

7.11.8 Kết thúc vòng đời

Điều khoản này chỉ rõ các yêu cầu an toàn khi mô-đun mật mã không tiếp tục sử dụng nữa hoặc không có chủ định sử dụng tiếp bởi người vận hành.

CÁC MỨC AN TOÀN 1 VÀ 2

Đối với Mức an toàn 1 và 2, tài liệu **shall [11.36]** chỉ rõ các thủ tục đối với làm vệ sinh an toàn mô-đun mật mã. Làm vệ sinh là một quá trình loại bỏ các thông tin nhạy cảm (chẳng hạn như các SSP, dữ liệu

người sử dụng,v.v...) khỏi mô-đun sao cho các dữ liệu nhạy cảm có thể được phân phối tới những người vận hành khác hoặc bị loại bỏ.

CÁC MỨC AN TOÀN 3 VÀ 4

Ngoài yêu cầu của các Mức an toàn 1 và 2, tài liệu **shall [11.37]** chỉ rõ các thủ tục được yêu cầu để phá hủy an toàn mô-đun.

7.11.9 Các tài liệu hướng dẫn

Các yêu cầu trong điều khoản này nhằm để đảm bảo rằng tất cả các thực thể sử dụng mô-đun mật mã có các hướng dẫn và thủ tục đầy đủ quản lý và sử dụng mô-đun trong một chế độ hoạt động đã được phê duyệt.

Tài liệu hướng dẫn bao gồm hướng dẫn dành cho người quản trị và người không phải người quản trị.

Tài liệu hướng dẫn dành cho người quản trị **shall [11.38]** chỉ rõ:

- Các chức năng quản trị, các sự kiện an toàn, các tham số an toàn (và các giá trị tham số khi phù hợp), các cổng vật lý, và giao diện lôgic của mô-đun mật mã có sẵn cho vai trò chuyên viên mật mã và/hoặc các vai trò quản trị khác;
- Các thủ tục được yêu cầu để duy trì các cơ chế xác thực người vận hành độc lập là độc lập về chức năng;
- Các thủ tục về việc làm thế nào để quản trị mô-đun mật mã trong chế độ hoạt động đã được phê duyệt; và
- Các giả thiết về hành vi của người sử dụng mà chúng có liên quan tới hoạt động an toàn của mô-đun mật mã.

Tài liệu hướng dẫn dành cho người không phải người quản trị **shall [11.39]** chỉ rõ:

- Các chức năng an toàn đã được phê duyệt và không được phê duyệt, các cổng vật lý, các giao diện lôgic có sẵn cho những người sử dụng của mô-đun mật mã; và
- Tất cả các trách nhiệm của người sử dụng cần thiết cho chế độ hoạt động đã được phê duyệt của mô-đun mật mã.

7.12 Giảm thiểu các tấn công khác

Tính nhạy cảm của mô-đun mật mã đối với các tấn công không được xác định ở bất kỳ đâu trong Tiêu chuẩn này phụ thuộc vào kiểu mô-đun, thực thi và môi trường thực thi. Các tấn công như vậy có thể là mối quan tâm đặc biệt đối với các mô-đun mật mã được thực thi trong các môi trường thù địch (chẳng hạn nơi mà những kẻ tấn công có thể là những người vận hành được phân quyền của mô-đun). Các tấn công này nói chung dựa trên phân tích thông tin thu được từ các nguồn mà chúng là bên ngoài về mặt vật lý đối với mô-đun. Trong tất cả các trường hợp, các tấn công cố gắng xác định một thông tin hiểu biết nào đó về các SSP bên trong mô-đun mật mã.

Các yêu cầu tài liệu được chỉ rõ trong A.2.12 **shall [12.01]** được cung cấp.

CÁC MỨC AN TOÀN 1, 2 VÀ 3

Nếu mô-đun mật mã được thiết kế để giảm thiểu một hoặc nhiều (các) tấn công cụ thể không được xác định ở bất kỳ đâu trong Tiêu chuẩn này, thì các tài liệu hỗ trợ của mô-đun **shall [12.02]** liệt kê (các) tấn công mà mô-đun được thiết kế để làm giảm thiểu các tấn công đó. Sự tồn tại và hoạt động chức năng

đúng đắn của các cơ chế an toàn được sử dụng để giảm thiểu (các) tấn công sẽ được kiểm tra hợp lệ khi các yêu cầu và các kiểm tra kết hợp được phát triển.

MỨC AN TOÀN 4

Ngoài các yêu cầu đối với các Mức an toàn 1, 2 và 3, thì yêu cầu sau **shall [12.03]** được áp dụng cho các mô-đun mật mã đối với Mức an toàn 4:

- Nếu sự giảm thiểu các tấn công cụ thể không được xác định ở bất kỳ đâu trong Tiêu chuẩn này được yêu cầu, thì tài liệu **shall [12.04]** chỉ rõ các phương pháp được sử dụng để làm giảm thiểu các tấn công và các phương pháp kiểm tra tính hiệu quả của các kỹ thuật giảm thiểu đó.

Phụ lục A

(Quy định)

Các yêu cầu về tài liệu

A.1 Mục đích

Phụ lục này chỉ rõ tài liệu tối thiểu mà nó **shall [A.01]** được yêu cầu đối với một mô-đun mật mã mà nó sẽ phải trải qua một lược đồ kiểm tra độc lập.

A.2 Các khoản mục

A.2.1 Tổng quan

Không có các yêu cầu tài liệu chung được chỉ rõ.

A.2.2 Đặc tả mô-đun mật mã

- Đặc tả kiểu mô-đun (mô-đun phần cứng, phần mềm, phần sụn, phần mềm lai ghép hoặc phần sụn lai ghép). *(các Mức an toàn 1, 2, 3 và 4)*
- Đặc tả ranh giới mô-đun. *(các Mức an toàn 1, 2, 3 và 4)*
- Đặc tả các thành phần phần cứng, phần mềm và phần sụn của mô-đun mật mã và mô tả cấu hình vật lý của mô-đun. *(các Mức an toàn 1, 2, 3 và 4)*
- Đặc tả các thành phần phần cứng, phần mềm hoặc phần sụn của mô-đun mật mã mà chúng được loại bỏ khỏi các yêu cầu an toàn của Tiêu chuẩn này và một giải thích cơ sở hợp lý đối với sự loại bỏ. *(các Mức an toàn 1, 2, 3 và 4)*
- Đặc tả các cổng vật lý và giao diện lôgic của mô-đun mật mã. *(các Mức an toàn 1, 2, 3 và 4)*
- Đặc tả các kiểm soát thủ công hoặc lôgic của mô-đun mật mã, các chỉ báo trạng thái vật lý hoặc lôgic và các đặc tính vật lý, lôgic và điện. *(các Mức an toàn 1, 2, 3 và 4)*
- Đặc tả tất cả các chức năng an toàn, cả được phê duyệt và chưa được phê duyệt, mà chúng được sử dụng bởi mô-đun mật mã và đặc tả tất cả các chế độ hoạt động cả được phê duyệt và chưa được phê duyệt. *(các Mức an toàn 1, 2, 3 và 4)*
- Sơ đồ khối mô tả tất cả các thành phần phần cứng chính yếu của mô-đun mật mã và các kết nối thành phần bao gồm bất kỳ các bộ vi xử lý, các bộ đệm vào/ra, các bộ đệm rõ/mã, các bộ đệm điều khiển, lưu trữ khóa, bộ nhớ làm việc và bộ nhớ chương trình nào. *(các Mức an toàn 1, 2, 3 và 4)*
- Đặc tả thiết kế phần cứng, phần mềm và phần sụn của mô-đun mật mã. *(các Mức an toàn 1, 2, 3 và 4)*
- Đặc tả tất cả thông tin liên quan đến an toàn, bao gồm các khóa mật mã bí mật và mật (cả dạng rõ và dạng mã hóa (encrypt)), dữ liệu xác thực (ví dụ như các mật khẩu, các số PIN), các CSP, PSP và thông tin được bảo vệ khác (ví dụ các sự kiện kiểm toán, dữ liệu kiểm toán) mà việc làm lộ hoặc sửa đổi chúng có thể làm hại tính an toàn của mô-đun mật mã. *(các Mức an toàn 1, 2, 3 và 4)*
- Đặc tả về việc mô-đun hỗ trợ một chế độ hoạt động xuống cấp như thế nào. *(các Mức an toàn 1, 2, 3 và 4)*
- Đặt tả chính sách an toàn của mô-đun mật mã bao gồm các quy tắc nhận được từ các yêu cầu của Tiêu chuẩn này và các quy tắc nhận được từ các yêu cầu bổ sung bất kỳ được áp đặt bởi nhà cung cấp. *(các Mức an toàn 1, 2, 3 và 4)*

A.2.3 Các giao diện mô-đun mật mã

- Đặc tả đầu vào dữ liệu, đầu ra dữ liệu, đầu vào điều khiển, đầu ra điều khiển, đầu ra trạng thái và các giao diện nguồn điện, cả vật lý và lôgic (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả giao diện kênh tin cậy (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả các ngoại lệ và cơ sở hợp lý nếu giao diện đầu ra điều khiển không bị chặn cấm trong suốt trạng thái có lỗi (các Mức an toàn 1, 2, 3 và 4).

A.2.4 Các vai trò, các dịch vụ và xác thực

- Đặc tả tất cả các vai trò được phân quyền được hỗ trợ bởi mô-đun mật mã (các Mức an toàn 1, 2, 3 và 4).
- Đặt tả tất cả dịch vụ, các hoạt động hoặc các chức năng được cung cấp bởi mô-đun mật mã cả đã được phê duyệt và chưa được phê duyệt. Đối với mỗi dịch vụ, đặc tả đầu vào dịch vụ. đầu ra dịch vụ tương ứng và (các) vai trò được phân quyền mà tại đó dịch vụ không thể được thực hiện (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả các dịch vụ bất kỳ được cung cấp bởi mô-đun mật mã mà đối với nó người vận hành không được yêu cầu đảm nhiệm một vai trò được phân quyền và các dịch vụ này không làm sửa đổi, tiết lộ hoặc thay thế các khóa mật mã và các CSP như thế nào hoặc mặt khác chúng ảnh hưởng đến tính an toàn của mô-đun ra làm sao (các Mức an toàn 1, 2, 3 và 4)...
- Đặc tả các cơ chế xác thực được hỗ trợ bởi mô-đun mật mã, các kiểu dữ liệu xác thực được yêu cầu để thực thi các cơ chế xác thực được hỗ trợ, các phương pháp được phân quyền được sử dụng để kiểm soát truy cập vào mô-đun trong lần đầu tiên và khởi hoạt cơ chế xác thực, và độ mạnh của các cơ chế xác thực được hỗ trợ bởi mô-đun bao gồm cơ sở hợp lý hỗ trợ việc sử dụng của đa cơ chế xác thực (các Mức an toàn 2, 3 và 4).
- Đặc tả các dịch vụ của các mô-đun mà nó chỉ ra thông tin đánh số phiên bản của mô-đun, chỉ ra trạng thái, thực hiện các tự kiểm tra, thực hiện các chức năng an toàn đã phê duyệt và thực hiện xóa trắng (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả các cơ chế bỏ qua (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả các cơ chế nạp phần mềm hoặc phần sụn (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả các kiểm soát và giao diện khả năng đầu ra mật mã tự khởi động (các Mức an toàn 1, 2, 3 và 4).

A.2.5 An toàn phần mềm/phần sụn.

- Đặc tả các kỹ thuật toàn vẹn đã phê duyệt được sử dụng (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả phương pháp để người vận hành thực hiện kỹ thuật toàn vẹn đã phê duyệt theo yêu cầu (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả dạng mã thực hiện (các Mức an toàn 2, 3 và 4).

A.2.6 Môi trường hoạt động

- Đặc tả môi trường hoạt động đối với mô-đun mật mã, bao gồm, nếu áp dụng được, hệ điều hành được sử dụng bởi mô-đun (các Mức an toàn 1, 2).
- Đặc tả về các quy tắc an toàn, các thiết lập hoặc các hạn chế đối với cấu hình của môi trường hoạt động (các Mức an toàn 1, 2).

- Tài liệu hướng dẫn người quản trị để cấu hình hệ điều hành theo các yêu cầu đặc tả (Mức an toàn 2).

A.2.7 An toàn vật lý

- Đặc tả thể hiện vật lý và mức an toàn mà đối với nó các cơ chế an toàn vật lý của mô-đun mật mã được thực thi. Đặc tả các cơ chế an toàn vật lý mà chúng được sử dụng bởi mô-đun (các Mức an toàn 1, 2, 3 và 4).
- Nếu một mô-đun mật mã bao gồm một vai trò duy trì mà nó yêu cầu truy cập vật lý vào các nội dung của mô-đun hoặc nếu mô-đun được thiết kế để cho phép truy cập vật lý, đặc tả của giao diện truy cập và các CSP sẽ phải được xóa trắng như thế nào khi giao diện truy cập duy trì bị truy cập (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả các dải hoạt động bình thường của mô-đun mật mã. Đặc tả của các đặc tính bảo vệ chống lỗi do môi trường được sử dụng bởi mô-đun mật mã hoặc đặc tả các kiểm tra chống lỗi do môi trường đã được thực hiện (Mức an toàn 4)
- Đặc tả các kỹ thuật giảm thiểu cảm ứng lỗi được sử dụng (Mức an toàn 4).

A.2.8 An toàn không xâm lấn

- Đặc tả các kỹ thuật giảm thiểu được sử dụng chống lại các tấn công không xâm lấn bao gồm các kỹ thuật được chỉ rõ trong Phụ lục F (các Mức an toàn 1, 2, 3 và 4).
- Bằng chứng về tính hiệu quả của mỗi trong các kỹ thuật giảm thiểu tấn công đã được sử dụng (các Mức an toàn 1, 2, 3 và 4).

A.2.9. Quản lý tham số an toàn nhạy cảm

- Đặc tả tất cả các CSP và PSP đã được sử dụng bởi mô-đun mật mã (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả tất cả các RBG và việc sử dụng chúng (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả entropy tối thiểu được yêu cầu bởi mô-đun đối với mỗi tham số đầu vào entropy được nhập vào (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả mỗi RGB (được phê duyệt và không được phê duyệt và các nguồn entropy) được sử dụng bởi mô-đun mật mã (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả entropy tối thiểu và phương pháp sinh entropy tối thiểu được yêu cầu nếu entropy được thu gom từ bên trong ranh giới mật mã của mô-đun mật mã (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả mỗi một phương pháp sinh SSP mà nó sử dụng một RGB (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả tất cả các phương pháp thiết lập SSP đã được sử dụng bởi mô-đun (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả mỗi một phương pháp sinh SSP đã được sử dụng bởi mô-đun (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả mỗi một trong các phương pháp sinh khóa (đã được phê duyệt và chưa được phê duyệt) được sử dụng bởi mô-đun mật mã (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả các phương pháp thiết lập SSP được sử dụng bởi mô-đun mật mã (các Mức an toàn 1, 2, 3 và 4).

- Đặc tả các phương pháp nhập vào và xuất ra SSP được sử dụng bởi mô-đun (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả các phương pháp nhập vào và xuất ra khóa được sử dụng bởi mô-đun mật mã (các Mức an toàn 1, 2, 3 và 4).
- Nếu các thủ tục phân chia thông tin được sử dụng thì tài liệu được cung cấp để chứng tỏ rằng nếu thông tin của n thành phần được yêu cầu để xây dựng lại CSP ban đầu thì thông tin của n-1 thành phần bất kỳ sẽ không cung cấp thông tin nào về CSP ban đầu ngoài thông tin về độ dài (các Mức an toàn 3 và 4).
- Đặc tả các thủ tục phân chia thông tin được sử dụng bởi mô-đun (các Mức an toàn 3 và 4).
- Đặc tả các SSP được lưu trữ trong mô-đun (Mức an toàn 1, 2, 3 và 4).
- Đặc tả xem các CSP được bảo vệ như thế nào khỏi truy cập, sử dụng, tiết lộ, sửa đổi và thay thế trái phép khi được lưu trữ trong mô-đun. (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả xem các PSP được bảo vệ như thế nào khỏi sửa đổi và thay thế trái phép khi được lưu trữ bên trong mô-đun. (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả xem mô-đun kết hợp với một PSP được lưu trữ trong mô-đun với thực thể như thế nào (người vận hành, vai trò hoặc tiến trình) mà đối với thực thể tham số được gán cho. (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả (các) phương pháp xóa trắng được sử dụng bởi mô-đun và cơ sở hợp lý như đối với việc làm thế nào mà (các) phương pháp ngăn chặn được sự khôi phục và sử dụng lại các giá trị đã bị xóa trắng (các Mức an toàn 1, 2, 3 và 4).

A.2.10 Các tự kiểm tra

- Đặc tả các tự kiểm tra được thực hiện bởi mô-đun mật mã bao gồm các kiểm tra có điều kiện và tiền hoạt động (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả về chỉ báo trạng thái tự kiểm tra thành công và thất bại. (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả các trạng thái có lỗi mà mô-đun mật mã có thể đi vào khi một tự kiểm tra thất bại và các điều kiện và các hành động cần thiết để thoát ra khỏi các trạng thái có lỗi và phục hồi hoạt động bình thường của mô-đun mật mã (chẳng hạn việc này có thể bao gồm duy trì mô-đun, bật lại nguồn điện cho mô-đun, khôi phục mô-đun tự động, đi vào hoạt động xuống cấp hoặc trả lại mô-đun cho nhà cung cấp để bảo dưỡng) (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả tất cả các chức năng an toàn quan trọng đến hoạt động an toàn của mô-đun mật mã và nhận biết các kiểm tra bật nguồn điện áp dụng được và các kiểm tra có điều kiện được thực hiện bởi mô-đun (các Mức an toàn 1, 2, 3 và 4).
- Nếu mô-đun mật mã thực thi một khả năng bỏ qua thì đặc tả cơ chế hoặc kiềm chế lôgic thủ tục chuyển mạch (các Mức an toàn 1, 2, 3 và 4).

A.2.11 Đảm bảo vòng đời

- Đặc tả hệ thống quản lý cấu hình được sử dụng đối với mô-đun mật mã (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả các tài liệu hỗ trợ đối với phát triển mô-đun mật mã và các tài liệu kết hợp được cung cấp bởi hệ thống quản lý cấu hình. (các Mức an toàn 1, 2, 3 và 4).
- Đặc tả các thủ tục để cài đặt, sinh, và khởi động an toàn mô-đun mật mã (các Mức an toàn 1, 2, 3 và 4)

- Đặc tả các thủ tục đối với duy trì an toàn trong khi phân phối và phân phát các phiên bản của mô-đun mật mã cho những người vận hành được phân quyền. (các Mức an toàn 2, 3 và 4).
- Đặc tả sự tương ứng giữa thiết kế các thành phần phần cứng, phần mềm, và/hoặc phần sụn của mô-đun mật mã và chính sách an toàn và FSM của mô-đun mật mã (các Mức an toàn 1, 2, 3 và 4).
- Nếu mô-đun mật mã chứa phần mềm, đặc tả mã nguồn đối với phần mềm được chú giải với các giải thích mà chúng mô tả rõ ràng sự tương ứng của phần mềm với thiết kế của mô-đun(các Mức an toàn 1, 2, 3 và 4).
- Nếu mô-đun mật mã chứa phần cứng, đặc tả các biểu đồ và/hoặc các bản in HDL đối với phần cứng (Mức an toàn 1, 2, 3 và 4).
- Đặc tả của một đặc tả mà nó môn tả không hình thức mô-đun mật mã, chức năng của mô-đun mật mã, các cổng vật lý ngoài và các giao diện lôgic của mô-đun mật mã và mục đích của các cổng vật lý và các giao diện lôgic (các Mức an toàn 2, 3 và 4).
- Đặc tả thiết kế chi tiết mà nó mô tả chức năng bên trong của các thành phần chính yếu của mô-đun mật mã, các giao diện thành phần bên trong, mục đích của các giao diện thành phần và luồng thông tin bên trong (bên trong ranh giới mật mã toàn bộ và cũng bên trong các thành phần chính yếu) (Mức an toàn 3 và 4).
- Đặc tả (bao gồm các tiền điều kiện và các hậu điều kiện) sự tương ứng giữa thiết kế của mô-đun mật mã và đặc tả chức năng. (Mức an toàn 4)
- Đặc tả FSM (hoặc tương đương) sử dụng một sơ đồ chuyển dịch trạng thái và bảng chuyển dịch trạng thái bao gồm: (các Mức an toàn 1, 2, 3 và 4).
    - Các trạng thái hoạt động và các trạng thái có lỗi của mô-đun mật mã;
    - Các chuyển dịch tương ứng từ một trạng thái tới trạng thái khác,
    - Các sự kiện đầu vào, bao gồm các đầu vào dữ liệu và các đầu vào điều khiển mà chúng gây ra các chuyển dịch từ một trạng thái tới trạng thái khác; và
    - Các sự kiện đầu ra, bao gồm các điều kiện mô-đun bên trong, các đầu ra dữ liệu và các đầu ra trạng thái được tạo ra từ các chuyển dịch từ một trạng thái tới trạng thái khác.
- Đặc tả mã nguồn cho phần mềm hoặc phần sụn (các Mức an toàn 1, 2, 3 và 4).
- Đối với mỗi thành phần phần cứng và phần mềm, chú giải mã nguồn với các giải thích mà nó chỉ rõ (1) các tiền điều kiện được yêu cầu trên đầu vào thành phần mô-đun, chức năng hoặc thủ tục để thực hiện đúng đắn và (2) các hậu điều kiện được kỳ vọng là đúng khi thực hiện của thành phần, chức năng hoặc thủ tục của mô-đun được hoàn thành. (Mức an toàn 4)
- Đối với hướng dẫn người quản trị, đặc tả (các Mức an toàn 1, 2, 3 và 4).:
    - Các chức năng quản lý, các sự kiện an toàn, các tham số an toàn (và các giá trị tham số khi thích hợp), các cổng vật lý và các giao diện lôgic của mô-đun mật mã có sẵn cho chuyên viên mật mã.
    - Các thủ tục về việc làm thế nào để quản lý mô-đun mật mã theo một cách an toàn và
    - Các giả thuyết về hành vi của người dùng mà nó liên quan đến hoạt động an toàn của mô-đun mật mã.
- Đối với tài liệu hướng dẫn cho người không phải là người quản trị, đặc tả về (các Mức an toàn 1, 2, 3 và 4):

- Các chức năng an toàn đã được phê duyệt, các cổng vật lý và các giao diện lôgic có sẵn cho những người dùng của mô-đun mật mã, và
- Tất cả các trách nhiệm của người dùng cần thiết đối với hoạt động an toàn của mô-đun.

A.2.12 Giảm thiểu các tấn công khác

- Nếu mô-đun mật mã được thiết kế để giảm thiểu một hoặc một số tấn công cụ thể mà không được xác định ở nơi nào khác trong Tiêu chuẩn này, thì liệt kê trong tài liệu của mô-đun các cơ chế an toàn được sử dụng bởi mô-đun mật mã để làm giảm thiểu (các) tấn công (các Mức an toàn 1, 2 và 3).
- Nếu mô-đun mật mã được thiết kế để giảm thiểu một hoặc một số tấn công cụ thể mà không được xác định ở nơi nào khác trong Tiêu chuẩn này, thì lập tài liệu các phương pháp được sử dụng để giảm thiểu các tấn công và các phương pháp kiểm tra tính hiệu quả của các kỹ thuật giảm thiểu (Mức an toàn 4)

Phụ lục B

(Quy định)

Chính sách an toàn của mô-đun mật mã

B.1 Tổng quan

Danh sách sau đây tổng hợp các yêu cầu **shall [B.01]** được cung cấp trong chính sách an toàn không đăng ký quyền sở hữu. Định dạng của chính sách an toàn **shall [B.02]** được giới thiệu trong trật tự được chỉ ra trong Phụ lục này hoặc là được chỉ rõ bởi một thẩm quyền kiểm tra hợp lệ. Chính sách an toàn **shall [B.03]** không được đánh dấu như đăng ký quyền sở hữu hoặc giữ bản quyền mà không có tuyên bố cho phép sao chép hoặc phân phối.

B.2 Các khoản mục

B.2.1 Thông tin chung

- Một bảng chỉ dẫn các mức điều khoản riêng lẻ và mức tổng thể.

B.2.2 Đặc tả mô-đun mật mã

- Mục đích hoặc sử dụng chủ định mô-đun bao gồm môi trường sử dụng chủ định.
- Sơ đồ minh họa, biểu đồ hoặc bức ảnh của mô-đun. Một bức ảnh được bao gồm đối với các mô-đun phần cứng. Nếu chính sách an toàn bao quát nhiều phiên bản của mô-đun, thì mỗi một phiên bản được thể hiện một cách tách biệt hoặc được chú giải để cho sự thể hiện được minh họa đối với tất cả các phiên bản. Đối với mô-đun phần mềm hoặc phần sụn, chính sách an toàn bao gồm một sơ đồ khối minh họa:
    - Vị trí của đối tượng lôgic của mô-đun phần mềm hoặc phần sụn tương ứng với hệ điều hành, các ứng dụng hỗ trợ khác và ranh giới mật mã sao cho tất cả các lớp lôgic và vật lý giữa đối tượng lôgic và ranh giới mật mã là được xác định một cách rõ ràng; và
    - Các tương tác của đối tượng lôgic của mô-đun phần mềm hoặc phần sụn với hệ điều hành và các ứng dụng hỗ trợ khác thường trú bên trong ranh giới mật mã.
- Mô tả (các) mô-đun:
    - Cung cấp phiên bản/định danh của (các) mô-đun và tất cả các thành phần (phần cứng, phần mềm hoặc phần sụn).
- Chọn lựa phần cứng, phần mềm, phần sụn hoặc phần lai ghép:
    - Đối với các mô-đun mật mã phần mềm, phần sụn và phần lai ghép, liệt kê (các) hệ điều hành mà mô-đun được kiểm tra trên đó và liệt kê (các) hệ điều hành mà nhà cung cấp xác nhận có thể được sử dụng bởi mô-đun
- Xếp loại độ an toàn tổng thể của mô-đun và các mức an toàn của các lĩnh vực riêng lẻ.
- Xác định chính xác về ranh giới mật mã và vật lý của mô-đun:
    - Phần cứng, phần mềm hoặc phần sụn được loại bỏ khỏi các ranh giới mật mã được chỉ rõ trong chính sách an toàn.

- Các chế độ hoạt động và đi vào/đi ra mỗi chế độ như thế nào. Chính sách an toàn mô tả mỗi một chế độ hoạt động đã phê duyệt được thực thi trong mô-đun mật mã và mỗi một chế độ được cấu hình như thế nào.
- Mô tả hoạt động bị xuống cấp.
- Bảng tất cả các chức năng an toàn, với các độ dài khóa cụ thể được sử dụng đối với dịch vụ được phê duyệt cũng như các chế độ hoạt động đã được thực thi, (chẳng hạn CBC, CCM) nếu phù hợp.
- Sơ đồ khối, khi áp dụng được.
- Thiết kế an toàn tổng thể và các quy tắc hoạt động.
- Các yêu cầu khởi động, khi áp dụng được.

B.2.3 Các giao diện mô-đun mật mã

- Liệt kê bảng tất cả các cổng và các giao diện (vật lý và lôgic).
- Xác định thông tin chuyển qua năm giao diện lôgic
- Chỉ rõ các cổng vật lý và dữ liệu chuyển qua chúng.
- Chỉ rõ kênh tin cậy.
- Đặc tả các ngoại lệ và cơ sở hợp lý nếu giao diện đầu ra điều khiển không bị chặn lại trong suốt trạng thái có lỗi .

B.2.4 Các vai trò, các dịch vụ và xác thực.

- Chỉ rõ tất cả các vai trò.
- Bảng các vai trò cùng với các lệnh dịch vụ tương ứng với đầu vào và đầu ra.
- Chỉ rõ mỗi phương pháp xác thực, cho dù phương pháp là dựa trên định danh hay dựa trên vai trò được yêu cầu.
- Độ mạnh của yêu cầu xác thực được đáp ứng như thế nào?
- Nếu có khả năng bỏ qua xảy ra, thì hai hành động độc lập là gì và trạng thái được kiểm tra thế nào?
- Nếu có một khả năng đầu ra mật mã tự khởi động, thì hai hành động độc lập là gì và trạng thái được chỉ báo như thế nào?
- Nếu phần mềm hoặc phần sụn ngoài được nạp, thì chỉ rõ các kiểm soát việc nạp và cách ly mã mà chúng ngăn chặn truy nhập và sử dụng trái phép mô-đun.
- Liệt kê tách riêng các dịch vụ an toàn và không an toàn, cả được phê duyệt và không được phê duyệt.
- Đối với mỗi dịch vụ, tên dịch vụ, một mô tả ngắn gọn về mục đích và/hoặc sử dụng của dịch vụ (tên dịch đứng riêng cũng có thể, trong một số trường hợp, cung cấp thông tin này), một danh sách các chức năng an toàn được phê duyệt ((các) thuật toán, (các) kỹ thuật quản lý khóa hoặc kỹ thuật xác thực) được sử dụng bởi, hoặc được thực thi thông qua, sự viện cầu dịch vụ và một danh sách các SSP kết hợp với dịch vụ hoặc với (các) chức năng an toàn phê duyệt mà nó sử dụng. Đối với mỗi vai trò người vận hành được phân quyền sử dụng thông tin dịch vụ mô tả các

quyền truy cập riêng đến tất cả các SSP và thông tin mô tả phương pháp được sử dụng để xác thực mỗi vai trò.

- Mô tả tiến trình cài đặt và (các) cơ chế xác thực mật mã.

B.2.5 An toàn phần mềm/ phần sụn

- Chỉ rõ các kỹ thuật toàn vẹn đã được phê duyệt được sử dụng.
- Chỉ rõ làm thế nào mà người vận hành có thể khởi động kiểm tra tính toàn vẹn theo yêu cầu.
- Chỉ rõ dạng và mỗi thành phần với mã thực hiện được cung cấp.
- Nếu mô-đun là nguồn mở, thì chỉ rõ các trình biên dịch và các tham số kiểm soát được yêu cầu để biên dịch mã thành một định dạng thực hiện.

B.2.6 Môi trường hoạt động

- Nhận biết môi trường hoạt động (chẳng hạn, không thể sửa đổi, bị giới hạn hoặc có thể sửa đổi).
- Nhận biết (các) hệ điều hành và (các) nền được kiểm tra.
- Đối với mỗi mức áp dụng được, giải thích xem các yêu cầu được thỏa mãn như thế nào.
- Nhà cung cấp có thể cung cấp các khẳng định về chuyển nền cho các OS khác mà còn chưa được kiểm tra một cách cụ thể tuy khẳng định của nhà cung cấp về hoạt động đúng đắn đã được tuyên bố.
- Đặc tả các quy tắc an toàn, các thiết lập hoặc các hạn chế lên cấu hình của môi trường hoạt động.
- Đặc tả các hạn chế bất kì lên cấu hình của môi trường hoạt động.

B.2.7 Chính sách an toàn vật lý

- Chỉ rõ thể hiện (đơn chip, đa chip nhúng hoặc đa chip đứng độc lập).
- Chỉ rõ các cơ chế an toàn vật lý mà chúng được thực thi trong mô-đun (ví dụ như các niêm phong bằng chứng xâm phạm, các khóa, đáp trả xâm phạm và các chuyển mạch xóa trắng và các báo động).
- Chỉ rõ các hành động được yêu cầu bởi (những) người vận hành để đảm bảo rằng an toàn vật lý được duy trì (chẳng hạn thanh tra định kỳ các niêm phong bằng chứng xâm phạm hoặc kiểm tra đáp trả xâm phạm và các chuyển mạch xóa trắng).
    - Chỉ rõ thông tin sau nếu mô-đun yêu cầu người vận hành các niêm phong bằng chứng xâm phạm được áp dụng hoặc các dụng cụ an toàn mà người vận hành sẽ áp dụng hoặc sửa đổi trên vòng đời của mô-đun: Ảnh hoặc các minh họa tham chiếu được yêu cầu trong B.2.2 sẽ phản ánh mô-đun được cấu hình hoặc được xây dựng như đã được đặc tả. Các bức ảnh/các minh họa bổ sung có thể được cung cấp để phản ánh các cấu hình khác.
    - Nếu các tấm pa-nen lấp chỗ trống được cần đến để che phủ các khe cắm hoặc các khe hổng để trống để đáp ứng các yêu cầu độ chắn sáng, thì chúng sẽ được bao gồm trong ảnh hoặc các minh họa với các niêm phong chống xâm phạm được dán vào như cần thiết. Các tấm pa-nen lấp chỗ trống sẽ được bao gồm trong danh sách các bộ phận.

- Các ảnh hoặc các minh họa sẽ chỉ ra bố trí chính xác của bất kỳ niêm phong bằng chứng xâm phạm hoặc các dụng cụ an toàn cần đến để đáp ứng các yêu cầu an toàn vật lý.
- Tổng số các niêm phong bằng chứng xâm phạm hoặc các dụng cụ an toàn cần đến sẽ được chỉ ra (ví dụ: 5 niêm phong bằng chứng xâm phạm, 2 tấm màn chắn sáng). Các ảnh hoặc các minh họa mà chúng cung cấp chỉ dẫn về bố trí chính xác sẽ có mỗi khoản mục được đánh số trong ảnh hoặc minh họa và sẽ bằng tổng số đã được chỉ ra (các niêm phong bằng chứng xâm phạm hoặc các dụng cụ an toàn không không được yêu cầu phải được đánh số).
- Nếu các niêm phong bằng chứng xâm phạm hoặc các dụng cụ an toàn là các bộ phận mà chúng có thể được sắp xếp lại từ nhà cung cấp mô-đun, thì chính sách an toàn sẽ chỉ ra số bộ phận của nhà cung cấp mô-đun của niêm phong, dụng cụ an toàn hoặc bộ công cụ an toàn áp dụng được. Sau khi cấu hình lại, người vận hành mô-đun có thể được yêu cầu để loại bỏ và đưa vào các niêm phong bằng chứng xâm phạm hay các dụng cụ an toàn mới.
- Chỉ rõ vai trò người vận hành chịu trách nhiệm đảm bảo an toàn và có kiểm soát tại tất cả các thời gian của các niêm phong không sử dụng bất kỳ, và kiểm soát và quan sát trực tiếp những thay đổi bất kỳ đối với mô-đun sao cho các cấu hình lại ở nơi mà các niêm phong bằng chứng xâm phạm hoặc các dụng cụ an toàn được gỡ bỏ hoặc cài đặt để đảm bảo an toàn của mô-đun được duy trì trong quá trình những thay đổi như vậy và mô-đun được trở về một trạng thái đã được phê duyệt của FIPS.
- Nếu các niêm phong bằng chứng xâm phạm hoặc các dụng cụ an toàn có thể được gỡ bỏ hoặc cài đặt, thì các chỉ dẫn rõ ràng sẽ được bao gồm về việc làm thế nào bề mặt hoặc thiết bị được chuẩn bị để áp dụng một niêm phong bằng chứng xâm phạm hoặc dụng cụ an toàn mới.

- Chỉ rõ các phương pháp giảm thiểu cảm ứng lỗi được thực thi.

B.2.8 An toàn không xâm lấn

- Chỉ rõ tất cả các kỹ thuật giảm thiểu không xâm lấn được tham chiếu trong Phụ lục F được sử dụng bởi mô-đun để bảo vệ các CSP của mô-đun khỏi các tấn công không xâm lấn.
- Mô tả tính hiệu quả của các kỹ thuật giảm thiểu không xâm lấn được tham chiếu trong Phụ lục F được sử dụng bởi mô-đun để bảo vệ các CSPcủa mô-đun khỏi các tấn công không xâm lấn.

CHÚ THÍCH: Mức độ chi tiết mô tả tính hiệu quả của các kỹ thuật giảm thiểu không xâm lấn được tham chiếu trong Phụ lục F được sử dụng bởi mô-đun để bảo vệ các CSP của mô-đun khỏi các tấn công không xâm lấn phải tương tự như những gì được tìm thấy trong tài liệu quảng cáo (các giấy bóng giới thiệu sản phẩm).

B.2.9 Quản lý các tham số an toàn nhạy cảm

- Cung cấp một bảng khóa chỉ rõ (các) kiểu khóa, (các) đội dài tính theo bít , (các) chức năng an toàn, (các) số chứng nhận chức năng an toàn, (các) khóa được sinh ra ở đâu và như thế nào, (các) khóa có được nhập vào hoặc xuất ra không, phương pháp thiết lập và sinh SSP được sử dụng bất kỳ và chỉ ra các khóa liên quan bất kỳ.
- Trình bày một bảng các SSP khác và chúng được sinh ra như thế nào.
- Chỉ rõ các bộ tạo bit ngẫu nhiên đã được phê duyệt hoặc chưa được phê duyệt.
- Mô tả các sử dụng (các) đầu ra RBG.

- Chỉ rõ (các) nguồn entropy RBG.
- Chỉ rõ (các) phương pháp vào/ra khóa thủ công và điện tử.
- Chỉ rõ (các) kỹ thuật lưu trữ SSP.
- Chỉ rõ (các) phương pháp xóa trắng SSP không được bảo vệ và cơ sở hợp lý và khả năng khởi động người vận hành.
- Chỉ rõ các giai đoạn chuyển tiếp áp dụng được hoặc các khung thời gian mà ở đó thuật toán hoặc độ dài khóa chuyển tiếp từ đã được phê duyệt sang chưa được phê duyệt.

B.2.10 Các tự kiểm tra

- Cung cấp danh sách các tự kiểm tra tiền hoạt động và có điều kiện với các tham số được định nghĩa và liệt kê các điều kiện mà theo đó các kiểm tra được thực hiện.
- Chỉ rõ khoảng thời gian và chính sách về các điều kiện bất kỳ mà chúng có thể tạo ra gián đoạn các hoạt động của mô-đun trong một thời gian để lặp lại các tự kiểm tra định kỳ.
- Mô tả tất cả các trạng thái có lỗi và các chỉ báo trạng thái.
- Mô tả khởi động hoạt động, nếu áp dụng được.

B.2.11 Đảm bảo vòng đời

- Chỉ rõ các thủ tục để cài đặt, khởi hoạt, khởi động và hoạt động an toàn của mô-đun.
- Chỉ rõ các yêu cầu bảo trì bất kỳ.
- Cung cấp hướng dẫn cho người quản trị và người không phải người quản trị (có thể là một tài liệu riêng biệt).

B.2.12 Giảm thiểu các tấn công khác

- Chỉ rõ những tấn công khác được giảm thiểu cho cái gì.
- Mô tả tính hiệu quả của các kỹ thuật giảm thiểu được liệt kê.
- Liệt kê sách hướng dẫn và những ràng buộc liên quan đến an toàn.

CHÚ THÍCH: Mức độ chi tiết mô tả (các) cơ chế an toàn được thực thi để giảm thiểu các tấn công khác phải tương tự như những gì được tìm thấy trong tài liệu quảng cáo (các giấy bóng giới thiệu sản phẩm).

Phụ lục C

(Quy định)

Các chức năng an toàn đã được phê duyệt

C.1 Mục đích

Phụ lục này cung cấp một danh sách các tiêu chuẩn được ISO/IEC hoặc Tiêu chuẩn Việt Nam, mà nó đặc tả các chức năng an toàn đã được phê duyệt áp dụng cho Tiêu chuẩn này. Các phân loại bao gồm các mã khối, các mã dòng, khóa phi đối xứng, các mã xác thực thông điệp, các hàm băm, xác thực thực thể, quản lý khóa và sinh bít ngẫu nhiên. Danh sách này là không giới hạn.

Điều này không ngăn cản việc sử dụng các chức năng an toàn đã được phê duyệt của thẩm quyền phê duyệt.

Một thẩm quyền phê duyệt có thể thay thế Phụ lục này trong toàn bộ nội dung của nó với dánh sách của chính nó của các các chức năng an toàn đã được phê duyệt.

C.1.1 Các mã khối

a. ISO/IEC 18033-3, *Các thuật toán mã hóa – Phần 3: Các hệ mã khối.* (ISO/IEC 18033-4, *Encryption Algorithms – Part 3: Block Ciphers).*

C.1.2 Các mã dòng

b. ISO/IEC 18033-4, *Các thuật toán mã hóa – Phần 4: Các hệ mã dòng.* (ISO/IEC 18033-4, *Encryption algorithms - Part 4: Stream ciphers).*

C.1.3 Các kỹ thuật và các thuật toán phi đối xứng

a. ISO/IEC 9796-2, Công nghệ thông tin – Kỹ thuật an toàn – Chữ ký số có khôi phục thông *điệp – Phần 2: Các kỹ thuật dựa trên phân tích nhân tử số nguyên* (ISO/IEC 9796-2, *Information technology - Security techniques - Digital signatures with message recovery - Part 2: Integer factorisation based techniques).*

b. ISO/IEC 9796-3, *Công nghệ thông tin – Kỹ thuật an toàn – Chữ ký số có khôi phục thông điệp – Phần 3: Các kỹ thuật dựa trên bài toán logarit rời rạc* (ISO/IEC 9796-3, *Information technology - Security techniques - Digital signatures with message recovery - Part 3: Discrete logarithm based techniques).*

c. ISO/IEC 14888 (tất cả các phần), *Công nghệ thông tin – Kỹ thuật an toàn – Chữ ký số kèm phụ lục* (ISO/IEC 14888 (all parts), *Information technology - Security techniques - Digital signatures with appendix).*

d. ISO/IEC 15946 (tất cả các phần), *Công nghệ thông tin – Kỹ thuật an toàn – Kỹ thuật mật mã dựa trên đường cong elliptic* (ISO/IEC 15946 (all parts), *Information technology — Security techniques — Cryptographic techniques based on elliptic curves).*

e. ISO/IEC 18033-2, *Công nghệ thông tin – Kỹ thuật an toàn – Các thuật toán mã hóa – Phần 2: Các thuật toán mã hóa phi đối xứng* (ISO/IEC 18033-2, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric cryptographic algorithms).*

C.1.4. Các mã xác thực thông điệp

a. ISO/IEC 9797-2, *Công nghệ thông tin – Kỹ thuật an toàn – Mã xác thực thông báo (MACs) – Phần 2: Các cơ chế sử dụng hàm băm chuyên dùng* (ISO/IEC 9797-2, *Information technology - Security techniques - Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function).*

C.1.5 Các hàm băm

a. ISO/IEC 10118-2, *Công nghệ thông tin – Kỹ thuật an toàn – Hàm băm – Phần 2: Các hàm băm sử dụng hệ mã khối n-bit* (ISO/IEC 10118-2, *Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher).*

b. ISO/IEC 10118-3, *Công nghệ thông tin – Kỹ thuật an toàn – Hàm băm – Phần 3: Các hàm băm chuyên dùng* (ISO/IEC 10118-3, *Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions).*

c. ISO/IEC 10118-4, *Công nghệ thông tin – Kỹ thuật an toàn – Hàm băm – Phần 4: Các hàm băm sử dụng số học modular* (ISO/IEC 10118-4, *Information technology - Security techniques - Hash-functions - Part 4: Hash-functions using modular arithmetic).*

C.1.6 Xác thực thực thể

a. ISO/IEC 9798-2, *Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 2: Các cơ chế sử dụng thuật toán mã hóa đối xứng* (ISO/IEC 9798-2, *Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms).*

b. ISO/IEC 9798-3, *Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 3: Các cơ chế sử dụng kỹ thuật chữ ký số* (ISO/IEC 9798-3, *Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques).*

c. ISO/IEC 9798-4, *Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 4: Các cơ chế sử dụng hàm kiểm tra mật mã* (ISO/IEC 9798-4, *Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function).*

d. ISO/IEC 9798-5, *Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 5: Các cơ chế sử dụng kỹ thuật không tiết lộ thông tin* (ISO/IEC 9798-5, *Information technology - Security techniques - Entity authentication - Part 5: Mechanisms using zero-knowledge techniques).*

e. ISO/IEC 9798-6, *Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 6: Các cơ chế sử dụng cách truyền dữ liệu thủ công* (ISO/IEC 9798-6, *Information technology — Security techniques - Entity authentication - Part 6: Mechanisms using manual data transfer).*

C.1.7 Quản lý khóa

a. TCVN 7817-2:2010 (ISO/IEC 11770-2:2008) *Công nghệ thông tin – Kỹ thuật an ninh – Quản lý khóa – Phần 2: Cơ chế sử dụng kỹ thuật đối xứng.*

b. TCVN 7817-3:2007 (ISO/IEC 11770-3:1999) *Công nghệ thông tin – Kỹ thuật mật mã – Quản lý khóa – Phần 3: Các cơ chế sử dụng kỹ thuật phi đối xứng.*

c. TCVN 7817-4:2010 (ISO/IEC 11770-4:2006) *Công nghệ thông tin – Các kỹ thuật an ninh – Quản lý khóa - Phần 4: Cơ chế dựa trên bí mật yếu.*

C.1.8 Sinh bit ngẫu nhiên

a. ISO/IEC 18031, *Công nghệ thông tin – Kỹ thuật an toàn – Tạo bit ngẫu nhiên* (ISO/IEC 18031, *Information technology — Security techniques — Random bit generation).*

Phụ lục D

(Quy định)

Các phương pháp thiết lập và sinh tham số an toàn nhạy cảm đã được phê duyệt

D.1 Mục đích

Phụ lục này cung cấp một danh sách các phương pháp thiết lập và sinh tham số an toàn nhạy cảm được phê duyệt của ISO/IEC hoặc Tiêu chuẩn Việt Nam áp dụng cho Tiêu chuẩn này.

Điều này không ngăn cản việc sử dụng các phương pháp thiết lập và sinh tham số an toàn nhạy cảm đã được phê duyệt của thẩm quyền phê duyệt. Danh sách này là không giới hạn.

Một thẩm quyền phê duyệt có thể thay thế Phụ lục này trong toàn bộ nội dung của nó với dánh sách của chính nó của các phương pháp thiết lập và sinh tham số an toàn nhạy cảm đã được phê duyệt.

D.1.1 Sinh tham số an toàn nhạy cảm

D.1.2 Các phương pháp thiết lập tham số an toàn nhạy cảm

a. TCVN 7817-2:2010 (ISO/IEC 11770-2:2008) *Công nghệ thông tin – Kỹ thuật an ninh – Quản lý khóa – Phần 2: Cơ chế sử dụng kỹ thuật đối xứng.*

b. TCVN 7817-3:2007 (ISO/IEC 11770-3:1999) *Công nghệ thông tin – Kỹ thuật mật mã – Quản lý khóa – Phần 3: Các cơ chế sử dụng kỹ thuật phi đối xứng.*

c. ISO/IEC 15946-3, *Công nghệ thông tin – Các kỹ thuật an toàn – Quản lý khóa - Phần 3: Thiết lập khóa* (ISO/IEC 15946-3, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment).*

Phụ lục E

(Quy định)

Các cơ chế xác thực đã được phê duyệt

E.1 Mục đích

Phụ lục này cung cấp một danh sách các cơ chế xác thực được phê duyệt của ISO/IEC hoặc Tiêu chuẩn Việt Nam áp dụng cho Tiêu chuẩn này.

Điều này không ngăn cản việc sử dụng các cơ chế xác thực đã được phê duyệt của thẩm quyền phê duyệt. Danh sách này là không giới hạn.

Một thẩm quyền phê duyệt có thể thay thế Phụ lục này trong toàn bộ nội dung của nó với dánh sách của chính nó của các cơ chế xác thực.

E.1.1 Các cơ chế xác thực

a. Không có các cơ chế đã được phê duyệt được xác định tại thời điểm này.

Phụ lục F

(Quy định)

Các độ đo kiểm tra giảm thiểu tấn công không xâm lấn đã được phê duyệt

F.1 Mục đích

Phụ lục này cung cấp một danh sách các độ đo kiểm tra giảm thiểu tấn công không xâm lấn đã được phê duyệt của ISO/IEC hoặc Tiêu chuẩn Việt Nam áp dụng cho Tiêu chuẩn này.

Điều này không ngăn cản việc sử dụng các độ đo kiểm tra giảm thiểu tấn công không xâm lấn đã được phê duyệt của thẩm quyền phê duyệt. Danh sách này là không giới hạn.

Một thẩm quyền phê duyệt có thể thay thế Phụ lục này trong toàn bộ nội dung của nó với dánh sách của chính nó của các độ đo kiểm tra giảm thiểu tấn công không xâm lấn đã được phê duyệt.

F.1.1 Các độ đo kiểm tra giảm thiểu tấn công không xâm lấn

a. Không có các độ đo kiểm tra giảm thiểu tấn công không xâm lấn đã được phê duyệt được xác định tại thời điểm này.

Thư mục Tài liệu tham khảo

[1]. ISO 10007:2003, *Quality management systems – Guildlines for configuration management*

[2]. National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication 140-2, May 25, 2001 (with latest change notices)

[3]. ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[4]. TCVN 7817-2:2010 (ISO/IEC 11770-2:2008) *Công nghệ thông tin – Kỹ thuật an ninh – Quản lý khóa – Phần 2: Cơ chế sử dụng kỹ thuật đối xứng*

[5]. TCVN 7817-3:2007 (ISO/IEC 11770-3:1999) *Công nghệ thông tin – Kỹ thuật mật mã – Quản lý khóa – Phần 3: Các cơ chế sử dụng kỹ thuật phi đối xứng*

[6]. TCVN 7817-4:2010 (ISO/IEC 11770-4:2006) *Công nghệ thông tin – Các kỹ thuật an ninh – Quản lý khóa - Phần 4: Cơ chế dựa trên bí mật yếu*