TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 13720:2023
ISO/IEC TS 20540:2018

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – KIỂM THỬ CÁC MÔ-ĐUN MẬT MÃ TRONG MÔI TRƯỜNG HOẠT ĐỘNG

Information technology — Security techniques — Testing cryptographic modules in their operational environment

HÀ NỘI – 2023

Mục lục

Lời nói đầu 6
Giới thiệu 7
1. Phạm vi áp dụng 9
2. Tài liệu viện dẫn 10
3. Thuật ngữ và định nghĩa 10
4. Ký hiệu và thuật ngữ viết tắt 14
5. Cấu trúc tiêu chuẩn 14
6. Phạm vi của kiểm thử xác nhận hoạt động 15
7. Mô-đun mật mã 16
7.1. Quy định chung 16
7.2. Các loại mô-đun mật mã 17
7.2.1. Quy định chung 17
7.2.2. Mô-đun phần mềm 17
7.2.3. Mô-đun phần sụn 17
7.2.4. Mô-đun phần cứng 17
7.2.5. Mô-đun phần mềm lai ghép 18
7.2.6. Mô-đun phần sụn lai ghép 18
7.3. Môi trường ứng dụng mô-đun mật mã 18
7.4. Các sản phẩm an toàn có mô-đun mật mã 18
7.5. Yêu cầu an toàn đối với mô-đun mật mã 20
7.5.1. Quy định chung 20
7.5.2. Mức an toàn 1 21
7.5.3. Mức an toàn 2 21
7.5.4. Mức an toàn 3 22
7.5.5. Mức an toàn 4 23
7.6. Đảm bảo vòng đời của các mô-đun mật mã 23
7.7. Chính sách an toàn của mô-đun mật mã 24
7.7.1. Quy định chung 24
7.7.2. Mô tả mô-đun mật mã 24
7.7.3. Giao diện mô-đun mật mã 24

7.7.4. Vai trò, dịch vụ và xác thực 24
7.7.5. An toàn phần mềm/phần sụn 25
7.7.6. Môi trường hoạt động 25
7.7.7. An toàn vật lý 25
7.7.8. An toàn không xâm lấn 25
7.7.9. Quản lý các thông số an toàn nhạy cảm 25
7.7.10. Tự kiểm tra 26
7.7.11. Đảm bảo vòng đời 26
7.7.12. Giảm thiểu các cuộc tấn công khác 26
7.8. Mục đích dự kiến của các mô-đun mật mã đã hợp lệ 26
8. Môi trường ứng dụng 27
8.1. An toàn tổ chức 27
8.2. Kiến trúc của môi trường ứng dụng 27
9. Môi trường hoạt động 28
9.1. Các yêu cầu an toàn liên quan đến các mô-đun mật mã cho môi trường hoạt động 28
9.1.1. Quy định chung 28
9.1.2. Nguồn Entropy 28
9.1.3. Cơ chế đánh giá 28
9.1.4. Chức năng không thể mở khóa về mặt vật lý 29
9.2. Các giả định về an toàn cho môi trường hoạt động 29
9.2.1. Quy định chung 29
9.2.2. Mức an toàn 1 30
9.2.3. Mức an toàn 2 30
9.2.4. Mức an toàn 3 31
9.2.5. Mức an toàn 4 32
10. Cách chọn mô-đun mật mã 33
10.1. Quy định chung 33
10.2. Chính sách sử dụng 34
10.3. Đảm bảo mô-đun mật mã 35
10.4. Khả năng tương tác 35
10.5. Lựa chọn xếp hạng an toàn cho bảo vệ SSP 35

11. Nguyên tắc kiểm thử xác nhận hoạt động 36
11.1. Quy định chung 36
11.2. Giả định 37
11.3. Hoạt động kiểm thử xác nhận hoạt động 37
11.4. Năng lực cho kiểm thử viên 38
11.5. Sử dụng bằng chứng xác thực 38
11.6. Tài liệu 38
11.7. Quy trình kiểm thử xác nhận hoạt động 39
12. Các khuyến nghị cho kiểm thử xác nhận hoạt động 39
12.1. Quy định chung 39
12.2. Các khuyến nghị để đánh giá cài đặt, cấu hình và hoạt động của mô-đun mật mã 40
12.2.1. Quy định chung 40
12.2.2. Đánh giá cài đặt mô-đun mật mã 40
12.2.3. Đánh giá cấu hình của mô-đun mật mã 41
12.2.4. Đánh giá hoạt động chính xác của mô-đun mật mã 42
12.3. Các khuyến nghị để kiểm tra một hệ thống quản lý chính 43
12.4. Khuyến nghị để kiểm tra các yêu cầu an toàn của thông tin xác thực 44
12.5. Các khuyến nghị để đánh giá tính khả dụng của các mô-đun mật mã 44
12.6. Các khuyến nghị để xác định các lỗ hổng tiềm ẩn bị bỏ sót của các mô-đun mật mã 45
12.7. Kiểm tra các chính sách an toàn của tổ chức 46
13. Báo cáo kết quả kiểm thử xác nhận hoạt động 46
Phụ lục A 48
Phụ lục B 49
Tài liệu tham khảo 56

Lời nói đầu

TCVN 13720:2023 hoàn toàn tương đương với ISO/IEC TS 20540:2018.

TCVN 13720:2023 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.

Giới thiệu

Trong lĩnh vực công nghệ thông tin, nhu cầu sử dụng các cơ chế mật mã ngày càng tăng như bảo vệ dữ liệu chống lại việc tiết lộ hay xâm nhập trái phép, để xác thực và chống chối bỏ. Tính an toàn và độ tin cậy của các cơ chế này phụ thuộc trực tiếp vào các mô-đun mật mã được sử dụng trong hệ thống an toàn nhằm bảo vệ thông tin nhạy cảm trong môi trường ứng dụng.

Mục đích của tiêu chuẩn này là mô tả các khuyến nghị và danh sách kiểm tra giúp lựa chọn các mô-đun mật mã để triển khai trong đa dạng các môi trường ứng dụng. Tiêu chuẩn này rất hữu ích cho người dùng và kiểm thử viên để xác minh triển khai chính xác trong môi trường ứng dụng.

Các kiểm thử xác nhận hoạt động được thực hiện để xác định sự phù hợp và sử dụng đúng mô-đun mật mã trong môi trường ứng dụng của nó.

Các mô-đun mật mã và môi trường ứng dụng của chúng thường phức tạp. Khi các mô-đun mật mã được triển khai trong môi trường hoạt động, một lỗi hoặc khiếm khuyết nhỏ có thể ảnh hưởng đến an toàn của toàn bộ môi trường hoạt động và ứng dụng. Điều quan trọng là phải thực hiện các kiểm thử xác nhận hoạt động để đảm bảo việc sử dụng đúng mô-đun mật mã trong môi trường hoạt động của chúng. Tiêu chuẩn này xác định các kiểm thử xác nhận hoạt động bằng cách cung cấp:

- Khuyến nghị đối với thực hiện đánh giá an toàn về cài đặt, cấu hình và vận hành mô-đun mật mã.
- Khuyến nghị đối với kiểm tra hệ thống quản lý khóa, bảo vệ thông tin xác thực và các tham số an toàn công khai, bí mật trong môi trường hoạt động.
- Khuyến nghị đối với việc xác định lỗ hổng mô-đun mật mã.
- Danh sách kiểm tra cho chính sách thuật toán mật mã, hướng dẫn và quy định mật mã, yêu cầu quản lý an toàn, mức độ an toàn của từng lĩnh vực trong 11 lĩnh vực được yêu cầu, mức an toàn của chức năng an toàn...
- Các khuyến nghị kiểm tra để xác định rằng việc triển khai mô-đun mật mã đáp ứng các yêu cầu an toàn.

Khi kiểm thử xác nhận hoạt động được thực hiện dựa trên việc sử dụng tiêu chuẩn này, có thể yêu cầu sử dụng đến các văn bản TCVN 11295:2016 (ISO/IEC 19790: 2012) và TCVN 12211:2018 (ISO/IEC 24759).

Công nghệ thông tin – Các Kỹ thuật an toàn – Kiểm tra các mô-đun mật mã trong môi trường hoạt động

Information technology — Security techniques — Testing cryptographic modules in their operational environment

1. Phạm vi áp dụng

Tiêu chuẩn này đưa ra các khuyến nghị và danh sách kiểm tra có thể được sử dụng để hỗ trợ đặc điểm kỹ thuật và kiểm thử xác nhận hoạt động của các mô-đun mật mã trong môi trường hoạt động của chính nó và trong hệ thống an toàn của tổ chức.

Các mô-đun mật mã có 4 mức an toàn được xác định tại TCVN 11295:2016 (ISO/IEC 19790:2012) 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, chuyển tiền hàng triệu đô la, dữ liệu an toàn đời 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 cơ sở được bảo vệ, một văn phòng, thiết bị tháo rời, và một địa điểm hoàn toàn không được bảo vệ).

Tiêu chuẩn này bao gồm:

a) Các khuyến nghị thực hiện đánh giá an toàn cài đặt, cấu hình và vận hành mô-đun mật mã;
b) Các khuyến nghị kiểm tra hệ thống quản lý khóa, bảo vệ thông tin xác thực và các tham số an toàn công khai và quan trọng trong môi trường hoạt động;
c) Các khuyến nghị định dạng lỗ hổng mô-đun mật mã.
d) Danh sách kiểm tra chính sách thuật toán mật mã, hướng dẫn và quy định an toàn, yêu cầu quản lý an toàn, mức độ an toàn của từng lĩnh vực trong 11 lĩnh vực được yêu cầu, mức an toàn của chức năng an toàn...
e) Các khuyến nghị xác định việc triển khai mô-đun mật mã đáp ứng theo các yêu cầu an toàn của tổ chức.

Tiêu chuẩn này giả định rằng mô-đun mật mã đã được xác nhận là phù hợp với TCVN 11295:2016 (ISO/IEC 19790: 2012).

Tiêu chuẩn này có thể được sử dụng bởi kiểm thử viên cùng với các khuyến nghị khác nếu cần thiết.

Tiêu chuẩn này được giới hạn trong phạm vi an toàn liên quan đến mô-đun mật mã. Tiêu chuẩn này không bao gồm việc đánh giá tính an toàn của môi trường hoạt động hoặc ứng dụng. Nó không xác định các kỹ thuật để xác định, đánh giá và chấp nhận rủi ro hoạt động của tổ chức.

Quy trình tổ chức, triển khai và vận hành của tổ chức, được trình bày trong Hình 1, không thuộc trong phạm vi của tiêu chuẩn này.

Tiêu chuẩn này đề cập đến những kiểm thử viên thực hiện kiểm thử xác nhận hoạt động cho các mô-đun mật mã trong môi trường hoạt động, có sự chấp thuận của người phụ trách các mô-đun mật mã.

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 không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

TCVN 11295:2016 (ISO/IEC 19790: 2012) Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu an toàn cho mô-đun mật mã.

TCVN 12211:2018 (ISO/IEC 24759) Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu kiểm thử cho mô-đun mật mã.

3. Thuật ngữ và định nghĩa

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

3.1

Công nhận (accreditation)

Quy trình quản trị theo đó quyền được cấp cho hoạt động của mô-đun mật mã trong môi trường hoạt động đầy đủ, bao gồm tất cả các phần không phải CNTT.

CHÚ THÍCH 1: Kết quả của quá trình kiểm thử xác nhận hoạt động (3.12) có thể là đầu vào cho quá trình công nhận.

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.

[Nguồn : 3.2, TCVN 11295:2016 (ISO/IEC 19790: 2012)]

3.3

Môi trường ứng dụng (application environment)

Tập hợp tất cả phần mềm và phần cứng bao gồm hệ điều hành và nền tảng phần cứng cần thiết cho một ứng dụng,sẽ gọi một mô-đun mật mã cho các dịch vụ, để hoạt động an toàn.

CHÚ THÍCH 1: môi trường ứng dụng có thể giống với môi trường hoạt động (VD: cả mô-đun mật mã và ứng dụng đang thực thi trong cùng một môi trường).

3.4

Năng lực (competence)

Khả năng áp dụng kiến thức và kỹ năng để đạt được kết quả dự kiến.

CHÚ THÍCH 1: Nó thể hiện tập hợp kiến thức, kỹ năng và hiệu quả cần thiết để thực hiện các hoạt động công việc liên quan đến một hoặc nhiều vai trò trong một vị trí làm việc.

[Nguồn: 3.6, TCVN ISO/IEC 17024:2012, đã sửa đổi - CHÚ THÍCH 1 đã được bổ sung].

3.5

Tham số an toàn quan trọng (critical security parameter)

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 thành phần được tin cậy khác.

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

[Nguồn: 3.18, TCVN 11295:2016 (ISO/IEC 19790: 2012)]

3.6

Thuật toán mật mã (cryptographic algorithm)

Quy trình tính toán được xác định rõ ràng sử dụng các đầu vào thay đổi, có thể bao gồm các khóa mật mã và tạo ra đầu ra.

[Nguồn: 3.20, TCVN 11295:2016 (ISO/IEC 19790: 2012)]

3.7

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.

[Nguồn: 3.25, TCVN 11295:2016 (ISO/IEC 19790: 2012), đã sửa đổi – Mô-đun mật mã đã được thêm vào như một thuật ngữ được thừa nhận.]

3.8

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 tổ chức có thẩm quyền kiểm tra hợp lệ.

[Nguồn : 3.26, TCVN 11295:2016 (ISO/IEC 19790: 2012), sửa đổi - trong định nghĩa, "tiêu chuẩn này" đã được thay đổi thành tài liệu tham khảo TCVN 11295:2016 (ISO/IEC 19790: 2012)]

3.9

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

Tài liệu viết ra được sử dụng bởi người sử dụng (3.20) và/hoặc các vai trò không phải quản trị để vận hành mô-đun mật mã (3.7) trong một chế độ hoạt động đã được chấp thuận.

CHÚ THÍCH 1: Tài liệu hướng dẫn dành cho người không 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.

[Nguồn: 3.77, TCVN 11295:2016 (ISO/IEC 19790: 2012)]

3.10

Môi trường hoạt động (operational environment)

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

[Nguồn: 3.83, TCVN 11295:2016 (ISO/IEC 19790: 2012)]

3.11

Kiểm thử viên vận hành (operational tester)

kiểm thử viên (tester)

Cá nhân được một tổ chức (3.15) giao nhiệm vụ thực hiện các hoạt động thử nghiệm phù hợp với quy trình kiểm thử xác nhận hoạt động (3.13)

3.12

Kiểm thử xác nhận hoạt động (operational testing)

OT

Kiểm tra để xác định tính đúng đắn trong việc cài đặt, cấu hình và hoạt động của mô-đun và mô-đun đó hoạt động an toàn trong môi trường hoạt động (3.10).

3.13

Quy trình kiểm thử xác nhận hoạt động (operational testing process)

OTP

Quy trình hỗ trợ xác định tính đúng đắn trong việc cài đặt, cấu hình và hoạt động của mô-đun và mô-đun đó hoạt động an toàn trong môi trường hoạt động (3.10)

3.14

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.

[Nguồn: 3.85, TCVN 11295:2016 (ISO/IEC 19790: 2012)]

3.15

Tổ chức (organization)

Thực thể chỉ định, triển khai và vận hành một mô-đun mật mã (3.7).

3.16

Kiểm thử tiền vận hành (pre-operational test)

Kiểm thử xác nhận hoạt động (3.12) được thực hiện bởi nhà cung cấp (3.23) trong quá trình phát triển mô-đun mật mã (3.7) hoặc thay mặt cho cơ quan xác nhận (3.22) trong quá trình xác nhận theo TCVN 11295:2016 (ISO/IEC 19790: 2012) cho môi trường hoạt động (3.10).

3.17

Tham số an toàn công khai (public security parameter)

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 (3.7).

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.

[Nguồn: 3.99, TCVN 11295:2016 (ISO/IEC 19790: 2012)]

3.18

Bộ tạo bit ngẫu nhiên (random bit generator)

RBG

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

[Nguồn: 3.100, TCVN 11295:2016 (ISO/IEC 19790: 2012)]

3.19

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

SSP

Các tham số an toàn quan trọng (CSP) (3.5) và các tham số an toàn công khai (PSP) (3.17).

[Nguồn: 3.110, TCVN 11295:2016 (ISO/IEC 19790: 2012)].

3.20

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 (3.7) để đạt được các dịch vụ mật mã.

[Nguồn: 3.130, TCVN 11295:2016 (ISO/IEC 19790: 2012)]

3.21

Được kiểm tra hợp lệ (validated)

Đảm bảo sự đáp ứng đã được kiểm tra bởi một tổ chức có thẩm quyền kiểm tra hợp lệ (3.22).

[Nguồn: 3.131, TCVN 11295:2016 (ISO/IEC 19790: 2012)].

3.22

Tổ chức có 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.

[Nguồn: 3.132, TCVN 11295:2016 (ISO/IEC 19790: 2012) , đã sửa đổi - trong định nghĩa, "này this" đã được thay đổi thành "an"]

3.23

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.

[Nguồn: 3.133, TCVN 11295:2016 (ISO/IEC 19790: 2012)]

4. Ký hiệu và thuật ngữ viết tắt

Áp dụng các thuật ngữ viết tắt trong TCVN 11295:2016 (ISO/IEC 19790: 2012:2012), Mục 4.

5. Cấu trúc tiêu chuẩn

Điều 6 mô tả bối cảnh của kiểm thử xác nhận hoạt động trong môi trường của tổ chức và các mối quan hệ với các bên liên quan chính khác trong việc sản xuất hoặc đặc tả các mô-đun mật mã.

Điều 7 quy định các mô-đun mật mã, các yêu cầu an toàn, đảm bảo vòng đời, các yêu cầu và hướng dẫn về chính sách an toàn, mục đích dự kiến cần được đáp ứng bởi sự tuân thủ của mô-đun mật mã đối với TCVN 11295:2016 (ISO/IEC 19790: 2012).

Điều 8 mô tả môi trường hoạt động của các mô-đun mật mã được sử dụng và các yêu cầu an toàn liên quan đến các mô-đun mật mã cho môi trường hoạt động của chúng.

Điều 9 cung cấp hướng dẫn về cách chọn các mô-đun mật mã trong môi trường hoạt động của chúng.

Điều 10 mô tả các nguyên tắc để kiểm tra hoạt động, bao gồm các giả định được đưa ra để thực hiện các hoạt động kiểm tra sẽ được thực hiện, yêu cầu năng lực dự kiến của các kiểm thử viên vận hành, việc sử dụng các dấu hiệu thu được từ việc kiểm tra hợp lệ các mô-đun mật mã, các yêu cầu về tài liệu để cuộc kiểm thử xác nhận hoạt động và các thủ tục để kiểm thử xác nhận hoạt động.

Điều 11 mô tả các nguyên tắc kiểm tra vận hành bao gồm:

1. Đánh giá cài đặt, cấu hình và hoạt động.
2. Xác định các lỗ hổng bị bỏ sót.
3. Kiểm tra hệ thống quản lý khóa.
4. Kiểm tra các yêu cầu an toàn của thông tin xác thực.
5. Đánh giá tính sẵn sàng của các mô-đun mật mã.
6. Kiểm tra các chính sách an toàn.

Điều 12 mô tả cách báo cáo kết quả kiểm thử xác nhận hoạt động, mô tả nội dung của báo cáo đưa ra kết quả kiểm thử xác nhận hoạt động.

6. Phạm vi của kiểm thử xác nhận hoạt động

Nhà cung cấp thiết kế, phát triển và sản xuất ra mô-đun mật mã. Nhà cung cấp có thể sở hữu mô-đun đã được xác nhận bởi một tổ chức có thẩm quyền kiểm tra hợp lệ, xác định mô-đun tuân thủ TCVN 11295:2016 (ISO/IEC 19790: 2012).

CHÚ THÍCH: Đối với một số tổ chức, có thể có chính sách an toàn của tổ chức, cũng như chính sách an toàn của mô-đun được xác nhận bởi một tổ chức có thẩm quyền kiểm tra hợp lệ, mà được mua lại từ một tổ chức khác để triển khai trong một hệ thống an toàn hoặc môi trường ứng dụng.

Hình 1 chỉ ra phạm vi của TCVN với vòng đời tổng quát của mô-đun mật mã. Hình 1 mô tả toàn bộ vòng đời phát triển của mô-đun bởi nhà cung cấp và vòng đời của mô-đun trong môi trường của tổ chức.

Nhà cung cấp bắt đầu với quy trình đánh giá rủi ro để xác định các yêu cầu an toàn cho các mô-đun mật mã. Đánh giá rủi ro này, dựa trên môi trường hoạt động dự kiến và mục đích thị trường, xác định các yêu cầu an toàn của mô-đun cho từng lĩnh vực cụ thể trong TCVN 11295:2016 (ISO/IEC 19790: 2012). Sau khi được xác định, nhà cung cấp tiến hành phát triển mô-đun bao gồm thiết kế, triển khai và thử nghiệm các quy trình.

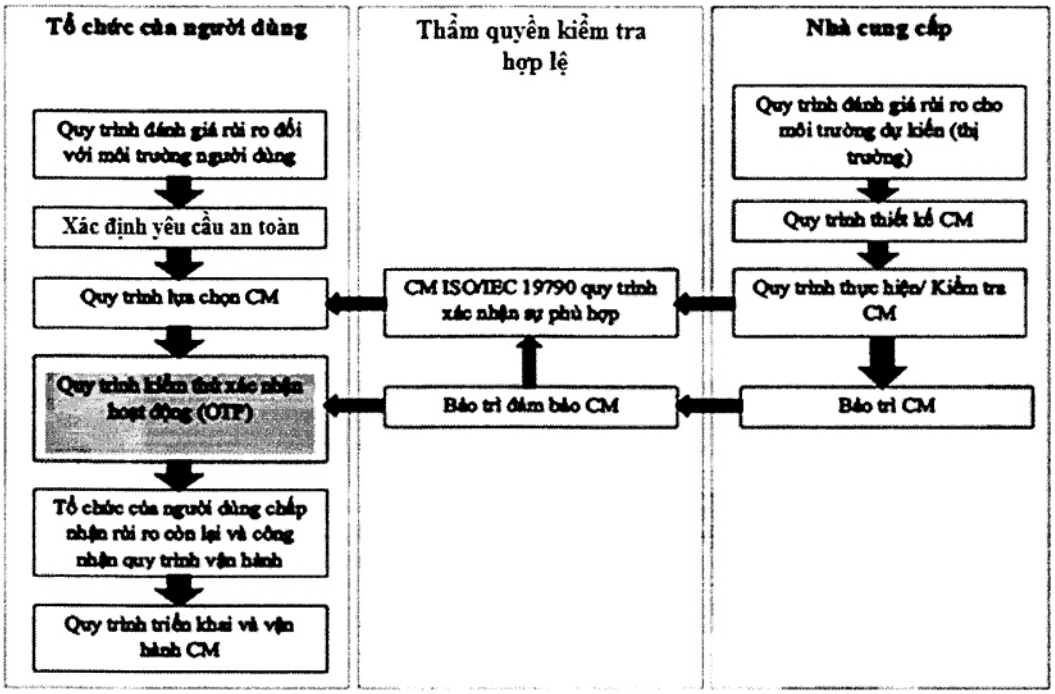
Thông thường, việc kiểm tra hợp lệ của một tổ chức có thẩm quyền kiểm tra hợp lệ sẽ do nhà cung cấp triển khai, tuy nhiên việc xác nhận cũng có thể được bắt đầu bởi nhà sản xuất thiết bị gốc, đơn vị lắp ráp hoặc bởi chính tổ chức.

Tổ chức thực hiện cần phải đánh giá rủi ro và xác định các yêu cầu an toàn cho môi trường hoạt động. Để giải quyết việc đánh giá rủi ro này, tổ chức có thể mua mô-đun mật mã đã được chứng nhận đáp ứng các yêu cầu an toàn và thực hiện quy trình kiểm thử xác nhận hoạt động, trước khi

mô-đun này được triển khai. Các mô-đun mật mã được đảm bảo thông qua việc bảo trì nên được sử dụng trong kiểm thử xác nhận hoạt động.

Quy trình kiểm thử xác nhận hoạt động được thể hiện trong Hình 1, là quy trình được thực hiện để chọn một mô-đun mật mã thích hợp để sử dụng trong một môi trường hoạt động cụ thể. Kết quả của quá trình kiểm thử xác nhận hoạt động có thể sử dụng để thực hiện việc công nhận mô-đun mật mã của tổ chức.

Quy trình kiểm thử xác nhận hoạt động ở giữa việc kiểm tra hợp lệ của mô-đun và công nhận của tổ chức. Phạm vi của tiêu chuẩn này là quy trình thử nghiệm hoạt động, được thể hiện trong Hình 1 ô màu xám.



Hình 1- Quy trình phát triển, xác nhận, công nhận, triển khai và vận hành mô-đun mật mã

7. Mô-đun mật mã

7.1. Quy định chung

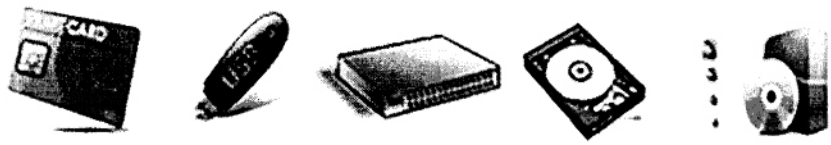
Điều này quy định các loại mô-đun mật mã, các yêu cầu an toàn, đảm bảo vòng đời, các yêu cầu, hướng dẫn về chính sách an toàn và mục tiêu dự kiến được đáp ứng khi mô-đun mật mã tuân thủ TCVN 11295:2016 (ISO/IEC 19790: 2012).

Nhà cung cấp phải cung cấp tài liệu chính sách an toàn và hướng dẫn bắt buộc được quy định trong TCVN 11295:2016 (ISO/IEC 19790: 2012). Nhà cung cấp cũng có thể cần cung cấp tài liệu, hướng dẫn, công cụ hoặc thông số kỹ thuật khác không được quy định, như một phần của việc tuân thủ TCVN 11295:2016 (ISO/IEC 19790: 2012).

7.2. Các loại mô-đun mật mã

7.2.1. Quy định chung

Mô-đun mật mã có thể có nhiều dạng mô-đun khác nhau như được minh họa trong Hình 2 và chứa nhiều loại chức năng an toàn khác nhau, độ mạnh của chức năng an toàn khác nhau. Các mô-đun mật mã có thể chứa các thuật toán giống nhau với các mức an toàn thích hợp.



Hình 2: Các loại mô-đun mật mã khác nhau

Các loại mô-đun mật mã sau đây được định nghĩa bởi TCVN 11295:2016 (ISO/IEC 19790: 2012): mô-đun phần mềm, mô-đun phần sụn, mô-đun phần cứng và mô-đun lai ghép. Mô tả chính xác về các loại mô-đun mật mã được nêu trong 7.2.2, TCVN 11295:2016 (ISO/IEC 19790: 2012) và được mô tả lại bên dưới.

7.2.2. Mô-đun phần mềm

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 tảng 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.

Xếp hạng an toàn tổng thể tối đa của mô-đun phần mềm là mức an toàn 2.

7.2.3. Mô-đun phần sụn

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) thực thi trong một môi trường hoạt động bị giới hạn hoặc không thể sửa đổi. Nền tảng tính toán và hệ điều hành của môi trường hoạt động nơi mà phần sụn thực thi ở ngoài ranh giới mô-đun phần sụn đã được xác định nhưng bị ràng buộc rõ ràng đối với mô-đun phần sụn.

Xếp hạng an toàn tổng thể tối đa của mô-đun phần sụn là mức an toàn 4.

7.2.4. Mô-đun phần cứng

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.

Xếp hạng an toàn tổng thể tối đa của mô-đun phần cứng là mức an toàn 4.

7.2.5. Mô-đun phần mềm lai ghép

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.

Xếp hạng an toàn tổng thể tối đa của mô-đun phần mềm lai ghép là mức an toàn 2.

7.2.6. Mô-đun phần sụn lai ghép

Mô-đun phần sụn kết hợp 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

Xếp hạng an toàn tổng thể tối đa của mô-đun mật mã phần sụn lai ghép là mức an toàn 4.

7.3. Môi trường ứng dụng mô-đun mật mã

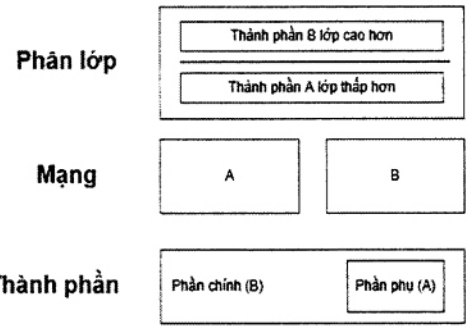
Các mô-đun mật mã được sử dụng trong một phổ rộng của độ nhạy cảm dữ liệu (ví dụ: Dữ liệu quản lý có giá trị thấp, chuyển tiền hàng triệu đô la, dữ liệu an toàn đời sống, thông tin định danh cá nhân, và thông tin nhạy cảm được sử dụng bởi chính phủ) và sự đa dạng của các môi trường ứng dụng (ví dụ: một cơ sở được bảo vệ, một văn phòng, thiết bị tháo rời, và một địa điểm hoàn toàn không được bảo vệ) như Hình 3:

Hình 3: Sự đa dạng của các môi trường ứng dụng.

7.4. Các sản phẩm an toàn có mô-đun mật mã

Các nhà cung cấp phát triển và thị trường hóa các sản phẩm bao gồm chức năng mật mã. Sản phẩm có thể là mô-đun mật mã nếu có ranh giới giống với mô-đun đã được kiểm tra hợp lệ. Một sản phẩm có thể tích hợp một mô-đun mật mã đã đã được kiểm tra hợp lệ được nhúng ngoài các chức năng khác. Do đó, ranh giới của sản phẩm không phải là ranh giới giống như mô-đun mật mã đã hợp lệ.

Một mô-đun mật mã có thể bao gồm các mô-đun mật mã đã được kiểm tra hợp lệ. Một sản phẩm có thể kết hợp thành phần của các mô-đun mật mã đã được kiểm tra hợp lệ cùng với các chức năng khác. Hình 4, bên dưới mô tả các kiểu thành phần khách nhau của các mô-đun mật mã. Các loại thành phần được phân loại ở dạng mô-đun bao gồm: các thành phần, mô-đun được kết nối trong mạng và các mô-đun được cấu thành bởi việc phân lớp.



Hình 4: Các loại thành phần của mô-đun mật mã

Nếu sản phẩm chỉ bao gồm các mô-đun đã được kiểm tra hợp lệ, tổ chức có thể xác minh tính hợp lệ dựa trên danh sách các mô-đun đã được kiểm tra hợp lệ của một tổ chức có thẩm quyền kiểm tra hợp lệ, bằng cách so sánh thông tin phiên bản được cung cấp trong tài liệu của mô-đun từ nhà cung cấp và truy cập trực tiếp trên mô-đun (xem 7.2.3.1 và 7.4.3.1, TCVN 11295:2016 (ISO/IEC 19790: 2012)).

Việc thực hiện xác minh mô-đun đã được kiểm tra hợp lệ có thể khó khăn nếu như mô-đun này là một thành phần được nhúng trong một sản phẩm lớn hơn. Nhà cung cấp phải cung cấp tài liệu sản phẩm bao gồm các tham chiếu đến thông tin phiên bản cho mô-đun mật mã được nhúng đã được kiểm tra hợp lệ. Sản phẩm cũng phải cung cấp cơ chế để người dùng truy cập mô-đun được nhúng đã được kiểm tra hợp lệ để xác định thông tin phiên bản của mô-đun đó. Khi mô-đun mật mã đã được kiểm tra hợp lệ là một phần của ranh giới mật mã cho sản phẩm lớn hơn, khi đó không có sự đảm bảo của một tổ chức có thẩm quyền kiểm tra hợp lệ về hoạt động chính xác của sản phẩm lớn hơn bằng cách sử dụng mô-đun được nhúng. Nhà cung cấp phải cung cấp một tuyên bố đảm bảo rằng tất cả các chức năng mật mã trong ranh giới mật mã sản phẩm chỉ được cung cấp bởi các mô-đun mật mã được nhúng đã được kiểm tra hợp lệ.

Nếu một sản phẩm chứa một tổ hợp mô-đun mật mã đã được kiểm tra hợp lệ thực hiện các chức năng an toàn đã được chấp thuận và một mô-đun mật mã không hợp lệ (để thực hiện các chức năng an toàn không được chấp thuận, ví dụ: thiết lập khóa, lưu trữ khóa, v.v.) mà các dịch vụ an toàn của sản phẩm đó được cung cấp bởi sự kết hợp của hai mô-đun trên, tổ chức phải xác định rằng dịch vụ sản phẩm có thể không được chấp thuận. Nếu tổ chức sử dụng các dịch vụ an toàn không được chấp thuận, môi trường hoạt động có thể tạo ra rủi ro đối với an ninh hoạt động.

VÍ DỤ 1 Nếu dữ liệu được mã hóa bởi mô-đun không hợp lệ và sau đó được mã hóa bởi mô-đun đã được kiểm tra hợp lệ, thì kết quả tổng hợp có thể được coi là đã được chấp thuận.

VÍ DỤ 2 Nếu một chức năng an toàn trên mô-đun đã được kiểm tra hợp lệ sử dụng chức năng thiết lập khóa từ mô-đun chưa hợp lệ, thì kết quả tổng hợp có thể được coi là không được chấp thuận.

Nếu một sản phẩm chứa nhiều mô-đun mật mã, thì thông tin phiên bản của từng mô-đun phải được xác minh riêng với danh sách các mô-đun đã được kiểm tra hợp lệ của một tổ chức có thẩm quyền kiểm tra hợp lệ.

Nếu mô-đun mật mã đã được kiểm tra hợp lệ là một thành phần của một sản phẩm lớn hơn chứa nhiều thành phần (tức là các thành phần không an toàn và các thành phần an toàn), thì tài liệu của nhà cung cấp phải cung cấp thông tin về cách lắp ráp hoặc biên soạn các thành phần với nhau một cách chính xác.

Nếu mô-đun mật mã đã được kiểm tra hợp lệ được phân phối dưới dạng mã nguồn mở, thì tài liệu chính sách an toàn của mô-đun phải cung cấp thông tin để xác minh tính toàn vẹn của các tệp mã nguồn và chỉ định các trình biên dịch, tham số điều khiển cần thiết để biên dịch mã thành định dạng thực thi (xem TCVN 11295:2016 (ISO/IEC 19790: 2012) B.2.5).

7.5. Yêu cầu an toàn đối với mô-đun mật mã

7.5.1. Quy định chung

Các yêu cầu an toàn đối với mô-đun mật mã được quy định trong TCVN 11295:2016 (ISO/IEC 19790: 2012). Có 11 lĩnh vực an toàn trong các yêu cầu an toàn. 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 lần tự kiểm tra; đảm bảo vòng đời; và giảm thiểu các tấn công khác.

Bốn mức an toàn được chỉ định cho từng lĩnh vực trong số 11 lĩnh vực yêu cầu. Mỗi mức an toàn cung cấp sự gia tăng an toàn so với mức trước đó. Mô-đun mật mã được đánh giá độc lập trong từng lĩnh vực. Một số lĩnh vực cung cấp mức an toàn tăng dần với các yêu cầu an toàn tích lũy cho mỗi mức an toàn. Trong các lĩnh vực này, mô-đun mật mã nhận được xếp hạng phản ánh mức an toàn cao nhất mà mô-đun đáp ứng tất cả các yêu cầu của lĩnh vực đó. Trong các lĩnh vực không cung cấp các mức an toàn khác nhau, mô-đun mật mã nhận được xếp hạng tương xứng với xếp hạng tổng thể.

Ngoài việc nhận được xếp hạng độc lập cho từng lĩnh vực an toàn, mô-đun mật mã cũng nhận được xếp hạng an toàn tổng thể. Xếp hạng an toàn tổng thể cho biết mức an toàn tối thiểu của các xếp hạng độc lập nhận được trong các lĩnh vực.

Bốn mức an toàn tăng dần cho phép các giải pháp hiệu quả về chi phí phù hợp với các mức độ nhạy cảm dữ liệu khác nhau và các môi trường ứng dụng khác nhau.

Các điều từ 7.5.2 đến 7.5.5 cung cấp tổng quan về bốn mức an toàn. Các kỹ thuật mật mã (ví dụ: thuật toán mật mã, chức năng an toàn, v.v.) giống nhau qua bốn mức an toàn. Mỗi mức an toàn yêu cầu mức độ tăng dần của các yêu cầu an toàn để bảo vệ chính mô-đun (ví dụ: quyền truy cập

và kiến thức về các thành phần bên trong và hoạt động) và các SSP được chứa và kiểm soát trong mô-đun.

7.5.2. Mức an toàn 1

Mức an toàn 1 cung cấp mức an toàn cơ bản. Các yêu cầu an toàn cơ bản được quy định cho mô-đun mật mã (ví dụ: phải sử dụng ít nhất một chức năng an toàn đã được chấp thuận hoặc phương pháp thiết lập thông số an toàn nhạy cảm đã được chấp thuận). 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.

7.5.3. 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.

7.5.4. 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 TCVN 11295:2016 (ISO/IEC 19790: 2012) 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 TCVN 11295:2016 (ISO/IEC 19790: 2012) cho 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.

7.5.5. Mức an toàn 4

Mức an toàn 4 cung cấp mức an toàn cao nhất được xác định trong TCVN 11295:2016 (ISO/IEC 19790: 2012). 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:

a) Một thứ gì đó được biết, chẳng hạn như một mật khẩu bí mật;
b) Một thứ gì đó được sở hữu, chẳng hạn như một thẻ hoặc khóa vật lý;
c) 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 SSP không được bảo vệ 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 TCVN 11295:2016 (ISO/IEC 19790: 2012) 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 TCVN 11295:2016 (ISO/IEC 19790: 2012) cho các mô-đun mật mã phần mềm.

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.

7.6. Đảm bảo vòng đời của các mô-đun mật mã

TCVN 11295:2016 (ISO/IEC 19790: 2012) 7.11 đề cập đến các yêu cầu xác thực của nhà cung cấp mô-đun mật mã trong quá trình thiết kế, phát triển, thử nghiệm nhà cung cấp, phân phối, vận hành và kết thúc vòng đời, cung cấp tính đảm bảo rằng mô-đun được thiết kế, phát triển phù hợp và nhà cung cấp đó thực hiện đúng việc kiểm tra, giao hàng, các yêu cầu về vận hành và kết thúc vòng đời. Tài liệu hướng dẫn cũng được quy định bao gồm tài liệu hướng dẫn dành cho người quản trị và dành cho người không quản trị. TCVN 11295:2016 (ISO/IEC 19790: 2012) 7.11 cũng giải quyết các yêu cầu về quản lý cấu hình và mô hình trạng thái hữu hạn của nhà cung cấp.

Kiểm thử viên phải kiểm tra TCVN 11295:2016 (ISO/IEC 19790: 2012) 7.11 và sử dụng thông tin này để cài đặt, cấu hình và kiểm tra đúng cách các mô-đun trong môi trường hoạt động của chúng.

7.7. Chính sách an toàn của mô-đun mật mã

7.7.1. Quy định chung

Nhà cung cấp phải cung cấp các yêu cầu về chính sách an toàn mật mã liên quan đến mô-đun mật mã như được quy định trong TCVN 11295:2016 (ISO/IEC 19790: 2012) Phụ lục B. Việc xác nhận mô-đun hợp lệ, tuân thủ với các chính sách an toàn do nhà cung cấp cung cấp (nếu có) đối với tập hợp các yêu cầu này. Kiểm thử viên có thể sử dụng chính sách an toàn.

CHÚ THÍCH: Phụ lục B cung cấp một ví dụ về danh sách kiểm tra hợp nhất các danh sách được đưa ra trong tiêu chuẩn này.

7.7.2. Mô tả mô-đun mật mã

- Sơ đồ minh họa, giản đồ và hình ảnh của mô-đun.
- Mô tả mô-đun, bao gồm tham chiếu rõ ràng và không bị che dấu về các phiên bản phần cứng và phần mềm.
- Ranh giới mật mã của mô-đun.
- Các chế độ hoạt động.
- Hoạt động bị xuống cấp.
- Các chức năng an toàn.
- Thiết kế an toàn tổng thể.
- Dịch vụ an toàn và phi an toàn.
- Các dịch vụ an toàn đã được chấp thuận và không hợp lệ.

7.7.3. Giao diện mô-đun mật mã

- Danh sách tất cả các cổng và giao diện (vật lý và logic).
- Thông tin truyền qua các giao diện logic.
- Các cổng vật lý và dữ liệu đi qua chúng.
- Kênh đáng tin cậy.

7.7.4. Vai trò, dịch vụ và xác thực

- Tất cả các vai trò, với các lệnh dịch vụ tương ứng với đầu vào và đầu ra.
- Mỗi phương thức xác thực.
- Độ mạnh của yêu cầu xác thực.
- Hai hành động bên trong độc lập nếu có khả năng đầu ra mật mã tự khởi tạo.
- Kiểm soát việc tải và cách ly các mã, nhằm ngăn chặn truy cập trái phép và sử dụng mô-đun trong trường hợp tải phần mềm hoặc phần sụn bên ngoài.
- Tất cả các dịch vụ.

7.7.5. An toàn phần mềm/phần sụn

- Các kỹ thuật toàn vẹn đã được chấp thuận.
- Biểu mẫu và từng thành phần của mã thực thi được cung cấp.
- Trình biên dịch và các tham số điều khiển cần thiết để biên dịch mã thành định dạng thực thi trong trường hợp mô-đun đó là mã nguồn mở.

7.7.6. Môi trường hoạt động

- Môi trường hoạt động: không thể sửa đổi, giới hạn và có thể sửa đổi.
- Hệ điều hành dự kiến và (các) nền tảng đã thử nghiệm.
- Mô tả về cách các yêu cầu được đáp ứng.
- Đặc tả các quy tắc an toàn, cài đặt hoặc hạn chế đối với cấu hình của môi trường hoạt động.
- Đặc điểm kỹ thuật của bất kỳ hạn chế nào đối với cấu hình của môi trường hoạt động.

7.7.7. An toàn vật lý

- Phương án: nhúng đơn chip, đa chip hoặc đa chip độc lập.
- Cơ chế an toàn vật lý (ví dụ: giả mạo con dấu, khóa, phản hồi giả mạo và công tắc tự động hóa và cảnh báo).
- Đặc tả các hành động do người (những người) vận hành yêu cầu để đảm bảo rằng an ninh vật lý được duy trì (ví dụ: kiểm tra định kỳ các con dấu có bằng chứng chống giả mạo hoặc kiểm tra phản hồi giả mạo và công tắc xóa trắng).
- Đã thực hiện các phương pháp giảm thiểu cảm ứng lỗi.

7.7.8. An toàn không xâm lấn

- Tất cả các kỹ thuật giảm thiểu không xâm lấn.
- Hiệu quả của các kỹ thuật giảm thiểu không xâm lấn. Cần được xem xét và tham khảo TCVN 12212:2018.

7.7.9. Quản lý các thông số an toàn nhạy cảm

- Danh sách các kiểu khóa được chỉ định, độ mạnh tính theo bit, các chức năng an toàn và các số chứng nhận chức năng an toàn, các khóa được tạo ở đâu và như thế nào, liệu các khóa có được nạp hay không hoặc xuất ra, và phương pháp thành lập được sử dụng.
- Các SSP khác và cách chúng được tạo.
- Công dụng của các đầu ra RBG.
- Các nguồn entropy RBG.
- Các phương thức nạp/xuất khóa thủ công và điện tử.
- Các kỹ thuật lưu trữ SSP.
- Các phương pháp số hóa SSP không được bảo vệ và cơ sở lý luận cũng như khả năng khởi tạo của người vận hành.
- Các khoảng thời gian hoặc khung thời gian chuyển tiếp có thể áp dụng trong đó thuật toán hoặc độ dài khóa chuyển đổi từ được hợp lệ sang không hợp lệ.

7.7.10. Tự kiểm tra

Tự kiểm tra trước khi vận hành và có điều kiện với các thông số xác định.

- Các điều kiện để tự kiểm tra được thực hiện.
- Khoảng thời gian và chính sách liên quan đến bất kỳ điều kiện nào có thể dẫn đến gián đoạn hoạt động của mô-đun trong thời gian lặp lại tự kiểm tra định kỳ.
- Tất cả các trạng thái lỗi và chỉ báo trạng thái.
- Vận hành khởi tạo, nếu có.

7.7.11. Đảm bảo vòng đời

- Quy trình cho cài đặt an toàn, khởi tạo, khởi động và vận hành của mô-đun.
- Yêu cầu bảo trì.
- Hướng dẫn cho người quản trị và người không phải quản trị.

7.7.12. Giảm thiểu các cuộc tấn công khác

- Các kỹ thuật giảm thiểu các cuộc tấn công khác.
- Hiệu quả của các kỹ thuật giảm thiểu.
- Hướng dẫn và ràng buộc liên quan đến an toàn.

Mức độ chi tiết mô tả các cơ chế an toàn được triển khai để giảm thiểu các cuộc tấn công khác phải tương tự như những gì được tìm thấy trên tài liệu giới thiệu sản phẩm (bảng chú giải về sản phẩm).

7.8. Mục đích dự kiến của các mô-đun mật mã đã hợp lệ

Điều khoản này mô tả mục đích dự kiến của mô-đun mật mã.

Các mức an toàn của TCVN 11295:2016 (ISO/IEC 19790: 2012) tập trung vào việc bảo vệ các mô-đun CSP bởi chính nó, bất kể môi trường mà mô-đun được triển khai. Do đó, việc lựa chọn mức an toàn bị ảnh hưởng rất nhiều bởi môi trường mà mô-đun đó triển khai.

Mức an toàn tổng thể của mô-đun mật mã phải được chọn để cung cấp mức an toàn phù hợp với các yêu cầu an toàn của môi trường hoạt động mà mô-đun sẽ được sử dụng và cho các dịch vụ an toàn mà mô-đun mật mã sẽ cung cấp theo mục đích của mô-đun mật mã.

Nếu môi trường dự kiến khác với môi trường hoạt động của tổ chức, thì có thể mục đích dự kiến của mô-đun mật mã đã được kiểm tra hợp lệ trong hệ thống máy tính hoặc hệ thống viễn thông không đủ để đảm bảo tính an toàn của hệ thống tổng thể.

Bộ phận chịu trách nhiệm trong mỗi tổ chức phải đảm bảo rằng các hệ thống máy tính và hệ thống viễn thông của họ sử dụng các mô-đun mật mã cung cấp mức an toàn có thể chấp nhận được cho môi trường hoạt động nhất định.

Tầm quan trọng của nhận thức về an toàn và việc đặt an toàn thông tin trở thành ưu tiên quản lý cần được truyền đạt cho tất cả người dùng. Vì các yêu cầu về an toàn thông tin khác nhau đối với các hoạt động khác nhau, các tổ chức nên xác định các nguồn thông tin của mình và xác định

mức độ nhạy cảm cũng như tác động tiềm tàng của tổn thất. Các biện pháp kiểm soát phải bao gồm các chính sách và thủ tục hành chính, kiểm soát vật lý và môi trường, kiểm soát thông tin và dữ liệu, kiểm soát phát triển và mua lại phần mềm cũng như lập kế hoạch sao lưu và dự phòng.

Một máy tính hoặc hệ thống viễn thông có thể chứa nhiều phiên bản của cùng một mô-đun mật mã hoặc nhiều phiên bản của các mô-đun mật mã khác nhau (ví dụ: nhiều mô-đun mật mã được cung cấp bởi một số nhà cung cấp khác nhau hoặc của các thuộc tính chức năng khác nhau).

8. Môi trường ứng dụng

8.1. An toàn tổ chức

Vì các mức an toàn của TCVN 11295:2016 (ISO/IEC 19790: 2012) tập trung vào việc bảo vệ các CSP của mô-đun mật mã bởi chính mô-đun đó bất kể môi trường mà mô-đun được triển khai, các tổ chức nên xác định các nguồn thông tin của họ và xác định độ nhạy cảm cũng như tác động tiềm ẩn của việc mất CSP trong môi trường hoạt động và ứng dụng.

Bộ phận chịu trách nhiệm trong mỗi tổ chức phải đảm bảo rằng các hệ thống máy tính và mạng viễn thông của họ sử dụng các mô-đun mật mã cung cấp mức an toàn có thể chấp nhận được cho môi trường hoạt động nhất định. Vì mỗi tổ chức chịu trách nhiệm lựa chọn các chức năng an toàn đã được chấp thuận phù hợp với ứng dụng nhất định, tổ chức cần lưu ý rằng sự phù hợp với TCVN 11295:2016 (ISO/IEC 19790: 2012) không bao hàm đầy đủ khả năng tương tác của các sản phẩm tuân thủ. Tầm quan trọng của nhận thức về an toàn, bao gồm các chính sách an toàn liên quan và việc đặt an toàn thông tin trở thành ưu tiên quản lý cần được thông báo cho tất cả những người có liên quan.

Các tổ chức phải xác định các chính sách và thủ tục hành chính của mình, các kiểm soát vật lý và môi trường, kiểm soát thông tin và dữ liệu, kiểm soát phát triển và mua lại phần mềm cũng như lập kế hoạch sao lưu và dự phòng.

- Chính sách quản lý, quy tắc và thủ tục chi phối hoạt động của môi trường ứng dụng;
- Các yêu cầu và quy tắc tương tác giữa cả hệ thống đáng tin cậy và không đáng tin cậy trong môi trường ứng dụng;
- Kiểm soát kỹ thuật, kiểm soát hoạt động và kiểm soát quản lý để duy trì tính an toàn của môi trường ứng dụng. TCVN ISO/IEC 27002:2020 cung cấp các biện pháp kiểm soát an toàn thường xuyên được quy định bởi một tổ chức.

8.2. Kiến trúc của môi trường ứng dụng

Về mặt logic, tất cả các phần của hệ thống trong cùng một bộ chính sách an toàn, yêu cầu an toàn và tài liệu an toàn có thể được gọi là miền an toàn.

Miền an toàn có thể cung cấp các dịch vụ an toàn mà các miền khác có thể sử dụng thông qua giao tiếp hoặc giao diện lập trình ứng dụng.

Có thể một số miền an toàn yêu cầu các mức an toàn khác nhau hoặc độ mạnh của thuật toán mật mã.

Hệ thống an toàn sử dụng các mô-đun mật mã có thể tách thành một hệ thống con và là một tập hợp của một hoặc nhiều thành phần hoạt động có khả năng thực thi độc lập với phần còn lại của hệ thống an toàn. Một thành phần hoạt động thực hiện một phần chức năng của hệ thống (cho dù có liên quan đến an toàn hay không).

Khi thiết kế kiến trúc của môi trường ứng dụng, một tổ chức nên xem xét những điều sau đây.

- Vì mỗi tổ chức chịu trách nhiệm lựa chọn các chức năng an toàn đã được chấp thuận phù hợp với một ứng dụng nhất định, tổ chức cần lưu ý rằng sự phù hợp với TCVN 11295:2016 (ISO/IEC 19790: 2012) không bao hàm đầy đủ khả năng tương tác của các sản phẩm tuân thủ.
- Môi trường ứng dụng có thể có các chính sách an toàn áp dụng cho một số miền an toàn nhất định mà không áp dụng cho các miền khác.
- Tất cả các giao diện giữa hệ thống hoạt động và môi trường ứng dụng của nó cần phải được xác định.

9. Môi trường hoạt động

9.1. Các yêu cầu an toàn liên quan đến các mô-đun mật mã cho môi trường hoạt động

9.1.1. Quy định chung

Các yêu cầu an toàn liên quan đến các mô-đun mật mã được yêu cầu trong môi trường hoạt động của chúng được quy định trong đặc điểm kỹ thuật cho môi trường hoạt động mà các mô-đun mật mã sẽ được triển khai. Tổ chức có trách nhiệm thiết lập các đặc điểm kỹ thuật cho môi trường hoạt động trong suốt quá trình đánh giá rủi ro mô-đun mật mã đối với môi trường và xác định các yêu cầu an toàn như được minh họa trong Hình 1.

Các yêu cầu an toàn đối với môi trường hoạt động có thể được trình bày dưới dạng hai loại: những điều được hỗ trợ bởi mô-đun mật mã và những điều được hỗ trợ bởi môi trường hoạt động.

9.1.2. Nguồn Entropy

Nếu mô-đun mật mã cần nguồn entropy được sử dụng làm nguồn cho bộ tạo bit ngẫu nhiên và nguồn entropy được thu thập trong môi trường hoạt động, thì nguồn entropy phải đáp ứng các yêu cầu về độ mạnh của các thuật toán mật mã và các yêu cầu an toàn được mô tả trong TCVN 13721:2023.

9.1.3. Cơ chế đánh giá

Nếu mô-đun mật mã sử dụng cơ chế đánh giá được thực hiện trong môi trường hoạt động, thì cơ chế đánh giá phải đáp ứng các yêu cầu an toàn đối với TCVN 11295:2016 (ISO/IEC 19790: 2012).

9.1.4. Chức năng không thể mở khóa về mặt vật lý

Nếu mô-đun mật mã cần một chức năng chống mở khóa vật lý để tạo ra các tham số an toàn không được lưu trữ trong môi trường hoạt động, thì nó phải đáp ứng các yêu cầu về độ mạnh của các thuật toán mật mã và các yêu cầu an toàn được mô tả trong ISO/IEC 20897.

9.2. Các giả định về an toàn cho môi trường hoạt động

9.2.1. Quy định chung

Điều 7.5 xác định các yêu cầu đối với bốn mức an toàn đối với 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, chuyển tiền hàng triệu đô la và dữ liệu an toàn đời sống) và và sự đa dạng của các môi trường ứng dụng (ví dụ: một cơ sở được bảo vệ, một văn phòng và một địa điểm hoàn toàn không được bảo vệ).

Bốn mức an toàn tăng dần này cho phép các giải pháp hiệu quả về chi phí phù hợp với các mức độ nhạy cảm dữ liệu khác nhau và các môi trường ứng dụng khác nhau.

Việc sử dụng mô-đun mật mã đã được kiểm tra hợp lệ trong máy tính hoặc hệ thống viễn thông là không đủ để đảm bảo các yêu cầu an toàn của hệ thống tổng thể. Mức an toàn tổng thể của mô-đun mật mã phải được chọn để cung cấp mức an toàn phù hợp với các yêu cầu an toàn của ứng dụng và môi trường hoạt động mà mô-đun sẽ được sử dụng và cho các dịch vụ an toàn mà mô-đun sẽ cung cấp. Bộ phận có trách nhiệm trong mỗi tổ chức phải đảm bảo rằng các hệ thống máy tính và viễn thông của họ sử dụng các mô-đun mật mã cung cấp mức an toàn có thể chấp nhận được cho ứng dụng và môi trường hoạt động nhất định.

Tầm quan trọng của nhận thức về an toàn và việc đặt an toàn thông tin trở thành ưu tiên quản lý cần được truyền đạt cho tất cả người dùng. Vì các yêu cầu về an toàn thông tin khác nhau đối với các ứng dụng khác nhau, các tổ chức nên xác định các nguồn thông tin của mình và xác định mức độ nhạy cảm cũng như tác động tiềm ẩn của tổn thất. Các biện pháp kiểm soát phải dựa trên các rủi ro tiềm ẩn và nên được lựa chọn từ các biện pháp kiểm soát sẵn có, bao gồm các chính sách và thủ tục hành chính, kiểm soát vật lý và môi trường, kiểm soát thông tin và dữ liệu, kiểm soát phát triển và mua lại phần mềm cũng như lập kế hoạch sao lưu và dự phòng.

Bốn mức an toàn của TCVN 11295:2016 (ISO/IEC 19790: 2012) tập trung vào việc bảo vệ các mô-đun CSP bởi chính nó, bất kể môi trường mà mô-đun được triển khai. đã triển khai. Ví dụ: mức an toàn 1, bản thân nó không cung cấp khả năng bảo vệ an ninh vật lý, có thể là một giải pháp được chấp nhận trong một số hệ thống an toàn vì môi trường cung cấp các tính năng bảo vệ an toàn vật lý cần thiết.

Điều 9.2.2 đến 9.2.4 xác định các giả định an toàn cho mô-đun mật mã. Thông tin này được cung cấp từ Tài liệu tham khảo [9] trong Thư mục tài liệu tham khảo.

CHÚ THÍCH: Phụ lục B cung cấp một ví dụ về danh sách kiểm tra hợp nhất các danh sách được đưa ra trong tiêu chuẩn này.

9.2.2. Mức an toàn 1

Bảo vệ được cung cấp:

Không có bảo vệ vật lý cho CSP do mô-đun cung cấp; quyền truy cập giả định

- Phần cứng: thăm dò và quan sát các thành phần giả định.
- Phần mềm: quyền truy cập vào môi trường hoạt động, ứng dụng và dữ liệu giả định.

CHÚ THÍCH: Mô-đun có thể sử dụng các phương pháp giảm thiểu không xâm lấn.

Các giả định:

- Hoạt động của các dịch vụ mật mã được chấp thuận và các chức năng an toàn là chính xác;
- Tất cả các cuộc tấn công dẫn đến quyền truy cập vào CSP và dữ liệu (bản rõ và bản mã) được lưu trong mô-đun;
- Người vận hành chịu trách nhiệm về việc bảo vệ vật lý của mô-đun; và
- Giá trị hoặc độ nhạy cảm của dữ liệu được bảo vệ bởi mô-đun được cho là không đáng kể trong môi trường không được bảo vệ.

Loại tấn công:

Tấn công thụ động để có quyền truy cập ngay lập tức vào CSP và dữ liệu do mô-đun nắm giữ.

Các giả định về đặc tính tấn công / thử nghiệm:

- Không có quyền truy cập trước vào mô-đun được giả định.
- Không cần công cụ và tài nguyên.

Giá trị:

Mô-đun cung cấp hoạt động chính xác của các chức năng và dịch vụ an toàn. Việc bảo vệ các CSP bản rõ và dữ liệu được lưu giữ trong mô-đun được cung cấp bởi người vận hành mô-đun (ví dụ: môi trường mà mô-đun có thể được sử dụng). Nếu mô-đun được sử dụng trong môi trường không được bảo vệ, thì mô-đun không được giữ hoặc duy trì các CSP hoặc dữ liệu bản rõ không được bảo vệ.

9.2.3. Mức an toàn 2

Bảo vệ được cung cấp:

- Bằng chứng quan sát được về việc giả mạo.
- Ranh giới vật lý của mô-đun đã làm mờ để ngăn cản việc quan sát trực tiếp các thành phần an toàn bên trong.
- Phần cứng: giả định là thăm dò.
- Phần mềm: bảo vệ truy cập logic của các CSP của mô-đun mật mã không được bảo vệ và dữ liệu được cung cấp bởi hệ điều hành đáp ứng các yêu cầu an toàn được quy định trong TCVN 11295:2016 (ISO/IEC 19790: 2012) 7.6.3.

CHÚ THÍCH: Mô-đun có thể sử dụng các phương pháp giảm thiểu không xâm lấn.

Các giả định:

- Hoạt động của các dịch vụ mật mã được chấp thuận và các chức năng an toàn là chính xác;
- Tất cả các cuộc tấn công dẫn đến quyền truy cập vào CSP và dữ liệu (bản rõ và bản mã) được giữ trong mô-đun;
- Người vận hành chịu trách nhiệm về việc bảo vệ vật lý của mô-đun; và
- Giá trị hoặc độ nhạy cảm của dữ liệu được bảo vệ bởi mô-đun được giả định là thấp trong môi trường không được bảo vệ.

Loại tấn công

Tấn công chủ động để có quyền truy cập ngay lập tức vào CSP và dữ liệu do mô-đun nắm giữ.

Các giả định về đặc tính tấn công/thử nghiệm:

- Không có quyền truy cập trước vào mô-đun được giả định.
- Các công cụ và tài nguyên với chi phí thấp luôn sẵn sàng, có sẵn tại thời điểm bị tấn công.
- Thời gian tấn công được cho là thấp.

Giá trị:

Mô-đun cung cấp hoạt động chính xác của các chức năng và dịch vụ an toàn. Việc bảo vệ các CSP bản rõ và dữ liệu được lưu giữ trong mô-đun được cung cấp bởi người vận hành mô-đun (ví dụ: môi trường mà mô-đun có thể được sử dụng). Người vận hành mô-đun nhận thức được bằng chứng giả mạo, cho biết rằng thông tin nội bộ có thể bị xâm phạm. Nếu mô-đun được sử dụng trong môi trường không được bảo vệ, thì mô-đun không được giữ hoặc duy trì các văn bản rõ không được bảo vệ của CSP hay các dữ liệu có giá trị trung bình hoặc cao.

9.2.4. Mức an toàn 3

Bảo vệ được cung cấp:

- Bằng chứng quan sát được về việc giả mạo.
- Ranh giới vật lý của mô-đun đã làm mờ để ngăn cản việc quan sát trực tiếp các thành phần an toàn bên trong.
- Đã ngăn chặn được các cuộc tấn công xâm nhập / thăm dò trực tiếp.
- Vật liệu đóng gói hoặc vỏ bọc chống giả mạo mức độ mạnh.
- Có thể áo dụng việc xóa trắng nếu lớp bọc hoặc các cổng bị mở.
- Phần mềm: không áp dụng

CHÚ THÍCH: Mô-đun có thể sử dụng các phương pháp giảm thiểu không xâm lấn.

Các giả định:

- Hoạt động của các dịch vụ mật mã được chấp thuận và các chức năng an toàn là chính xác;
- Khi kẻ tấn công có quyền truy cập vật lý hoặc ở gần mô-đun, các cuộc tấn công không trực tiếp có thể dẫn đến quyền truy cập vào CSP và dữ liệu (bản rõ và bản mã) được giữ trong mô-đun; và

- Giá trị của dữ liệu được bảo vệ bởi mô-đun được giả định là vừa phải trong môi trường không được bảo vệ.

Loại tấn công

Tấn công mạnh vừa phải để có quyền truy cập ngay lập tức vào CSP và dữ liệu do mô-đun nắm giữ.

Các giả định về đặc tính tấn công / thử nghiệm:

1. Quyền truy cập trước hoặc kiến thức cơ bản của mô-đun được giả định.
2. Các công cụ và tài nguyên sẵn có.
3. Thời gian tấn công thực tế được giả định là vừa phải (điều này không bao gồm thời gian dành cho việc truy cập trước hoặc kiến thức cơ bản về mô-đun).

Giá trị:

Mô-đun cung cấp hoạt động chính xác của các chức năng và dịch vụ an toàn. Việc bảo vệ các CSP bản rõ và dữ liệu được giữ trong mô-đun được cung cấp bởi người vận hành mô-đun (ví dụ: môi trường mà mô-đun có thể được sử dụng) và bởi các cơ chế bảo vệ vật lý của mô-đun (ví dụ: vỏ bọc chắc chắn, chống xâm nhập qua vỏ bọc và các cổng, ngăn chặn sự thăm dò, EFP hoặc EFT đối với nhiệt độ và điện áp, giảm thiểu sự tấn công không xâm lấn). Người vận hành mô-đun nhận thức được bằng chứng giả mạo rằng thông tin nội bộ có thể bị xâm phạm. Một cuộc tấn công đã được tính toán trước nhưng có độ khó vừa phải. Nếu mô-đun được sử dụng trong môi trường không được bảo vệ, thì mô-đun không được giữ hoặc duy trì các văn bản rõ không được bảo vệ của CSP hoặc dữ liệu có giá trị cao.

9.2.5. Mức an toàn 4

Bảo vệ được cung cấp:

- Bằng chứng quan sát được về việc giả mạo.
- Ranh giới vật lý của mô-đun đã làm mờ để ngăn cản việc quan sát trực tiếp các thành phần an toàn bên trong.
- Đã ngăn chặn được các cuộc tấn công xâm nhập/thăm dò trực tiếp.
- Vật liệu đóng gói hoặc vỏ bọc chống giả mạo mức độ mạnh.
- Có thể áp dụng việc xóa trắng nếu lớp bọc hoặc các cổng bị mở.

CHÚ THÍCH: Mô-đun có thể sử dụng các phương pháp giảm thiểu không xâm lấn.

Một lớp bảo vệ hoàn chỉnh xung quanh mô-đun ngăn chặn các nỗ lực truy cập vật lý trái phép.

- Việc thâm nhập vào vỏ bọc của mô-đun từ bất kỳ hướng nào có khả năng bị phát hiện rất cao, dẫn đến việc lập tức xóa trắng các văn bản rõ của các CPS hoặc gây hư hỏng nghiêm trọng đối với mô-đun khiến mô-đun không thể hoạt động được.

- Khi kẻ tấn công có quyền truy cập vật lý hoặc ở gần mô-đun, mô-đun sẽ ngăn chặn quyền truy cập vào CSP và dữ liệu (bản rõ và bản mã) được giữ trong mô-đun khỏi các cuộc tấn công không trực tiếp.
- Phần mềm: không áp dụng

Các giả định:

- Hoạt động chính xác của các dịch vụ mật mã được chấp thuận và các chức năng an toàn;
- Mô-đun có khả năng chống giả mạo chống lại tất cả các cuộc tấn công vật lý được xác định trong TCVN 11295:2016 (ISO/IEC 19790: 2012);
- Giá trị của dữ liệu được bảo vệ bởi mô-đun được giả định là cao trong môi trường không được bảo vệ.

Loại tấn công

Tấn công chủ động để giành quyền truy cập ngay lập tức vào CSP và dữ liệu do mô-đun nắm giữ.

Các giả định về đặc tính tấn công/thử nghiệm:

- Quyền truy cập trước hoặc kiến thức nâng cao của mô-đun được giả định.
- Dụng cụ và tài nguyên chuyên dụng.
- Các cuộc tấn công về nhiệt độ và điện áp.
- Không giới hạn thời gian tấn công.

Giá trị:

Mô-đun cung cấp hoạt động chính xác của các chức năng và dịch vụ an toàn. Việc bảo vệ các văn bản rõ của các CPS và dữ liệu được giữ trong mô-đun được cung cấp bởi người vận hành mô-đun (ví dụ: môi trường mà mô-đun có thể được sử dụng) và bởi các cơ chế bảo vệ vật lý của mô-đun (ví dụ: vỏ bọc chắc chắn, chống xâm nhập qua vỏ bọc và các cổng, bao bọc hoàn toàn nhằm bảo vệ và phát hiện thâm nhập dẫn để xóa trắng ngay lập tức các văn bản rõ của các CPS, EFP cho điện áp và nhiệt độ, giảm thiểu tấn công không xâm nhập, bảo vệ khỏi cảm ứng lỗi). Người vận hành mô-đun nhận biết được bằng chứng giả mạo rằng mô-đun đã được đính kèm. Mô-đun phải xóa trắng tất cả các CSP không được bảo vệ trước khi kẻ tấn công có thể xâm phạm mô-đun. Một cuộc tấn công được tính toán trước, có sự tài trợ lớn, có tổ chức và được xác định.

10. Cách chọn mô-đun mật mã

10.1. Quy định chung

Điều khoản này cung cấp hướng dẫn về việc chọn mô-đun mật mã. Tổ chức lựa chọn các mô-đun mật mã đáp ứng các yêu cầu an toàn của tổ chức đối với môi trường hoạt động. Sau khi được chọn, cùng một mô-đun mật mã và môi trường hoạt động được sử dụng để thực hiện kiểm tra xác nhận hoạt động của mô-đun.

10.2. Chính sách sử dụng

Trước khi có thể chọn mô-đun mật mã, tổ chức phải xác định dữ liệu nào cần được bảo vệ bằng mật mã, nơi bảo vệ bằng mật mã đó cần được cung cấp và độ mạnh an toàn, các thuật toán và giao thức sẽ được sử dụng cho việc bảo vệ bằng mật mã đó. Việc xác định phụ thuộc vào trường hợp sử dụng.

Ví dụ về dữ liệu được xem xét để bảo vệ bằng mật mã:

- Thông tin nhận dạng cá nhân (PII);
- Thông tin nhận dạng doanh nghiệp (BII);
- Thông tin liên lạc;
- Dữ liệu ở trạng thái nghỉ;
- Thông tin nhạy cảm khác.

Ví dụ về nơi dữ liệu có thể yêu cầu bảo vệ bằng mật mã:

- Lưu trữ dữ liệu:
    + Dữ liệu được lưu trữ;
    + Dữ liệu hoạt động;
- Dữ liệu được vận chuyển:
    + Máy khách tới máy khách khác (ví dụ VPN, mã hóa đầu cuối);
    + LAN;
    + WAN;
    + Wireless:
        - Wi-Fi;
        - Bluetooth;
        - Radio;
        - Tín hiệu vệ tinh;
    + Thiết bị tháo rời:
        - Thẻ nhớ;
        - USB lưu trữ;
        - Ổ cứng lưu trữ có thể tháo rời hoặc gắn ngoài;
        - Đĩa CD/DVD;
        - Thẻ thông minh;
- Dữ liệu nhạy cảm về thời gian;
- Quản lý truy cập thiết bị và hệ thống;
- Thiết bị và hệ thống sinh trắc;
- Ranh giới bảo vệ của thiết bị và hệ thống;
- Cơ sở dữ liệu;
- Các thiết bị và hệ thống phát hiện;
- Các IC, thẻ thông minh và các thiết bị hệ thống liên quan tới thẻ thông minh;
- Hệ thống quản lý chính;

- Các thiết bị đa chức năng;
- Mạng và các thiết bị hệ thống liên quan tới mạng;
- Các hệ điều hành;
- Các sản phẩm cho chữ ký số;
- Máy tính tin cậy.

Độ an toàn, thuật toán và giao thức an toàn:

Các thuật toán được chấp thuận và độ mạnh an toàn liên quan có thể được tìm thấy trong TCVN 11295:2016 (ISO/IEC 19790: 2012), Phụ lục C và D.

Tổ chức cũng nên xem xét khả năng tương tác của các mô-đun mật mã khác nhau vì API được cung cấp có thể không tương thích giữa các sản phẩm hoặc nhà cung cấp.

Khi tất cả dữ liệu yêu cầu bảo vệ bằng mật mã được xác định, vị trí an toàn mật mã cần được triển khai, lựa chọn các thuật toán an toàn, độ mạnh và các giao thức, và khả năng tương tác, tổ chức nên phát triển các chính sách an toàn nêu rõ những quyết định này. Các chính sách an toàn phải giải quyết cả nơi dữ liệu cần được bảo vệ và trường hợp dữ liệu trùng nhau không cần bảo vệ.

10.3. Đảm bảo mô-đun mật mã

Khi một chính sách đã xác định rằng dữ liệu sẽ được bảo vệ trong 10.2, tổ chức sẽ bắt đầu tìm kiếm mô-đun mật mã thích hợp. Người dùng nên giới hạn việc lựa chọn mô-đun mật mã của họ ở một mô-đun đã được kiểm tra hợp lệ bởi một tổ chức có thẩm quyền kiểm tra hợp lệ theo TCVN 11295:2016 (ISO/IEC 19790: 2012). Việc xác nhận này cung cấp mức đảm bảo cơ bản về các thuộc tính của mô-đun mật mã. Thông thường, tổ chức có thẩm quyền kiểm tra hợp lệ cung cấp danh sách công khai các mô-đun đó đã được tổ chức có thẩm quyền kiểm tra hợp lệ đó xác nhận (ví dụ: Phụ lục A). Một tổ chức có thể xác định danh sách nào sẽ sử dụng để lựa chọn mô-đun. Ví dụ: một tổ chức chính phủ có thể có một danh sách là một phần của danh sách các tổ chức có thẩm quyền kiểm tra hợp lệ.

10.4. Khả năng tương tác

Như đã đề cập trong 10.2, nhiều mô-đun mật mã có thể triển khai các thuật toán giống nhau với các độ an toàn thích hợp, nhưng các API được cung cấp bởi mỗi mô-đun mật mã đó có thể không tương thích. Vấn đề này thường xuất hiện giữa các nhà cung cấp khác nhau, nhưng có thể xảy ra ngay cả trong các sản phẩm của cùng nhà cung cấp. Ngoài các API, các giao thức được sử dụng để quản lý khóa và khả năng tương tác với các hệ thống quản lý khóa cần được xem xét.

10.5. Lựa chọn xếp hạng an toàn cho bảo vệ SSP

Như đã đề cập trong Điều 9, môi trường vật lý và hoạt động cần được xem xét để xác định xếp hạng an toàn tổng thể hoặc xếp hạng an toàn riêng lẻ được lựa chọn. Tùy thuộc vào xếp hạng an toàn được chọn, khả năng bảo vệ SSP của mô-đun có thể được cung cấp bởi môi trường vật lý (ví dụ: trong cơ sở được kiểm soát truy cập) hoặc bởi chính mô-đun. Đối với mỗi mô-đun được tổ

chức triển khai, môi trường vật lý cần được xem xét dựa trên giá trị hoặc độ nhạy cảm của dữ liệu hay các SSP mà mô-đun đó xử lý.

11. Nguyên tắc kiểm thử xác nhận hoạt động

11.1. Quy định chung

Điều khoản này mô tả các nguyên tắc kiểm thử xác nhận hoạt động đánh giá các yêu cầu về cài đặt, cấu hình, vận hành và quản lý khóa và an toàn của thông tin xác thực trong môi trường hoạt động để đảm bảo rằng mô-đun mật mã hoạt động chính xác và an toàn, các lỗ hổng an toàn đã được xem xét thích hợp và xác minh rằng thông tin được cung cấp trong tài liệu chính sách an toàn tuân thủ ISO/IEC

Các mô-đun mật mã và môi trường hoạt động của chúng nói chung rất phức tạp. Khi các mô-đun mật mã được triển khai trong môi trường hoạt động của chúng, ngay cả một lỗi nhỏ hoặc sai sót trong cấu hình hoặc khởi tạo cũng có thể ảnh hưởng đến tính an toàn của toàn bộ hệ thống an toàn. Vì vậy, điều quan trọng là phải thực hiện kiểm thử xác nhận hoạt động và cần phải chọn một mô-đun mật mã phù hợp trong môi trường hoạt động trong suốt quá trình kiểm thử xác nhận hoạt động.

Trong quá trình vận hành mô-đun mật mã, cần xem xét rằng người dùng mô-đun mật mã có thể kém tin cậy hơn, ít kinh nghiệm hơn, kém năng lực hơn và/hoặc ít động lực hơn những gì được giả định trong quá trình xác thực. Kiểm thử xác nhận hoạt động cho các mô-đun mật mã phải được thực hiện sau khi các mô-đun được tích hợp vào môi trường hoạt động của chúng và trước khi hoạt động của các mô-đun mật mã bắt đầu.

Để đảm bảo an ninh, tổ chức nên kiểm tra mô-đun mật mã đã được kiểm tra hợp lệ trong môi trường hoạt động hoặc ứng dụng của nó để đánh giá xem mô-đun có hoạt động đúng như được cài đặt và cấu hình (như được chỉ định trong chính sách an toàn) và tương tác với hệ thống an toàn mà nó được triển khai hay không.

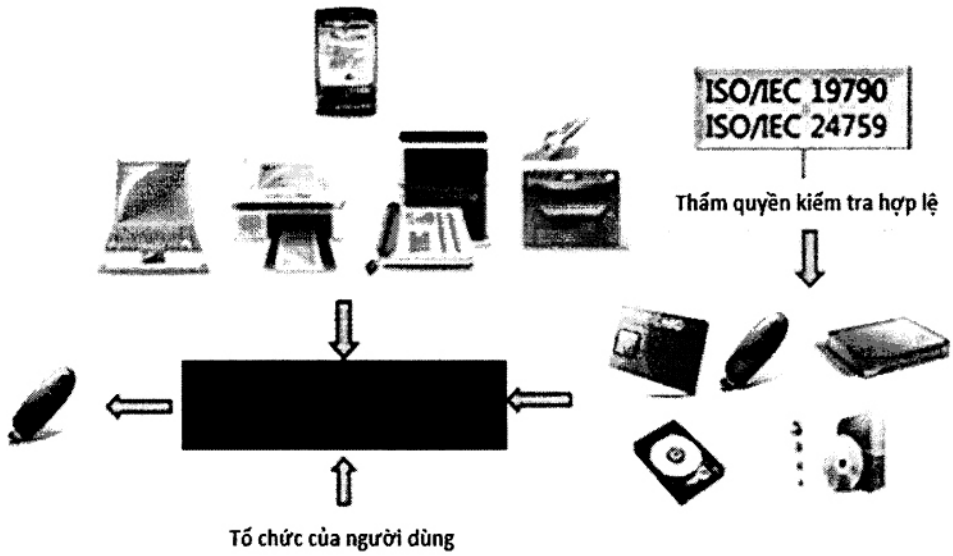
Chủ sở hữu hệ thống an toàn nên chỉ định các yêu cầu an toàn để bảo vệ tài sản (dữ liệu cần được bảo vệ bằng mật mã) sau khi xem xét ngân sách, chính sách an toàn của tổ chức, giá trị của tài sản, các mối đe dọa, lỗ hổng an toàn, v...v…

Khi một mô-đun mật mã được sử dụng trong nhiều môi trường ứng dụng, việc kiểm thử xác nhận hoạt động phải được thực hiện để xác nhận rằng mô-đun mật mã có thể được sử dụng đúng cách trong mỗi môi trường ứng dụng.

Trong trường hợp của TCVN 11295:2016 (ISO/IEC 19790: 2012), việc xác nhận các mô-đun mật mã diễn ra khi quá trình phát triển của chúng hoàn tất và trước khi mô-đun mật mã được đưa vào hoạt động trong môi trường của nó.

Việc kiểm thử xác nhận hoạt động phải diễn ra trước khi mô-đun được đưa vào hoạt động. Kiểm thử xác nhận hoạt động cũng có thể được lặp lại sau khi tổ chức đã cấp quyền hoạt động, tùy thuộc vào chính sách của tổ chức.

Quá trình kiểm thử xác nhận hoạt động, như được thể hiện trong Hình 5, được thực hiện để chọn một mô-đun mật mã thích hợp để sử dụng cho một mô-đun cụ thể giữa sự đa dạng của các môi trường hoạt động. Kết quả của quá trình kiểm thử xác nhận hoạt động có thể được sử dụng làm đầu vào cho việc công nhận mô-đun mật mã của tổ chức.



Hình 5: Quá trình kiểm thử xác nhận hoạt động

11.2. Giả định

Tiêu chuẩn này giả định rằng các yêu cầu an toàn liên quan đến các mô-đun mật mã được yêu cầu trong môi trường hoạt động của chúng do tổ chức cung cấp. Nếu các yêu cầu an toàn chưa sẵn sàng hoặc chưa được cung cấp, người thử nghiệm không thể tiến hành kiểm thử xác nhận hoạt động.

Tiêu chuẩn này giả định rằng có các mô-đun mật mã đáp ứng các yêu cầu an toàn của TCVN 11295:2016 (ISO/IEC 19790: 2012) đã được xác nhận bởi tổ chức có thẩm quyền kiểm tra hợp lệ. Thông thường, tổ chức có thẩm quyền kiểm tra hợp lệ cung cấp danh sách công khai của các mô-đun đó đã được xác nhận bởi tổ chức có thẩm quyền kiểm tra hợp lệ.

11.3. Hoạt động kiểm thử xác nhận hoạt động

Kiểm thử viên phải thực hiện kiểm thử xác nhận hoạt động trong môi trường hoạt động của tổ chức để kiểm tra xem các mô-đun mật mã có đáp ứng các yêu cầu an toàn được chỉ định cho môi trường hoạt động hay không.

Tập hợp các hoạt động tối thiểu để kiểm thử viên tuân theo trong quá trình kiểm thử xác nhận hoạt động như sau:

a) Lập kế hoạch kiểm thử xác nhận hoạt động bao gồm:

1. Thời gian mà kiểm thử xác nhận hoạt động sẽ diễn ra;
2. Các tài liệu liên quan đến thử nghiệm vận hành sẽ được chuẩn bị;
3. Các nguồn lực mà kiểm tra thử nghiệm vận hành sẽ yêu cầu, bao gồm nhân lực, thiết bị thử nghiệm và thời gian cần thiết để hoàn thành thử nghiệm;
4. Bằng chứng có thể thu được từ các thử nghiệm khác, v...v...; và
5. Các công cụ cần thiết và môi trường thử nghiệm cần thiết được sử dụng;

b) Đưa ra bằng chứng thử nghiệm từ kiểm thử xác nhận hoạt động;

c) Đánh giá bằng chứng để đưa ra kết quả của kiểm thử xác nhận hoạt động;

d) Báo cáo.

11.4. Năng lực cho kiểm thử viên

Tổ chức cần xác định các yêu cầu về năng lực đối với kiểm thử viên.

Để hỗ trợ mục tiêu là lựa chọn mô-đun mật mã phù hợp trong môi trường hoạt động, kiểm thử viên cần phải đạt được kiến thức, kỹ năng, kinh nghiệm và trình độ chuyên môn cần thiết tối thiểu phù hợp với TCVN 11295:2016 (ISO/IEC 19790: 2012) và TCVN 12211:2018 (ISO/IEC 24759:2017).

Tổ chức có thể yêu cầu các yếu tố bổ sung về năng lực như năng khiếu, sự nhiệt tình, sáng kiến, khả năng lãnh đạo, tinh thần đồng đội và sự sẵn sàng.

11.5. Sử dụng bằng chứng xác thực

Đối với các mô-đun mật mã đã được kiểm tra hợp lệ, có thể có sẵn bằng chứng từ việc đánh giá hợp lệ mô-đun có thể được sử dụng lại trong kiểm thử xác nhận hoạt động. Tuy nhiên, bằng chứng chi tiết không nhất thiết phải được công bố rộng rãi. Trong một số trường hợp, bằng chứng chi tiết có thể được lấy trực tiếp từ nhà cung cấp.

Nếu không có sẵn bằng chứng chi tiết cần thiết để xác định khả năng áp dụng của nó vào môi trường hoạt động, thì người thử nghiệm phải xác định xem liệu có thể chấp nhận bằng chứng không chi tiết đã công bố hay không.

Nhà cung cấp cũng có thể cung cấp tài liệu khác không được tham chiếu bởi chính sách an toàn của đánh giá hợp lệ. Do đó, nhà cung cấp có thể được yêu cầu cung cấp tài liệu bổ sung hoặc tạo tài liệu bổ sung mới.

11.6. Tài liệu

Có các yêu cầu tài liệu tối thiểu để kiểm thử xác nhận hoạt động trong đó mô tả mô-đun mật mã và môi trường hoạt động cần được cung cấp bởi nhà cung cấp, tổ chức có thẩm quyền kiểm tra hợp lệ và tổ chức:

- Tài liệu hướng dẫn mô tả cài đặt, cấu hình và hoạt động của mô-đun mật mã;
- Tài liệu Chính sách An toàn tuân thủ TCVN 11295:2016 (ISO/IEC 19790: 2012); và

– Tài liệu của tổ chức chỉ định các chức năng an toàn cho các mô-đun mật mã và các yêu cầu an toàn cho môi trường hoạt động.

11.7. Quy trình kiểm thử xác nhận hoạt động

Quy trình kiểm thử xác nhận hoạt động bao gồm sáu bước:

a) Bước 1: Lập kế hoạch kiểm thử xác nhận hoạt động;
b) Bước 2: Chuẩn bị hồ sơ;
c) Bước 3: Chuẩn bị cấu hình và thiết bị kiểm tra;
d) Bước 4: Thực hiện kiểm thử xác nhận hoạt động;
e) Bước 5: Đánh giá kết quả; và
f) Bước 6: Báo cáo kết quả.

12. Các khuyến nghị cho kiểm thử xác nhận hoạt động

12.1. Quy định chung

Tổ chức nên thực hiện kiểm thử xác nhận hoạt động đối với các mô-đun mật mã trong môi trường hoạt động của họ để xác định rằng chúng đáp ứng các yêu cầu an toàn liên quan đến chúng đối với môi trường hoạt động.

Tổ chức tìm kiếm mô-đun mật mã đáp ứng chính sách sử dụng và các yêu cầu an toàn cho môi trường hoạt động của họ. Một tổ chức nên giới hạn việc lựa chọn mô-đun mật mã của họ ở một mô-đun đã được xác nhận bởi tổ chức có thẩm quyền kiểm tra hợp lệ theo TCVN 11295:2016 (ISO/IEC 19790: 2012). Việc xác nhận này cung cấp mức đảm bảo cơ bản về các thuộc tính của mô-đun mật mã. Thông thường, tổ chức có thẩm quyền kiểm tra hợp lệ cung cấp danh sách công khai các mô-đun đó đã được xác nhận bởi tổ chức có thẩm quyền kiểm tra hợp lệ đó. Một tổ chức nên xác định danh sách xác nhận nào được chấp thuận để sử dụng cho việc lựa chọn mô-đun mật mã.

Sau khi tổ chức lựa chọn mô-đun mật mã theo phương pháp quy định tại Điều 10, sao cho các yêu cầu an toàn đối với mô-đun mật mã quy định tại Điều 7 đáp ứng các yêu cầu an toàn đối với môi trường hoạt động quy định tại Điều 9, tổ chức thực hiện kiểm thử xác nhận hoạt động với các mô-đun mật mã đã chọn .

Người thử nghiệm có thể sử dụng bằng chứng của quá trình thử nghiệm trước khi vận hành (dựa trên việc xác nhận) để rút ngắn thời gian thử nghiệm vận hành nếu môi trường vận hành và môi trường tiền vận hành giống nhau.

CHÚ THÍCH: Phụ lục B cung cấp một ví dụ về danh sách kiểm tra hợp nhất các danh sách được đưa ra trong tiêu chuẩn này.

12.2. Các khuyến nghị để đánh giá cài đặt, cấu hình và hoạt động của mô-đun mật mã

12.2.1. Quy định chung

Điều khoản này cung cấp các khuyến nghị để đánh giá rằng các mô-đun mật mã hoặc sự tích hợp của chúng, được cài đặt, cấu hình, khởi động, vận hành và tương tác một cách an toàn và chính xác bằng cách sử dụng kết quả từ thử nghiệm trước khi vận hành. Ngoài ra, nó cung cấp các khuyến nghị để xác nhận rằng các mô-đun mật mã, hoặc sự tích hợp của chúng, tương tác với nhau một cách an toàn và chính xác trong hệ thống an toàn. (ví dụ: hệ thống quản lý khóa như PKI).

Kiểm thử viên cần đánh giá xem liệu các thành phần và giao diện bao gồm các mô-đun mật mã, có thể được cài đặt, cấu hình trong môi trường hoạt động của chúng theo các tài liệu hỗ trợ bao gồm quy trình cài đặt, cấu hình và vận hành hay không.

12.2.2. Đánh giá cài đặt mô-đun mật mã

Điều khoản này cung cấp các khuyến nghị cho kiểm thử viên về cách đánh giá các mô-đun được cài đặt an toàn và chính xác trong môi trường hoạt động cụ thể của chúng.

Yêu cầu an toàn đối với việc lắp đặt mô-đun mật mã được tham chiếu trong TCVN 11295:2016 (ISO/IEC 19790: 2012) 7.11.7.

Kiểm thử viên nên thu thập bằng chứng cần thiết để xác minh cài đặt an toàn, khởi động và tương tác của các mô-đun mật mã trong môi trường hoạt động của chúng.

Ví dụ về bằng chứng:

- Tài liệu quy định các thủ tục cài đặt trong môi trường vận hành;
- Cài đặt hoặc cài đặt lại mô-đun mật mã dựa trên hướng dẫn dành cho quản trị viên;
- Kết quả từ quá trình tự kiểm tra (ví dụ: kiểm tra tính toàn vẹn của phần mềm/phần sụn, v.v.) của mô-đun mật mã trong môi trường hoạt động của nó;
- Kết quả từ việc kiểm tra bằng chứng giả mạo cho mô-đun phần cứng;
- Các tệp nhật ký; và
- Tập tin lỗi, các kịch bản tấn công.

Trong quá trình cài đặt, các kiểm soát kỹ thuật và hoạt động có thể được thực hiện và chuẩn bị cho việc sử dụng các mô-đun mật mã trong môi trường hoạt động của chúng. Có thể có các kiểm soát dành riêng cho địa điểm và các kiểm soát khác cần được kiểm tra như một phần của kiểm thử xác nhận hoạt động để đảm bảo rằng chúng hoạt động chính xác trong môi trường hoạt động.

Vì mục đích chính xác, các biện pháp kiểm soát phải tuân thủ các yêu cầu an toàn đối với các mô-đun mật mã và môi trường hoạt động của chúng và được người quản lý có thẩm quyền cho phép sử dụng.

CHÚ THÍCH: Tham khảo TCVN ISO/IEC 27001:2019 để biết các ví dụ về các biện pháp kiểm soát đối với môi trường hoạt động.

Ví dụ về kiểm soát kỹ thuật:

- Quản lý cấu hình cho các mô-đun mật mã;
- Tạo SSP bên ngoài mô-đun mật mã;
- Cập nhật SSP và truy cập bên ngoài mô-đun mật mã;
- Tạo một tệp để tích hợp các mô-đun mật mã; và
- Thu thập nguồn Entropy từ bên ngoài của mô-đun mật mã.

Ví dụ về kiểm soát hoạt động:

- Báo cáo cấu hình hiện tại; và
- Ứng xử trong trường hợp có lỗi, báo động, chế độ mặc định.

Kiểm thử viên phải đảm bảo rằng tất cả các cài đặt có thể được lặp lại và được xóa một cách chính xác trong môi trường hoạt động.

12.2.3. Đánh giá cấu hình của mô-đun mật mã

Cấu hình mô-đun mật mã thường được thực hiện ban đầu trong quá trình cài đặt. Kiểm thử viên phải đánh giá rằng các quy trình cài đặt an toàn để có được cấu hình an toàn.

Có hai loại cấu hình:

1, Cấu hình của các mô-đun mật mã để cung cấp các dịch vụ an toàn nhằm đảm bảo an toàn cho sứ mệnh mà môi trường hoạt động hỗ trợ; và

2, Cấu hình của hệ thống con hoạt động để tương tác với nhau như các thành phần của môi trường hoạt động.

Người thử nghiệm so sánh cấu hình thực tế với cấu hình dự kiến và phải đảm bảo rằng mô-đun được định cấu hình chính xác và an toàn trong môi trường hoạt động.

Hướng dẫn này mô tả đánh giá rằng các mô-đun được cấu hình trong môi trường hoạt động theo cách đáp ứng tính an toàn mà môi trường hoạt động yêu cầu.

Danh sách sau đây cung cấp các yêu cầu cấu hình thường liên quan đến các mô-đun mật mã:

- Sử dụng các dịch vụ an toàn đã được chấp thuận: TCVN 12211:2018 (ISO / IEC 24759:2017) không đề cập đến việc kiểm tra các dịch vụ an toàn không được chấp thuận mà là kiểm tra các dịch vụ an toàn đã được chấp thuận. Nếu tổ chức sử dụng các dịch vụ an toàn không được chấp thuận, môi trường hoạt động có thể tạo ra rủi ro cho an ninh hoạt động.
- Sử dụng các thuật toán và điểm mạnh của chức năng an toàn đã được chấp thuận.
- Các chức năng an toàn hoạt động và các chức năng an toàn không hoạt động (ví dụ: hoạt động xuống cấp).
- Cấu hình SSP, CSP, PSP. Việc sử dụng khóa và tách khóa được xác định.
- SSP (Khóa, mật khẩu, dữ liệu xác thực, v.v.) được đặt theo giá trị mặc định.
- Kiểm tra cấu hình ghi, truy cập hoặc lưu trữ dữ liệu.
- Cấu hình bộ phận phát hiện xâm nhập, nếu có.

- Cấu hình môi trường hoạt động (kiểm soát truy cập, ngoại tuyến, trực tuyến, v.v.).
- Sử dụng các mô-đun mật mã đã được kiểm tra hợp lệ
- Đảm bảo rằng mô-đun mật mã là phiên bản đã được kiểm tra hợp lệ;
- Biết những gì nên được kết hợp vào mô-đun đã được kiểm tra hợp lệ.

Kiểm thử viên nên xác định xem nhân viên phụ trách về mật mã (quản trị viên của mô-đun mật mã) có biết và hiểu tối thiểu các vấn đề sau không:

a) Tác động của việc cập nhật, loại bỏ hoặc chèn các mô-đun mật mã;

b) Cấu hình của mô-đun mật mã và môi trường hoạt động liên quan đến nó. Ngoài ra, kiểm thử viên nên thu thập bằng chứng để xác minh cấu hình an toàn. Ví dụ về bằng chứng:

- Hồ sơ cài đặt và sửa đổi so với tình trạng hệ thống thực tế;
- Xây dựng lại hệ thống một cách độc lập; và
- Kiểm tra tính nhất quán.

Người thử nghiệm phải đảm bảo rằng tất cả các quy trình cấu hình có thể được lặp lại trong môi trường hoạt động.

12.2.4. Đánh giá hoạt động chính xác của mô-đun mật mã

Điều này mô tả việc đánh giá rằng các mô-đun được vận hành trong môi trường hoạt động của chúng để đáp ứng các yêu cầu an toàn được chỉ định cho môi trường hoạt động. Kiểm thử viên vận hành nên sử dụng dữ liệu thử nghiệm (dữ liệu mẫu) thay vì dữ liệu thực trong khi kiểm thử xác nhận hoạt động.

Kiểm thử viên phải đánh giá rằng các chức năng bình thường bao gồm cài đặt và cấu hình hoạt động một cách an toàn và chính xác (ví dụ: chế độ bỏ qua).

Sau đây là các mục kiểm thử xác nhận hoạt động liên quan đến mô-đun mật mã và cần được đánh giá:

- Nhập các giá trị mẫu đầu vào cho mô-đun trong môi trường hoạt động. Tập hợp các giá trị mẫu đầu vào phải được xác định là phù hợp với mục đích của kiểm thử xác nhận hoạt động (ví dụ: trường hợp sử dụng của mô-đun mật mã);
- Các chức năng an toàn đã được chấp thuận hoặc các chức năng an toàn không được chấp thuận được thực hiện như dự kiến trong quá trình hoạt động của mô-đun mật mã;
- Các mô-đun mật mã đã được kiểm tra hợp lệ hoặc không hợp lệ được sử dụng như dự kiến trong môi trường hoạt động;
- Khả năng tương tác chính xác của mô-đun với hệ thống quản lý khóa (ví dụ: PKI)
- Khả năng tương tác chính xác của mô-đun với các hệ thống và thiết bị an toàn khác;
- Hoạt động trái phép cho mô-đun mật mã chưa xảy ra;
- Các mô-đun mật mã đang thực hiện các chức năng của chúng một cách an toàn trong quá trình hoạt động.

12.3. Các khuyến nghị để kiểm tra một hệ thống quản lý chính

Điều khoản này đưa ra các khuyến nghị để kiểm tra các yêu cầu an toàn đối với hệ thống quản lý khóa và kiểm tra xem các mô-đun mật mã có đáp ứng các yêu cầu an toàn cho hệ thống đó hay không.

Kiểm thử viên nên kiểm tra các chính sách an toàn cho hệ thống quản lý khóa, loại SSP được quản lý trong hệ thống quản lý khóa và các giao diện trong đó hệ thống quản lý khóa và mô-đun mật mã tương tác với nhau.

Ví dụ về các chính sách an toàn cho hệ thống quản lý khóa:

- Kích thước khóa, tạo khóa, bảo vệ khóa (lưu trữ, xóa trắng, khôi phục);
- Các chức năng an toàn đã được chấp thuận;
- Phương pháp phân phối cho các SSP;
- Phương thức thỏa thuận cho các SSP;
- Phương pháp xác thực cho khóa công khai.

Kiểm thử viên nên kiểm tra các chức năng an toàn sử dụng SSP trong hệ thống quản lý khóa. Ví dụ về các chức năng an toàn trong hệ thống quản lý khóa:

- Các chức năng an toàn đã được chấp thuận và không được chấp thuận trong hệ thống quản lý khóa;
- Các chức năng và giao diện an toàn mà hệ thống quản lý khóa và mô-đun mật mã tương tác với nhau;
- Tạo SSP trong hệ thống quản lý khóa;
- Thiết lập SSP trong hệ thống quản lý chính;
- Xác thực PSP trong hệ thống quản lý khóa;
- Thu hồi SSP trong hệ thống quản lý khóa;
- Phá hủy SSP trong hệ thống quản lý khóa (ví dụ: xóa trắng);
- Nguồn entropy RBG; nguồn entropy được nhập từ hệ thống quản lý khóa vào mô-đun mật mã hay được trích xuất từ mô-đun mật mã.

Kiểm thử viên nên kiểm tra các chức năng an toàn sử dụng SSP trong mô-đun mật mã. Ví dụ về các chức năng trong mô-đun mật mã:

- Tạo SSP;
- Cơ sở SSP:

  + vận chuyển SSP tự động hoặc thỏa thuận SSP;

  + nhập hoặc xuất SSP thủ công qua trực tiếp hoặc điện tử;

- Đầu vào và đầu ra SSP;
- Lưu trữ SSP;
- Số hóa SSP.

Kiểm thử viên phải đảm bảo rằng các giao diện cho mục nhập và đầu ra SSP giữa mô-đun mật mã và hệ thống quản lý khóa là chính xác.

Kiểm thử viên phải đảm bảo rằng khả năng tương tác giữa hệ thống quản lý khóa và mô-đun mật mã về SSP là chính xác.

12.4. Khuyến nghị để kiểm tra các yêu cầu an toàn của thông tin xác thực

Điều khoản này đưa ra các khuyến nghị để hỗ trợ việc kiểm tra xem các mô-đun mật mã có đáp ứng các yêu cầu an toàn được chỉ định cho thông tin xác thực hay không.

Kiểm thử viên nên kiểm tra thông tin xác thực được sử dụng trong môi trường hoạt động và phương pháp bảo vệ chống lại thông tin xác thực.

Ví dụ về thông tin xác thực:

- Cặp khóa công khai / khóa bí mật;
- Chứng chỉ do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp;
- Thông tin liên quan đến tổ chức cung cấp dịch vụ chứng thực chữ ký số;
- Mật khẩu;
- Thông tin xác thực cá nhân.

Nếu mô-đun mật mã phát hành thông tin xác thực hoặc được sử dụng để bảo vệ thông tin xác thực, thì mô-đun mật mã phải đáp ứng bất kỳ yêu cầu an toàn nào.

Ví dụ về các yêu cầu an toàn đối với thông tin xác thực:

- Cặp khóa công khai / khóa bí mật: Khóa cá nhân của người dùng cần được bảo vệ và phải được lưu trữ an toàn theo mức an toàn của mô-đun mật mã. Người dùng nên sử dụng khóa công khai sau khi nó đã được xác thực;
- Lưu trữ, mặc định, xóa khóa, khôi phục, số lần thử được phép.

12.5. Các khuyến nghị để đánh giá tính khả dụng của các mô-đun mật mã

Điều khoản này cung cấp các khuyến nghị để đánh giá tính khả dụng của các mô-đun mật mã trong môi trường hoạt động của chúng và kiểm tra xem các mô-đun mật mã có đáp ứng các yêu cầu về hiệu suất cho nó hay không. Các chế độ lỗi cũng nên được xem xét.

Tính khả dụng của các dịch vụ an toàn được cung cấp bởi mô-đun mật mã phải được duy trì trong quá trình hoạt động.

Hiệu suất của mô-đun mật mã có thể ảnh hưởng đến tính khả dụng của các dịch vụ an toàn. Ví dụ về hiệu suất cho mô-đun mật mã:

- Thời gian hoạt động hoặc độ trễ cho mô-đun mật mã;
- Kích thước dữ liệu mà mô-đun mật mã có thể cung cấp cho các dịch vụ an toàn; và
- Số lượng người dùng mà mô-đun mật mã có thể hỗ trợ.

12.6. Các khuyến nghị để xác định các lỗ hổng tiềm ẩn bị bỏ sót của các mô-đun mật mã

Điều khoản này cung cấp các khuyến nghị để xác định các lỗ hổng tiềm ẩn bị bỏ sót cho các mô-đun mật mã, sự tích hợp của chúng hoặc các hệ thống liên quan đến các mô-đun mật mã. Các kết quả từ thử nghiệm trước khi vận hành có thể được sử dụng nếu chúng có sẵn. Tiêu chuẩn này chỉ xem xét các lỗ hổng tiềm ẩn bị bỏ sót áp dụng cho các mô-đun mật mã.

Mục đích của việc xác định các lỗ hổng tiềm ẩn bị bỏ sót là để xác định xem liệu các mô-đun mật mã có xuất hiện các lỗ hổng có thể bị kẻ tấn công khai thác hay không. Mô-đun mật mã có thể có các lỗ hổng không được phát hiện trong quá trình xác thực hoặc được phát hiện sau đó.

TCVN 11295:2016 (ISO/IEC 19790: 2012) bao gồm các thông số kỹ thuật để giảm thiểu một số cuộc tấn công. Khi các mức an toàn được xác định bởi TCVN 11295:2016 (ISO/IEC 19790: 2012) tăng lên, giả định về các nguồn lực sẵn có cho những kẻ tấn công cũng tăng lên. Các lỗ hổng theo TCVN 11295:2016 (ISO/IEC 19790: 2012) bao gồm:

- giả mạo;
- Các cuộc tấn công kênh kề;
- Các cuộc tấn công vật lý, bao gồm cả việc thao túng các điều kiện môi trường;
- Truy cập trái phép;
- Các thuật toán mật mã được triển khai không chính xác và các chức năng mật mã (chẳng hạn như tạo bit ngẫu nhiên); và
- Nguồn entropy yếu.

CHÚ THÍCH: Nhà cung cấp có cơ hội mô tả bất kỳ cuộc tấn công nào được giảm thiểu trong phần "Giảm thiểu các cuộc tấn công khác" của tài liệu Chính sách An toàn tuân thủ theo TCVN 11295:2016 (ISO/IEC 19790: 2012).

Những điều này được mô tả chi tiết hơn trong 9.2.

Việc xác định các lỗ hổng tiềm ẩn bị bỏ sót được thực hiện bằng cách kiểm tra các lỗ hổng phổ biến được tìm thấy trong các môi trường hoạt động tương tự, tìm kiếm các lỗ hổng được biết đến công khai liên quan đến mô-đun mật mã và nếu nhà cung cấp cung cấp thông tin không công khai, điều tra bất kỳ lỗ hổng tiềm ẩn nào được xác định trong quá trình phát triển và xác thực.

Việc phân tích rủi ro của tổ chức nên đã xác định được đặc điểm tấn công giả định. Quá trình phân tích tính dễ bị tổn thương được mô tả trong TCVN 8709-3:2011(ISO/IEC 15408-3:2008) và trong TCVN 11386:2016 (ISO/IEC 18045:2008) ở lớp AVA. ISO / IEC TR 20004 cung cấp thêm thông tin mà người thử nghiệm vận hành có thể sử dụng.

Nếu các mô-đun riêng biệt được tích hợp trong một môi trường hoạt động, thì việc tích hợp có thể tạo ra các lỗ hổng an toàn mà mỗi mô-đun riêng biệt không có. Các kỹ thuật tích hợp hoặc thành phần thường được phân loại thành Phân lớp, Mạng và Thành phần như được mô tả trong Hình 4.

Khi bất kỳ lỗ hổng tiềm ẩn nào đã được xác định, chúng phải được đánh giá trong bối cảnh với đánh giá rủi ro của tổ chức và đưa ra quyết định về việc giảm thiểu chúng và liệu rủi ro tồn đọng có thể được chấp nhận hay không.

Tổ chức có thể yêu cầu kiểm tra thâm nhập dựa trên các lỗ hổng tiềm ẩn đã được xác định và bất kỳ giả thuyết lỗ hổng nào được phát triển trong quá trình phân tích, để xác định khả năng khai thác của chúng trong môi trường của tổ chức.

Khi các lỗ hổng được xác định, thì kiểm thử viên có thể cần xác định xem có bất kỳ bản vá hoặc bản cập nhật nào có sẵn và cần được cài đặt để giảm thiểu những lỗ hổng này hay không.

12.7. Kiểm tra các chính sách an toàn của tổ chức

Điều khoản này chứa danh sách kiểm tra cho chính sách an toàn của tổ chức. (ví dụ: chính sách thuật toán mật mã, hướng dẫn và quy định an toàn, yêu cầu của người quản lý an toàn, mức an toàn cho từng lĩnh vực trong số 11 lĩnh vực yêu cầu, độ mạnh của các chức năng an toàn, v.v.) Danh sách kiểm tra bao gồm các mục để kiểm tra xem mô-đun mật mã có đáp ứng các chính sách an toàn của tổ chức hay không .Sau đây là các ví dụ về các chính sách an toàn do tổ chức chỉ định:

- Tham chiếu đến 10.2;
- Chính sách thuật toán mật mã;
- Hướng dẫn và quy định an ninh; các chính sách quản lý, quy tắc và thủ tục chi phối hoạt động của hệ thống hoạt động; các yêu cầu và quy tắc tương tác với các hệ thống hoạt động được an toàn và không an toàn khác;
- Yêu cầu quản lý an ninh;
- Mức an toàn cho từng lĩnh vực trong số 11 lĩnh vực yêu cầu;
- Độ mạnh của chức năng an toàn;
- Dịch vụ bảo vệ được chấp thuận hoặc không được chấp thuận;
- Các chức năng an toàn được chấp thuận hoặc không được chấp thuận;
- Phương thức hoạt động được chấp thuận hoặc không được chấp thuận;
- Mô-đun mật mã hợp lệ hoặc không hợp lệ;
- Quy trình bảo trì, quản lý và loại bỏ mô-đun
- Chính sách giám sát bằng chứng giả mạo các mô-đun mật mã;
- Chính sách kiểm tra tệp nhật ký để theo dõi một cuộc tấn công; và
- Thủ tục quản lý khóa.

Sau đây là các ví dụ về chính sách an toàn cho các mô-đun mật mã:

- Tham chiếu đến 7.7;
- Sử dụng mô-đun mật mã đã được kiểm tra hợp lệ hoặc mô-đun mật mã không hợp lệ;
- Chế độ hoạt động để phát triển/thử nghiệm được tách biệt với chế độ hoạt động bình thường.

13. Báo cáo kết quả kiểm thử xác nhận hoạt động

Điều quan trọng là phải báo cáo kết quả kiểm thử xác nhận hoạt động vì chúng có thể được sử dụng trong quá trình để cho phép triển khai mô-đun mật mã trong môi trường của tổ chức.

Sau đây là những nội dung tối thiểu của báo cáo thử nghiệm vận hành:

- Phạm vi kiểm thử xác nhận hoạt động;
- Phiên bản tài liệu khuyến nghị;
- Gia hạn khuyến nghị;
- Phương pháp được sử dụng để kiểm tra mô-đun trong môi trường hoạt động;
- Kết quả được đánh giá và ghi lại như thế nào;
- Môi trường hoạt động mà kiểm thử hoạt động tập trung vào;
- Thời gian kiểm thử xác nhận hoạt động;
- Những phát hiện và quan sát; và
- Hành động và khuyến nghị khi kết quả không đáp ứng các yêu cầu của môi trường hoạt động.

Phụ lục A

(Tham khảo)

Ví dụ về danh sách mô-đun mật mã đã được xác thực

A.1 Quy định chung

Sau khi một mô-đun được kiểm tra hợp lệ bởi tổ chức có thẩm quyền kiểm tra hợp lệ, tổ chức có thẩm quyền kiểm tra hợp lệ có thể cung cấp danh sách công khai xác định các mô-đun đó cùng với chính sách an toàn của mô-đun và thông tin có liên quan khác. Điều khoản A.2 cung cấp các tham chiếu đến một vài trong số các danh sách có sẵn công khai này.

A.2 Các mô-đun mật mã đã được kiểm tra hợp lệ

Danh sách các mô-đun mật mã đã được kiểm tra hợp lệ bởi NIST: Cryptographic Module Validation Program (CMVP): https://csrc.nist.gov/groups/STM/cmvp/validation.html

Danh sách các mô-đun mật mã đã được kiểm tra hợp lệ bởi Japan Cryptographic Module Validation Program (JCMVP): https://www.ipa.go.jp/security/jcmvp/jcmvp_e/val.html

Danh sách các mô-đun mật mã đã được kiểm tra hợp lệ bởi Korea Cryptographic Module Validation Program (KCMVP): http://www.nis.go.kr/AF/1_7_3_3/list.do

Phụ lục B

(Tham khảo)

Danh sách kiểm tra để kiểm thử xác nhận hoạt động của các mô-đun mật mã

B.1 Danh sách kiểm tra để kiểm thử xác nhận hoạt động

Điều khoản này mô tả danh sách kiểm tra để kiểm thử xác nhận hoạt động để giúp kiểm thử viên. Danh sách kiểm tra này có nguồn gốc từ các Điều 7, 9 và 12.

Chính sách sử dụng	Mô-đun mật mã	Xác định dữ liệu (tài sản) cần được bảo vệ bằng mật mã
		Xác định dữ liệu (tài sản) không cần bảo vệ bằng mật mã
		Giá trị của dữ liệu (tài sản) cần được bảo vệ
		Mức an toàn nào trong TCVN 11295:2016 (ISO/IEC 19790: 2012) là cần thiết để bảo vệ dữ liệu
		Chính sách thuật toán mật mã
		Chính sách giao thức an toàn
		Các chính sách giám sát khả năng chống giả mạo của các mô-đun mật mã
		Các chính sách kiểm tra tệp nhật ký để theo dõi một cuộc tấn công
	Khả năng tương tác của các mô-đun mật mã khác nhau	Giao diện phần cứng / phần mềm
		Giao diện lập trình ứng dụng (API)
		Các giao thức được sử dụng để quản lý khóa
		Khả năng tương tác của hệ thống quản lý khóa
		Khả năng tương tác của thông tin xác thực ở cấp hệ thống
Yêu cầu an toàn đối với ứng dụng	Hướng dẫn và quy định an toàn; các chính sách quản lý, quy tắc và thủ tục chi phối hoạt động của hệ thống hoạt động; các yêu cầu và quy tắc tương tác với các hệ thống hoạt động được an toàn và không an toàn khác	

hoặc môi trường hoạt động	Mức an toàn cho từng lĩnh vực trong số mười một lĩnh vực yêu cầu an toàn trong TCVN 11295:2016 (ISO/IEC 19790: 2012) theo 9.2
	Yêu cầu của người quản lý an toàn
	Yêu cầu về độ mạnh chức năng an toàn
	Dịch vụ an ninh
	Nguồn Entropy được thu thập trong môi trường hoạt động
	Cơ chế kiểm toán được thực hiện trong môi trường hoạt động
	Khối/chức năng không thể nhân bản/sao chép vật lý được hỗ trợ trong môi trường hoạt động
	Quy trình bảo trì, quản lý và loại bỏ mô-đun
	Chức năng an toàn được chấp thuận hoặc chức năng an toàn không được chấp thuận
	Chế độ hoạt động đã được chấp thuận hoặc chế độ hoạt động không được chấp thuận
	Mô-đun mật mã đã hợp lệ hoặc mô-đun mật mã không hợp lệ
	Quy trình quản lý chính
Yêu cầu an toàn cho các mô-đun mật mã	Xem 7.7
	Mô-đun mật mã đã được kiểm tra hợp lệ hoặc mô-đun mật mã không hợp lệ
	Chế độ hoạt động phát triển / thử nghiệm được tách biệt với chế độ hoạt động bình thường
Lựa chọn mô-đun mật mã	Tìm kiếm mô-đun mật mã đáp ứng chính sách sử dụng và các yêu cầu an toàn cho môi trường hoạt động
	Chọn mô-đun mật mã cho một mô-đun đã được xác nhận bởi tổ chức có thẩm quyền kiểm tra hợp lệ theo TCVN 11295:2016 (ISO/IEC 19790: 2012)
Cài đặt	Kiểm tra xem các thành phần và giao diện bao gồm các mô-đun mật mã có thể được cài đặt, khởi động, cấu hình và tương tác trong môi trường hoạt động của chúng có tuân theo theo các tài liệu quy định các quy trình cài đặt hay

	không Đảm bảo rằng tất cả các cài đặt có thể được lặp lại và được xóa một cách chính xác trong môi trường hoạt động
	Kiểm tra kết quả từ quá trình tự kiểm tra (ví dụ: kiểm tra tính toàn vẹn của phần mềm / phần sụn, v.v.) của mô-đun mật mã trong môi trường hoạt động của nó, kết quả từ việc kiểm tra bằng chứng giả mạo cho mô-đun phần cứng, tệp nhật ký và tệp chèn lỗi, các tình huống tấn công
	Xác minh các kiểm soát kỹ thuật và hoạt động có thể được thực hiện và chuẩn bị cho việc sử dụng các mô-đun mật mã trong môi trường hoạt động của chúng
Cấu hình	So sánh cấu hình thực tế với cấu hình dự kiến và đảm bảo rằng mô-đun được định cấu hình chính xác và an toàn trong môi trường hoạt động
	Kiểm tra việc sử dụng các dịch vụ an toàn đã được chấp thuận TCVN 12211:2018 (ISO/IEC 24759:2017) không đề cập đến việc kiểm tra các dịch vụ an toàn không được chấp thuận mà là kiểm tra mức an toàn đã được chấp thuận. Nếu người dùng sử dụng các dịch vụ an toàn không được chấp thuận, môi trường hoạt động có thể tạo ra rủi ro đối với an toàn hoạt động.
	Kiểm tra việc sử dụng các thuật toán và điểm mạnh của chức năng an toàn đã được chấp thuận
	Kiểm tra các chức năng an toàn có sẵn và cấu hình các chức năng an toàn không khả dụng
	Kiểm tra cấu hình SSP, CSP, PSP
	Cấu hình bộ phận phát hiện xâm nhập, nếu có
	Kiểm tra các SSP (khóa, mật khẩu, dữ liệu xác thực, v.v.) được đặt theo giá trị mặc định, nếu có
	Kiểm tra cấu hình lưu trữ, truy cập hoặc ghi dữ liệu kiểm tra
	Kiểm tra việc sử dụng các mô-đun mật mã đã được kiểm tra hợp lệ: - Nếu nhiều mô-đun mật mã được tích hợp với các mô-đun mật mã đã được kiểm tra hợp lệ thực hiện các chức năng an toàn và các mô-đun mật mã không hợp lệ thực hiện các chức năng an toàn (ví dụ: thiết lập khóa), chúng là những

	mô-đun không hợp lệ - Mặc dù mô-đun mật mã chứa chức năng an toàn đã được chấp thuận, nhưng mô-đun mật mã trong mỗi môi trường hoạt động có thể không hợp lệ bởi tổ chức có thẩm quyền kiểm tra hợp lệ hoặc do nhà cung cấp chỉ định như đã nêu trong chính sách an toàn của mô-đun đã hợp lệ
	Kiểm tra cấu hình môi trường hoạt động (kiểm soát truy cập, ngoại tuyến, trực tuyến, v.v.)
	Kiểm tra xem các mô-đun mật mã hợp lệ bởi tổ chức có thẩm quyền kiểm tra hợp lệ có phải là phiên bản đã hợp lệ hay không
	Kiểm tra cấu hình đó giúp quản trị viên biết tác động của việc cập nhật, loại bỏ và chèn các mô-đun mật mã
	Kiểm tra xem cấu hình của mô-đun mật mã và môi trường hoạt động liên quan đến nó phải được biết và hiểu trong quá trình vận hành nó
Hoạt động	Nhập giá trị đầu vào cho mô-đun trong môi trường hoạt động và kiểm tra xem nó hoạt động theo cách chính xác và an toàn
	Sử dụng dữ liệu thử nghiệm (dữ liệu mẫu) thay vì dữ liệu thực trong khi kiểm thử xác nhận hoạt động
	Kiểm tra xem các chế độ hoạt động đã được chấp thuận hoặc các chế độ hoạt động không được chấp thuận có đang tiến hành chính xác trong quá trình hoạt động của mô-đun mật mã hay không
	Kiểm tra xem các chức năng an toàn đã được chấp thuận hoặc các chức năng an toàn không được chấp thuận có đang hoạt động chính xác trong quá trình hoạt động của mô-đun mật mã hay không
	Kiểm tra xem các mô-đun mật mã đã hợp lệ hay các mô-đun mật mã không hợp lệ đang hoạt động hay không
	Kiểm tra xem khả năng tương tác của mô-đun với hệ thống quản lý khóa (ví dụ: PKI) có đúng không
	Kiểm tra xem khả năng tương tác của mô-đun với các hệ thống và thiết bị an toàn khác có đúng không
	Kiểm tra rằng hoạt động trái phép cho mô-đun mật mã đã không xảy ra

	Kiểm tra để đảm bảo rằng các trạng thái an toàn sẽ được phục hồi từ các trạng thái không an toàn trong thời gian cần thiết
Hệ thống quản lý chính	Kiểm tra xem các mô-đun mật mã có đáp ứng các yêu cầu an toàn đối với hệ thống quản lý khóa nếu có
	Giải quyết các chính sách an toàn cho hệ thống quản lý khóa, loại SSP được sử dụng trong hệ thống quản lý khóa và các giao diện mà hệ thống quản lý khóa và mô-đun mật mã tương tác với nhau
	Xác định các chức năng an toàn được thực hiện cho các SSP trong hệ thống quản lý khóa
	Giải quyết các chức năng an toàn mà mô-đun mật mã cần trong số các chức năng an toàn được thực hiện cho các SSP trong hệ thống quản lý khóa
	Kiểm tra xem các giao diện cho đầu vào và đầu ra SSP giữa mô-đun mật mã và hệ thống quản lý khóa có đúng không
	Kiểm tra xem khả năng tương tác giữa hệ thống quản lý khóa và mô-đun mật mã về SSP có chính xác không
Thông tin xác thực	Kiểm tra xem các mô-đun mật mã có đáp ứng các yêu cầu an toàn đối với thông tin xác thực nếu có
	Xác định thông tin xác thực được sử dụng trong môi trường hoạt động
	Xác định phương pháp để bảo vệ chống lại thông tin xác thực Mô-đun mật mã có thể cấp thông tin xác thực hoặc được sử dụng để bảo vệ thông tin xác thực
Tính sẵn sàng	Tính sẵn có của các dịch vụ an toàn được cung cấp bởi mô-đun mật mã phải được duy trì trong quá trình hoạt động
	Thời gian chờ hoạt động cho mô-đun mật mã
	Kích thước dữ liệu mà mô-đun mật mã có thể cung cấp cho các dịch vụ an toàn
	Số lượng người dùng mà mô-đun mật mã có thể hỗ trợ
Lỗ hổng bị bỏ	Xác định xem liệu các lỗ hổng tiềm ẩn bị bỏ sót được tính hoặc bị ảnh hưởng bởi các mô-đun mật mã đại diện cho các lỗ hổng thực tế có thể bị kẻ tấn công

sót	khai thác hay không
	Kiểm tra và phân tích các lỗ hổng phổ biến được tìm thấy trong các môi trường hoạt động tương tự
	Điều tra các lỗ hổng tiềm ẩn được xác định trong quá trình phát triển và xác thực
	Điều tra các lỗ hổng tiềm ẩn được xác định sau khi xác thực: - Thâm nhập trái phép - Các cuộc tấn công kênh kề - Các cuộc tấn công vật lý, bao gồm cả việc thao túng các điều kiện môi trường - Truy cập trái phép - Các thuật toán mật mã được triển khai không chính xác
	Xác định các lỗ hổng tiềm ẩn bị bỏ sót cho các mô-đun mật mã, sự tích hợp của chúng hoặc các hệ thống liên quan đến các mô-đun mật mã

B.2 Quy trình kiểm thử xác nhận hoạt động

Điều khoản này mô tả chi tiết hơn các bước của quy trình kiểm thử xác nhận hoạt động để giúp kiểm thử viên. Xem thêm 11.7.

a) Lập kế hoạch cho kiểm thử xác nhận hoạt động:
   1. Chỉ định kiểm thử viên;
   2. Xác định và cung cấp các nguồn lực.

b) Chuẩn bị tài liệu:
   1. Xác định các yêu cầu an toàn đối với môi trường hoạt động;
   2. Xác định các yêu cầu an toàn cho các mô-đun mật mã;
   3. Lựa chọn các ứng viên mô-đun mật mã từ danh sách được tổ chức có thẩm quyền kiểm tra hợp lệ xuất bản bằng cách so sánh các yêu cầu an toàn.

c) Thực hiện kiểm thử xác nhận hoạt động:
   1. Chuẩn bị cấu hình và thiết bị kiểm tra;
   2. Kiểm tra hệ thống quản lý chính;
   3. Kiểm tra thông tin xác thực;
   4. Đánh giá tính khả dụng;
   5. Đánh giá cài đặt;
   6. Đánh giá cấu hình;
   7. Đánh giá hoạt động;
   8. Xác định các lỗ hổng bị bỏ sót;
   9. Kiểm tra các chính sách an toàn.

d) Đánh giá kết quả.

e) Báo cáo kết quả

Tài liệu tham khảo

[1] TCVN 8709-3:2011 (ISO/IEC 15408-3:2008) về Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 3: Các thành phần đảm bảo an toàn

[2] TCVN ISO/IEC 17024:2012 (ISO/IEC 17024:2012) về Đánh giá sự phù hợp - Yêu cầu chung đối với tổ chức chứng nhận năng lực cá nhân.

[3] TCVN 12212:2018 (ISO/IEC 17825:2016) về Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp kiểm thử giảm thiểu các lớp tấn công không xâm lấn chống lại các mô-đun mật mã.

[4] TCVN 11386:2016 (ISO/IEC 18045:2008) về Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp đánh giá an toàn công nghệ thông tin.

[5] ISO/IEC/TR 20004, Information technology — Security techniques — Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045.

[6] ISO/IEC 20085-1, Test tool requirements and test tool calibration methods for use in testing non-invasive attach mitigation techniques in cryptographic modules — Part1: Test tools and techniques.

[7] ISO/IEC 20085-2, Test tool requirements and test tool calibration methods for use in testing noninvasive attach mitigation techniques in cryptographic modules — Part 2: Test calibration methods and apparatus.

[8] TCVN 13721:2023, Công nghệ thông tin – Các kỹ thuật an toàn Phương pháp kiểm thử và phân tích cho các bộ tạo bit ngẫu nhiên trong TCVN 11295 (ISO/IEC 19790) và TCVN 8709 (ISO/IEC 15408).

[9] ISO/IEC 20897, Information technology — Security techniques — Security requirements, test and evaluation methods for physically unclonable functions for generating non-stored security parameters.

[10] TCVN ISO/IEC 27002:2020 (ISO/IEC 27002:2013) về Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành quản lý an toàn thông tin.

[11] National Institute of Standards and Technology. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, August 01, 2016 (latest dated version as of this document's publication).