TCVN TIÊU CHUẨN QUỐC GIA

TCVN 13723-2:2023
ISO/IEC 19896-2:2018
Xuất bản lần 1

KỸ THUẬT AN TOÀN CÔNG NGHỆ THÔNG TIN – YÊU CẦU VỀ NĂNG LỰC ĐỐI VỚI KIỂM THỬ VIÊN VÀ ĐÁNH GIÁ VIÊN BẢO MẬT THÔNG TIN – PHẦN 2: YÊU CẦU VỀ KIẾN THỨC, KỸ NĂNG VÀ TÍNH HIỆU QUẢ ĐỐI VỚI KIỂM THỬ VIÊN THEO TCVN 11295 (ISO/IEC 19790)

IT security techniques — Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers

HÀ NỘI – 2023

Mục lục

Lời nói đầu

TCVN 13723-2:2023 hoàn toàn tương đương với ISO/IEC 19896-2:2018.

TCVN 13723-2:2023 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.

Bộ tiêu chuẩn TCVN 13723, Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với Kiểm thử viên và Đánh giá viên bảo mật thông tin, gồm 3 phần:

- TCVN 13723-1, Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với Kiểm thử viên và Đánh giá viên bảo mật thông tin – Phần 1: Giới thiệu, khái niệm và yêu cầu chung.
- TCVN 13723-2, Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với Kiểm thử viên và Đánh giá viên bảo mật thông tin – Phần 2: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với Kiểm thử viên theo TCVN 11295 (ISO/IEC 19790).
- TCVN 13723-3, Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với Kiểm thử viên và Đánh giá viên bảo mật thông tin – Phần 3: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với Đánh giá viên theo TCVN 8709 (ISO/IEC 15408).

Giới thiệu

Tiêu chuẩn này cung cấp các yêu cầu về chuyên ngành để chứng minh cho các yêu cầu về kiến thức, kỹ năng và hiệu quả của các cá nhân trong việc thực hiện các dự án kiểm thử an toàn phù hợp với các tiêu chuẩn TCVN 11295:2016 (ISO/IEC 19790:2012) và TCVN 12211:2018 (ISO/IEC 24759). TCVN 11295:2016 (ISO/IEC 19790:2012) cung cấp chi tiết các yêu cầu an toàn đối với mô-đun mật mã. Nhiều chứng nhận, kế hoạch xác nhận và các thỏa thuận công nhận đã được phát triển sử dụng nó làm cơ sở. TCVN 11295:2016 (ISO/IEC 19790:2012) cho phép so sánh giữa các kết quả của các dự án kiểm thử an toàn độc lập. TCVN 12211:2018 (ISO/IEC 24759:2017) hỗ trợ điều này bằng cách cung cấp một tập hợp các yêu cầu kiểm thử chung để kiểm thử mô-đun mật mã để phù hợp với TCVN 11295:2016 (ISO/IEC 19790:2012).

Một yếu tố quan trọng trong việc đảm bảo khả năng so sánh các kết quả của các phê duyệt hoặc chứng nhận đó là các yêu cầu về kiến thức, kỹ năng và hiệu quả của từng Kiểm thử viên chịu trách nhiệm thực hiện các dự án kiểm thử.

TCVN ISO/IEC 17025:2017 (ISO/IEC 17025:2017), thường được quy định các cơ sở thử nghiệm tuân theo tiêu chuẩn, trong điều khoản 5.2.1 nêu rõ rằng "Tất cả nhân sự của phòng thử nghiệm, cả nội bộ hoặc bên ngoài, có thể ảnh hưởng đến hoạt động thử nghiệm đều phải có năng lực, hành động một cách khách quan và thực hiện công việc đúng theo hệ thông quản lý của phòng thử nghiệm".

Đối tượng của tiêu chuẩn này bao gồm: các cơ quan có thẩm quyền phê duyệt và chứng nhận, các tổ chức công nhận phòng thử nghiệm, các kế hoạch theo từng dự án, cơ sở thử nghiệm, Kiểm thử viên và các tổ chức cung cấp chứng chỉ nghề nghiệp và tổ chức thừa nhận.

Tiêu chuẩn này thiết lập cơ sở cho các yêu cầu về kiến thức, kỹ năng và hiệu quả của Kiểm thử viên khi áp dụng theo TCVN 11295:2016 (ISO/IEC 19790:2012), với mục tiêu thiết lập sự phù hợp trong các yêu cầu đào tạo chuyên gia kiểm thử khi áp dụng theo TCVN 11295:2016 (ISO/IEC 19790:2012) liên quan đến các chương trình kiểm thử sự phù hợp của mô-đun mật mã.

Phụ lục D minh họa việc sử dụng tiêu chuẩn này bởi những người phê duyệt trong một chương trình xác nhận.

TIÊU CHUẨN QUỐC GIA TCVN 13723-2:2023

Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với Kiểm thử viên và Đánh giá viên bảo mật thông tin – Phần 2: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với Kiểm thử viên theo TCVN 11295 (ISO/IEC 19790)

IT security techniques – Competence requirements for information security testers and evaluators – Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers

1 Phạm vi áp dụng

Tiêu chuẩn này cung cấp các yêu cầu tối thiểu về kiến thức, kỹ năng và yêu cầu về tính hiệu quả của các cá nhân thực hiện các hoạt động đánh giá sự phù hợp theo TCVN 11295:2016 (ISO/IEC 19790:2012) và TCVN 12211:2018 (ISO/IEC 24759:2017).

2 Tài liệu viện dẫn

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

- TCVN ISO/IEC 17025:2017 (ISO/IEC 17025:2017), Yêu cầu chung về năng lực của các phòng thử nghiệm và hiệu chuẩn.
- TCVN 12212:2018 (ISO/IEC 17825:2016), 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.
- TCVN 12211:2018 (ISO/IEC 24759:2017), Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu kiểm thử cho mô-đun mật mã.
- 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 13723-1:2023 (ISO/IEC 19896-1), Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với Kiểm thử viên và Đánh giá viên bảo mật thông tin – Phần 1: Giới thiệu, khái niệm và yêu cầu chung.
- ISO/IEC 18367, Information technology – Security techniques – Cryptographic algorithms and security mechanisms conformance testing.
- ISO/IEC 20085-1, Information technology – Security techniques – Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules – Part 1: Test tools and techniques.
- ISO/IEC 20085-2, Information technology – Security techniques – Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules - Part: 2 Test calibration methods and apparatus.
- ISO/IEC 20543, Information technology – Security techniques – Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408.

3 Các thuật ngữ viết tắt

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

HDD	Hard Disk Drive	Ổ đĩa cứng
RSA	Rivest-Shamir-Adleman	Thuật toán mã hóa RSA
SSD	Solid State Drive	Ổ đĩa bán dẫn
SHA	Secure Hash Algorithm	Secure Hash Algorithm
AES	Advanced Encryption Standard	Advanced Encryption Standard

4 Nội dung của tiêu chuẩn

Tiêu chuẩn này được chia thành các điều khoản sau: Kiến thức (Điều 5), Kỹ năng (Điều 6), Kinh nghiệm (Điều 7), Trình độ đào tạo (Điều 8) và Tính hiệu quả (Điều 9). Mỗi điều khoản tương ứng với một khía cạnh về các yêu cầu về kiến thức, kỹ năng, kinh nghiệm, đào tạo và yêu cầu hiệu quả của các cá nhân thực hiện các hoạt động kiểm thử như được giới thiệu trong TCVN 13723-1:2023 (ISO/IEC 19896-1) với phương án áp dụng phù hợp theo TCVN 11295:2016 (ISO/IEC 19790:2012) và TCVN 12211:2018 (ISO/IEC 24759:2017).

5 Kiến thức

5.1 Yêu cầu chung

Kiến thức là những gì Kiểm thử viên hiểu biết và có thể mô tả. Từ điều khoản 5 đến 8 đề cập đến phạm vi kiến thức và các yêu cầu đào tạo cần thiết để kiểm thử phù hợp theo TCVN 11295:2016 (ISO/IEC 19790:2012) và TCVN 12211:2018 (ISO/IEC 24759:2017).

5.2 Đào tạo đại học

5.2.1 Yêu cầu chung

Kiểm thử viên phải có trình độ đào tạo như: bằng Cao đẳng, bằng Cử nhân hoặc bằng cấp cao hơn có liên quan đến các yêu cầu an toàn được đề cập trong TCVN 11295:2016 (ISO/IEC 19790:2012) và các yêu cầu kiểm thử trong TCVN 12211:2018 (ISO/IEC 24759:2017). Kiểm thử viên phải chứng minh rằng họ đáp ứng tối thiểu các yêu cầu sau:

a) Hoàn thành tốt chương trình đào tạo đại học phù hợp với ít nhất 3 năm học trong các ngành liên quan đến công nghệ thông tin hoặc an toàn thông tin;
b) Có kinh nghiệm tương đương với trình độ đại học trong các ngành liên quan đến công nghệ thông tin, an toàn thông tin hoặc quản trị hệ thống thông tin.

5.2.2 Chuyên môn kĩ thuật

Ngoài các yêu cầu về trình độ học vấn tối thiểu trong điều khoản 5.2.1, Kiểm thử viên phải có trình độ đào tạo như bằng Cao đẳng, bằng Cử nhân hoặc cao hơn, đáp ứng các chuyên ngành kỹ thuật cụ thể. Ví dụ về các chuyên ngành kỹ thuật cụ thể bao gồm:

- Các khái niệm về mật mã;
- Kỹ thuật công nghệ;
- Kỹ thuật điện;
- Kỹ thuật cơ khí;
- Kỹ thuật vật liệu;
- Kỹ thuật hóa học;
- Công nghệ thông tin;
- Kỹ thuật máy tính;
- Khoa học máy tính;
- Mạng máy tính;
- An toàn mạng;
- Hệ thống thông tin;
- Quản lý phòng thử nghiệm;
- An toàn và phát triển phần mềm;
- Kỹ thuật phần mềm.

5.2.3 Chuyên ngành

TCVN 11295:2016 (ISO/IEC 19790:2012) và các yêu cầu kiểm thử theo TCVN 12211:2018 (ISO/IEC 24759:2017) đề cập đến các kiến thức chuyên ngành, chuyên môn cụ thể sau đây. Kiểm thử viên tối thiểu phải thể hiện kiến thức, sự hiểu biết về ít nhất một chuyên ngành, chuyên môn cụ thể.

Đội ngũ nhân viên một phòng thử nghiệm đánh giá phải có kiến thức về chuyên ngành trong các lĩnh vực. Tiêu chuẩn TCVN 11295:2016 (ISO/IEC 19790:2012) và TCVN 12211:2018 quy định các chủ đề theo chuyên ngành:

a) Phát triển phần mềm và phần sụn:
   1. Ngôn ngữ lập trình (Ví dụ: assembler hoặc cao hơn);
   2. Trình biên dịch;
   3. Công cụ gỡ lỗi;

4. Kiểm thử sản phẩm được thực hiện bởi nhà cung cấp:
   i. Kiểm thử đơn vị;
   ii. Kiểm thử tích hợp;
   iii. Kiểm thử hồi quy.

b) Hệ điều hành:
1. Cài đặt;
2. Cấu hình;
3. Hoạt động;
4. Kiến trúc;
5. Tăng tính an toàn hệ thống;
6. Máy ảo;
7. Môi trường java runtime.

c) Phát triển phần cứng:
1. Các phương án phần cứng:
   i. Chip đơn (single-chip);
   ii. Nhúng đa chip (multi-chip embedded);
   iii. Độc lập đa chip (multi-chip standalone).
2. Công nghệ:
   i. Chế tạo chip đơn;
   ii. Các thành phần điện và thiết kế, sơ đồ nguyên lý và khái niệm bao gồm thiết kế logic và biểu diễn HDL;
   iii. Thiết kế cơ khí và lắp ráp.
3. Sản xuất:
   i. Cung cấp chuỗi toàn vẹn;
   ii. Phương pháp chế tạo;
   iii. Khởi tạo các tham số;
   iv. Lắp ráp và vận chuyển;
   v. Kiểm thử và mô tả đặc tính.
4. Tính năng an toàn phần cứng;

d) Môi trường hoạt động:
1. Bộ nạp khởi động;
2. Phụ tải;
3. Liên kết;
4. Quản lý và bảo vệ bộ nhớ;
5. Giao tiếp giữa các tiến trình;
6. Kiểm soát truy cập theo ý muốn;
7. Kiểm soát truy cập dựa trên vai trò;
8. Các biểu mẫu thực thi;
9. Cơ chế kiểm thử.

e) Các thuật toán, cơ chế và kỹ thuật mật mã:
1. Thuật toán mật mã và chức năng an toàn:
   i. Khóa đối xứng;
   ii. Khóa phi đối xứng;
   iii. Hàm băm;
   iv. Bộ tạo bit ngẫu nhiên;
   v. Xác thực thông báo;
   vi. Entropy;
   vii. Chế độ hoạt động.
2. Quản lý tham số an toàn nhạy cảm:
   i. Sinh tham số an toàn nhạy cảm;
   ii. Thiết lập tham số an toàn nhạy cảm;
      I. Tự động vận chuyển SSP hoặc thỏa thuận SSP;
      II. Nhập hoặc xuất SSP thủ công thông qua trực tiếp hoặc điện tử;
   iii. Nhập và xuất tham số an toàn nhạy cảm;
   iv. Lưu trữ tham số an toàn nhạy cảm;
   v. Xóa trắng tham số an toàn nhạy cảm.

f) Cơ chế định danh và xác thực:

1. Xác thực dựa trên danh tính;
2. Xác thực dựa trên vai trò;
3. Xác thực dựa trên đa yếu tố.

g) Phương pháp trong thiết kế và phát triển vượt trội:
1. Đảm bảo thiết kế như quản lý cấu hình, phân phối, vận hành và phát triển;
2. Thiết kế theo hợp đồng.

h) Mô hình hóa phi chính thức;
1. Kiểu trạng thái hữu hạn;
   i. An toàn không xâm lấn.
2. Tấn công không xâm lấn:
   ii. DPA/DEMA;
   iii. SPA/SEMA;
   iv. Tấn công tính toán thời gian.
3. Biện pháp đối phó:
   i. Các biện pháp đối phó vật lý;
   Ví dụ 1: Precharge logic, dual-rail logic, nắn phẳng dòng điện, phát hiện đầu dò, thêm nhiễu, ngắt ngẫu nhiên, làm lệch xung nhịp.
   ii. Các biện pháp đối phó logic.
   Ví dụ 2: Tạo mặt nạ, ẩn, hoạt động giả, cân bằng thời gian, xáo trộn, tự động khóa lại.

i) Các cơ chế tự kiểm tra:
1. Kiểm tra trước khi hoạt động;
2. Kiểm tra điều kiện.

j) Các cơ chế an toàn:
1. Xóa trắng;
2. Đường dẫn tin cậy;
3. Bằng chứng giả mạo thiết bị;
4. Nhựa dính epoxit, vật liệu đóng gói và chất kết dính (bao gồm cả tính chất hóa học);
5. Vỏ bọc và vật liệu đóng gói;
6. Cơ chế giả mạo;
7. Các biện pháp chống lại các cuộc tấn công tiêm lỗi;
   Ví dụ 3: Lược đồ dựa trên độ dư, phát hiện mã lỗi, vết tiếp xúc.
8. Các giao thức kết nối an toàn (ví dụ: Secure Sockets Layer, Transport Layer Security, Internet Key Exchange, Secure Socket Shell, Over the Air Rekeying, v.v..);
9. Các thuộc tính về chính sách an toàn;
10. Hiểu biết thủ tục phân tách.

k) Tính năng thiết kế:
1. Cổng và giao diện;
2. Phương thức hoạt động đã được phê duyệt;
3. Đặc điểm kỹ thuật của dịch vụ;
4. Đặc điểm kỹ thuật của các tham số an toàn nhạy cảm.

l) Các công cụ và phương pháp thử:
1. Xây dựng lắp đồ gá kiểm tra (phần mềm hoặc phần cứng);
2. Các phương pháp đánh giá môi trường như sử dụng nhiệt độ (ví dụ: nóng và lạnh) và điện áp (ví dụ: thay đổi đối với nguồn điện đầu vào);
   i. Buồng nhiệt độ (ví dụ: cơ chế sưởi ấm và làm mát);
   ii. Nguồn cung cấp có thể thay đổi.
3. Sử dụng các công cụ cầm tay (ví dụ: cưa, khoan, dụng cụ cạy, mài, dụng cụ quay thay đổi tốc độ, kẹp nha khoa và gương, v.v.);
4. Sử dụng các dung môi hóa học (ví dụ như: axit và kiềm);
5. Nguồn sáng nhân tạo;
6. Công cụ phóng đại;
7. Sử dụng máy hiện sóng kỹ thuật số hoặc máy phân tích logic;
8. Sử dụng đồng hồ đo vôn hoặc đồng hồ đo kỹ thuật số đa năng;
9. Máy quét kỹ thuật số;
10. Máy ảnh kỹ thuật số (bao gồm khả năng lấy nét gần hoặc macro);
11. Các công cụ cung cấp chương trình xác nhận.

Ghi chú: Chỉ yêu cầu hiệu chuẩn dụng cụ tùy thuộc vào phương pháp thử.

Thông tin bổ sung về xác định kiến thức cụ thể với tính an toàn của các mô-đun mật mã được quy định trong Phụ lục C.

5.3 Kiến thức về các tiêu chuẩn

5.3.1 Yêu cầu chung

Kiểm thử viên phải có kiến thức về các tài liệu viện dẫn được quy định trong điều khoản 2. Kiểm thử viên có thể phải chứng minh về kiến thức hoặc sự hiểu biết về một hoặc nhiều chủ đề sau đây.

5.3.2 Khái niệm TCVN 11295:2016 (ISO/IEC 19790:2012)

Kiểm thử viên phải có kiến thức về các khái niệm trong TCVN 11295:2016 (ISO/IEC 19790:2012). TCVN 11295:2016 (ISO/IEC 19790:2012) quy định các yêu cầu an toàn đối với mô-đun mật mã được sử dụng trong hệ thống an toàn bảo vệ thông tin nhạy cảm trong hệ thống máy tính và hệ thống viễn thông. TCVN 11295:2016 (ISO/IEC 19790:2012) định nghĩa bốn mức an toàn cho từng phần trong số 11 phạm vi yêu cầu, với mỗi mức sẽ tăng cường an toàn so với mức trước đó cho các mô-đun mật mã.

5.3.3 TCVN 12211:2018 (ISO/IEC 24759:2017)

5.3.3.1 Yêu cầu chung

TCVN 12211:2018 (ISO/IEC 24759:2017) quy định các yêu cầu kiểm thử đối với mô-đun mật mã được các nhà cung cấp và phòng thử nghiệm sử dụng. TCVN 12211:2018 (ISO/IEC 24759:2017) bao gồm 11 điều khoản phụ tương ứng với 11 lĩnh vực yêu cầu an toàn và 6 điều khoản phụ tương ứng với TCVN 11295:2016 (ISO/IEC 19790:2012), Phụ lục A đến F. Các yêu cầu an toàn tương ứng này được liệt kê trong TCVN 11295:2016 (ISO/IEC 19790:2012), tương ứng điều khoản 5.2.2.5 và 5.2.2.6.

5.3.3.2 Yêu cầu của nhà cung cấp

TCVN 12211:2018 (ISO/IEC 24759:2017) quy định tất cả các yêu cầu về bằng chứng của nhà cung cấp (vendor evidence - VE) mà họ cung cấp cho các phòng thử nghiệm, áp dụng cho mô-đun được kiểm thử, làm bằng chứng để hỗ trợ chứng minh sự phù hợp của mô-đun mật mã của họ với các yêu cầu an toàn được quy định trong TCVN 11295:2016 (ISO/IEC 19790:2012).

Nhà cung cấp cũng phải đáp ứng mọi đề nghị sửa đổi, bổ sung hoặc xóa bỏ đối với bằng chứng VE mà cơ quan có thẩm quyền phê duyệt đã thực hiện theo TCVN 12211:2018 (ISO/IEC 24759:2017).

Kiểm thử viên phải nắm rõ tất cả các yêu cầu của nhà cung cấp.

5.3.3.3 Yêu cầu kiểm thử

TCVN 12211:2018 (ISO/IEC 24759:2017) quy định các yêu cầu về bằng chứng của Kiểm thử viên (tester evidence - TE), áp dụng cho mô-đun được kiểm thử, được các phòng thử nghiệm sử dụng để kiểm thử xem mô-đun mật mã có phù hợp với các yêu cầu quy định trong TCVN 11295:2016 (ISO/IEC 19790:2012). Các phương pháp này được phát triển để cung cấp mức độ khách quan cao trong quá trình kiểm thử và đảm bảo tính thống nhất giữa các phòng thử nghiệm.

Kiểm thử viên cũng phải đáp ứng mọi sửa đổi, bổ sung hoặc xóa bỏ bằng chứng TE mà cơ quan thẩm định đã thực hiện đối với TCVN 12211:2018 (ISO/IEC 24759:2017).

Nhà cung cấp phải nắm rõ tất cả các yêu cầu kiểm thử.

5.3.4 Tiêu chuẩn bổ sung

Kiểm thử viên phải nắm rõ những điều sau đây.

- TCVN 12212:2018 (ISO/IEC 17825:2016), 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.
- TCVN 13177:2020 (ISO/IEC 18367:2016), Công nghệ thông tin - Các kỹ thuật an toàn - Kiểm thử sự phù hợp của các thuật toán mật mã và cơ chế an toàn.
- TCVN 13721:2023 (ISO/IEC 20543:2019), Kỹ thuật an toàn công nghệ thông tin – 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).
- ISO/IEC 20085-1, Specifies test tool requirements for use in testing non-invasive attack mitigation techniques in cryptographic modules.

- ISO/IEC 20085-2, Specifies test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules.

5.4 Kiến thức về chương trình xác nhận

5.4.1 Chương trình xác nhận

5.4.1.1 Yêu cầu chung

Các chương trình xác nhận, thường hoạt động dưới sự bảo trợ của tổ chức công nhận, thường xác định các khía cạnh hoạt động cụ thể. Điều này thường dựa trên luật pháp và chính sách hiện hành, chẳng hạn như chính sách quốc gia, được áp dụng cho hoạt động của tổ chức công nhận đó. Kiểm thử viên phải có kiến thức về chương trình xác nhận và bất kỳ khía cạnh cụ thể nào như những khía cạnh được liệt kê trong 5.4.1.2 đến 5.4.1.7.

5.4.1.2 Tổ chức

Khía cạnh này liên quan đến tổ chức của chương trình và các cơ quan liên quan đến hoạt động của chương trình.

5.4.1.3 Trao đổi thông tin

Khía cạnh này liên quan đến cách truyền đạt thông tin liên quan đến các bên liên quan, đặc biệt là với các cơ sở thử nghiệm và những Kiểm thử viên liên quan. Điều này phải bao gồm cách thức bảo vệ thông tin và truyền thông.

5.4.1.4 Quy định nhiệm vụ và pháp lý

Khía cạnh này liên quan đến khuôn khổ lập pháp hoặc quy định mà theo đó chương trình xác nhận hoạt động.

5.4.1.5 Chính sách

Khía cạnh này liên quan đến các chính sách cụ thể có thể áp dụng cho chương trình xác nhận. Chúng có thể bao gồm các chính sách liên quan đến quy trình và yêu cầu kỹ thuật liên quan đến việc chấp nhận các kế hoạch xác nhận mô-đun mật mã. Sau đây là một số ví dụ.

a) Kiểm tra đầy đủ: việc kiểm thử phải có kiến thức về những công việc thiết để đảm bảo mục tiêu rằng mô-đun mật mã được kiểm tra đầy đủ.
b) Thu thập bằng chứng: quy trình xử lý hợp lý các bằng chứng hỗ trợ sau khi hoàn thành một kế hoạch.
c) Tính an toàn: bất kỳ yêu cầu nào về tính an toàn (về phía Kiểm thử viên và việc không tiết lộ thông tin thu được trong các kế hoạch kiểm thử).
d) Giải quyết vấn đề: quá trình thực hiện hành động nếu một vấn đề gặp phải trong kế hoạch (cho dù công việc tiếp tục sau khi sự cố được khắc phục hay kết thúc kế hoạch ngay lập tức và sản phẩm đã được khắc phục cần được trình lại).
e) Ngôn ngữ: bất kỳ ngôn ngữ cụ thể (tự nhiên) nào sẽ được cung cấp trong tài liệu.
f) Yêu cầu đối về lập hồ sơ bằng chứng: bất kỳ bằng chứng đã được ghi lại nào do Kiểm thử viên lập cần được trình cho chương trình xác nhận.
g) Các chính sách báo cáo bổ sung: bất kỳ báo cáo cụ thể nào được yêu cầu từ Kiểm thử viên, (ví dụ như: báo cáo kiểm thử).
h) Hướng dẫn thực hiện: cơ quan xác nhận có thể cung cấp hướng dẫn theo chương trình hoặc làm rõ để Kiểm thử viên xem xét.
i) Tái sử dụng: tài liệu và cơ sở hợp lý do chương trình xác nhận yêu cầu để hỗ trợ việc sử dụng lại bằng chứng kiểm tra.
j) Xử lý bất kỳ đặc điểm nào đối với các mã định danh chương trình xác thực, biểu tượng, nhãn hiệu, ...
k) Xử lý và áp dụng cách diễn giải chương trình xác nhận.
l) Danh sách hoặc các đặc điểm của các phương pháp tiếp cận thay thế phù hợp với chương trình xác nhận khi kiểm thử ban đầu được khuyến cáo là không khả thi đối với một mô-đun mật mã đang xét.
m) Các chính sách mà chương trình xác nhận xác định các bước mà Kiểm thử viên đã thực hiện trong khi kiểm thử.

5.4.1.6 Tài liệu tham khảo

Khía cạnh trong điều khoản này liên quan đến việc cung cấp và sử dụng bất kỳ tài liệu cụ thể nào của chương trình xác nhận. Có thể bao gồm các mẫu, biểu mẫu, tài liệu đào tạo và tài liệu thông tin. Các tài liệu cụ thể của chương trình xác nhận có thể bao gồm các tài liệu như:

- Sổ tay quản lý;
- Tài liệu các câu hỏi thường gặp;
- Tài liệu triển khai hoặc tài liệu hướng dẫn thực hiện theo chương trình;
- Tài liệu hướng dẫn sử dụng các công cụ do chương trình cung cấp.

5.4.1.7 Công cụ

Chương trình xác nhận có thể cung cấp các công cụ cụ thể để kiểm thử, tạo báo cáo hoặc cung cấp bảo vệ (tức là mã hóa). Những ví dụ bao gồm:

- Các công cụ kiểm thử thuật toán;
- Tạo các vector kiểm thử và các phản hồi kết quả dự kiến;
- Tài liệu về các hoạt động kiểm thử và báo cáo;
- Công cụ mã hóa để bảo vệ các báo cáo kiểm thử được truyền tới chương trình xác nhận;
- Đặc điểm kỹ thuật cụ thể của thuật toán mã hóa và các phương pháp ký (ví dụ: AES độ dài khóa 128-bit cho mã hóa và RSA độ dài khóa 2048-bit với SHA-2 cho ký số).

5.5 Yêu cầu về kiến thức của TCVN ISO/IEC 17025:2017

Vì các cơ sở thử nghiệm thường được yêu cầu phù hợp theo TCVN ISO/IEC 17025:2017, Kiểm thử viên phải nắm rõ các yêu cầu của TCVN ISO/IEC 17025:2017 và cách thức thực hiện các yêu cầu này trong cơ sở thử nghiệm hoặc các cơ sở mà Kiểm thử viên có liên quan. Nếu có thêm các tài liệu công nhận theo chương trình liên quan đến TCVN ISO/IEC 17025:2017, làm cơ sở cho việc công nhận phòng thử nghiệm, thì Kiểm thử viên cũng phải nắm bắt các tiêu chuẩn này.

6 Kỹ năng

6.1 Yêu cầu chung

Việc đào tạo cho Kiểm thử viên thường có được thông qua kinh nghiệm nghề nghiệp trong chuyên ngành công nghệ thông tin hoặc trong quá trình họ liên kết với cơ sở thử nghiệm hoặc do yêu cầu của các tổ chức chuyên nghiệp.

Ví dụ: Các chứng chỉ chuyên gia như chứng chỉ ISC2™ CISSP™ có liên quan đến yêu cầu phát triển chuyên môn liên tục.

6.2 Kiểm thử thuật toán

Kiểm thử viên phải có khả năng cài đặt, cấu hình và thực thi chương trình xác thực thuật toán mật mã hoặc các công cụ kiểm thử thuật toán có giao diện cho người điều khiển.

6.3 Kiểm thử an toàn vật lý

Kiểm thử viên phải có các kỹ năng để thực hiện các kiểm thử an toàn vật lý mà họ được đào tạo thích hợp và có kỹ năng.

6.4 Phân tích kênh kề

Kiểm thử viên phải có các kỹ năng để thực hiện các kiểm thử kênh kề mà họ được đào tạo thích hợp và có kỹ năng.

6.5 Loại công nghệ

Các kỹ năng và kỹ thuật cần thiết trong kiểm thử mô-đun mật mã cho từng loại công nghệ khác nhau có thể sẽ khác nhau. Kiểm thử viên sẽ có thể phải chứng minh rằng họ có kiến thức, kỹ năng và kỹ thuật cần thiết liên quan đến các loại công nghệ của mô-đun mật mã mà họ kiểm thử.

Ghi chú 1: Chương trình xác nhận chỉ định đến các mô-đun mật mã đại diện cho nhiều loại công nghệ đang được xem xét để kiểm thử. Danh sách các loại công nghệ thường được tham khảo và đề xuất các kỹ năng và kiến thức cơ bản mà Kiểm thử viên cần có mô tả tại Phụ lục B.

Ghi chú 2: Nhiều chứng chỉ chuyên gia bao hàm phạm vi kiến thức mà Kiểm thử viên cần có. Các chứng nhận đó có thể là phạm vi quốc gia, trong một khu vực hoặc phạm vi quốc tế. Việc liệt kê tất cả chúng nằm ngoài phạm vi của tiêu chuẩn này, tuy nhiên một số tài liệu đó được được liệt kê tại mục Tài liệu tham khảo.

7 Kinh nghiệm

7.1 Yêu cầu chung

Kiểm thử viên phải ghi lại các hoạt động đào tạo và kiểm thử của họ phù hợp với chương trình xác nhận và hoặc các yêu cầu của cơ sở thử nghiệm.

7.2 Chứng minh năng lực kỹ thuật đối với chương trình xác nhận

7.2.1 Kinh nghiệm thực hiện kiểm thử

Kiểm thử viên phải ghi lại tất cả hoạt động kiểm thử vào nhật ký. Hồ sơ phải được lưu giữ cùng với bằng chứng kiểm thử thu được (xem Phụ lục A). Kiểm thử viên nên tạo nhật ký để kiểm thử hoạt động nhằm làm rõ cả kết quả kiểm thử dự kiến và kết quả kiểm thử thực tế.

Ví dụ: Chỉ số báo trạng thái sẽ xảy ra.

7.2.2 Kinh nghiệm với các loại công nghệ cụ thể

Kiểm thử viên phải ghi lại nhật ký hoạt động của họ về các loại công nghệ đã được kiểm thử.

8 Trình độ đào tạo

Kiểm thử viên phải ghi lại trình độ học vấn của họ phù hợp với chương trình xác nhận và các yêu cầu của cơ sở thử nghiệm.

Yêu cầu về đào tạo được tham chiếu trong mục 5.2.

9 Tính hiệu quả

Kiểm thử viên có thể sẽ phải áp dụng kiến thức và kỹ năng một cách hiệu quả, được đặc trưng bởi các đặc trưng như: năng khiếu, sáng kiến, nhiệt tình, sẵn sàng, kỹ năng giao tiếp, tham gia nhóm và lãnh đạo.

Phụ lục A
(Tham khảo)

Bảng A.1: Ví dụ về nhật ký của Kiểm thử viên theo TCVN 12211:2018

<table>
<tr><td colspan="3">Tên</td></tr>
<tr><td colspan="3">Ký hiệu</td></tr>
<tr><td colspan="2">Chương trình xác nhận</td><td>Bộ phận kiểm thử</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">Tên mô-đun mật mã</td><td>Loại mô-đun mật mã</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">Tổng thể mức an toàn</td><td>Mã định danh chứng nhận (nếu biết)</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">Nhà tài trợ/nhà phát triển</td><td>Ngày thực hiện kiểm thử</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="3">Mô tả của IUT</td></tr>
<tr><td rowspan="3">AS 01.01</td><td colspan="2">Yêu cầu kiểm thử áp dụng được quy định theo TCVN 12211:2018</td></tr>
<tr><td colspan="2">Mô tả thiết kế IUTs để phù hợp với yêu cầu kiểm thử</td></tr>
<tr><td colspan="2">Mô tả phương pháp và kết quả kiểm thử</td></tr>
</table>

Phụ lục B

(Tham khảo)

Các loại công nghệ và bộ kiến thức cốt lõi liên quan

B.1 Yêu cầu chung

Chương trình xác nhận giải quyết các mô-đun mật mã đại diện cho nhiều loại công nghệ đang được xem xét để kiểm thử. Dưới đây là danh sách các loại công nghệ thường được tham khảo và đề xuất về các kỹ năng và kiến thức cơ bản mà Kiểm thử viên cần có.

B.2 Loại công nghệ

B.2.1 Yêu cầu chung

Mô-đun mật mã có thể là phần mềm, phần sụn, phần cứng hoặc kết hợp giữa phần mềm và phần sụn với phần cứng.

B.2.2 Phần mềm/Phần sụn

Phần mềm hoặc phần sụn có thể được viết bằng nhiều ngôn ngữ lập trình khác nhau và sau đó được biên dịch thành các dạng tệp thực thi khác nhau. Một tệp thực thi có thể đại diện cho một phần mềm mật mã hoặc mô-đun phần sụn. Trình gỡ lỗi có thể được sử dụng để tìm và sửa lỗi trong quá trình thực hiện.

B.2.2.1 Ngôn ngữ lập trình

Ví dụ về các ngôn ngữ lập trình phần mềm khác nhau có thể được sử dụng (Danh sách này không phải là đầy đủ và chỉ dành cho mục đích minh họa):

- Ada;
- APL;
- Assembly language;
- C++;
- dBase;
- Google Apps Script;
- Java;
- JavaScript;
- Microcode;
- Unix shell;
- Visual Basic;
- VHDL.

B.2.2.2 Biên dịch

Ví dụ về các trình biên dịch phần mềm nguồn mở khác nhau có thể được sử dụng (Danh sách này không phải là đầy đủ và chỉ dành cho mục đích minh họa):

- FreeBASIC;
- Clang C/C++/Objective-C Compiler;
- Free Pascal;
- GCC [C, C++, (G++), Java (GCJ) and Ada (GNAT)];
- Local C compiler;
- Open Watcom;
- Open64;
- XPL PL/I;
- C to HDL.

B.2.2.3 Trình gỡ lỗi hoặc trình mô phỏng

Ví dụ về các trình gỡ rối mã nguồn mở khác nhau có thể được sử dụng (Danh sách này không phải là đầy đủ và chỉ dành cho mục đích minh họa):

- Firefox JavaScript debugger;
- GDB – the GNU debugger;

- Eclipse debugger;
- Opera Dragonfly;
- Python debugger;
- X64dbg;
- ZeroBUGS;
- VHDL;
- Verilog.

B.2.2.4 Phần cứng

B.2.2.4.1 Yêu cầu chung về kiến thức

Phần cứng có thể được triển khai theo nhiều phương án và loại công nghệ khác nhau. Dưới đây là các ví dụ về các phương án phần cứng và loại công nghệ trong mỗi phương án. Danh sách sau đây không phải là đầy đủ và chỉ dành cho mục đích minh họa.

B.2.2.4.2 Mô-đun chip đơn

B.2.2.4.2.1 Kiến thức chung về mô-đun chip đơn

Một mô-đun mật mã chip đơn là một phương án vật lý trong đó một mạch chip tích hợp (IC) duy nhất có thể được sử dụng như một thiết bị độc lập hoặc được nhúng trong một vỏ bọc hoặc một sản phẩm có thể không được bảo vệ vật lý.

B.2.2.4.2.2 Vật liệu nền chip đơn

Ví dụ về vật liệu nền của chip đơn:

- Gallium arsenide;
- Germanium;
- Monocrystalline silicon - Silicon đơn tinh thể.

B.2.2.4.2.3 Kiểu đóng gói chip đơn

Ví dụ về kiểu đóng gói của chip đơn:

- Dual in-line package (DIP);
- Pin grid array (PGA);
- Leadless chip carrier (LCC);
- Surface mount;
- Thin small-outline package (TSOP);
- Plastic quad flat pack (PQFP);
- Ball grid array (BGA);
- Flip-chip ball grid array (FCBGA).

B.2.2.4.3 Mô-đun nhúng đa chip

Mô-đun mật mã nhúng đa chip là một phương án vật lý trong đó hai hoặc nhiều chip mạch tích hợp được kết nối với nhau và được nhúng trong một vỏ bọc hoặc một sản phẩm có thể không được bảo vệ vật lý.

Ví dụ:

- Thẻ bộ điều hợp;
- Bảng mạch mở rộng;
- Phích cắm và thẻ mở rộng mạch.

B.2.2.4.4 Mô đun đa chip độc lập

Mô-đun mật mã đa chip độc lập là một phương án vật lý trong đó hai hoặc nhiều chip mạch tích hợp được kết nối với nhau và toàn bộ vỏ được bảo vệ vật lý.

Ví dụ:

- Mã hóa bộ định tuyến và thiết bị chuyển mạch;
- Bộ đàm an toàn;
- USB tokens.

Phụ lục C

(Tham khảo)

Kiến thức cụ thể liên quan đến an toàn của mô-đun mật mã

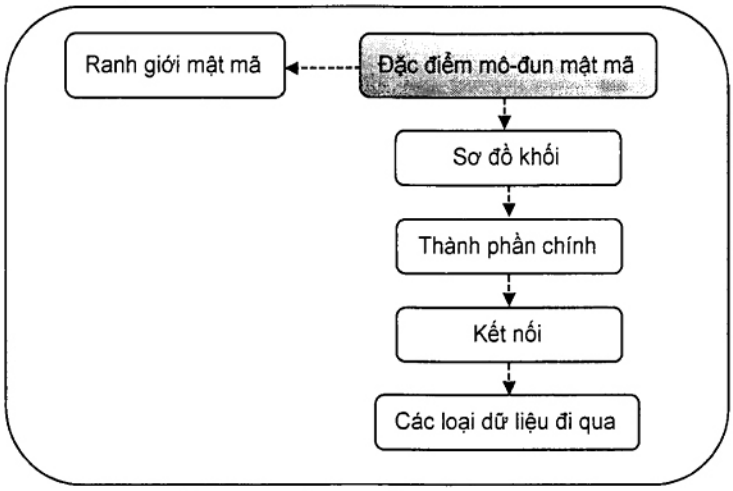
C.1 Yêu cầu chung

Các yêu cầu an toàn [**xx.yy**] đề cập đến trong tiêu chuẩn này được quy định trong TCVN 11295:2016 (ISO/IEC 19790:2012). Mỗi yêu cầu an toàn trong TCVN 11295:2016 (ISO/IEC 19790:2012) bao gồm: một chỉ số tham chiếu [xx.yy], trong đó: **xx** chỉ ra điều khoản và **yy** là một chỉ mục trong điều khoản đó.

C.2 Đặc điểm mô-đun mật mã

C.2.1 Yêu cầu chung

Hình C.1 minh họa tổng quan về đặc điểm kỹ thuật của mô-đun mật mã liên quan đến các phần tử khác bao gồm: ranh giới mật mã, sơ đồ khối, các thành phần chính của mô-đun mật mã, các kết nối và các kiểu dữ liệu đi qua mô-đun.



Hình C.1 - Tổng quan về đặc điểm kỹ thuật mô-đun mật mã

C.2.2 Bộ đệm (Buffers)

Có thể có bộ đệm dữ liệu hoặc bộ đệm SSP (Sensitive Security Parameters) bên trong các thành phần (đặc biệt là đối với mô-đun nhúng đa chip hoặc mô-đun đa chip độc lập). Ngoài ra, có nhiều mức bộ nhớ đệm dữ liệu trong CPU. Trong những trường hợp như vậy, Kiểm thử viên nên xác định vùng đệm từ thông tin công khai có sẵn và thông tin cung cấp bởi nhà cung cấp. Thông tin sẽ là đầu vào để kiểm thử cơ chế xóa trắng tham số an toàn nhạy cảm của mô-đun mật mã.

C.2.3 Các thành phần liên quan đến an toàn

Bằng cách xem xét sơ đồ khối, Kiểm thử viên hiểu được luồng thông tin và các loại thông tin được chuyển qua từng thành phần. Bằng cách xác định các thành phần: truyền/lưu trữ/đọc/ghi/tạo/sử dụng/xóa trắng tham số an toàn nhạy cảm, Kiểm thử viên có thể xác định các thành phần liên quan đến an toàn.

C.2.4 Xác định các giao diện lập trình, giao diện gỡ lỗi và các kênh che giấu

Các thành phần cấp thương mại có thể có các giao diện lập trình, các giao diện gỡ lỗi và các kênh che giấu. Một thói quen tốt cho Kiểm thử viên là tìm kiếm thông tin công khai có sẵn và thông tin cung cấp bởi nhà cung cấp để xác định xem các giao diện đó có tồn tại hay không. Nếu có một giao diện như vậy, Kiểm thử viên xác minh từ việc kiểm thử mô-đun mật mã để xác định rằng một giao diện như vậy không khả dụng do thiết kế mô-đun mật mã.

Trong trường hợp mô-đun phần mềm, đặc biệt là đối với các thư viện liên kết động hoặc các đối tượng được chia sẻ, có các công cụ đã biết để xác định các hàm API sử dụng. Bằng cách sử dụng các công cụ như vậy, Kiểm thử viên có thể xác định xem các API không có tài liệu có được sử dụng hay không.

Nếu phân tích cú pháp các lệnh đầu vào mô-đun mật mã, Kiểm thử viên có thể xác định xem các lệnh đầu vào không có tài liệu có được hỗ trợ hay không bằng cách kiểm thử thực hiện một hoặc nhiều cài đặt phân tích cú pháp. Lưu ý rằng trình phân tích cú pháp có thể được triển khai trong nhiều lớp.

C.2.5 Xác định các chức năng an toàn đã được phê duyệt và không được phê duyệt

Kiểm thử viên phải xác định các chức năng an toàn đã được phê duyệt và cả các chức năng an toàn không được phê duyệt. Để việc triển khai chức năng an toàn được coi là đã được phê duyệt, cần có những điều sau đây.

a) Việc triển khai chức năng an toàn đã vượt qua kiểm thử thuật toán mật mã.
b) Việc thực hiện chức năng an toàn đáp ứng các yêu cầu tự kiểm thử thuật toán mật mã có điều kiện.
c) Nếu một SSP được sử dụng, thì SSP có thể được xóa trắng khi hoạt động ở chế độ hoạt động đã được phê duyệt, và:
    1) SSP được tạo bằng phương pháp tạo SSP đã được phê duyệt bởi người vận hành đảm nhận vai trò được ủy quyền khi vận hành ở chế độ hoạt động đã được phê duyệt, hoặc;
    2) SSP được thiết lập theo phương pháp thiết lập SSP đã được phê duyệt bởi người vận hành đảm nhận vai trò được ủy quyền khi vận hành ở phương thức hoạt động đã được phê duyệt.
d) Nếu một số ngẫu nhiên được sử dụng, thì số ngẫu nhiên được tạo bởi một bộ tạo nhị phân ngẫu nhiên (Random Binary Generate – RBG) đã được phê duyệt khi hoạt động ở chế độ hoạt động đã được phê duyệt, trừ khi có quy định khác.
e) Nếu sử dụng RBG đã được phê duyệt thì các yêu cầu an toàn entropy [09.07] và [09.08] sẽ được đáp ứng.

Nếu một hoặc nhiều điều kiện được mô tả ở trên không được đáp ứng, thì việc triển khai chức năng an toàn được coi là không được chấp thuận.

C.2.6 Các thành phần loại trừ

Để xác minh lý do các thành phần loại trừ, Kiểm thử viên cần thông tin sau:

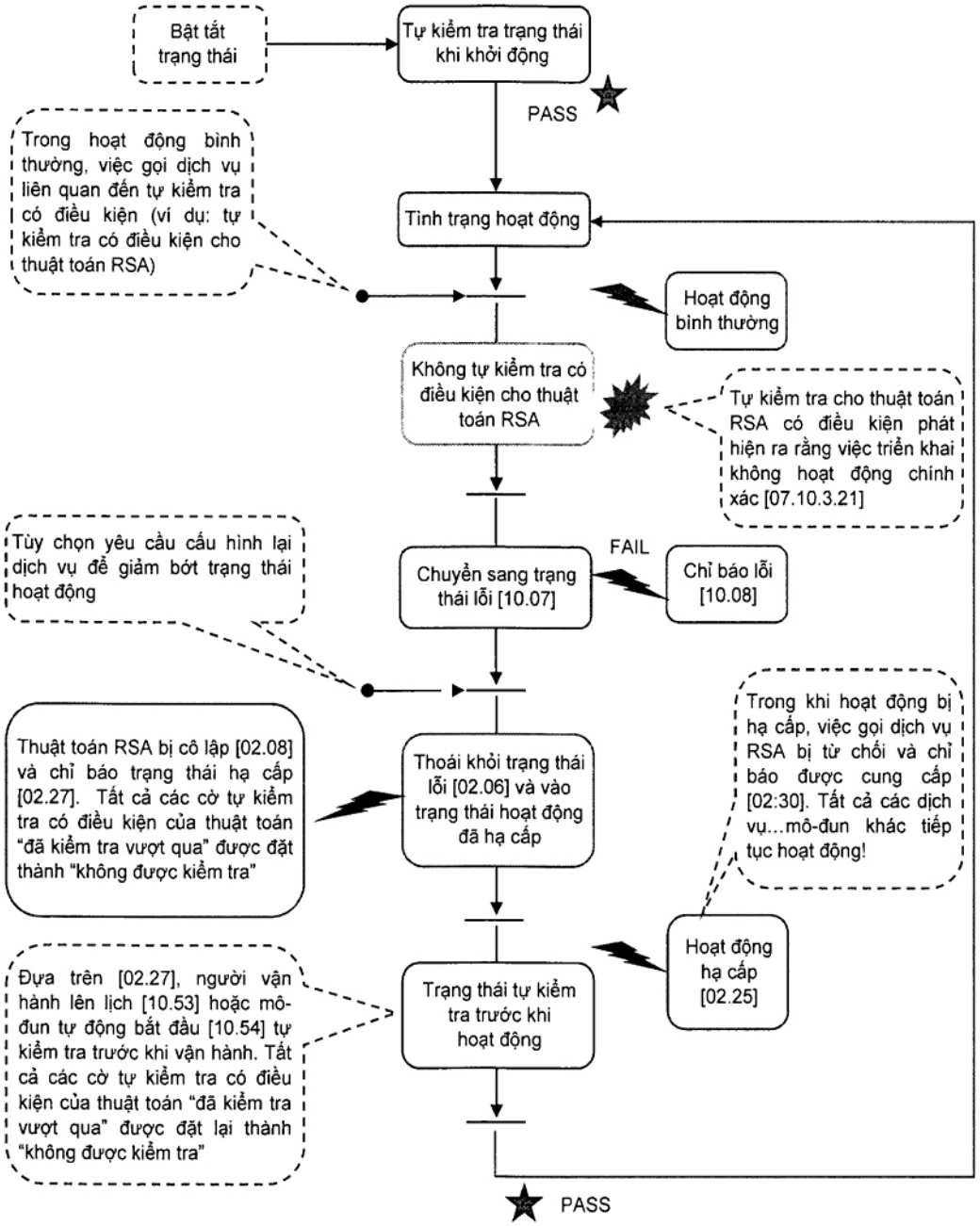
a) Xác định thành phần kiểu dữ liệu nào (Ví dụ: các tham số an toàn nhạy cảm) đi qua các ranh giới xác định của mô đun.
b) Kết nối giữa các thành phần và giao diện;
c) Liệu có giao diện lập trình được hoặc giao diện gỡ lỗi có thể cung cấp một kênh không an toàn để truy cập các tham số an toàn nhạy cảm hay không.

C.2.7 Hoạt động hạ cấp

Một mô-đun mật mã có thể được thiết kế để hỗ trợ chức năng hạ cấp nếu mô-đun này đi vào trạng thái lỗi. Các nhà cung cấp có thể triển khai chức năng hạ cấp cho các mô-đun mật mã để đạt được khả năng chịu lỗi hoặc để duy trì khả năng hoạt động. Một mô-đun mật mã có thể thông báo cho các mô-đun mật mã hợp tác khác thông qua trạng thái đầu ra rằng mô-đun mật mã đi vào hoạt động hạ cấp.

Lưu ý rằng hoạt động suy giảm chất lượng bắt nguồn từ lỗi được phát hiện trong quá trình tự kiểm tra có điều kiện. Như đã nêu trong yêu cầu [02.32], không được phép đi vào hoạt động hạ cấp nếu mô-đun mật mã không đạt yêu cầu tự kiểm tra trước khi hoạt động. Để thoát khỏi hoạt động hạ cấp và đi vào hoạt động bình thường, mô-đun mật mã vượt qua tất cả các quá trình tự kiểm tra trước khi hoạt động thành công, như đã nêu trong yêu cầu [02.31].

Do nội dung của tự kiểm tra trước khi vận hành khác với nội dung của tự kiểm tra có điều kiện, nên không đảm bảo mô-đun mật mã có thể vượt qua các lần tự kiểm tra có điều kiện nếu mô-đun vượt qua các lần tự kiểm tra trước khi hoạt động. Hình C.2 cho thấy một ví dụ về chuyển đổi trạng thái cho mô-đun mật mã hỗ trợ chức năng hạ cấp. Trong Hình C.2, tự kiểm tra có điều kiện cho thuật toán RSA được hiển thị như một ví dụ, trong đó lỗi được phát hiện.



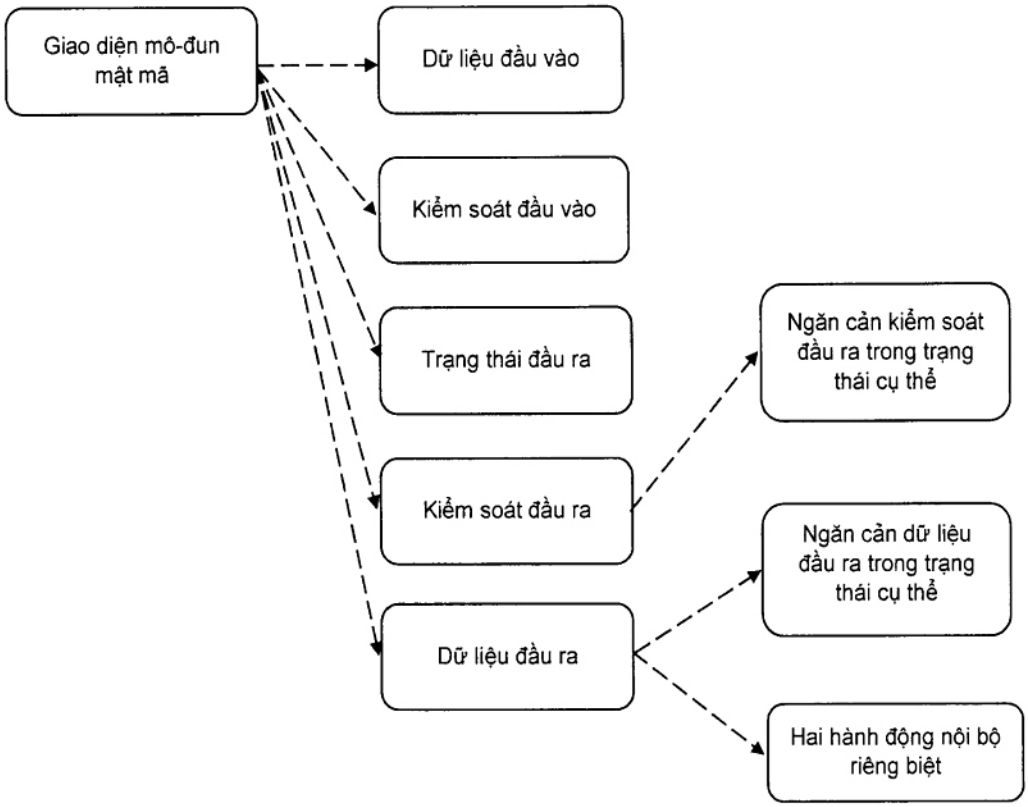
Hình C.2 - Ví dụ về chuyển đổi trạng thái hỗ trợ chức năng bị hạ cấp

Nếu lỗi được phát hiện trong quá trình tự kiểm tra có điều kiện gây ra bởi một sự cố thường xuyên, lỗi đó sẽ được tìm thấy một lần nữa trong quá trình kiểm tra có điều kiện và mô-đun mật mã sẽ lặp lại hoạt động hạ cấp. Một mô-đun mật mã có thể được thiết kế để chuyển đổi vĩnh viễn sang trạng thái lỗi nếu chế độ hạ cấp lặp lại quá nhiều lần.

C.3 Giao diện mô-đun mật mã

C.3.1 Tổng quan

Trong TCVN 11295:2016 (ISO/IEC 19790:2012), yêu cầu rằng phần mềm, phần sụn và mô-đun phần cứng phải được xác định ranh giới mật mã như là một phần của dịch vụ được yêu cầu và có các giao diện phần mềm, phần sụn và giao diện mô-đun phần cứng sử dụng các dịch vụ yêu cầu của mô-đun, bao gồm nhập hoặc bỏ các tham số. Hình C.3 minh họa các kiểu giao diện chức năng khác nhau mà một mô-đun bắt buộc phải có và các điều khiển nếu có.



Hình C.3 - Tổng quan về giao diện mô-đun mật mã

C.3.2 Tách dữ liệu đầu vào khỏi dữ liệu đầu ra

Khi xem xét các giao diện lập trình ứng dụng (API), các tham số được chia thành:

a) Tham số đầu vào;

b) Tham số đầu ra;

c) Tham số đầu vào/đầu ra.

Giá trị của API trả về được coi là dữ liệu đầu ra hoặc dữ liệu điều khiển đầu ra. Các tham số đầu vào/đầu ra có thể được chia thành tham số đầu vào hoặc tham số đầu ra kết hợp với thông tin của các tham số khác hoặc giá trị trả về.

C.3.3 Kiến thức về các chức năng, dịch vụ quan trọng hoặc các dịch vụ liên quan đến an toàn

Trong TCVN 11295:2016 (ISO/IEC 19790:2012), mục 7.2, yêu cầu rằng đường dẫn dữ liệu đầu ra bị ngắt kết nối logic khỏi mạch và quá trình xử lý trong khi thực hiện tạo khóa, nhập khóa thủ công hoặc xóa trắng khóa. Điều này có nghĩa là ba dịch vụ này được coi là có liên quan đến an toàn. Do một lỗi duy nhất hoặc sử dụng sai, các giá trị khóa trung gian, khóa được nhập theo cách thủ công hoặc các giá trị khóa trong quá trình xóa trắng có thể vô tình được xuất ra thông qua đường dẫn dữ liệu đầu ra.

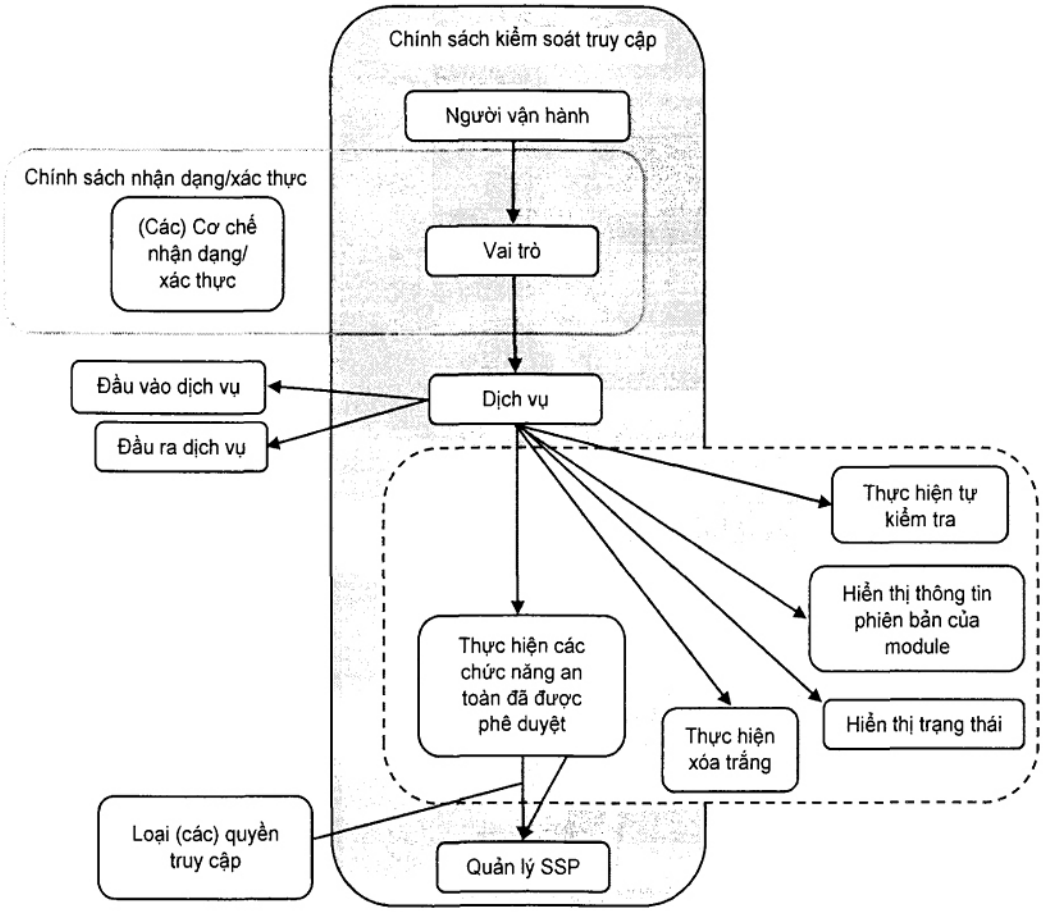
C.3.4 Kênh tin cậy

Một kênh tin cậy cung cấp kết nối liên kết an toàn và bảo mật giữa mô-đun mật mã và người gửi hoặc người nhận để kết nối dữ liệu không được bảo vệ. Kênh tin cậy bảo vệ chống lại việc nghe trộm, cũng như giả mạo vật lý hoặc logic bởi người vận hành/thực thể, quy trình hoặc thiết bị khác không mong muốn, giữa các cổng đầu vào hoặc đầu ra được xác định của mô-đun và dọc theo kết nối liên kết với điểm cuối dự kiến. Kiến thức về các cơ chế được sử dụng để thiết lập và sử dụng kênh đáng tin cậy là rất quan trọng để bảo vệ dữ liệu không được bảo vệ.

C.4 Vai trò, dịch vụ và xác thực

C.4.1 Yêu cầu chung

Hình C.4 minh họa tổng quan và mối quan hệ giữa các vai trò, dịch vụ và cơ chế xác thực và cách mà một chính sách kiểm soát truy cập phân tách với các dịch vụ được xác định trước của mô-đun.



Hình C.4 - Tổng quan về vai trò, dịch vụ và xác thực

C.4.2 Dịch vụ

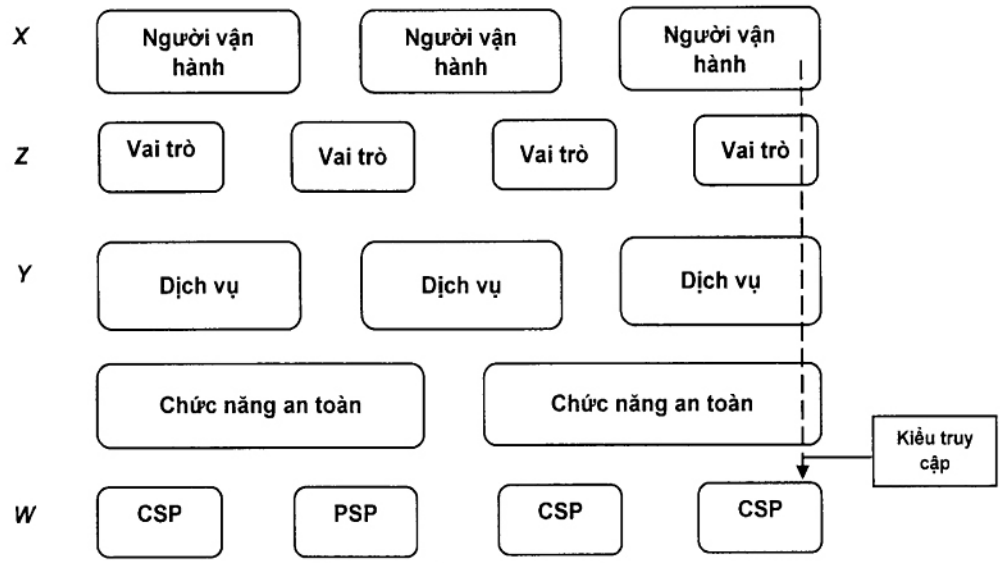
Trong mục B.2.4 của TCVN 11295:2016 (ISO/IEC 19790:2012), chính sách kiểm soát truy cập bắt buộc phải chi tiết để trả lời câu hỏi sau:

- Người vận hành X, đang thực hiện dịch vụ Y trong vai trò của Z, có quyền truy cập nào để bảo mật phần dữ liệu liên quan W cho mọi vai trò, dịch vụ và phần dữ liệu liên quan đến an toàn có trong mô-đun mật mã?

Trong mục B.2.4 của TCVN 11295:2016 (ISO/IEC 19790:2012), yêu cầu như sau:

- Đối với mỗi dịch vụ, tên dịch vụ, mô tả ngắn gọn về mục đích và việc sử dụng dịch vụ (trong một số trường hợp có thể cung cấp thông tin riêng, tên dịch vụ), danh sách các thuật toán đã được phê duyệt các chức năng an toàn, (các) kỹ thuật quản lý (các) khóa hoặc kỹ thuật xác thực) được sử dụng bởi hoặc được triển khai thông qua việc gọi dịch vụ và danh sách các SSP được liên kết với dịch vụ hoặc với (các) chức năng an toàn đã được phê duyệt mà nó sử dụng.

Đối với mỗi vai trò nhà vận hành được phép sử dụng dịch vụ, thông tin mô tả các quyền truy cập cá nhân đối với tất cả các SSP và thông tin mô tả phương pháp được sử dụng để xác thực từng vai trò.



Hình C.5 - Tổng quan về chính sách kiểm soát truy cập

C.4.3 Xác thực

Khi thay thế dữ liệu xác thực mặc định của mô-đun mật mã được thay thế ở mức an toàn 3 hoặc 4, dữ liệu xác thực mới của người vận hành cụ thể cần được nhập vào mô-đun mật mã theo các yêu cầu [04.45] và [09.20].

Khi dữ liệu xác thực bản rõ được nhập vào mô-đun mật mã, xác thực dựa trên danh tính được yêu cầu trước, theo yêu cầu [03.20].

Khi dữ liệu xác thực được mã hóa và nhập vào mô-đun mật mã, dữ liệu xác thực sẽ được mã hóa theo yêu cầu [09.13]. Lưu ý rằng việc mã hóa sử dụng khóa bí mật chung không được coi là "đã được phê duyệt". Người ta có thể nghĩ để tạo ra một khóa mã bí mật cho kênh tin cậy, nhưng có thể nó không được chấp nhận là một ngoại lệ theo hướng dẫn cụ thể của cơ quan xác thực.

Cơ quan xác thực có thể cung cấp hướng dẫn khi giả định rằng việc xác thực người vận hành có thể được thực hiện nhiều lần mà không cần giả định bất kỳ vai trò được ủy quyền nào. Nếu CSP được sử dụng trong xác thực người vận hành, thì có nguy cơ CSP đó có thể bị phát tán hoặc tiết lộ bằng cách sử dụng các cuộc tấn công tiêm lỗi hoặc bằng cách sử dụng các cuộc tấn công không xâm lấn. Các CSP sử dụng để xác thực người vận hành có thể được an toàn nếu chúng được tách biệt khỏi các CSP được sử dụng cho các mục đích khác.

C.5 An toàn phần mềm/phần sụn

Mỗi hệ điều hành xác định các dạng thực thi của phần mềm. Các biểu mẫu thực thi hiện tại có các phân đoạn tiêu đề được phân tích cú pháp trong giai đoạn nạp. Nếu nội dung của tiêu đề bị sửa đổi, hệ điều hành có thể dừng nạp phần mềm. Các biểu mẫu có thể thực thi cũng có thể có các phân đoạn dữ liệu, có thể hệ điều hành không dừng nạp phần mềm nếu nội dung của các phân đoạn dữ liệu bị sửa đổi.

Nếu kiểm tra tính toàn vẹn của phần mềm/phần sụn được thực hiện bởi chính mô-đun, thì việc sửa đổi phân đoạn tiêu đề là không đủ để kiểm tra tính toàn vẹn của phần mềm/phần sụn.

C.6 Môi trường hoạt động

C.6.1 Quản lý tiến trình bộ nhớ

Yêu cầu [06.06] phụ thuộc vào quá trình quản lý bộ nhớ do hệ điều hành cung cấp.

Bảo vệ bộ nhớ do hệ điều hành cung cấp được áp dụng cho mức tiến trình, vì vậy bảo vệ mức luồng không được áp dụng trong các hệ điều hành có sẵn trên thị trường.

C.6.2 Nạp tải

Khi xem xét mô-đun phần mềm, một hệ điều hành nạp mô-đun phần mềm và sau đó mô-đun phần mềm bắt đầu hoạt động từ điểm đầu vào. Trong trường hợp một đối tượng được chia sẻ hoặc thư viện liên kết động, một số hệ điều hành cung cấp các tùy chọn để bỏ qua đầu vào của mô-đun phần mềm.

Nếu đầu vào bắt buộc thực hiện kiểm tra tính toàn vẹn của phần mềm trước khi vận hành, thì người kiểm tra phải xác minh rằng tài liệu hướng dẫn chỉ định không sử dụng các tùy chọn như vậy.

C.6.3 Sự liên kết

Nếu hai hoặc nhiều ký hiệu tạo ra xung đột, thì quyết định cuối cùng là tùy thuộc vào trình liên kết. Tài liệu hướng dẫn phải đề cập đến khía cạnh đó.

Có các mô-đun phần mềm bao gồm nhiều tệp thực thi. Hiện tại có các công cụ để phân tích sự phụ thuộc của các tệp thực thi. Sau khi hiểu sự phụ thuộc của các tệp thực thi, Kiểm thử viên nên xác minh rằng tính toàn vẹn của tất cả các thành phần phần mềm được kiểm tra tính toàn vẹn của phần mềm trước khi hoạt động.

C.6.4 Bộ nhớ ảo

Các hệ điều hành hiện tại hỗ trợ bộ nhớ ảo, sử dụng ổ cứng HDD (hoặc SSD) như thể chúng là bộ nhớ vật lý. Vì lý do an toàn, nếu tiến trình mật mã được phép lưu trên bộ nhớ ảo và bộ nhớ ảo được lưu trữ trên ổ đĩa mạng thì sẽ có nguy cơ quá trình này bị hệ điều hành khác truy cập. Kiểm thử viên phải xác minh rằng tài liệu hướng dẫn không cho phép sử dụng như vậy.

C.7 An toàn vật lý

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

C.8 An toàn không xâm lấn

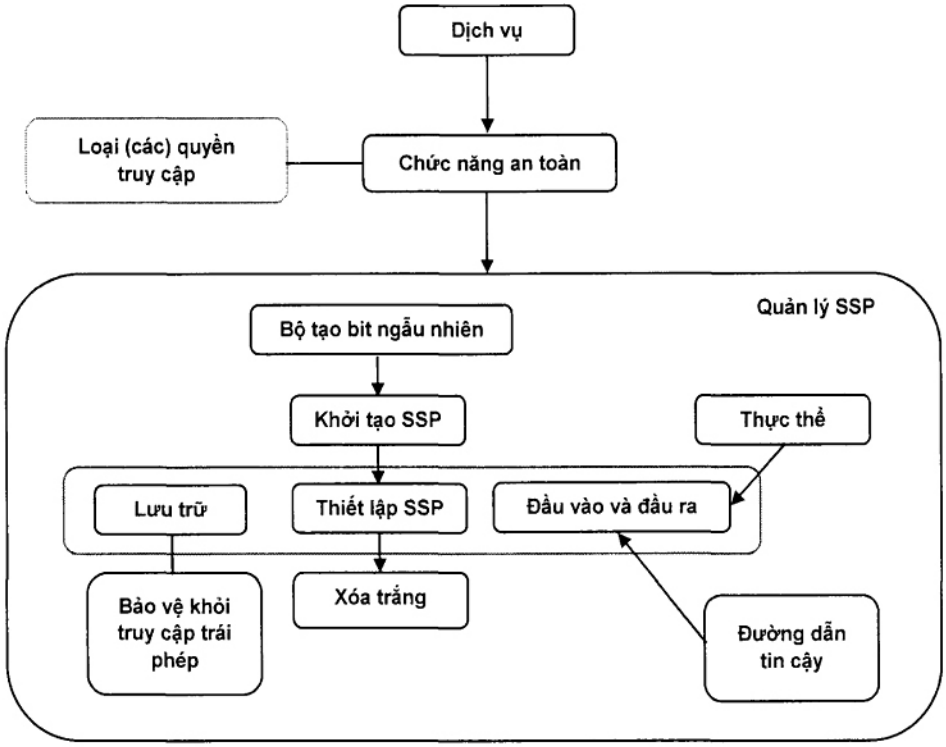
Các cuộc tấn công không xâm lấn cố gắng xâm phạm mô-đun mật mã bằng cách thu thập tin tức về các CSP của mô-đun mà không cần sửa đổi vật lý hoặc xâm nhập vào mô-đun. Các mô-đun có thể thực hiện các kỹ thuật khác nhau để giảm thiểu các loại tấn công này. Các chỉ số kiểm thử để giảm thiểu tấn công không xâm lấn cho từng chức năng an toàn liên quan được đề cập bởi TCVN 11295:2016 (ISO/IEC 19790:2012), Phụ lục F.

C.9 Quản lý tham số an toàn nhạy cảm

C.9.1 Yêu cầu chung

Mô-đun mật mã sử dụng nhiều tham số trong việc thực thi và đảm bảo hiệu năng các dịch vụ của nó.

Các thông số này có thể yêu cầu hoặc không yêu cầu quản lý an toàn. Các tham số an toàn nhạy cảm cần được quản lý đúng cách để đảm bảo an toàn cho các tham số. Hình C.6 minh họa mối quan hệ giữa các tham số an toàn khác nhau liên quan đến chức năng an toàn được thực hiện.



Hình C.6 - Tổng quan về quản lý SSP

C.9.2 Mật khẩu so với khóa mã

Nói chung, thông tin nguồn ngẫu nhiên của mật khẩu ít hơn nhiều so với các khóa mã.

Do đó, không phải bất kỳ mật khẩu nào cũng có thể được sử dụng làm khóa mã theo TCVN 11295:2016 (ISO/IEC 19790:2012), trừ khi được nêu rõ ràng trong tiêu chuẩn thuật toán đã chọn của chức năng an toàn đã được phê duyệt.

Ví dụ: NIST SP 800-132, Khuyến nghị cho việc dẫn suất khóa dựa trên mật khẩu.

C.9.3 Entropy và hiểu biết của kẻ tấn công

Theo ISO/IEC 19790, mã hóa sử dụng bất kỳ bí mật chung không được coi là được bảo vệ bằng mật mã. Tương tự như vậy, nếu mầm của thuật toán DRBG được nhập tại nhà máy trong trường hợp xấu nhất nhà sản xuất hiểu biết về mầm và sau đó có khả năng dự đoán đầu ra từ DRBG. Cần hiểu rằng những kẻ tấn công càng thu được nhiều thông tin, thì lượng entropy còn lại càng ít.

Trong trường hợp mô-đun phần mềm, nhà cung cấp có thể yêu cầu entropy khác không cho một phần thông tin (ví dụ: ID tiến trình) có thể có sẵn cho các tiến trình khác đang chạy trên hệ điều hành. Nếu kẻ tấn công có quyền truy cập vào hệ điều hành hoặc kiểm soát các quy trình khác, thì phần thông tin không thêm bất kỳ entropy nào.

RBG vật lý được triển khai bên trong thẻ thông minh và các số ngẫu nhiên từ RBG có thể là:

a) Được sử dụng bên trong thẻ;

b) Đầu ra của thẻ (ví dụ: như một thử thách).

Trong trường hợp trước đây, bí mật được giữ khi không có thực thể không đáng tin cậy bên trong thẻ và không cần phải xem xét các cuộc tấn công không xâm lấn. Trong trường hợp thứ hai, bí mật sẽ không được giữ khi số ngẫu nhiên được xuất ra.

C.9.4 Hệ thống phân cấp SSP

C.9.4.1 Yêu cầu chung

Như đã nêu trong các yêu cầu [09.03] và [09.25], mô-đun mật mã sẽ liên kết mọi SSP trong mô-đun với một thực thể. Thực thể có thể là một người, một nhóm, một vai trò hoặc một tiến trình.

C.9.4.2 Phân tách thông tin

Trong TCVN 11295:2016 (ISO/IEC 19790:2012), thuật ngữ "phân tách thông tin" được định nghĩa là một tiến trình mà khóa mã được chia thành nhiều khóa thành phần, chia sẻ riêng lẻ mà không có hiểu biết nào về khóa gốc, sau đó có thể được nhập vào hoặc xuất ra từ mô-đun mật mã bởi các thực thể riêng biệt và được kết hợp để tạo lại khóa mã ban đầu.

Ví dụ: Việc phân chia khóa 128-bit thành 64-bit trước đây và 64-bit mới hơn không được coi là phân tách thông tin.

Như đã nêu trong yêu cầu [09.22], để nhập hoặc xuất mỗi thành phần chính, một người vận hành khác phải tham gia. Ví dụ, người vận hành A được liên kết với thành phần chính 1 và người vận hành B được liên kết với thành phần chính 2. Trong TCVN 11295:2016 (ISO/IEC 19790:2012), không đề cập đến thực thể (hoặc người vận hành) nào có khả năng thiết kế lại khóa gốc. Dựa trên thiết kế của mô-đun mật mã, dịch vụ thiết kế lại khóa gốc có thể được chỉ định cho người vận hành A hoặc B, hoặc một thực thể khác hoặc một vai trò cụ thể khác.

C.9.5 Các vai trò được ủy quyền để quản lý SSPs

Cần có vai trò được ủy quyền trước khi sử dụng các chức năng an toàn đã được phê duyệt nếu các khóa mã và CSP được tạo, sửa đổi, tiết lộ hoặc thay thế.

Như đã nêu trong yêu cầu [09.20], kênh tin cậy là bắt buộc khi nhập CSP và dữ liệu xác thực vào hoặc xuất CSP và dữ liệu xác thực từ mô-đun mật mã cho mức an toàn 3 và 4. Như đã nêu trong yêu cầu [03.20], việc dựa trên danh tính xác thực là bắt buộc khi thực hiện các dịch vụ bằng kênh tin cậy.

Những yêu cầu này có vẻ mâu thuẫn. Để thiết lập một kênh tin cậy, người vận hành nhập dữ liệu xác thực. Tuy nhiên, dữ liệu xác thực nhập yêu cầu kênh tin cậy.

Ở đây, như một ngoại lệ, chức năng an toàn đã được phê duyệt có thể được sử dụng cho các tiến trình được sử dụng để xác thực (ví dụ: thuật toán đối xứng để chia sẻ bí mật, thuật toán phi đối xứng để xác thực), trước khi đảm nhận vai trò được ủy quyền.

C.9.6 Xóa trắng

C.9.6.1 Bản sao của SSP

Thông qua việc kiểm tra đặc điểm kỹ thuật mô-đun mật mã, Kiểm thử viên hiểu được vị trí nơi các SSP và bản sao của chúng ở lại tạm thời hoặc vĩnh viễn. Các vị trí có thể là thanh ghi khóa, CPU, cache, RAM, bộ đệm hoặc ổ cứng. Kiểm thử viên nên xác minh rằng các SSP được xóa trắng bằng cách kiểm thử thiết kế của các mô-đun mật mã.

C.9.6.2 Biểu hiện của thiết bị lưu trữ

C.9.6.2.1 Bộ nhớ flash

Các thiết bị bộ nhớ flash hiện nay sử dụng kỹ thuật "cân bằng hao mòn". Kết quả của "cân bằng hao mòn" là việc ghi đè dữ liệu cụ thể không phải lúc nào cũng có nghĩa là ghi đè vật lý, tức là giá trị dữ liệu mới được ghi vào địa chỉ bộ nhớ vật lý khác với địa chỉ bộ nhớ vật lý ban đầu nơi giá trị dữ liệu ban đầu được ghi. Nếu các thiết bị bộ nhớ sử dụng kỹ thuật "cân bằng hao mòn", Kiểm thử viên phải xác minh rằng các SSP được xóa trắng bằng cách kiểm thử thiết kế của các mô-đun mật mã.

Ví dụ: Kỹ thuật "cân bằng hao mòn" bị ngắt đối với địa chỉ bộ nhớ vật lý cụ thể lưu trữ các SSP.

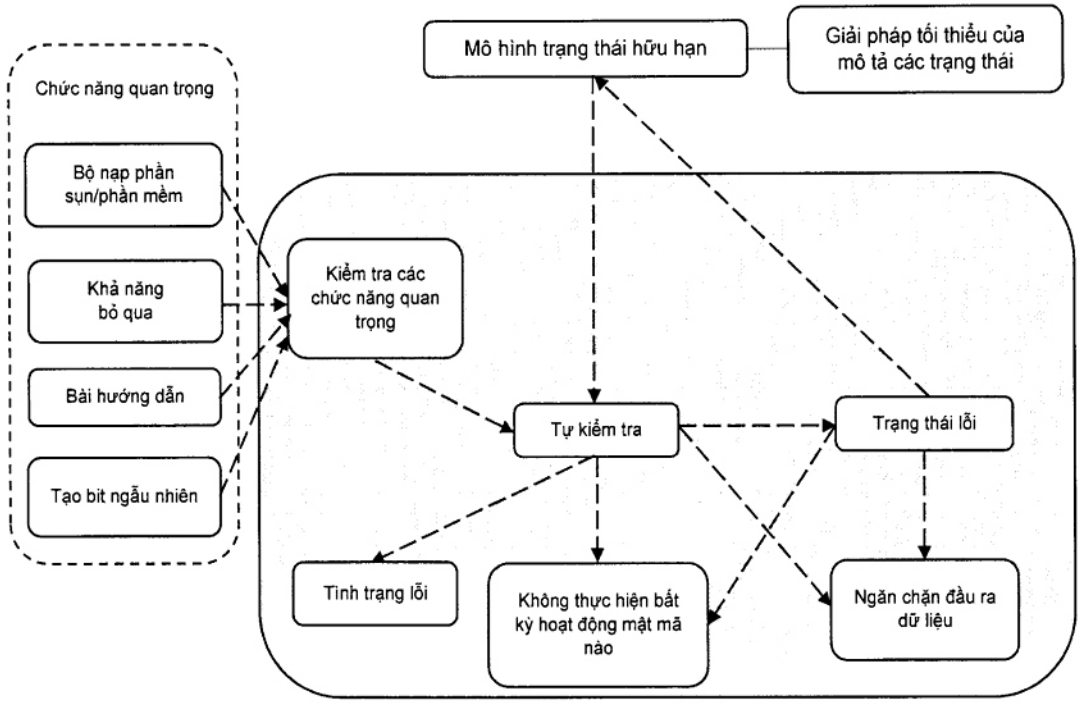
C.9.6.2.2 Ổ đĩa cứng

Tương tự đối với ổ cứng. Để đạt được khả năng ghi đè vật lý, việc định dạng lại và ghi đè phải được thực hiện ít nhất một lần.

C.10 Tự kiểm tra

C.10.1 Yêu cầu chung

TCVN 11295:2016 (ISO/IEC 19790:2012) quy định rằng một mô-đun thực hiện việc tự kiểm tra để đảm bảo hoạt động chính xác các chức năng của của mô-đun. Bản chất của mật mã là nếu một lỗi xảy ra trong một hoạt động mật mã, chẳng hạn như mã hóa, kết quả được mã hóa có thể không giải mã đúng cách để khôi phục dữ liệu bản rõ. Điều này sẽ dẫn đến mất dữ liệu. Các ví dụ khác về ảnh hưởng mà lỗi có thể gây ra là sai khóa mã được sử dụng cho một dịch vụ an toàn, xác thực không thành công hoặc mô-đun không phản ứng chính xác với một cuộc tấn công (ví dụ: vô hiệu hóa các tham số an toàn quan trọng). Hình C.7 minh họa các chức năng quan trọng được mô-đun sử dụng và mối quan hệ với các yêu cầu tự kiểm tra.



Hình C.7 - Tổng quan về tự kiểm tra

C.10.2 Các chức năng quan trọng

C.10.2.1 Khái niệm về các chức năng quan trọng

TCVN 11295:2016 (ISO/IEC 19790:2012) đề cập đến kiểm tra các chức năng quan trọng. Khi xem xét tính an toàn của mô-đun mật mã, các mục sau được coi là liên quan đến an toàn:

a) Tính toàn vẹn của phần mềm/phần sụn;
b) Tính đúng đắn của việc triển khai thuật toán mật mã;
c) Tính toàn vẹn của cặp khóa công khai và bí mật;
d) Tính toàn vẹn của (các) cơ chế bỏ qua;
e) Tính xác thực của phần mềm/phần sụn được nạp;
f) Tính toàn vẹn của các SSP được nhập thủ công.

C.10.2.2 Các chức năng quan trọng được xác định trước

Để đáp ứng các mục nêu trong C.10.2.1, các bài tự kiểm tra sau được đề cập trong TCVN 11295:2016 (ISO/IEC 19790:2012):

a) Kiểm tra tính toàn vẹn của phần mềm/phần sụn trước khi vận hành;
b) Tự kiểm tra thuật toán mật mã có điều kiện;
c) Kiểm thử có điều kiện tính nhất quán theo cặp;
d) Kiểm thử bỏ qua trước khi vận hành;
e) Kiểm thử bỏ qua có điều kiện;
f) Kiểm tra nạp phần mềm/phần sụn có điều kiện;
g) Kiểm tra đầu vào thủ công có điều kiện.

C.10.2.3 Các chức năng quan trọng do nhà cung cấp xác định

Các nhà cung cấp có thể yêu cầu kiểm tra các chức năng quan trọng khác ngoài việc tự kiểm tra đã đề cập trong tiêu chuẩn TCVN 11295:2016 (ISO/IEC 19790:2012).

Ví dụ 1: Nếu mô-đun mật mã nhúng một bộ tạo bit ngẫu nhiên vật lý, thì sức khỏe của nguồn entropy được sử dụng bên trong bộ tạo bit ngẫu nhiên vật lý sẽ rất quan trọng đối với hoạt động an toàn của mô-đun mật mã.

Ví dụ 2: Khi kiểm tra tính dư tuần hoàn (CRC - cyclic redundancy check) được áp dụng trong kiểm tra tính toàn vẹn của phần mềm/phần sụn, nên tính toàn vẹn của bộ đồng xử lý CRC được kiểm tra như một phần của kiểm tra chức năng quan trọng trước khi vận hành.

Ví dụ 3: Vì tính toàn vẹn và tính khả dụng của nội dung bộ nhớ được coi là rất quan trọng, một số mô-đun mật mã thực hiện kiểm tra chuẩn đoán bộ nhớ.

C.10.3 Kiểm tra tính toàn vẹn của phần mềm/chương trình cơ sở trước khi vận hành

C.10.3.1 Phạm vi kiểm tra tính toàn vẹn của phần mềm/phần sụn trước khi vận hành

Một mã thực thi được nạp vào một bộ nhớ không ổn định, thông qua một Bus hệ thống. Do lỗi môi trường, các cuộc tấn công tiêm lỗi hoặc các lý do khác, có khả năng xảy ra sửa đổi, thay thế mã thực thi được nạp. Kiểm tra tính toàn vẹn của phần mềm/chương trình cơ sở trước khi vận hành giúp bảo vệ chống lại hoặc giảm thiểu việc sửa đổi hoặc thay thế như vậy.

Như đã nêu trong các yêu cầu [02.16] và [02.17], việc khởi tạo mô-đun mật mã được lưu trong bộ nhớ được đưa vào bên trong ranh giới mật mã. Ở đây, tất cả các thành phần phần mềm và thành phần phần sụn trong ranh giới mật mã phải được kiểm tra tính toàn vẹn phần mềm/phần sụn trước khi vận hành, như đã nêu trong yêu cầu [10.17]. Từ các yêu cầu này, không chỉ tập hợp các tệp thực thi hoặc các tệp mà còn cả phần khởi tạo được lưu trong bộ nhớ đều phải kiểm tra tính toàn vẹn của phần mềm/chương trình cơ sở trước khi vận hành.

C.10.3.2 Sử dụng phiên bản rút gọn của mã xác thực thông báo đã được phê duyệt

Nhà cung cấp có thể chọn sử dụng phiên bản rút gọn của xác thực thông báo đã được phê duyệt để kiểm tra tính toàn vẹn của phần mềm/chương trình cơ sở trước khi hoạt động. Để xác nhận toàn vẹn một kỹ thuật đã được phê duyệt, nó không được chấp nhận sử dụng phiên bản bị rút gọn trừ khi phiên bản bị rút gọn được chấp thuận rõ ràng.

Liên quan đến tự kiểm tra thuật toán mật mã có điều kiện, nhà cung cấp có thể chọn không triển khai tự kiểm tra thuật toán mật mã riêng biệt cho thuật toán mật mã cơ bản được sử dụng cho kỹ thuật toàn vẹn đã được phê duyệt, nếu tất cả các chức năng mật mã của thuật toán mật mã cơ bản được kiểm tra.

Nếu phiên bản rút gọn của mã xác thực thông báo đã được phê duyệt sử dụng và nếu phần tự kiểm tra thuật toán mật mã riêng biệt bị bỏ qua đối với mã xác thực thông báo được phê duyệt và đối với các thuật toán mã hóa cơ bản của nó, thì có thể nói rằng phần bị rút gọn không bao giờ được kiểm tra thông qua kiểm tra các bài tự kiểm tra.

Điều này có thể trở thành một vấn đề đặc biệt là đối với việc triển khai phần cứng của các thuật toán mật mã.

C.10.3.3 Hoàn thiện một hay nhiều mã xác thực thông báo rời rạc

Như đã nêu trong yêu cầu [05.09], nhiều mã xác thực thông báo rời rạc hoặc chữ ký có thể được sử dụng trong kiểm tra tính toàn vẹn. Thiết kế cấu trúc bên trong của mô-đun mật mã ảnh hưởng đến việc hoàn thiện một hay nhiều mã xác thực thông báo rời rạc.

Ví dụ về hoàn thiện một hay nhiều mã xác thực thông báo rời rạc được hiển thị bên dưới.

Ví dụ 1: Bộ nạp bootstrap và phần mềm chính cung cấp dịch vụ được kết hợp thành một tệp nguyên khối và tệp nguyên khối được lưu trữ trong bộ nhớ ổn định trong phạm vi địa chỉ bộ nhớ cụ thể. Một mã xác thực thông báo bao trùm duy nhất được áp dụng cho tệp nguyên khối. Đầu tiên, bộ nạp bootstrap nạp phần sụn chính và tiếp theo phần sụn chính thực hiện kiểm tra tính toàn vẹn của bộ nạp bootstrap và phần sụn chính, dựa trên ảnh tệp và ảnh tiến trình. Mã xác thực thông báo dự kiến được lưu trong địa chỉ bộ nhớ cụ thể.

Ví dụ 2: Bộ nạp bootstrap và phần mềm chính cung cấp dịch vụ được lưu trữ riêng biệt trong các dải địa chỉ bộ nhớ khác nhau của bộ nhớ ổn định. Một mã xác thực thông báo được áp dụng cho bộ nạp bootstrap, một mã xác thực thông báo khác được áp dụng cho phần sụn chính và các mã xác thực thông báo dự kiến được lưu trữ trong các địa chỉ bộ nhớ cụ thể.

C.10.4 Tự kiểm tra thuật toán mật mã có điều kiện

Kiểm thử viên nên xác minh việc tự kiểm tra các thuật toán mật mã được thực hiện đúng cách.

Khi xem xét hoạt động điều chỉnh chức năng xác minh chữ ký số, chữ ký hợp lệ phải được xác nhận là hợp lệ và chữ ký không hợp lệ phải được xác nhận là không hợp lệ. Thuật toán mật mã tự kiểm tra để xác minh chữ ký số bao gồm cả chữ ký hợp lệ và chữ ký không hợp lệ dưới dạng các vectơ kiểm tra.

Một số mô-đun mật mã rút gọn các thông báo hoặc thẻ MAC. Nếu giữa thông báo bị rút gọn và thông báo không bị rút gọn được tính bằng mô-đun mã hóa, thì các phép tự kiểm tra sẽ kiểm tra các thông báo gốc (tức là không bị rút gọn).

C.10.5 Kiểm tra tính nhất quán theo cặp

Nói chung, có một số điều kiện cần được đáp ứng bởi mỗi cặp khóa phi đối xứng. Để đáp ứng các điều kiện đó, quá trình tạo cặp khóa phi đối xứng trở thành quá trình mật mã phức tạp và tốn thời gian hơn so với tạo khóa đối xứng.

Khi xem xét bản chất này của quá trình tạo cặp khóa bất đối xứng, kiểm tra tính nhất quán theo cặp dự định kiểm tra tính toàn vẹn của từng cặp khóa bất đối xứng bằng cách thực hiện việc triển khai (các) thuật toán mật mã khóa phi đối xứng với các cặp khóa được tạo.

C.11 Đảm bảo vòng đời

C.11.1 Yêu cầu chung

Đảm bảo vòng đời đề cập đến việc nhà cung cấp mô-đun mật mã sử dụng các phương pháp tốt nhất trong quá trình thiết kế, phát triển, vận hành và kết thúc vòng đời của mô-đun mật mã, cung cấp sự đảm bảo rằng mô-đun được thiết kế, phát triển, kiểm tra, cấu hình và phân phối đúng cách, được cài đặt và xử lý và cung cấp tài liệu hướng dẫn vận hành thích hợp. Các yêu cầu an toàn được chỉ định để quản lý cấu hình, mô hình trạng thái hữu hạn, phát triển, kiểm tra nhà cung cấp, phân phối và vận hành, kết thúc vòng đời và tài liệu hướng dẫn.

C.11.2 Quản lý cấu hình

Quản lý cấu hình chỉ định các yêu cầu đối với cấu hình hệ thống quản lý do nhà cung cấp mô-đun mật mã thực hiện, cung cấp sự đảm bảo rằng tính toàn vẹn của mô-đun mật mã được duy trì quy tắc cần phải có và kiểm soát trong các quá trình tinh chỉnh và sửa đổi mô-đun mật mã và tài liệu liên quan. Một hệ thống quản lý cấu hình được thiết lập để ngăn chặn các sửa đổi ngẫu nhiên hoặc trái phép và cung cấp khả năng thay đổi truy xuất nguồn gốc cho mô-đun mật mã và tài liệu liên quan.

C.11.3 *Mô hình trạng thái hữu hạn*

Hoạt động của mô-đun mật mã theo yêu cầu [11.08] phải được chỉ định bằng cách sử dụng mô hình trạng thái hữu hạn (hoặc tương đương) được biểu diễn bằng biểu đồ chuyển đổi trạng thái và bảng chuyển đổi trạng thái và các mô tả trạng thái.

FSM theo yêu cầu [11.09] phải đủ chi tiết để chứng minh rằng mô-đun mật mã tuân thủ tất cả các yêu cầu của TCVN 11295:2016 (ISO/IEC 19790:2012).

C.11.3.1 Độ chính xác tối thiểu của trạng thái

Yêu cầu [11.10] liệt kê một số trạng thái là độ chính xác tối thiểu của trạng thái. Lưu ý rằng các trạng thái được liệt kê không phải lúc nào cũng là các trạng thái tách biệt nhau.

Ví dụ 1: Trạng thái được phê duyệt có thể là trạng thái phụ của trạng thái chuyên viên mật mã hoặc trạng thái người dùng, khi một vai trò được ủy quyền được đảm nhận để thực hiện chức năng an toàn đã được phê duyệt.

Ví dụ 2: Trạng thái nhập CSP có thể là trạng thái phụ của trạng thái chuyên viên mật mã, khi chuyên viên mật mã đang nhập khóa bí mật hoặc các thành phần chính vào mô-đun mật mã.

Ví dụ 3: Có thể trạng thái mục nhập CSP không phải là trạng thái phụ của trạng thái chuyên viên mật mã hoặc trạng thái người dùng, khi dữ liệu xác thực được nhập vào trạng thái mục nhập CSP.

Yêu cầu [11.12] nêu rõ rằng mỗi dịch vụ mô-đun mật mã riêng biệt, sử dụng chức năng an toàn, trạng thái lỗi, tự kiểm tra hoặc xác thực người vận hành được mô tả như một trạng thái riêng biệt. Ví dụ, điều này có nghĩa là:

a) Một trạng thái được phê duyệt được chia nhỏ cho từng dịch vụ riêng biệt;
b) Trạng thái được chấp thuận là trạng thái phụ của trạng thái chuyên viên mật mã (hoặc tùy chọn của trạng thái người dùng);

Trạng thái nhập CSP trong đó đầu vào của thành phần khóa phân tách là trạng thái con của trạng thái thái chuyên viên mật mã.

C.11.3.2 Định nghĩa các trạng thái lỗi

TCVN 11295:2016 (ISO/IEC 19790:2012) đề cập đến lỗi "cứng" hoặc lỗi "mềm". Có thể khó xác định lỗi là lỗi “cứng” hay lỗi “mềm”. Nếu có các lỗi “mềm” liên tiếp, điều này cho thấy cần phải bảo trì hoặc sửa chữa. Các lỗi “mềm” liên tiếp như vậy có thể được coi là lỗi “cứng”.

C.11.4 Triển khai

C.11.4.1 Ánh xạ tới mô hình trạng thái hữu hạn

Sự phù hợp với các yêu cầu [11.16] đến [11.18] được kiểm tra từ khía cạnh của sự tương ứng giữa mã nguồn, sơ đồ hoặc HDL và mô hình trạng thái hữu hạn. Lưu ý rằng không phải lúc nào cũng có ánh xạ 1-1 giữa mỗi trạng thái và mỗi hàm/thủ tục trong mã nguồn.

Ví dụ 1: Nếu có một hàm/thủ tục chung được gọi từ nhiều trạng thái thì hàm/thủ tục được ánh xạ tới một phần của nhiều trạng thái.

Ví dụ 2: Có thể có một hàm hoặc thủ tục trong đó nhiều trạng thái cùng tồn tại (ví dụ: một trình phân tích lệnh cú pháp).

C.11.4.2 Công cụ và tính tự động

Yêu cầu [11.25] được đưa ra để có kết quả lặp lại được. Khi mô-đun mật mã triển khai chữ ký số đã được phê duyệt để kiểm tra tính toàn vẹn của phần mềm/phần sụn, thì cặp khóa bí mật hoặc công khai được sử dụng để tính toán chữ ký số đã được phê duyệt sẽ được tạo trong môi trường phát triển. Để xác nhận "chữ ký số được phê duyệt", cần có một mô-đun đã được xác thực để tạo cặp khóa. Do đó, mô-đun đã được xác thực là một phần của các công cụ phát triển cho các thành phần phần mềm hoặc phần sụn của mức an toàn 3 hoặc 4.

C.11.4.3 Mã, tham số và ký hiệu không cần thiết

Như đã nêu trong yêu cầu [11.26], tất cả phần mềm hoặc phần sụn phải được thiết kế và triển khai theo cách tránh việc sử dụng mã, tham số hoặc ký hiệu không cần thiết cho chức năng và việc thực thi của mô-đun. Yêu cầu này không chỉ đề cập đến mã/tham số/ký hiệu không cần thiết trong các cấp mã nguồn, mà còn trong các dạng thực thi.

Ví dụ 1: Các ký hiệu gỡ lỗi ở dạng thực thi có thể được sử dụng để gỡ lỗi.

Ví dụ 2: Các biến bên trong có thể được truy cập và sửa đổi từ bên ngoài ranh giới logic của mô-đun phần mềm, để chúng có thể được chia sẻ với các ứng dụng khác của mô-đun phần mềm.

CHÚ THÍCH: Khi xem xét các mô-đun mật mã giảm thiểu các cuộc tấn công không xâm lấn, có thể có các biến bên trong để ẩn hoặc che giấu trong mã nguồn của các mô-đun mật mã. Các thông số như vậy được coi là chức năng cần thiết cho mô-đun.

Kết hợp với yêu cầu [05.16], người kiểm tra nên kiểm tra các biểu mẫu có thể thực thi và xác minh rằng không có ký hiệu không cần thiết trong các biểu mẫu có thể thực thi.

C.11.4.4 Điều kiện trước và điều kiện sau

Điều kiện trước và điều kiện sau được giải quyết trong yêu cầu [11.28]. Nếu mức an toàn vật lý là 3 hoặc 4, thì EFT hoặc EFP là bắt buộc. Trong trường hợp này, điều kiện trước và điều kiện sau được thiết lập bằng cách xem xét các lỗi môi trường. Nếu mức an toàn vật lý là 4, thì cần phải bảo vệ khỏi các cuộc tấn công tiêm lỗi. Trong trường hợp này, điều kiện trước và điều kiện sau được thiết lập bằng cách xem xét các lỗi gây ra.

Khi xem xét mô-đun mật mã hỗ trợ các toán tử đồng thời, các mô-đun mật mã không biết trước khi nào một nhà khai thác yêu cầu dịch vụ số hóa. Khi xem xét mô-đun mật mã của mức an toàn vật lý 3 hoặc 4, mô-đun mật mã không biết trước khi nào có nỗ lực giả mạo mô-đun và mô-đun sẽ phản hồi. Các trường hợp như vậy được xem xét trong thiết kế mô-đun mật mã. Như đã nêu trong các yêu cầu [09.35] và [09.36], quá trình xóa trắng phải ngay lập tức, không gián đoạn và xảy ra trong thời gian đủ nhỏ. Mô-đun mật mã có thể không thực hiện được bài kiểm tra nếu không thể truy cập bộ nhớ nơi các SSP không được bảo vệ được lưu trữ bằng dịch vụ số hóa hoặc cơ chế phản hồi giả mạo, do sự không nhất quán giữa các điều kiện trước và sau và các trường hợp sử dụng có thể xảy ra.

Ví dụ: Kiểm soát loại trừ không thích hợp hoặc sự tắc nghẽn.

C.11.5 Đánh giá nhà cung cấp

C.11.5.1 Yêu cầu chung

Như đã nêu trong TCVN 11295:2016 (ISO/IEC 19790:2012), 7.11.6, mục đích của kiểm thử nhà cung cấp là cung cấp sự đảm bảo rằng mô-đun mật mã hoạt động phù hợp với chính sách an toàn mô-đun và các đặc điểm chức năng kỹ thuật. Tài liệu kiểm tra nhà cung cấp phải đề cập đến các mục sau:

a) Chính sách an toàn:
    1) Chính sách kiểm soát truy cập:
        i. Chính sách quản lý SSP;
        ii. Entropy;

2) Chính sách nhận dạng và xác thực:
    i. Chính sách được thực thi bởi mô-đun mật mã;
    ii. Việc thay thế dữ liệu xác thực mặc định;
3) Chính sách an toàn vật lý:
    i. Cơ chế phản ứng giả mạo;
4) Các quy tắc khác bắt nguồn từ TCVN 11295:2016 (ISO/IEC 19790:2012):
    i. Ức chế đầu ra dữ liệu ở trạng thái lỗi hoặc trong quá trình tự kiểm tra trước khi vận hành;
    ii. Ức chế đầu ra điều khiển ở trạng thái lỗi hoặc trong quá trình tự kiểm tra trước khi vận hành;
    iii. Mô hình trạng thái hữu hạn và chuyển đổi trạng thái:
        I. Không leo thang đặc quyền;
    iv. Cơ chế xóa trắng;
    v. Các chức năng tùy chọn:
        I. Hoạt động hạ cấp;
        II. Chức năng bỏ qua;
        III. Chức năng tự khởi tạo đầu ra mật mã;
5) Các quy tắc khác bắt nguồn từ các yêu cầu bổ sung do nhà cung cấp áp đặt:
    i. Hoạt động của mô-đun mật mã khi nhiều toán tử đồng thời được đăng nhập;
6) Chính sách giảm thiểu các cuộc tấn công khác;

b) Đặc điểm chức năng kỹ thuật:
1) Giao diện mô-đun mật mã:
    i. Vật lý;
    ii. Logical:
        I. Đầu vào dữ liệu;
        II. Kiểm soát đầu vào;
        III. Đầu ra dữ liệu;
        IV. Kiểm soát đầu ra;
        V. Trạng thái đầu ra.

Nếu kiểm thử phỏng đoán được chọn, có nhiều khía cạnh được đề cập trong bằng chứng cho kiểm thử nhà cung cấp:

- Kiểm thử tích cực;
- Kiểm thử không tích cực;
- Kiểm tra tham số;
- Xử lý lỗi chính xác;
- Quản lý tài nguyên chính xác;
- Phân tích tĩnh;
- Phân tích động.

Bằng chứng để đánh giá nhà cung cấp phải bao gồm:

- Các kịch bản để thực hiện mỗi bài đánh giá;
- Kết quả đánh giá dự kiến cho mỗi lần đánh giá;
- Kết quả kiểm tra thực tế cho mỗi lần đánh giá.

C.11.5.2 Đánh giá mức độ thấp

Mục đích của đánh giá mức độ thấp là cung cấp sự đảm bảo rằng mô-đun mật mã được kiểm thử ở mức thành phần của nó hoặc ở mức sâu hơn. TCVN 11295:2016 (ISO/IEC 19790:2012) không đưa ra các quy tắc cụ thể về mức độ chi tiết của đánh giá mức độ thấp. Do đó, một cách tiếp cận hiện có vẫn hữu ích (ví dụ: một tập hợp các bài đánh giá đơn vị và các bài đánh giá tích hợp). Tuy nhiên, cần có một quan điểm an toàn trong việc lấy ra các mục đánh giá.

C.11.6 Phân phối và vận hành

Các nhà cung cấp có thể yêu cầu sử dụng một nhà vận chuyển đáng tin cậy để đáp ứng yêu cầu phân phối an toàn.

Tuy nhiên, các điều kiện vận chuyển thay đổi theo thời gian, do đó yêu cầu hiện tại không phải được đáp ứng bởi hợp đồng mà do các nhà cung cấp tự đáp ứng.

C.11.7 Kết thúc vòng đời

Thời hạn sử dụng chỉ định các yêu cầu an toàn khi một mô-đun mật mã không còn được triển khai hoặc dự định để người vận hành sử dụng thêm. Tài liệu yêu cầu [11.36] chỉ rõ các thủ tục để làm sạch an toàn mô-đun mật mã. Vệ sinh là quá trình xóa thông tin nhạy cảm (ví dụ: SSP, dữ liệu người dùng, v.v.) khỏi mô-đun để có thể phân phối hoặc xử lý thông tin đó cho các nhà khai thác khác. Tùy thuộc vào mức an toàn, tài liệu [11.37] sẽ chỉ rõ các thủ tục cần thiết để phá hủy an toàn mô-đun.

C.11.8 Tài liệu hướng dẫn

Các tài liệu hướng dẫn nhằm đảm bảo rằng tất cả các thực thể sử dụng mô-đun mật mã đều có hướng dẫn và thủ tục đầy đủ để quản lý và sử dụng mô-đun trong một phương thức hoạt động đã được phê duyệt.

Tài liệu hướng dẫn phải bao gồm hướng dẫn của quản trị viên [11.38] và hướng dẫn không phải của quản trị viên [11.39].

C.12 Giảm thiểu các cuộc tấn công khác

Tính nhạy cảm của mô-đun mật mã đối với các cuộc tấn công không được định nghĩa trong TCVN 11295:2016 (ISO/IEC 19790:2012) phụ thuộc vào loại mô-đun, triển khai và môi trường thực hiện. Các cuộc tấn công như vậy có thể được quan tâm đặc biệt đối với các mô-đun mật mã được thực hiện trong các môi trường thù địch (ví dụ: nơi những kẻ tấn công có thể là người vận hành được ủy quyền của mô-đun). Các cuộc tấn công này thường dựa vào việc phân tích thông tin thu được từ các nguồn vật lý bên ngoài mô-đun. Trong mọi trường hợp, các cuộc tấn công cố gắng xác định một số kiến thức về CSP trong mô-đun mật mã.

Nếu mô-đun mật mã được thiết kế để giảm thiểu một hoặc nhiều (các) cuộc tấn công cụ thể không được định nghĩa ở nơi khác trong TCVN 11295:2016 (ISO/IEC 19790:2012), thì các tài liệu hỗ trợ của mô-đun sẽ [12.02] liệt kê (các) cuộc tấn công mà mô-đun được thiết kế để giảm thiểu và tùy thuộc vào mức mức an toàn, [12.04] phải chỉ định các phương pháp được sử dụng để giảm thiểu các cuộc tấn công và các phương pháp để kiểm tra tính hiệu quả của các kỹ thuật giảm thiểu.

Phụ lục D

(Tham khảo)

Yêu cầu về năng lực đối với trình xác nhận TCVN 11295:2016 (ISO/IEC 19790:2012)

Các chương trình xác nhận, thường hoạt động dưới sự bảo trợ của tổ chức công nhận, thường xem xét các kết quả kiểm thử do phòng thử nghiệm cung cấp. Đánh giá này có thể cung cấp phản hồi cho chương trình xác nhận để từ đó cho phép theo dõi năng lực của các phòng thử nghiệm cũng như tính nhất quán giữa các phòng thử nghiệm về các kỹ năng kiểm thử được xác định trong tiêu chuẩn này. Để thực hiện nhiệm vụ này, chúng tôi đặc biệt khuyến nghị: nhân sự thực hiện các đánh giá trong tổ chức công nhận phải có trình độ học vấn, kiến thức về các tiêu chuẩn và nhận thức được về các phương pháp thử nghiệm tương tự với tư cách là Kiểm thử viên trong phòng thử nghiệm.

Tài liệu tham khảo

[1]. National Institute of Standards and Technology, Special Publication 800-132, "*Recommendation for Password-Based Key Derivation*", December 2010.