



TIÊU CHUẨN QUỐC GIA

DỰ THẢO

TCVN 12211:2026
ISO/IEC 24759:2025

Xuất bản lần 2

**BẢO MẬT THÔNG TIN, AN NINH MẠNG
VÀ BẢO VỆ QUYỀN RIÊNG TƯ – CÁC YÊU CẦU KIỂM THỬ
CHO MÔ-ĐUN MẬT MÃ**

*Information security, cybersecurity and privacy protection — Test requirements for
cryptographic modules*

HÀ NỘI – 2026

Mục lục

Trang

Lời nói đầu	6
Lời giới thiệu	7
1 Phạm vi áp dụng.....	8
2 Tài liệu viện dẫn.....	8
3 Thuật ngữ và định nghĩa.....	8
4 Ký hiệu và thuật ngữ viết tắt	9
5 Bố cục tiêu chuẩn	9
5.1 Tổng quan	9
5.2 Các khẳng định và yêu cầu an toàn.....	10
5.3 Khẳng định có tham chiếu chéo.....	10
6 Các yêu cầu an toàn	10
6.1 Quy định chung	10
6.2 Đặc tả mô-đun mật mã	12
6.2.1 Yêu cầu chung về đặc tả mô-đun mật mã.....	12
6.2.2 Các loại mô-đun mật mã.....	12
6.2.3 Biên mật mã	13
6.2.4 Các hoạt động của mô-đun.....	24
6.3 Giao diện mô-đun mật mã	32
6.3.1 Yêu cầu chung về giao diện mô-đun mật mã.....	32
6.3.2 Các hạng mục giao diện	35
6.3.3 Đường dẫn tin cậy dạng rõ	46
6.3.4 Đường dẫn nội bộ được bảo vệ.....	49
6.4 Vai trò, dịch vụ và xác thực	50
6.4.1 Yêu cầu chung về vai trò, dịch vụ và xác thực	50
6.4.2 Vai trò	51
6.4.3 Dịch vụ	52
6.4.4 Xác thực	61
6.5 An toàn phần mềm/phần sụn.....	73
6.5.1 Yêu cầu chung về an toàn phần mềm/phần sụn	73
6.5.2 Mức an toàn 1	76
6.5.3 Mức an toàn 2.....	82
6.5.4 Mức an toàn 3 và 4.....	83
6.6 Môi trường hoạt động	85
6.6.1 Yêu cầu chung về môi trường hoạt động.....	85
6.6.2 Khả năng áp dụng của điều khoản.....	85
6.6.3 Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi	86
6.7 An toàn vật lý.....	99
6.7.1 Các hình thái an toàn vật lý	99
6.7.2 Yêu cầu chung về an toàn vật lý	100
6.7.3 Yêu cầu an toàn vật lý đối với từng hình thái an toàn vật lý	112
6.7.4 Bảo vệ chống/Thử nghiệm sự cố môi trường	118

6.7.5	Các tính năng bảo vệ chống sự cố môi trường.....	118
6.7.6	Các thủ tục thử nghiệm sự cố môi trường	120
6.8	An toàn không xâm lấn	122
6.8.1	Yêu cầu chung về an toàn không xâm lấn	122
6.8.2	Mức an toàn 1 và 2.....	123
6.8.3	Mức an toàn 3.....	123
6.8.4	Mức an toàn 4.....	124
6.9	Quản lý tham số an toàn nhạy cảm	124
6.9.1	Yêu cầu chung về quản lý tham số an toàn nhạy cảm	124
6.9.2	Các bộ tạo bit ngẫu nhiên	127
6.9.3	Tạo tham số an toàn nhạy cảm.....	128
6.9.4	Thiết lập tham số an toàn nhạy cảm tự động	129
6.9.5	Nhập và xuất tham số an toàn nhạy cảm	129
6.9.6	Lưu trữ tham số an toàn nhạy cảm	136
6.9.7	Xóa trắng tham số an toàn nhạy cảm	137
6.10	Tự kiểm thử	141
6.10.1	Yêu cầu chung về tự kiểm thử	141
6.10.2	Mức an toàn 3 và 4.....	146
6.10.3	Tự kiểm thử trước khi vận hành.....	147
6.10.4	Tự kiểm thử có điều kiện.....	151
6.11	Đảm bảo vòng đời	166
6.11.1	Yêu cầu chung về đảm bảo vòng đời	166
6.11.2	Quản lý cấu hình.....	166
6.11.3	Thiết kế	168
6.11.4	Mô hình trạng thái hữu hạn	168
6.11.5	Phát triển.....	173
6.11.6	Kiểm thử từ phía nhà cung cấp	179
6.11.7	Phân phối và hoạt động	181
6.11.8	Tài liệu hướng dẫn.....	185
6.12	Giảm thiểu các tấn công khác.....	186
6.12.1	Yêu cầu chung về giảm thiểu các tấn công khác.....	186
6.12.2	Mức an toàn 1, 2 và 3.....	186
6.12.3	Mức an toàn 4	186
7	Các yêu cầu về tài liệu.....	187
7.1	Mục đích.....	187
7.2	Các hạng mục	187
7.2.1	Đặc tả mô-đun mật mã	188
7.2.2	Giao diện mô-đun mật mã	188
7.2.3	Vai trò, dịch vụ và xác thực.....	189
7.2.4	An toàn phần mềm/phần sụn	190
7.2.5	Môi trường hoạt động	190
7.2.6	An toàn vật lý.....	191
7.2.7	An toàn không xâm lấn	192
7.2.8	Quản lý tham số an toàn nhạy cảm.....	192
7.2.9	Tự kiểm thử	193
7.2.10	Đảm bảo vòng đời.....	194

7.2.11	Giảm thiểu các tấn công khác	196
8	Chính sách an toàn cho mô-đun mật mã	197
8.1	Quy định chung	197
8.2	Các hạng mục	198
8.2.1	Quy định chung.....	198
8.2.2	Đặc tả mô-đun mật mã	198
8.2.3	Giao diện mô-đun mật mã	199
8.2.4	Vai trò, dịch vụ và xác thực.....	200
8.2.5	An toàn phần mềm/phần sụn.....	201
8.2.6	Môi trường hoạt động	201
8.2.7	An toàn vật lý.....	202
8.2.8	An toàn không xâm lấn	203
8.2.9	Quản lý tham số an toàn nhạy cảm.....	203
8.2.10	Tự kiểm thử	204
8.2.11	Đảm bảo vòng đời.....	205
8.2.12	Giảm thiểu các tấn công khác	205
	Thư mục tài liệu tham khảo	207

TCVN 12211:2026

Lời nói đầu

TCVN 12211:2026 hoàn toàn tương đương với ISO/IEC 24759:2025.

TCVN 12211:2026 do Ban Cơ yếu Chính phủ biên soạn, Bộ Quốc phòng đề nghị, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Trong công nghệ thông tin, nhu cầu sử dụng các cơ chế mật mã ngày càng gia tăng, chẳng hạn như để bảo vệ dữ liệu chống lại việc tiết lộ hoặc thao túng trái phép, để xác thực thực thể, và để chống chối bỏ. Tính an toàn và độ tin cậy của các cơ chế như vậy phụ thuộc trực tiếp vào các mô-đun mật mã nơi chúng được triển khai.

Tiêu chuẩn ISO/IEC 19790 cung cấp bốn mức độ yêu cầu an toàn định tính, tăng dần nhằm bao quát một phạm vi rộng các ứng dụng và môi trường tiềm năng. Các kỹ thuật mật mã là giống hệt nhau trên cả bốn Mức an toàn được định nghĩa trong tiêu chuẩn này. Các yêu cầu an toàn bao hàm các lĩnh vực liên quan đến việc thiết kế và triển khai một mô-đun mật mã. Các lĩnh vực này bao gồm:

- đặc tả mô-đun mật mã;
- giao diện mô-đun mật mã;
- vai trò, 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;
- tự kiểm thử;
- đảm bảo vòng đời; và
- giảm thiểu các tấn công khác.

Tiêu chuẩn này quy định các yêu cầu kiểm thử đối với các mô-đun mật mã tuân thủ tiêu chuẩn ISO/IEC 19790:2025.

BẢO MẬT THÔNG TIN, AN NINH MẠNG VÀ BẢO VỆ QUYỀN RIÊNG TƯ – CÁC YÊU CẦU KIỂM THỬ CHO MÔ – ĐUN MẬT MÃ

Information security, cybersecurity and privacy protection – Test requirements for cryptographic modules

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các phương pháp mà phòng thử nghiệm sử dụng để kiểm thử mô-đun mật mã có phù hợp với các yêu cầu quy định trong ISO/IEC 19790:2025 hay không. Các phương pháp này được xây dựng để đảm bảo mức độ khách quan cao trong quá trình kiểm thử và bảo đảm tính nhất quán giữa các phòng thử nghiệm.

Tiêu chuẩn này cũng quy định thông tin mà nhà cung cấp phải cung cấp cho phòng thử nghiệm làm chứng cứ chứng minh sự phù hợp của các mô-đun mật mã của họ với các yêu cầu quy định trong ISO/IEC 19790:2025.

Nhà cung cấp cũng có thể sử dụng tiêu chuẩn này để kiểm tra xem các mô-đun mật mã của họ có đáp ứng các yêu cầu quy định trong ISO/IEC 19790:2025 hay không trước khi đăng ký kiểm thử tại phòng thử nghiệm.

2 Tài liệu viện dẫn

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

ISO/IEC 19790:2025, *Information security, cybersecurity and privacy protection - Security requirements for cryptographic modules*

ISO/IEC 20085-1, *IT 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, *IT 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 và ISO/IEC 15408*

3 Thuật ngữ và định nghĩa

Trong tiêu chuẩn này, áp dụng các thuật ngữ và định nghĩa nêu trong ISO/IEC 19790 cùng với các thuật ngữ, định nghĩa nêu dưới đây.

3.1

chứng chỉ xác nhận (validation certificate)

khẳng định của tổ chức chứng nhận rằng một chức năng mật mã đã được kiểm thử và được xác định là một cách triển khai đúng của chức năng mật mã đích

3.2

cam kết của nhà cung cấp (vendor affirmation)

tuyên bố của nhà cung cấp khẳng định rằng một cách triển khai cụ thể của chức năng an toàn là đúng và đáp ứng tất cả các yêu cầu thích hợp từ các tiêu chuẩn liên quan, dựa trên các hoạt động bảo đảm nội bộ của chính họ

Chú thích 1: Từng tổ chức chứng nhận riêng biệt tự đặt ra các quy định về việc cam kết nào của nhà cung cấp được chấp nhận. Các tổ chức này tự xác định các yêu cầu về chứng cứ đối với một cam kết cụ thể của nhà cung cấp, và có thể yêu cầu một phòng thử nghiệm độc lập thẩm định cam kết đó.

4 Ký hiệu và thuật ngữ viết tắt

Trong tiêu chuẩn này, áp dụng các ký hiệu và thuật ngữ viết tắt sau.

ACL	access control list	danh sách kiểm soát truy cập
API	application programming interface	giao diện lập trình ứng dụng
CBC	cipher block chaining	chuỗi khối mã
CPLD	complex programmable logic device	thiết bị logic lập trình phức tạp
CSP	critical security parameter	tham số an toàn trọng yếu
ECB	electronic code book	sách mã điện tử
EDC	error detection code	mã phát hiện sai
EFP	environmental failure protection	bảo vệ chống sự cố môi trường
EFT	environmental failure testing	thử nghiệm sự cố môi trường
FPGA	field programmable gate array	mảng cổng lập trình được trên trường
FSM	finite state model	mô hình trạng thái hữu hạn
HDL	hardware description language	ngôn ngữ mô tả phần cứng
IC	integrated circuit	mạch tích hợp
PC	personal computer	máy tính cá nhân
PIN	personal identification number	số định danh cá nhân
PSP	public security parameter	tham số an toàn công khai
RBG	random bit generator	bộ tạo bit ngẫu nhiên
SSP	sensitive security parameter	tham số an toàn nhạy cảm

5 Bố cục tiêu chuẩn**5.1 Tổng quan**

Điều 6 quy định các phương pháp mà phòng thử nghiệm phải sử dụng và các yêu cầu đối với tài liệu mà nhà cung cấp phải cung cấp cho phòng thử nghiệm.

Các mục 6.2 đến 6.12 gồm mười một điều nhỏ, tương ứng với mười một lĩnh vực yêu cầu an toàn theo ISO/IEC

TCVN 12211:2026

19790:2025. Điều 7 tương ứng với Phụ lục A của ISO/IEC 19790:2025, và Điều 8 tương ứng với Phụ lục B của ISO/IEC 19790:2025.

Các Phụ lục C, D, E, F và G của ISO/IEC 19790:2025 hiện không bao gồm bất kỳ khẳng định nào và không được đề cập trong tiêu chuẩn này.

5.2 Các khẳng định và yêu cầu an toàn

Trong các Điều 6, 7 và 8, các yêu cầu an toàn tương ứng từ ISO/IEC 19790:2025 được trình bày từ Bảng 1 đến Bảng 429, mỗi bảng trình bày một khẳng định riêng lẻ (tức là các phát biểu phải đúng để mô-đun thoả mãn yêu cầu của một lĩnh vực nhất định ở một cấp độ nhất định).

Toàn bộ các khẳng định đều là trích dẫn trực tiếp từ ISO/IEC 19790:2025, tuy nhiên nội dung được trích dẫn trong mỗi bảng có thể là một phần của một câu hoặc một danh sách dài hơn mà không được sao chép lại toàn bộ trong tiêu chuẩn này. Vì lý do này, điều quan trọng là đối chiếu toàn bộ văn bản của ISO/IEC 19790:2025 để hiểu đầy đủ định nghĩa, ngữ cảnh và các điều kiện của từng khẳng định.

Các khẳng định được biểu thị theo định dạng:

AS {requirement_number}. {requirement_number}

trong đó "requirement_number" (số yêu cầu) là số hiệu của lĩnh vực tương ứng được quy định trong ISO/IEC 19790:2025 (tức là 1 đến 11 và A đến G), và "sequence_number" (số thứ tự) là định danh tuần tự cho các khẳng định trong một điều nhỏ.

Sau phát biểu của mỗi khẳng định, các mức an toàn mà khẳng định đó áp dụng (tức là các mức 1 đến 4) được liệt kê trong dấu ngoặc đơn.

Sau mỗi khẳng định trong bảng tương ứng có một tập hợp các yêu cầu đặt ra đối với nhà cung cấp. Các yêu cầu này mô tả những loại tài liệu hoặc thông tin cụ thể mà nhà cung cấp phải cung cấp để kiểm thử viên kiểm tra sự phù hợp với khẳng định đang xét. Các yêu cầu này được biểu thị theo định dạng:

VE {requirement_number}. {assertion_sequence_number}. {sequence_number}

trong đó "requirement_number" (số yêu cầu) và "assertion_sequence_number" (số thứ tự khẳng định) trùng với số yêu cầu và số thứ tự của khẳng định tương ứng, và "sequence_number" (số thứ tự) là định danh tuần tự cho các yêu cầu đối với nhà cung cấp trong phạm vi của yêu cầu khẳng định đó.

Sau mỗi khẳng định và các yêu cầu đặt ra cho nhà cung cấp trong bảng, có một tập hợp các yêu cầu đặt ra cho kiểm thử viên mô-đun mật mã. Các yêu cầu này hướng dẫn cho kiểm thử viên về những việc người đó phải làm để kiểm thử mô-đun mật mã đối với khẳng định đang xét. Các yêu cầu này được biểu thị theo định dạng:

TE {requirement_number}. {assertion_sequence_number}. {sequence_number}

trong đó "requirement_number" (số yêu cầu) và "assertion_sequence_number" (số thứ tự khẳng định) trùng với số yêu cầu và số thứ tự của khẳng định tương ứng, và "sequence_number" (số thứ tự) là định danh tuần tự cho các yêu cầu đối với kiểm thử viên trong phạm vi yêu cầu khẳng định đó.

Các bảng cung cấp các khẳng định AS, các yêu cầu đặt ra đối với nhà cung cấp VE, các yêu cầu đặt ra đối với kiểm thử viên TE, các chú thích nếu có và ví dụ nếu có.

Tổ chức chứng nhận được phép sửa đổi, bổ sung hoặc xoá bỏ các VE hoặc các TE, hoặc cả hai, trong tiêu chuẩn này.

5.3 Khẳng định có tham chiếu chéo

Để rõ ràng, đối với một số khẳng định, các tham chiếu chéo đến những khẳng định khác và các văn bản liên quan đã được cung cấp, và được đặt giữa hai dấu ngoặc nhọn "{" và "}".

6 Các yêu cầu an toàn

6.1 Quy định chung

Bảng 1 - VE và TE của AS01.01

Quy định chung - mức 1, 2, 3 và 4	
AS01.01 ISO/IEC 19790:2025, 7.1	Điều này quy định các yêu cầu an toàn mà các mô-đun mật mã phải tuân thủ.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 2 - VE và TE của AS01.02

Quy định chung - mức 1, 2, 3 và 4	
AS01.02 ISO/IEC 19790:2025, 7.1	Một mô-đun mật mã phải được kiểm thử theo các yêu cầu của từng lĩnh vực được đề cập trong điều này.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	
CHÚ THÍCH 1 Các phép kiểm thử có thể được thực hiện theo một hoặc nhiều phương thức sau: a) Kiểm thử viên thực hiện các phép kiểm thử tại cơ sở của kiểm thử viên. b) Kiểm thử viên thực hiện các phép kiểm thử tại cơ sở của nhà cung cấp. c) Kiểm thử viên giám sát nhà cung cấp thực hiện các phép kiểm thử tại cơ sở của nhà cung cấp. 1) Phân giải trình được đưa vào để giải thích lý do tại sao kiểm thử viên không thể thực hiện các phép kiểm thử. 2) Kiểm thử viên xây dựng kế hoạch kiểm thử bắt buộc và các phép kiểm thử bắt buộc. 3) Kiểm thử viên trực tiếp quan sát các phép kiểm thử đang được thực hiện. d) Kiểm thử viên có thể tham chiếu chứng cứ đã có về sự phù hợp (ví dụ, chứng chỉ của bên thứ ba hoặc báo cáo kiểm thử) khi được tổ chức chứng nhận liên quan hoặc tổ chức công nhận phòng thử nghiệm cho phép. CHÚ THÍCH 2 Một khẳng định không đạt nếu bất kỳ phép kiểm thử tiếp theo nào của nó không đạt. CHÚ THÍCH 3 Tổ chức công nhận đối với phòng thử nghiệm tham chiếu đến ISO/IEC TS 23532-2.	

Bảng 3 - VE và TE của AS01.03

Quy định chung - mức 1, 2, 3 và 4	
AS01.03 ISO/IEC 19790:2025, 7.1	Mức của mô-đun mật mã phải được xác định độc lập theo từng lĩnh vực.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 4 - VE và TE của AS01.04

Quy định chung - mức 1, 2, 3 và 4	
AS01.04 ISO/IEC 19790:2025 , 7.1	Toàn bộ tài liệu, bao gồm các bản sao tài liệu hướng dẫn sử dụng và hướng dẫn cài đặt, các đặc tả thiết kế và tài liệu về vòng đời, phải được cung cấp đối với mô-đun mật mã trải qua kiểm thử độc lập.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

6.2 Đặc tả mô-đun mật mã

6.2.1 Yêu cầu chung về đặc tả mô-đun mật mã

Bảng 5 - VE và TE của AS02.01

Yêu cầu chung về đặc tả mô-đun mật mã - mức 1, 2, 3 và 4	
AS02.01 ISO/IEC 19790:2025, 7.2.1	Một mô-đun mật mã phải là một tập hợp phần cứng, phần mềm, phần sụn, hoặc một sự kết hợp giữa chúng, tối thiểu thực thi một dịch vụ mật mã xác định bằng cách sử dụng một chức năng an toàn được phê duyệt hoặc một quy trình được phê duyệt như quy định trong Phụ lục C của ISO/IEC 19790:2025, và được chứa trong một biên mật mã đã được xác định.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 6 - VE và TE của AS02.02

Yêu cầu chung về đặc tả mô-đun mật mã - mức 1, 2, 3 và 4	
AS02.02 ISO/IEC 19790:2025, 7.2.1	Tài liệu về đặc tả mô-đun mật mã được quy định trong A.2.1, ISO/IEC 19790:2025 phải được cung cấp.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

6.2.2 Các loại mô-đun mật mã

Bảng 7 - VE và TE của AS02.03

Các loại mô-đun mật mã - mức 1, 2, 3 và 4	
AS02.03 ISO/IEC 19790:2025, 7.2.2	Một mô-đun mật mã phải được định nghĩa là mô-đun phần cứng, mô-đun phần sụn, mô-đun phần sụn lại ghép, mô-đun phần mềm, hoặc mô-đun phần mềm lại ghép.
Thông tin bắt buộc từ nhà cung cấp	
VE02.03.01	Nhà cung cấp phải cung cấp bản mô tả về mô-đun mật mã, trong đó nêu rõ loại mô-đun mật mã. Bản mô tả này sẽ giải thích cơ sở hợp lý của việc lựa chọn loại mô-đun đó.
VE02.03.02	Nhà cung cấp phải cung cấp bản đặc tả của mô-đun mật mã, trong đó xác định tất cả các thành phần phần cứng, phần mềm và phần sụn của mô-đun mật mã, nếu có.
Quy trình kiểm thử bắt buộc	
TE02.03.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp xác định một

	trong các loại mô-đun được liệt kê tại AS02.03.
TE02.03.02	Kiểm thử viên phải xem xét tài liệu của nhà cung cấp, nhận diện toàn bộ các thành phần phần cứng và phần mềm hoặc phần sụn (AS02.13 đến AS02.16), để xác minh rằng mô-đun phù hợp với loại mô-đun đã công bố.”

Bảng 8 - VE và TE của AS02.04

Các loại mô-đun mật mã - mức 1, 2, 3 và 4	
AS02.04 ISO/IEC 19790:2025, 7.2.2	Đối với các mô-đun phần cứng, phần sụn hoặc phần sụn lại ghép, các yêu cầu an toàn vật lý và an toàn không xâm lấn hiện hành, quy định tại 7.7 và 7.8 của ISO/IEC 19790:2025, phải được áp dụng.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

6.2.3 Biên mật mã**6.2.3.1 Yêu cầu chung về biên mật mã****Bảng 9 - VE và TE của AS02.05**

Biên mật mã - mức 1, 2, 3 và 4	
AS02.05 ISO/IEC 19790:2025, 7.2.3.1	Một biên mật mã phải gồm một vành đai được xác định rõ ràng (tức là tập hợp các thành phần phần cứng, phần mềm hoặc phần sụn) thiết lập nên ranh giới cho toàn bộ các thành phần của mô-đun mật mã.
Thông tin bắt buộc từ nhà cung cấp	
VE02.05.01	Tài liệu do nhà cung cấp cung cấp phải quy định rõ tất cả các thành phần nằm trong biên mật mã.
Quy trình kiểm thử bắt buộc	
TE02.05.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun mật mã để xác minh rằng tất cả các thành phần được quy định từ AS02.13 đến AS02.16 đều nằm trong biên mật mã.
TE02.05.02	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun mật mã để xác minh rằng không có thành phần nào chưa được nhận diện (tức là không được nêu trong AS02.13 đến AS02.16) nằm trong biên mật mã.

Bảng 10 - VE và TE của AS02.06

Biên mật mã - mức 1, 2, 3 và 4	
AS02.06 ISO/IEC 19790:2025, 7.2.3.1	Các yêu cầu của tiêu chuẩn này phải được áp dụng cho tất cả các chức năng an toàn, quy trình và thành phần nằm trong biên mật mã của mô-đun.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 11 - VE và TE của AS02.07

Biên mật mã - mức 1, 2, 3 và 4

TCVN 12211:2026

AS02.07 ISO/IEC 19790:2025, 7.2.3.1	Biên mật mã, tối thiểu, phải bao hàm tất cả các chức năng an toàn, quy trình và thành phần liên quan đến an toàn của một mô-đun mật mã như quy định tại Điều 7 trong ISO/IEC 19790:2025.
Thông tin bắt buộc từ nhà cung cấp	
VE02.07.01	Nhà cung cấp phải cung cấp danh mục tất cả các chức năng an toàn, quy trình và thành phần liên quan đến an toàn nằm trong biên mật mã.
Quy trình kiểm thử bắt buộc	
TE02.07.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp đã quy định và liệt kê rõ ràng tất cả các chức năng an toàn, quy trình và thành phần liên quan đến an toàn của mô-đun nằm trong biên mật mã.

Bảng 12 - VE và TE của AS02.08

Biên mật mã - mức 1, 2, 3 và 4	
AS02.08 ISO/IEC 19790:2025, 7.2.3.1	Các chức năng an toàn, quy trình hoặc thành phần không liên quan đến an toàn mà được sử dụng trong các dịch vụ đã phê duyệt phải được triển khai theo cách sao cho không gây trở ngại hoặc tổn hại đến hoạt động đã được phê duyệt của mô-đun mật mã.
Thông tin bắt buộc từ nhà cung cấp	
VE02.08.01	Tài liệu do nhà cung cấp cung cấp phải liệt kê các chức năng không liên quan đến an toàn được sử dụng trong một dịch vụ đã phê duyệt và chứng minh rằng chúng không gây trở ngại đến dịch vụ đã được phê duyệt của mô-đun.
Quy trình kiểm thử bắt buộc	
TE02.08.01	Kiểm thử viên phải xem xét tài liệu và kiểm tra mô-đun để xác minh rằng các chức năng không liên quan đến an toàn không gây trở ngại hoặc tổn hại đến dịch vụ đã được phê duyệt của mô-đun.
TE02.08.02	Kiểm thử viên phải xác minh tính đúng đắn của mọi giải trình do nhà cung cấp đưa ra về việc không gây trở ngại và không tổn hại đến dịch vụ. Trách nhiệm chứng minh thuộc về nhà cung cấp; nếu có bất kỳ sự không chắc chắn hoặc mơ hồ nào, kiểm thử viên phải yêu cầu nhà cung cấp bổ sung thông tin khi cần.

Bảng 13 - VE và TE của AS02.09

Biên mật mã - mức 1, 2, 3 và 4	
AS02.09 ISO/IEC 19790:2025, 7.2.3.1	Tên xác định của mô-đun mật mã phải phản ánh đúng tập hợp các thành phần nằm trong biên mật mã, không được phản ánh một tổ hợp hay sản phẩm lớn hơn.
Thông tin bắt buộc từ nhà cung cấp	
VE02.09.01	Nhà cung cấp phải cung cấp tên được định nghĩa của mô-đun.
Quy trình kiểm thử bắt buộc	
TE02.09.01	Kiểm thử viên phải xác minh rằng tên mô-đun do nhà cung cấp cung cấp phù hợp với cấu thành của các thành phần nằm trong biên mật mã.
TE02.09.02	Kiểm thử viên phải xác minh rằng tên mô-đun không đại diện cho một cách cấu thành các thành phần hoặc chức năng không phù hợp với cấu thành của các thành phần nằm trong biên mật mã.

Bảng 14 - VE và TE của AS02.10

Biên mật mã - mức 1, 2, 3 và 4	
AS02.10 ISO/IEC 19790:2025, 7.2.3.1	Mô-đun mật mã tối thiểu phải có thông tin phiên bản cụ thể đại diện cho từng thành phần phần cứng và phần mềm hoặc phần sụn riêng biệt, nếu có.
Thông tin bắt buộc từ nhà cung cấp	
VE02.10.01	Nhà cung cấp phải cung cấp thông tin phiên bản của từng thành phần phần cứng và phần mềm hoặc phần sụn riêng biệt của mô-đun.
Quy trình kiểm thử bắt buộc	
TE02.10.01	Kiểm thử viên phải xác minh rằng thông tin phiên bản đại diện cho từng thành phần phần cứng và phần mềm hoặc phần sụn riêng biệt của mô-đun.

Bảng 15 - VE và TE của AS02.11

Biên mật mã - mức 1, 2, 3 và 4	
AS02.11 ISO/IEC 19790:2025, 7.2.3.1	Các thành phần phần cứng, phần mềm hoặc phần sụn bị loại trừ phải được triển khai theo cách sao cho không gây trở ngại hoặc tổn hại đến hoạt động an toàn đã được phê duyệt của mô-đun mật mã.
Thông tin bắt buộc từ nhà cung cấp	
VE02.11.01	Nhà cung cấp phải mô tả các thành phần bị loại trừ của mô-đun và giải trình rằng các thành phần này sẽ không gây trở ngại đến hoạt động an toàn đã được phê duyệt của mô-đun.
VE02.11.02	Tài liệu do nhà cung cấp cung cấp phải đưa ra giải trình cho việc loại trừ từng thành phần. Trong giải trình phải mô tả cách thức mà từng thành phần bị loại trừ, khi hoạt động bình thường hoặc khi gặp sự cố, không được gây trở ngại đến hoạt động an toàn đã được phê duyệt của mô-đun. Giải trình có thể được chấp nhận, nếu được chứng minh đầy đủ bằng tài liệu, bao gồm các trường hợp sau: Thành phần đó không được kết nối với các thành phần liên quan đến an toàn của mô-đun theo cách có thể cho phép việc truyền tải không phù hợp các SSP, dữ liệu dạng rõ, hoặc thông tin khác có thể gây trở ngại đến hoạt động an toàn đã được phê duyệt của mô-đun. Tất cả thông tin được xử lý bởi thành phần đó chỉ được dùng cho mục đích nội bộ của mô-đun, và không ảnh hưởng dưới bất kỳ hình thức nào đến tính đúng đắn của các đầu ra điều khiển, trạng thái hoặc dữ liệu.
Quy trình kiểm thử bắt buộc	
TE02.11.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp để kiểm tra rằng các thành phần bị loại trừ nằm trong biên mật mã sẽ không gây trở ngại đến hoạt động an toàn đã được phê duyệt của mô-đun.
TE02.11.02	Kiểm thử viên phải xác minh tính đúng đắn của mọi giải trình về việc loại trừ do nhà cung cấp đưa ra. Trách nhiệm chứng minh thuộc về nhà cung cấp; nếu có bất kỳ sự không chắc chắn hoặc mơ hồ nào, kiểm thử viên phải yêu cầu nhà cung cấp bổ sung thông tin khi cần.
TE02.11.03	Kiểm thử viên phải can thiệp (ví dụ, để làm cho thành phần hoạt động không đúng như thiết kế) vào các thành phần bị loại trừ theo cách khiến thành phần bị loại trừ đó hoạt động không đúng. Kiểm thử viên phải xác minh rằng hoạt động không đúng của thành phần bị loại trừ không được gây trở ngại đến hoạt động an toàn đã phê duyệt của mô-đun.

	CHÚ THÍCH 1 Việc kiểm thử có thể dựa vào việc rà soát mã nguồn, tài liệu, hoặc cả hai, nếu các phương pháp hành vi hoặc vật lý làm cho thành phần bị loại trừ hoạt động không đúng là không khả thi hoặc không thực tế đối với một mô-đun cụ thể đó. Các phương pháp hành vi bao gồm việc sử dụng trình gỡ lỗi, công cụ thao tác/tiêm mã, bộ mô phỏng, hoặc công cụ khác để tác động đến dữ liệu có thể ảnh hưởng đến hành vi của một thành phần bị loại trừ; các phương pháp vật lý bao gồm việc nối tắt/tháo chân cắm và điều chỉnh điện áp. Việc kiểm thử được coi là không khả thi hoặc không thực tế khi các thao tác đó được hiểu là gây hỏng hóc vĩnh viễn cho mô-đun, hoặc cho hệ thống chứa mô-đun, mà không đạt được bất kỳ mục tiêu an toàn mong muốn nào ngoài việc chỉ đơn thuần làm cho toàn bộ mô-đun không thể hoạt động. CHÚ THÍCH 2 Các phép kiểm thử nhằm mục đích tập trung vào hoạt động an toàn của mô-đun và không tập trung vào các khía cạnh khác như độ tin cậy hoặc chất lượng, trừ khi chúng giúp chứng minh việc không gây trở ngại đến hoạt động an toàn đã được phê duyệt của mô-đun
--	---

Bảng 16 - VE và TE của AS02.12

Biên mật mã - mức 1, 2, 3 và 4	
AS02.12 ISO/IEC 19790:2025, 7.2.3.1	Mọi phần cứng, phần mềm hoặc phần sụn bị loại trừ nằm trong biên mật mã của mô-đun phải được quy định trong Phụ lục A của ISO/IEC 19790:2025 và được liệt kê trong chính sách an toàn của mô-đun theo Phụ lục B của ISO/IEC 19790:2025.
Thông tin bắt buộc từ nhà cung cấp	
VE02.12.01	Mọi thành phần bị loại trừ khỏi các yêu cầu an toàn phải được liệt kê một cách rõ ràng trong tài liệu do nhà cung cấp cung cấp theo quy định tại Phụ lục A của ISO/IEC 19790:2025.
VE02.12.02	Mọi thành phần bị loại trừ khỏi các yêu cầu an toàn phải được liệt kê một cách rõ ràng trong chính sách an toàn phi độc quyền.
Quy trình kiểm thử bắt buộc	
TE02.12.01	Kiểm thử viên phải xác minh dựa trên tài liệu do nhà cung cấp cung cấp xem nhà cung cấp có chỉ ra rằng bất kỳ thành phần nào của mô-đun bị loại trừ khỏi các yêu cầu của ISO/IEC 19790:2025 hay không.

6.2.3.2 Định nghĩa biên mật mã**Bảng 17 - VE và TE của AS02.13**

Biên mật mã - mức 1, 2, 3 và 4	
AS02.13 ISO/IEC 19790:2025, 7.2.3.2	Biên mật mã của một mô-đun mật mã phần cứng phải phân định và xác định: a) tập hợp các thành phần phần cứng, có thể bao gồm: 1) các cấu trúc vật lý, bao gồm bo mạch, đế hoặc bề mặt gá lắp khác cung cấp hệ dây dẫn vật lý liên kết giữa các thành phần; 2) các thành phần điện tích cực như mạch bán tích hợp, mạch tích hợp chuyên dụng hoặc mạch tích hợp thông thường, bộ xử lý, bộ nhớ, nguồn điện, bộ chuyển đổi, v.v.; và 3) các cấu trúc vật lý, như vỏ bọc, vật liệu đỡ keo hoặc đóng gói, đầu nối, và giao diện. b) một môi trường hoạt động (OE) bị hạn chế hoặc không thể sửa đổi được; c) phần sụn, có thể bao gồm một hệ điều hành; và

	d) các loại thành phần khác không được liệt kê tại a), b) hoặc c), (ví dụ, các tệp cấu hình cho CPLD).
Thông tin bắt buộc từ nhà cung cấp	
VE02.13.01	Toàn bộ các thành phần phần cứng của mô-đun mật mã phải được xác định trong tài liệu do nhà cung cấp cung cấp. Các thành phần được liệt kê phải bao gồm toàn bộ những nội dung sau đây: a) các cấu trúc vật lý, bao gồm bo mạch, đế hoặc bề mặt gá lắp khác cung cấp hệ dây dẫn vật lý liên kết giữa các thành phần: 4) các bo mạch, đế và bề mặt gá lắp; b) các thành phần điện tích cực như mạch bán tích hợp, mạch tích hợp chuyên dụng hoặc mạch tích hợp thông dụng, bộ xử lý, bộ nhớ, nguồn điện, bộ chuyển đổi, v.v.: 1) các bộ xử lý, bao gồm bộ vi xử lý, bộ xử lý tín hiệu số, bộ xử lý tùy chỉnh, bộ vi điều khiển, hoặc bất kỳ loại bộ xử lý nào khác (xác định rõ nhà sản xuất và loại); 2) các mạch tích hợp bộ nhớ chỉ đọc (ROM) dùng cho mã lệnh thực thi chương trình và dữ liệu [có thể bao gồm ROM lập trình bằng mặt nạ, ROM có thể lập trình (PROM) như PROM xoá được bằng tia cực tím (EPROM), PROM xoá được bằng điện (EEPROM), hoặc bộ nhớ Flash]; 3) bộ nhớ truy cập ngẫu nhiên (RAM) hoặc các mạch tích hợp khác dùng để lưu trữ dữ liệu tạm thời; 4) các mạch tích hợp bán tùy chỉnh, chuyên dụng, như mảng cổng, mảng logic lập trình được, mảng cổng lập trình được trên trường, hoặc các thiết bị logic lập trình được khác; 5) các mạch tích hợp hoàn toàn tùy chỉnh, chuyên dụng, bao gồm bất kỳ mạch tích hợp mật mã tùy chỉnh nào; 6) các thành phần nguồn điện, bao gồm bộ nguồn, bộ chuyển đổi nguồn (ví dụ, các mô-đun AC-to-DC hoặc DC-to-DC, máy biến áp), đầu nối nguồn vào và đầu nối nguồn ra; 7) các thành phần mạch điện tử tích cực khác (các thành phần mạch thụ động như điện trở kéo lên/kéo xuống hoặc tụ điện khử nhiễu không cần phải đưa vào nếu chúng không cung cấp chức năng liên quan đến an toàn như là một phần của mô-đun mật mã); c) các cấu trúc vật lý, như vỏ bọc, vật liệu đổ keo hoặc đóng gói, đầu nối, và giao diện: 1) các cấu trúc vật lý và vỏ bọc, bao gồm mọi cửa hoặc nắp truy cập có thể tháo rời; 2) vật liệu đổ keo hoặc đóng gói; 3) các đầu nối biên; 4) các đầu nối giữa các cụm con độc lập chính bên trong mô-đun;

	d) phần sụn, có thể bao gồm một hệ điều hành: 1) mã thực thi: i) không thể sửa đổi; ii) bị hạn chế; e) các loại thành phần khác không được liệt kê ở trên: 1) các bố trí làm mát hoặc sưởi ấm, chẳng hạn như tấm dẫn nhiệt, luồng khí làm mát, bộ trao đổi nhiệt, cánh tản nhiệt, quạt, bộ sưởi hoặc các bố trí khác để loại bỏ hoặc bổ sung nhiệt.
VE02.13.02	Tài liệu do nhà cung cấp cung cấp phải chỉ ra bố cục bên trong và các phương pháp lắp ráp (ví dụ, chất kẹp giữ hoặc phụ kiện gá lắp) của mô-đun, bao gồm các bản vẽ ít nhất phải xấp xỉ theo tỉ lệ.
VE02.13.03	Tài liệu do nhà cung cấp cung cấp phải mô tả các tham số vật lý chính của mô-đun, bao gồm các mô tả về vỏ bọc, các điểm truy cập, bo mạch, vị trí của nguồn điện, các tuyến đi dây liên kết, các bố trí làm mát và bất kỳ tham số quan trọng nào khác.
VE02.13.04	Tài liệu do nhà cung cấp cung cấp phải bao gồm một sơ đồ khối thể hiện biên mặt mã của mô-đun và quan hệ giữa các thành phần phần cứng.
VE02.13.05	Đối với mỗi bộ xử lý trong mô-đun, nhà cung cấp phải xác định, theo các dịch vụ chính, phần sụn được thực thi bởi bộ xử lý đó và các thiết bị nhớ chứa mã thực thi và dữ liệu.
VE02.13.06	Đối với mỗi bộ xử lý, nhà cung cấp phải xác định mọi phần cứng mà bộ xử lý đó giao tiếp.
Quy trình kiểm thử bắt buộc	
TE02.13.01	Kiểm thử viên phải xác định tất cả các thành phần phần cứng của mô-đun mặt mã. Các thành phần được liệt kê phải bao gồm các nội dung sau: a) các cấu trúc vật lý, bao gồm bo mạch, đế hoặc bề mặt gá lắp khác cung cấp hệ dây dẫn vật lý liên kết giữa các thành phần: 1) các bo mạch, đế và bề mặt gá lắp; b) các thành phần điện tích cực như mạch bán tích hợp, mạch tích hợp tùy biến hoặc mạch tích hợp thông thường, bộ xử lý, bộ nhớ, nguồn điện, bộ chuyển đổi, v.v.: 1) các bộ xử lý, bao gồm bộ vi xử lý, bộ xử lý tín hiệu số, bộ xử lý tùy chỉnh, bộ vi điều khiển, hoặc bất kỳ loại bộ xử lý nào khác (xác định rõ nhà sản xuất và loại); 2) các mạch tích hợp bộ nhớ chỉ đọc (ROM) dùng cho mã thực thi chương trình và dữ liệu [có thể bao gồm ROM lập trình bằng mặt nạ, PROM xóa được bằng điện (EEPROM), hoặc bộ nhớ Flash]; 3) bộ nhớ truy cập ngẫu nhiên (RAM) hoặc các mạch tích hợp khác dùng cho lưu trữ dữ liệu tạm thời; 4) các thành phần tùy chỉnh (ASIC), bán tùy chỉnh (FPGA, CPLD), hoặc có sẵn trên thị trường như mảng cổng, mảng logic lập trình được, mảng cổng logic lập trình được trên trường, hoặc các thiết bị logic lập trình được khác; 5) các mạch tích hợp hoàn toàn tùy chỉnh, chuyên dụng, bao gồm bất kỳ mạch tích hợp mặt mã tùy chỉnh nào.

	6) các thành phần nguồn điện, bao gồm nguồn, bộ chuyển đổi nguồn, (ví dụ, các mô-đun AC-sang-DC hoặc DC-sang-DC, máy biến áp), đầu nối nguồn vào và đầu nối nguồn ra; 7) các thành phần mạch điện tích cực khác (các thành phần mạch thụ động như điện trở kéo lên/kéo xuống hoặc tụ điện khử nhiễu không cần phải đưa vào nếu chúng không cung cấp chức năng liên quan đến an toàn như một phần của mô-đun mật mã; c) các cấu trúc vật lý, như là vỏ bọc, vật liệu đổ khuôn hoặc đóng gói, đầu nối, giao diện: 1) các cấu trúc vật lý và vỏ bọc, bao gồm mọi cửa hoặc nắp truy cập có thể tháo rời; 2) các vật liệu đổ keo hoặc đóng gói; 3) các đầu nối biên; 4) các đầu nối giữa các cụm lắp ráp con độc lập chính bên trong mô-đun; d) phần sụn, có thể bao gồm một hệ điều hành: 1) mã thực thi: i) không thể sửa đổi; ii) bị hạn chế; e) các loại thành phần khác không được liệt kê ở trên: 1) các bố trí làm mát hoặc sưởi ấm, chẳng hạn như tấm dẫn nhiệt, luồng khí làm mát, bộ trao đổi nhiệt, cánh tản nhiệt, quạt, bộ sưởi hoặc các bố trí khác để loại bỏ hoặc bổ sung nhiệt.
TE02.13.02	Kiểm thử viên phải xác minh rằng danh mục các thành phần phù hợp với thông tin được cung cấp cho các khẳng định khác của 6.2.3, như định nghĩa dưới đây. a) Đặc tả về biên mật mã theo khẳng định AS02.05. Xác minh rằng tất cả các thành phần bên trong biên mật mã đều được đưa vào danh mục thành phần và ngược lại. Đồng thời xác minh rằng mọi thành phần bên ngoài biên mật mã không được liệt kê là thành phần của mô-đun mật mã b) Đặc tả về sơ đồ khối theo khẳng định A.2.1 trong ISO/IEC 19790:2025. Xác minh rằng mọi thành phần riêng lẻ xác định trong sơ đồ khối (ví dụ, các bộ xử lý, mạch tích hợp chuyên dụng) cũng được liệt kê trong danh mục thành phần. c) Mọi thành phần được loại trừ khỏi các yêu cầu của ISO/IEC 19790:2025 theo quy định trong các khẳng định AS02.11 và AS02.12. Xác minh rằng các thành phần bị loại trừ vẫn được liệt kê trong danh mục thành phần.
TE02.13.03	Kiểm thử viên phải xác minh rằng biên mật mã liên tục về mặt vật lý, sao cho không có khe hở nào có thể cho phép đầu vào, đầu ra, hoặc sự truy cập khác không được kiểm soát vào mô-đun mật mã. Kiểm thử viên phải xác minh rằng, trong thiết kế mô-đun không có giao diện không được kiểm soát nào đi vào hoặc đi ra khỏi mô-đun mật mã. CHÚ THÍCH Bảo vệ vật lý và bảo vệ chống can thiệp được đề cập riêng trong các yêu cầu tại 7.7 của ISO/IEC 19790:2025.

TE02.13.04	Kiểm thử viên phải xác minh rằng biên mật mã bao trùm tất cả các thành phần được xác định trong sơ đồ khối theo khẳng định A.2.1 của ISO/IEC 19790:2025 là các thành phần thực hiện việc đưa vào, đưa ra, hoặc xử lý các SSP, dữ liệu dạng rõ, hoặc thông tin khác.
TE02.13.05	Như một ngoại lệ một phần đối với AS02.13, nhà cung cấp được phép loại trừ một số thành phần nhất định khỏi các yêu cầu của ISO/IEC 19790:2025 sau khi đáp ứng yêu cầu theo các khẳng định AS02.11 và AS02.12 trong 6.2.3. Kiểm thử viên phải xác minh rằng mọi giao diện hoặc kết nối vật lý giữa các phần tử bị loại trừ đó và phần còn lại của mô-đun không cho phép các hành vi sau đây: a) việc tiết lộ không được kiểm soát các tham số an toàn trọng yếu (CSP), dữ liệu dạng rõ, hoặc thông tin khác mà nếu bị sử dụng sai có thể dẫn đến sự tổn hại; b) các sửa đổi không được kiểm soát đối với các SSP hoặc thông tin khác có thể dẫn đến sự tổn hại.
TE02.13.06	Kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp thể hiện bố trí bên trong của mô-đun, bao gồm vị trí đặt và kích thước gần đúng của các thành phần chính có thể nhận biết của mô-đun. Điều này phải bao gồm các bản vẽ ít nhất phải gần đúng theo tỉ lệ.
TE02.13.07	Kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp chỉ ra các cụm lắp ráp vật lý chính của mô-đun và cách chúng được lắp ráp hoặc được đưa vào mô-đun.
TE02.13.08	Kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp mô tả các tham số vật lý chính của mô-đun. Mô tả này phải bao gồm ít nhất những nội dung sau: a) hình dạng và kích thước gần đúng của vỏ bọc, bao gồm mọi cửa hoặc nắp tiếp cận; b) kích thước gần đúng, bố trí, và các liên kết của bo mạch; c) vị trí của nguồn điện, các bộ chuyển đổi nguồn, và các đầu vào và đầu ra nguồn; d) các tuyến đi dây liên kết: định tuyến và các đầu cuối; e) các bố trí làm mát hoặc sưởi ấm, như tấm dẫn nhiệt, luồng khí làm mát, bộ trao đổi nhiệt, cánh tản nhiệt, quạt, bộ gia nhiệt, hoặc các bố trí khác để loại bỏ nhiệt khỏi mô-đun hoặc bổ sung nhiệt vào mô-đun; f) các loại thành phần khác không được liệt kê ở trên.
TE02.13.09	Kiểm thử viên phải xác minh rằng sơ đồ khối do nhà cung cấp cung cấp thể hiện biên mật mã của mô-đun và quan hệ của các thành phần phần cứng.
TE02.13.10	Kiểm thử viên phải xác minh tài liệu được cung cấp theo khẳng định AS02.02, tập trung vào sơ đồ khối mô tả toàn bộ các thành phần phần cứng chính của một mô-đun mật mã và liên kết giữa các thành phần, bao gồm mọi bộ vi xử lý, bộ đệm đầu vào/đầu ra, bộ đệm bản rõ/bản mã, bộ đệm điều khiển, lưu trữ khóa, bộ nhớ làm việc và bộ nhớ chương trình.
TE02.13.11	Kiểm thử viên phải xác minh rằng sơ đồ khối chỉ ra toàn bộ các liên kết và luồng dữ liệu đáng kể giữa các thành phần chính của mô-đun, và giữa mô-đun với thiết bị bên ngoài. Cụ thể, mỗi đường trên sơ đồ khối chỉ ra một liên kết phải được gán nhãn bằng loại thông tin mà đường đó truyền tải.
TE02.13.12	Kiểm thử viên phải xác minh rằng sơ đồ khối chỉ ra biên mật mã cho mô-đun mật mã, như được yêu cầu theo khẳng định này.
TE02.13.13	Kiểm thử viên phải xác minh rằng, đối với từng bộ xử lý, nhà cung cấp đã xác định các mô-đun mã phần mềm hoặc phần sụn được thực thi bởi bộ xử lý đó, các dịch vụ được thực hiện bởi bộ xử lý đó và mã liên quan, và các thiết bị nhớ chứa mã thực thi và dữ liệu.

TE02.13.14	Kiểm thử viên phải xác minh rằng, đối với từng bộ xử lý, nhà cung cấp đã xác định mọi phần cứng mà bộ xử lý đó giao tiếp. Nội dung này phải bao gồm, nếu có, mọi thành phần phần cứng cung cấp dữ liệu vào, dữ liệu điều khiển, hoặc dữ liệu trạng thái cho bộ xử lý và phần mềm/phần sụn liên quan, và mọi thành phần phần cứng nhận dữ liệu ra, dữ liệu điều khiển, hoặc dữ liệu trạng thái từ bộ xử lý và phần mềm/phần sụn liên quan. Các thành phần phần cứng đó có thể nằm trong mô-đun mật mã hoặc có thể là thiết bị người dùng bên ngoài mô-đun như các thiết bị đầu vào/đầu ra.
------------	---

Bảng 18 - VE và TE của AS02.14

Biên mật mã - mức 1, 2, 3 và 4	
AS02.14 ISO/IEC 19790:2025, 7.2.3.2	Biên mật mã của một mô-đun mật mã phần mềm phải phân định và xác định: a) tập hợp các tệp thực thi hoặc các tệp khác cấu thành nên mô-đun mật mã; và b) thể hiện của mô-đun mật mã được lưu trong bộ nhớ và được thực thi bởi một hoặc nhiều bộ xử lý.
Thông tin bắt buộc từ nhà cung cấp	
VE02.14.01	Toàn bộ các tệp phần mềm của mô-đun mật mã phải được xác định trong tài liệu do nhà cung cấp cung cấp. Các tệp phải được liệt kê bao gồm toàn bộ những nội dung sau đây: a) tập hợp tệp thực thi hoặc các tệp khác cấu thành nên mô-đun mật mã; b) các loại tệp liên quan đến an toàn khác không được liệt kê ở trên.
VE02.14.02	Tài liệu do nhà cung cấp cung cấp phải chỉ ra kiến trúc phần mềm bên trong, bao gồm cách các tệp phần mềm tương tác với nhau.
VE02.14.03	Tài liệu do nhà cung cấp cung cấp phải chỉ ra môi trường hoạt động (ví dụ, hệ điều hành, thư viện, thời gian chạy, v.v.) mà mô-đun thực thi trên đó.
Quy trình kiểm thử bắt buộc	
TE02.14.01	Kiểm thử viên phải xác minh rằng tài liệu bao gồm một danh mục tệp bao gồm toàn bộ các tệp phần mềm của mô-đun mật mã.
TE02.14.02	Kiểm thử viên phải xác minh rằng danh mục tệp bao gồm tất cả các tệp thuộc các loại sau đây, chỉ loại trừ các loại tệp không được sử dụng trong mô-đun: a) tập hợp tệp thực thi hoặc các tệp khác cấu thành nên mô-đun mật mã; b) các loại tệp an toàn khác không được liệt kê ở trên.
TE02.14.03	Kiểm thử viên phải xác minh rằng danh sách tệp phù hợp với thông tin được cung cấp cho các khẳng định khác của 6.2.3, như được định nghĩa dưới đây: a) Đặc tả của biên mật mã theo khẳng định AS02.05: Xác minh rằng tất cả các tệp bên trong biên mật mã đều được bao gồm trong danh mục tệp và ngược lại. Đồng thời xác minh rằng bất kỳ tệp nào bên ngoài biên mật mã đều không được liệt kê là các tệp của mô-đun mật mã. b) Đặc tả của phần mềm theo khẳng định A.2.1 của ISO/IEC 19790:2025: Xác minh rằng danh sách các tệp phần mềm giống với đặc tả theo khẳng định AS02.05. c) Đặc tả của sơ đồ khối theo khẳng định A.2.1 của ISO/IEC 19790:2025: Xác minh rằng bất kỳ tệp riêng lẻ nào được xác định trong sơ đồ khối cũng được liệt kê trong danh sách tệp.

	d) Bất kỳ tệp nào phải được loại trừ khỏi các yêu cầu của tiêu chuẩn ISO/IEC 19790:2025 theo các quy định của khẳng định AS02.13 và AS02.14: Xác minh rằng các tệp bị loại trừ vẫn được liệt kê trong danh sách tệp.
TE02.14.04	Như một ngoại lệ một phần đối với các yêu cầu trên, nhà cung cấp được phép loại trừ một số tệp nhất định khỏi các yêu cầu của tiêu chuẩn ISO/IEC 19790:2025 sau khi đáp ứng các yêu cầu thuộc các khẳng định AS02.11 và AS02.12 trong 6.2.3. Kiểm thử viên phải xác minh rằng bất kỳ giao diện hoặc kết nối vật lý nào giữa các tệp bị loại trừ đó và phần còn lại của mô-đun không cho phép: a) Việc tiết lộ không được kiểm soát các CSP, dữ liệu dạng rõ, hoặc thông tin khác mà nếu bị lạm dụng có thể dẫn đến sự tổn hại; b) Sự sửa đổi không được kiểm soát đối với các SSP hoặc thông tin khác có thể dẫn đến sự tổn hại an toàn.
TE02.14.05	Kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp chỉ ra các tệp phần mềm chính của mô-đun và cách chúng được liên kết với nhau để tạo thành mô-đun.

Bảng 19 - VE và TE của AS02.15

Biên mật mã - mức 1, 2, 3 và 4	
AS02.15 ISO/IEC 19790:2025, 7.2.3.2	Biên mật mã của một mô-đun mật mã phần sụn phải phân định và xác định: a) Tập hợp các tệp thực thi hoặc các tệp khác cấu thành nên mô-đun mật mã; và b) Thể hiện của mô-đun mật mã được lưu trong bộ nhớ và được thực thi bởi một hoặc nhiều bộ xử lý.
Thông tin bắt buộc từ nhà cung cấp	
VE02.15.01	Tất cả các tệp phần sụn của mô-đun mật mã phải được xác định trong tài liệu do nhà cung cấp cung cấp. Các tệp cần liệt kê phải bao gồm tất cả các thành phần sau: a) Tập hợp các tệp thực thi hoặc các tệp khác cấu thành nên mô-đun mật mã; b) Các loại tệp liên quan đến an toàn khác không được liệt kê ở trên.
VE02.15.02	Tài liệu do nhà cung cấp cung cấp phải chỉ ra kiến trúc phần sụn nội bộ, bao gồm cách các tệp phần sụn tương tác với nhau.
VE02.15.03	Tài liệu do nhà cung cấp cung cấp phải chỉ ra môi trường hoạt động (ví dụ: hệ điều hành, thư viện thời gian chạy/runtime) mà trên đó mô-đun thực thi.
VE02.15.04	Đối với mỗi bộ xử lý trong nền tảng máy tính của môi trường hoạt động được gắn với mô-đun phần sụn, nhà cung cấp phải xác định, theo các dịch vụ chính, phần sụn được thực thi bởi bộ xử lý và các thiết bị bộ nhớ chứa mã lệnh thực thi và dữ liệu.
VE02.15.05	Đối với mỗi bộ xử lý trong nền tảng máy tính của môi trường hoạt động được gắn với mô-đun phần sụn, nhà cung cấp phải xác định bất kỳ phần cứng nào mà bộ xử lý đó giao tiếp.
Quy trình kiểm thử bắt buộc	
TE02.15.01	Kiểm thử viên phải xác minh rằng tài liệu bao gồm một danh sách tệp chứa tất cả các tệp phần sụn của mô-đun mật mã.
TE02.15.02	Kiểm thử viên phải xác minh rằng danh sách tệp bao gồm tất cả các sự xuất hiện của các loại tệp sau, chỉ loại trừ các loại tệp không được sử dụng trong mô-đun:

	a) Tập hợp các tệp thực thi hoặc các tệp khác cấu thành nên mô-đun mật mã; b) Các loại tệp an toàn khác không được liệt kê ở mục a).
TE02.15.03	Kiểm thử viên phải xác minh rằng danh sách tệp nhất quán với thông tin được cung cấp cho các khẳng định khác của 6.2.3, như được định nghĩa dưới đây: a) Đặc tả của biên mật mã theo khẳng định AS02.07. Xác minh rằng tất cả các tệp bên trong biên mật mã đều được bao gồm trong danh sách tệp và ngược lại. Đồng thời xác minh rằng bất kỳ tệp nào bên ngoài biên mật mã đều không được liệt kê là các tệp của mô-đun mật mã. b) Đặc tả của phần sụn theo khẳng định A.2.1 trong ISO/IEC 19790:2025. Xác minh rằng danh sách các tệp phần sụn giống với các đặc tả theo khẳng định AS02.05. c) Đặc tả của sơ đồ khối theo khẳng định A.2.1 trong ISO/IEC 19790:2025. Xác minh rằng bất kỳ tệp riêng lẻ nào được xác định trong sơ đồ khối cũng được liệt kê trong danh sách tệp. d) Bất kỳ tệp nào phải được loại trừ khỏi các yêu cầu của tiêu chuẩn ISO/IEC 19790:2025 theo các quy định của khẳng định AS02.11 và AS02.12. Xác minh rằng các tệp bị loại trừ vẫn được liệt kê trong danh sách tệp.
TE02.15.04	Như một ngoại lệ một phần đối với các yêu cầu trên, nhà cung cấp được phép loại trừ một số tệp nhất định khỏi các yêu cầu của tiêu chuẩn ISO/IEC 19790:2025 sau khi đáp ứng các yêu cầu thuộc các khẳng định AS02.11 và AS02.12 trong 6.2.3. Kiểm thử viên phải xác minh rằng bất kỳ giao diện hoặc kết nối vật lý nào giữa các tệp bị loại trừ đó và phần còn lại của mô-đun không cho phép: a) Việc tiết lộ không được kiểm soát các CSP, dữ liệu dạng rõ, hoặc thông tin khác mà nếu bị sử dụng sai có thể dẫn đến sự tổn hại; b) Sự sửa đổi không được kiểm soát đối với các SSP hoặc thông tin khác có thể dẫn đến sự tổn hại.
TE02.15.05	Kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp chỉ ra các tệp phần sụn chính của mô-đun và cách chúng được liên kết với nhau để tạo thành mô-đun.
TE02.15.06	Kiểm thử viên phải xác minh tài liệu được cung cấp theo khẳng định AS02.02, tập trung vào sơ đồ khối mô tả tất cả các phần tử phần cứng chính của một mô-đun mật mã và các đường liên kết phần tử, bao gồm vi xử lý, bộ đệm đầu vào/đầu ra, bộ đệm dữ liệu dạng rõ/dữ liệu mã hóa, bộ đệm điều khiển, bộ nhớ lưu trữ khóa, bộ nhớ làm việc và bộ nhớ chương trình.
TE02.15.07	Kiểm thử viên phải xác minh rằng sơ đồ khối chỉ ra tất cả các đường liên kết quan trọng và luồng dữ liệu giữa các phần tử chính của mô-đun, cũng như giữa mô-đun và thiết bị bên ngoài. Đặc biệt, mỗi đường trên sơ đồ khối thể hiện một đường liên kết phải được dán nhãn với loại thông tin mà nó truyền tải.
TE02.15.08	Kiểm thử viên phải xác minh rằng sơ đồ khối chỉ ra biên mật mã cho mô-đun mật mã, theo yêu cầu của khẳng định này.
TE02.15.09	Kiểm thử viên phải xác minh rằng, đối với mỗi bộ xử lý trong nền tảng máy tính của môi trường hoạt động được gắn với mô-đun phần sụn, nhà cung cấp đã xác định các mô-đun mã phần sụn được thực thi bởi bộ xử lý đó, các dịch vụ được thực hiện bởi bộ xử lý đó cùng mã tương ứng, và các thiết bị bộ nhớ chứa mã thực thi và dữ liệu.
TE02.15.10	Kiểm thử viên phải xác minh rằng, đối với mỗi bộ xử lý trong nền tảng máy tính của

	môi trường hoạt động được gắn với mô-đun phần sụn, nhà cung cấp đã xác định bất kỳ phần cứng nào mà bộ xử lý đó giao tiếp. Điều này phải bao gồm, tùy từng trường hợp áp dụng, bất kỳ phần tử phần cứng nào cung cấp dữ liệu đầu vào, điều khiển, hoặc trạng thái cho bộ xử lý và phần sụn tương ứng, và bất kỳ phần tử phần cứng nào nhận dữ liệu đầu ra, điều khiển, hoặc trạng thái từ bộ xử lý và phần sụn tương ứng. Các phần tử phần cứng như vậy có thể nằm bên trong mô-đun mật mã hoặc có thể là thiết bị người dùng bên ngoài mô-đun như các thiết bị đầu vào/đầu ra.
--	---

Bảng 20 - VE và TE của AS02.16

Biên mật mã - mức 1, 2, 3 và 4	
AS02.16 ISO/IEC 19790:2025, 7.2.3.2	Biên mật mã của một mô-đun mật mã lai phải: a) là tổ hợp của thành phần phần cứng của mô-đun và các thành phần phần mềm hoặc phần sụn tách biệt; và b) bao gồm tập hợp tất cả các cổng và giao diện từ mỗi thành phần.
Thông tin bắt buộc từ nhà cung cấp	
VE02.16.01	Mô-đun mật mã phải được xác định trong tài liệu do nhà cung cấp cung cấp là một mô-đun phần mềm lai ghép hoặc một mô-đun phần sụn lai ghép. a) Đối với các thành phần của mô-đun phần mềm lai ghép, tài liệu của nhà cung cấp phải cung cấp thông tin được yêu cầu từ VE02.13.01 đến VE02.13.06 và từ VE02.14.01 đến VE02.14.03. b) Đối với các thành phần của mô-đun phần sụn lai ghép, tài liệu của nhà cung cấp phải cung cấp thông tin được yêu cầu từ VE02.13.01 đến VE02.13.06 và từ VE02.15.01 đến VE02.15.05.
Quy trình kiểm thử bắt buộc	
TE02.16.01	Kiểm thử viên phải xác minh rằng tài liệu xác định rõ mô-đun là một mô-đun phần mềm lai ghép hoặc một mô-đun phần sụn lai ghép. a) Đối với các thành phần của mô-đun phần mềm lai ghép, kiểm thử viên phải tuân thủ các quy trình được yêu cầu từ TE02.13.01 đến TE02.13.14 và từ TE02.14.01 đến TE02.14.05. b) Đối với các thành phần của mô-đun phần sụn lai ghép, kiểm thử viên phải tuân thủ các quy trình được yêu cầu từ TE02.13.01 đến TE02.13.14 và từ TE02.15.01 đến TE02.15.10.
CHÚ THÍCH Ngoài các thành phần phần mềm hoặc phần sụn tách biệt, thành phần phần cứng cũng có thể bao gồm phần mềm hoặc phần sụn nhúng.	

6.2.4 Các hoạt động của mô-đun**6.2.4.1 Yêu cầu chung về các hoạt động của mô-đun****Bảng 21 - VE và TE của AS02.17**

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.17 ISO/IEC 19790:2025, 7.2.4.1	Người vận hành phải có khả năng vận hành mô-đun bằng cách sử dụng các dịch vụ đã phê duyệt.
Thông tin bắt buộc từ nhà cung cấp	
VE02.17.01	Chính sách an toàn phi độc quyền do nhà cung cấp cung cấp phải đưa ra mô tả về

	các dịch vụ đã phê duyệt.
VE02.17.02	Chính sách an toàn phi độc quyền do nhà cung cấp cung cấp phải đưa ra các hướng dẫn để gọi các dịch vụ đã phê duyệt.
Quy trình kiểm thử bắt buộc	
TE02.17.01	Kiểm thử viên phải xác minh rằng chính sách an toàn phi độc quyền do nhà cung cấp cung cấp có chứa mô tả về các dịch vụ đã phê duyệt.
TE02.17.02	Kiểm thử viên phải gọi các dịch vụ đã phê duyệt bằng cách sử dụng các hướng dẫn do nhà cung cấp cung cấp có trong Chính sách an toàn phi độc quyền. Kiểm thử viên phải xác minh, bằng cách kiểm tra và từ tài liệu do nhà cung cấp cung cấp, rằng mô-đun mật mã sử dụng các dịch vụ đã phê duyệt khi được vận hành theo các hướng dẫn đã lập tài liệu.

Bảng 22 - VE và TE của AS02.18

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.18 ISO/IEC 19790:2025, 7.2.4.1	Một dịch vụ đã phê duyệt phải được định nghĩa là một dịch vụ bao gồm ít nhất một chức năng hoặc quá trình an toàn đã phê duyệt, và có thể bao gồm các chức năng hoặc quá trình không liên quan đến an toàn.
Thông tin bắt buộc từ nhà cung cấp	
VE02.18.01	Nhà cung cấp phải cung cấp một chứng chỉ xác nhận, nếu có, cho mỗi chức năng an toàn đã phê duyệt.
VE02.18.02	Nhà cung cấp phải cung cấp danh sách tất cả các chức năng an toàn không được phê duyệt.
VE02.18.03	Nhà cung cấp phải cung cấp danh sách tất cả các chức năng an toàn theo cam kết của nhà cung cấp.
VE02.18.04	Chính sách an toàn phi độc quyền do nhà cung cấp cung cấp phải bao gồm danh sách tất cả các chức năng an toàn theo cam kết của nhà cung cấp.
Quy trình kiểm thử bắt buộc	
TE02.18.01	Kiểm thử viên phải xác minh rằng nhà cung cấp đã cung cấp chứng chỉ xác nhận, nếu có, cho từng chức năng an toàn đã phê duyệt do một tổ chức chứng nhận cấp.
TE02.18.02	Kiểm thử viên phải xác minh rằng nhà cung cấp đã cung cấp danh sách các chức năng an toàn không được phê duyệt.
TE02.18.03	Kiểm thử viên phải xác minh rằng nhà cung cấp đã cung cấp danh sách các chức năng an toàn theo cam kết của nhà cung cấp.
TE02.18.04	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định rõ cách thức mà các chức năng an toàn theo cam kết của nhà cung cấp đã triển khai tuân thủ các tiêu chuẩn liên quan.

Bảng 23 - VE và TE của AS02.19

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.19 ISO/IEC 19790:2025, 7.2.4.1	Các chức năng và quá trình an toàn không được phê duyệt không được người vận hành sử dụng trong một dịch vụ đã phê duyệt trừ khi chức năng hoặc quá trình an toàn không được phê duyệt đó không liên quan đến an toàn đối với hoạt động của quá trình hoặc dịch vụ đã phê duyệt (ví dụ: một chức năng an toàn không được

	phê duyệt hoặc khóa được tạo bằng phương pháp không được phê duyệt có thể được dùng để làm xáo trộn dữ liệu hoặc các CSP, nhưng kết quả được coi là dữ liệu dạng rõ và không cung cấp tính năng liên quan đến an toàn nào cho đến khi nó được bảo vệ bằng một chức năng an toàn đã phê duyệt).
Thông tin bắt buộc từ nhà cung cấp	
VE02.19.01	Tài liệu do nhà cung cấp cung cấp phải xác định tất cả các chức năng hoặc quá trình an toàn không được phê duyệt được sử dụng cho mỗi dịch vụ hoặc quá trình đã phê duyệt.
VE02.19.02	Tài liệu do nhà cung cấp cung cấp phải đưa ra cơ sở lý luận về lý do tại sao các chức năng hoặc quá trình an toàn không được phê duyệt được sử dụng lại được coi là không liên quan đến an toàn đối với hoạt động của các quá trình hoặc dịch vụ đã phê duyệt. Cơ sở lý luận này phải giải quyết cách thức mà các CSP của thuật toán đã phê duyệt được giữ độc quyền cho các thuật toán đã phê duyệt trong dịch vụ và được bảo vệ khỏi các thuật toán không được phê duyệt trong cùng dịch vụ đó.
Quy trình kiểm thử bắt buộc	
TE02.19.01	Kiểm thử viên phải kiểm tra mô-đun để xác minh rằng tài liệu do nhà cung cấp cung cấp đã xác định tất cả các chức năng hoặc quá trình an toàn không được phê duyệt được sử dụng cho mỗi dịch vụ hoặc quá trình đã phê duyệt.
TE02.19.02	Kiểm thử viên phải xác minh tính đúng đắn của bất kỳ cơ sở lý luận nào do nhà cung cấp cung cấp. Trách nhiệm chứng minh thuộc về nhà cung cấp; nếu có bất kỳ sự không chắc chắn hoặc mơ hồ nào, kiểm thử viên phải yêu cầu nhà cung cấp cung cấp thêm thông tin khi cần thiết.

6.2.4.2 Hoạt động bình thường

Bảng 24 - VE và TE của AS02.20

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.20 ISO/IEC 19790:2025, 7.2.4.2	Các CSP phải được dùng riêng biệt cho dịch vụ đã phê duyệt và dịch vụ không được phê duyệt (ví dụ: không được dùng chung hoặc truy cập chéo).
Thông tin bắt buộc từ nhà cung cấp	
VE02.20.01	Nhà cung cấp phải cung cấp danh sách tất cả các CSP trong mô-đun và xác định mục đích sử dụng của chúng giữa các dịch vụ đã phê duyệt và không được phê duyệt.
VE02.20.02	Nhà cung cấp phải cung cấp mô tả về cách mỗi CSP được tách biệt giữa các dịch vụ đã phê duyệt và không được phê duyệt.
VE02.20.03	Nhà cung cấp phải cung cấp danh sách các CSP có thể được truy cập bởi cả dịch vụ đã phê duyệt và không được phê duyệt, đồng thời phải lập tài liệu về việc quyền truy cập chia sẻ đó không thể làm suy yếu an toàn của CSP hoặc làm tăng nguy cơ bị tổn hại của nó như thế nào.
Quy trình kiểm thử bắt buộc	
TE02.20.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp chứa mô tả về mục đích sử dụng của từng CSP giữa các dịch vụ đã phê duyệt và không được phê duyệt.
TE02.20.02	Kiểm thử viên phải kiểm tra mô-đun và xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng các CSP là độc quyền giữa các dịch vụ đã phê duyệt và không

	được phê duyệt.
TE02.20.03	Kiểm thử viên phải xác minh rằng bất kỳ CSP nào có thể được truy cập bởi cả dịch vụ đã phê duyệt và không được phê duyệt đều không thể làm suy yếu an toàn của CSP hoặc làm tăng nguy cơ bị tổn hại của nó.

Bảng 25 - VE và TE của AS02.21

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.21 ISO/IEC 19790:2025, 7.2.4.2	Chính sách an toàn của mô-đun phải định nghĩa tập hợp hoàn chỉnh các dịch vụ: đã phê duyệt, không được phê duyệt và không liên quan đến an toàn.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	
CHÚ THÍCH Tập hợp hoàn chỉnh các dịch vụ được định nghĩa là tất cả các dịch vụ do mô-đun cung cấp. Điều này bao gồm cả các dịch vụ đã phê duyệt và không được phê duyệt.	

Bảng 26 - VE và TE của AS02.22

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.22 ISO/IEC 19790:2025, 7.2.4.2	Mỗi dịch vụ phải cung cấp một chỉ báo đầu ra khi hoàn thành dịch vụ để chỉ ra liệu dịch vụ đó có thực thi một chức năng hoặc quá trình an toàn đã phê duyệt hay không.
Thông tin bắt buộc từ nhà cung cấp	
VE02.22.01	Tài liệu do nhà cung cấp cung cấp phải quy định rõ chỉ báo đầu ra cho từng dịch vụ.
VE02.22.02	Nếu một dịch vụ mã hóa đơn lẻ hỗ trợ cả độ mạnh của khóa đã phê duyệt và không được phê duyệt, hoặc các chức năng an toàn đã phê duyệt và không được phê duyệt, tài liệu do nhà cung cấp cung cấp phải mô tả cách chỉ báo đầu ra thay đổi để chỉ ra một dịch vụ đã phê duyệt hoặc không được phê duyệt.
Quy trình kiểm thử bắt buộc	
TE02.22.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp chứa mô tả về chỉ báo đầu ra chỉ ra liệu dịch vụ có thực thi một chức năng hoặc quá trình an toàn đã phê duyệt theo một phương thức đã phê duyệt hay không.
TE02.22.02	Kiểm thử viên phải thực thi tất cả các dịch vụ và xác minh rằng chỉ báo đầu ra cung cấp một dấu hiệu rõ ràng về việc liệu dịch vụ có sử dụng một chức năng hoặc quá trình an toàn đã phê duyệt theo một phương thức đã phê duyệt hay không.
TE02.22.03	Nếu một dịch vụ mã hóa đơn lẻ hỗ trợ cả độ mạnh của khóa đã phê duyệt và không được phê duyệt, hoặc các chức năng an toàn đã phê duyệt và không được phê duyệt, kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp mô tả cách chỉ báo đầu ra thay đổi để chỉ ra một dịch vụ đã phê duyệt hoặc không được phê duyệt.
TE02.22.04	Nếu một dịch vụ mã hóa đơn lẻ hỗ trợ cả độ mạnh của khóa đã phê duyệt và không được phê duyệt, kiểm thử viên phải thực thi dịch vụ với cả độ mạnh của khóa đã phê duyệt và không được phê duyệt, đồng thời xác minh rằng chỉ báo đầu ra thay đổi để chỉ ra một dịch vụ đã phê duyệt hoặc không được phê duyệt.
TE02.22.05	Nếu một dịch vụ mã hóa đơn lẻ hỗ trợ cả các chức năng hoặc quá trình an toàn đã phê duyệt và không được phê duyệt, kiểm thử viên phải thực thi dịch vụ với cả các chức năng hoặc quá trình an toàn đã phê duyệt và không được phê duyệt, đồng thời

	xác minh rằng chỉ báo đầu ra thay đổi để chỉ ra một dịch vụ đã phê duyệt hoặc không được phê duyệt.
--	---

6.2.4.3 Hoạt động suy giảm

Bảng 27 - VE và TE của AS02.23

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.23 ISO/IEC 19790:2025, 7.2.4.3	Để một mô-đun mật mã hoạt động ở chế độ hoạt động suy giảm, các điều kiện sau đây phải được áp dụng: {AS02.24 đến AS02.28}.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 28 - VE và TE của AS02.24

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.24 ISO/IEC 19790:2025, 7.2.4.3	chỉ được vào hoạt động suy giảm sau khi thoát khỏi một trạng thái lỗi;
Thông tin bắt buộc từ nhà cung cấp	
VE02.24.01	Nếu mô-đun mật mã cho phép hoạt động suy giảm, nhà cung cấp phải cung cấp mô tả về tất cả các hoạt động suy giảm sau khi thoát khỏi mỗi trạng thái lỗi.
VE02.24.02	Nhà cung cấp phải cung cấp đặc tả về hoạt động suy giảm. Đối với mỗi hoạt động suy giảm, đặc tả phải bao gồm: a) các điều kiện để vào và thoát khỏi hoạt động suy giảm; b) các chức năng, dịch vụ, hoặc quá trình an toàn đang hoạt động; c) các chức năng, dịch vụ, hoặc quá trình an toàn không hoạt động; d) các cơ chế, chức năng, hoặc thành phần bị cô lập trong hoạt động suy giảm; e) các kỹ thuật để cô lập các cơ chế, chức năng, hoặc thành phần; f) thông tin trạng thái được cung cấp trong hoạt động suy giảm; g) chỉ báo trạng thái trong trường hợp nếu có nỗ lực sử dụng một chức năng an toàn hoặc tiến trình không còn hoạt động.
Quy trình kiểm thử bắt buộc	
TE02.24.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp xác định rõ hoạt động suy giảm cũng như các điều kiện để vào và thoát khỏi nó.
TE02.24.02	Kiểm thử viên phải sử dụng tài liệu do nhà cung cấp cung cấp để kiểm tra rằng chỉ có thể truy cập hoạt động suy giảm sau khi thoát khỏi một trạng thái lỗi. Kiểm thử viên phải kiểm tra rằng chỉ báo trạng thái lỗi (xem AS03.11) được định vị chính xác.
TE02.24.03	Kiểm thử viên phải vận hành mô-đun mật mã, khiến nó hoạt động ở từng chế độ hoạt động suy giảm. Đối với mỗi hoạt động suy giảm, kiểm thử viên phải thử thực hiện một dịch vụ để xác minh rằng tất cả các tự kiểm thử chức năng an toàn có điều kiện đều được thực hiện trước lần sử dụng vận hành đầu tiên của bất kỳ chức năng an toàn nào.

TE02.24.04	Đầu tiên, kiểm thử viên phải vận hành mô-đun mật mã, khiến nó hoạt động ở từng chế độ hoạt động suy giảm. Tiếp theo, kiểm thử viên phải thực hiện tất cả các bài tự kiểm thử trước khi vận hành. Nếu mô-đun mật mã vượt qua tất cả các bài tự kiểm thử trước khi vận hành mà không có lỗi, kiểm thử viên sẽ xác minh rằng mô-đun mật mã thoát khỏi hoạt động suy giảm và quay trở lại hoạt động bình thường.
TE02.24.05	Đầu tiên, kiểm thử viên phải vận hành mô-đun mật mã, khiến nó hoạt động ở từng chế độ hoạt động suy giảm. Tiếp theo, kiểm thử viên phải thực hiện tất cả các bài tự kiểm thử trước khi vận hành gây ra điều kiện lỗi trong các tự kiểm thử trước khi vận hành. Kiểm thử viên phải xác minh rằng mô-đun mật mã không duy trì ở hoạt động suy giảm mà bước vào một trạng thái lỗi.

Bảng 29 - VE và TE của AS02.25

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.25 ISO/IEC 19790:2025, 7.2.4.3	Mô-đun phải cung cấp thông tin trạng thái khi được cấu hình lại và bước vào hoạt động suy giảm;
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS02.24.	

Bảng 30 - VE và TE của AS02.26

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.26 ISO/IEC 19790:2025, 7.2.4.3	cơ chế hoặc quá trình bị lỗi phải được cô lập;
Thông tin bắt buộc từ nhà cung cấp	
VE02.26.01	Yêu cầu về tài liệu do nhà cung cấp cung cấp được quy định tại VE02.24.02. Thiết kế của nhà cung cấp phải đảm bảo rằng bất kỳ sự cố nào từ các cơ chế, quá trình, và thành phần bị lỗi đều không thể gây trở ngại hoặc tổn hại đến hoạt động đã phê duyệt của mô-đun mật mã.
Quy trình kiểm thử bắt buộc	
TE02.26.01	Kiểm thử viên phải kiểm tra mô-đun và xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng các cơ chế, quá trình, và thành phần bị lỗi đã được cô lập trước khi bước vào hoạt động suy giảm.
TE02.26.02	Kiểm thử viên phải kiểm tra mô-đun và xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng các cơ chế, quá trình, và thành phần bị lỗi không thể gây trở ngại hoặc tổn hại đến hoạt động đã phê duyệt của mô-đun mật mã.

Bảng 31 - VE và TE của AS02.27

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.27 ISO/IEC 19790:2025, 7.2.4.3	Tất cả các bài tự kiểm thử thuật toán mật mã có điều kiện áp dụng được phải được thực hiện trước lần sử dụng vận hành đầu tiên của thuật toán mật mã sau khi bước vào hoạt động suy giảm;
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS02.24.	

Bảng 32 - VE và TE của AS02.28

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.28 ISO/IEC 19790:2025, 7.2.4.3	Các dịch vụ phải cung cấp một chỉ báo nếu có hành vi cố thử sử dụng cơ chế hoặc quá trình bị lỗi.
Thông tin bắt buộc từ nhà cung cấp	
VE02.28.01	Yêu cầu về tài liệu do nhà cung cấp cung cấp được quy định tại VE02.24.02. Thiết kế của nhà cung cấp phải đảm bảo rằng đầu ra của dịch vụ bao gồm một chỉ báo nếu có hành vi cố thử sử dụng cơ chế hoặc quá trình bị lỗi.
Quy trình kiểm thử bắt buộc	
TE02.28.01	Kiểm thử viên phải xác minh từ tài liệu của nhà cung cấp rằng các dịch vụ cung cấp các chỉ báo đã được lập tài liệu nếu có hành vi cố thử sử dụng cơ chế hoặc quá trình bị lỗi.
TE02.28.02	Kiểm thử viên phải vận hành mô-đun mật mã và xác minh rằng chỉ báo đã được lập tài liệu được cung cấp nếu có hành vi cố thử sử dụng cơ chế hoặc quá trình bị lỗi.

Bảng 33 - VE và TE của AS02.29

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.29 ISO/IEC 19790:2025, 7.2.4.3	Khi một lỗi cục bộ hóa được sử dụng, phải chỉ ra được rằng lỗi mục tiêu đó không thể tác động đến các dịch vụ đã phê duyệt khác đang chạy bên ngoài cơ chế hoặc quá trình bị cô lập.
Thông tin bắt buộc từ nhà cung cấp	
VE02.29.01	Tài liệu do nhà cung cấp cung cấp phải quy định rõ rằng lỗi cục bộ hóa không tác động đến các dịch vụ đã phê duyệt khác đang chạy bên ngoài cơ chế hoặc quá trình bị cô lập.
Quy trình kiểm thử bắt buộc	
TE02.29.01	Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp rằng lỗi mục tiêu không tác động đến các dịch vụ đã phê duyệt khác đang chạy bên ngoài cơ chế hoặc quá trình bị cô lập.
TE02.29.02	Kiểm thử viên phải vận hành mô-đun mật mã và xác minh rằng mô-đun hoạt động theo đúng tài liệu.
TE02.29.03	Kiểm thử viên phải kích hoạt các lỗi đối với mô-đun. Kiểm thử viên phải xác định xem một lỗi được kích hoạt là cục bộ hay không (tức là khiến toàn bộ mô-đun bước vào trạng thái lỗi).
TE02.29.04	Kiểm thử viên phải tiêm các lỗi vào mô-đun. Nếu kiểm thử viên xác định rằng một lỗi được tiêm là cục bộ, thì kiểm thử viên phải tiếp tục vận hành mô-đun để xác định rằng lỗi đó không lan truyền đến các dịch vụ đã phê duyệt khác đang chạy bên ngoài cơ chế hoặc quá trình bị cô lập.

Bảng 34 - VE và TE của AS02.30

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.30 ISO/IEC 19790:2025,	Mô-đun mật mã phải duy trì ở hoạt động suy giảm cho đến khi mô-đun mật mã lập lại các bài tự kiểm thử trước khi vận hành bao quát toàn bộ mô-đun hoặc các cơ chế và quá trình bị cô lập đã lỗi.

7.2.4.3	
Thông tin bắt buộc từ nhà cung cấp	
VE02.30.01	Tài liệu do nhà cung cấp cung cấp phải quy định rõ rằng mô-đun mật mã duy trì ở hoạt động suy giảm cho đến khi mô-đun mật mã lập lại các bài tự kiểm thử trước khi vận hành.
VE02.30.02	Tài liệu do nhà cung cấp cung cấp phải quy định rõ những tự kiểm thử trước khi vận hành nào là cần thiết để thoát khỏi trạng thái suy giảm đối với mọi cơ chế hoặc quá trình bị cô lập được định nghĩa.
Quy trình kiểm thử bắt buộc	
TE02.30.01	Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp rằng mô-đun mật mã duy trì ở hoạt động suy giảm cho đến khi mô-đun mật mã lập lại các bài tự kiểm thử trước khi vận hành.
TE02.30.02	Kiểm thử viên phải vận hành mô-đun mật mã và xác minh rằng mô-đun hoạt động theo đúng tài liệu.
TE02.30.03	Sau khi kiểm thử viên đã tiêm một lỗi và mô-đun chuyển sang trạng thái suy giảm, kiểm thử viên phải khiến mô-đun khởi tạo các bài tự kiểm thử trước khi vận hành cho toàn bộ mô-đun và xác định rằng mô-đun chuyển từ trạng thái suy giảm sang trạng thái không suy giảm.
TE02.30.04	Sau khi kiểm thử viên đã tiêm một lỗi và mô-đun chuyển sang trạng thái suy giảm, kiểm thử viên phải thực thi các bài tự kiểm thử trước khi vận hành chỉ dành riêng cho các cơ chế và quá trình bị cô lập đã lỗi, và xác định xem mô-đun có chuyển từ trạng thái suy giảm sang trạng thái không suy giảm hay không.

Bảng 35 - VE và TE của AS02.31

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.31 ISO/IEC 19790:2025, 7.2.4.3	Khi chỉ một tập con các bài tự kiểm thử trước khi vận hành được chạy lại trước khi thoát khỏi hoạt động suy giảm, phải chứng minh được tại sao không cần thiết phải chạy lại các bài tự kiểm thử bị loại trừ.
Thông tin bắt buộc từ nhà cung cấp	
VE02.31.01	Tài liệu của nhà cung cấp phải chứng minh lý do tại sao không cần thiết phải chạy lại các bài tự kiểm thử bị loại trừ khi chỉ một tập con các tự kiểm thử trước khi vận hành được chạy lại trước khi thoát khỏi hoạt động suy giảm.
Quy trình kiểm thử bắt buộc	
TE02.31.01	Kiểm thử viên phải xem xét tài liệu của nhà cung cấp để đảm bảo rằng, khi các bài tự kiểm thử trước khi vận hành chạy lại trước khi thoát khỏi hoạt động suy giảm chỉ bao quát một tập con các bài kiểm thử được thực hiện lúc bật nguồn, thì không yêu cầu phải chạy lại các tự kiểm thử bị loại trừ.
TE02.31.02	Kiểm thử viên phải vận hành mô-đun mật mã và xác minh rằng mô-đun hoạt động theo đúng tài liệu.
TE02.31.03	Sau khi kiểm thử viên chỉ chạy tập con các bài tự kiểm thử, kiểm thử viên phải cho mô-đun hoạt động bình thường trong một khoảng thời gian đủ dài, sử dụng tất cả các dịch vụ của mô-đun, để xác định rằng lỗi ở các khu vực bị cô lập đã không lan truyền sang các khu vực khác của mô-đun.

Bảng 36 - VE và TE của AS02.32

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.32 ISO/IEC 19790:2025, 7.2.4.3	Nếu mô-đun mật mã vượt qua tất cả các tự kiểm thử trước khi vận hành trong khi ở hoạt động suy giảm, mô-đun phải thoát khỏi hoạt động suy giảm.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS02.24.	

Bảng 37 - VE và TE của AS02.33

Các hoạt động của mô-đun - mức 1, 2, 3 và 4	
AS02.33 ISO/IEC 19790:2025, 7.2.4.3	Nếu mô-đun mật mã không vượt qua các tự kiểm thử trước khi vận hành trong khi ở hoạt động suy giảm, mô-đun phải bước vào một trạng thái lỗi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS02.24.	

6.3 Giao diện mô-đun mật mã

6.3.1 Yêu cầu chung về giao diện mô-đun mật mã

Bảng 38 - VE và TE của AS03.01

Yêu cầu chung về giao diện mô-đun mật mã - mức 1, 2, 3 và 4	
AS03.01 ISO/IEC 19790:2025, 7.3.1	Một mô-đun mật mã phải hạn chế tất cả luồng thông tin logic chỉ trong những điểm truy cập vật lý và các giao diện logic được xác định là điểm vào và điểm ra đến và từ biên mật mã của mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE03.01.01	Tài liệu do nhà cung cấp cung cấp phải quy định rõ từng cổng vật lý và giao diện logic của mô-đun mật mã, bao gồm các nội dung sau: a) các cổng vật lý và sự phân bổ chân cắm của chúng; b) các nắp che, cửa, hoặc khe hở vật lý; c) các giao diện logic (ví dụ: API và tất cả các tín hiệu dữ liệu/điều khiển/trạng thái khác) cùng tên và chức năng của tín hiệu; d) các điều khiển thủ công (ví dụ: nút bấm hoặc công tắc) đối với các đầu vào điều khiển vật lý có thể áp dụng; e) các chỉ báo trạng thái vật lý (ví dụ: đèn hoặc màn hình hiển thị) đối với các đầu ra trạng thái vật lý có thể áp dụng; f) sự ánh xạ các giao diện logic tới các cổng vật lý, các điều khiển thủ công, và các chỉ báo trạng thái vật lý của mô-đun mật mã; g) các đặc tính vật lý, logic và điện, nếu có thể áp dụng, của các cổng và giao diện được chỉ định từ a) đến f).
VE03.01.02	Tài liệu do nhà cung cấp cung cấp phải quy định rõ các luồng thông tin và các điểm truy cập vật lý của mô-đun mật mã bằng cách làm nổi bật hoặc chú thích vào các bản sao của sơ đồ khối, đặc tả thiết kế, và mã nguồn cũng như sơ đồ mạch, nếu phù hợp, được cung cấp trong mục 6.2 và 6.11. Nhà cung cấp cũng phải cung cấp bất kỳ tài liệu nào khác cần thiết để quy định rõ mối quan hệ của các luồng thông tin và điểm

	truy cập vật lý với các cổng vật lý và giao diện logic. Nhà cung cấp phải đảm bảo thông tin trên nhất quán với thông tin được cung cấp ở các khẳng định AS02.05 và AS02.13 đến AS02.16, không có mâu thuẫn nào trong việc mô tả các thành phần và bố cục vật lý cho các cổng đầu vào/đầu ra.
VE03.01.03	Đối với mỗi đầu vào vật lý hoặc logic vào mô-đun mật mã, hoặc đầu ra vật lý và logic từ mô-đun, tài liệu của nhà cung cấp phải quy định rõ giao diện logic mà đầu vào hoặc đầu ra vật lý đó thuộc về, và cổng vào/ra vật lý. Các đặc tả được cung cấp phải nhất quán với các đặc tả của các thành phần mô-đun mật mã được nêu tại ISO/IEC 19790:2025, 7.2 và 7.11, và các đặc tả của các giao diện logic được nêu trong các khẳng định AS03.04 đến AS03.13 của mục 6.3.2.
Quy trình kiểm thử bắt buộc	
TE03.01.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định rõ từng cổng vật lý và giao diện logic của mô-đun mật mã. Các đặc tả bắt buộc phải bao gồm: a) tất cả các cổng đầu vào và đầu ra vật lý, bao gồm sự phân bổ chân cắm của chúng, vị trí vật lý bên trong mô-đun, tóm tắt về các tín hiệu logic chạy qua mỗi cổng, và trình tự định thời của các luồng tín hiệu nếu có hai hoặc nhiều tín hiệu dùng chung một chân cắm vật lý; b) tất cả các nắp che, cửa, hoặc khe hở vật lý, bao gồm vị trí vật lý của chúng bên trong mô-đun mật mã, và các thành phần hoặc chức năng có thể được truy cập hoặc sửa đổi thông qua mỗi nắp che/cửa/khe hở đó; c) tất cả các giao diện đầu vào và đầu ra logic (ví dụ: API và tất cả các tín hiệu dữ liệu/điều khiển/trạng thái khác), bao gồm danh sách hoặc sơ đồ khối có chú thích về tất cả các đầu vào dữ liệu và điều khiển logic, cũng như các đầu ra dữ liệu và trạng thái của mô-đun mật mã, cùng danh sách và mô tả về tên và chức năng của các tín hiệu; d) tất cả các điều khiển thủ công được sử dụng để nhập tín hiệu điều khiển vật lý, chẳng hạn như công tắc hoặc nút bấm, bao gồm vị trí vật lý của chúng bên trong mô-đun mật mã, cùng danh sách và mô tả về các tín hiệu điều khiển có thể được nhập thủ công; e) tất cả các chỉ báo trạng thái vật lý, bao gồm vị trí vật lý của chúng bên trong mô-đun và danh sách cùng mô tả về các tín hiệu chỉ báo trạng thái được xuất ra về mặt vật lý; f) sự ánh xạ các giao diện đầu vào và đầu ra logic tới các cổng đầu vào và đầu ra vật lý, các điều khiển thủ công, và các chỉ báo trạng thái vật lý của mô-đun mật mã; g) các đặc tính vật lý, logic và điện, nếu có thể áp dụng, của các cổng và giao diện vật lý kể trên, bao gồm tóm tắt về thiết kế chân cắm, các tín hiệu logic được mang trên mỗi cổng, mức điện áp và ý nghĩa logic của chúng (ví dụ: điện áp thấp hoặc cao biểu thị mức logic "0", "1" hoặc ý nghĩa khác) và định thời của các tín hiệu.
TE03.01.02	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định rõ tất cả các luồng thông tin và các điểm truy cập vật lý của mô-đun mật mã, bằng cách kiểm tra sơ đồ khối, đặc tả thiết kế, và mã nguồn cũng như sơ đồ mạch, nếu phù hợp, được cung cấp tại mục 6.2 và 6.11, và bất kỳ tài liệu nào khác do nhà cung cấp cung cấp. Tài liệu phải quy định rõ mối quan hệ của các luồng thông tin và các điểm truy cập vật

	lý với các cổng vật lý và giao diện logic của mô-đun mật mã. Kiểm thử viên phải so sánh thông tin trên với thông tin được cung cấp tại các khẳng định AS02.05 và AS02.12 đến AS02.16 và xác minh rằng không có sự mâu thuẫn nào trong mô tả các thành phần và bố cục vật lý cho các cổng đầu vào/đầu ra.
TE03.01.03	Kiểm thử viên phải xác minh rằng đối với mỗi đầu vào vật lý hoặc logic vào mô-đun mật mã, hoặc đầu ra vật lý và logic từ mô-đun, tài liệu do nhà cung cấp cung cấp quy định rõ giao diện logic mà đầu vào hoặc đầu ra vật lý đó thuộc về, và cổng vào/ra vật lý. Các đặc tả được cung cấp phải nhất quán với đặc tả của các thành phần mô-đun mật mã được cung cấp tại mục 6.2 và 6.11, và các đặc tả của các giao diện logic được cung cấp tại các khẳng định AS03.04 đến AS03.12 của mục 6.3.2.
TE03.01.04	Kiểm thử viên phải kiểm tra mô-đun mật mã, để xác minh rằng tất cả các đặc tả cho khẳng định này do tài liệu của nhà cung cấp cung cấp đều nhất quán với thiết kế và triển khai của mô-đun mật mã.

Bảng 39 - VE và TE của AS03.02

Yêu cầu chung về giao diện mô-đun mật mã - mức 1, 2, 3 và 4	
AS03.02 ISO/IEC 19790:2025, 7.3.1	Các giao diện logic của mô-đun mật mã phải phân biệt với nhau mặc dù chúng có thể dùng chung một cổng vật lý (ví dụ: dữ liệu đầu vào có thể đi vào và dữ liệu đầu ra có thể đi ra qua cùng một cổng) hoặc có thể được phân bổ trên một hoặc nhiều cổng vật lý (ví dụ: dữ liệu đầu vào có thể đi vào thông qua cả cổng nối tiếp và cổng song song).
Thông tin bắt buộc từ nhà cung cấp	
VE03.02.01	Thiết kế của nhà cung cấp phải tách các giao diện mô-đun mật mã thành các hạng mục phân biệt và riêng biệt về mặt logic, sử dụng các hạng mục được liệt kê ở khẳng định AS03.04, và, nếu áp dụng, AS03.12 và AS03.13 tại mục 6.3.2. Thông tin này phải nhất quán với đặc tả của các giao diện logic và cổng vật lý được cung cấp tại AS03.01 ở mục 6.3.1.
VE03.02.02	Tài liệu do nhà cung cấp cung cấp phải cung cấp sự ánh xạ của mỗi hạng mục giao diện logic tới một cổng vật lý của mô-đun mật mã. Một giao diện logic có thể được phân bổ vật lý trên nhiều cổng vật lý, hoặc hai hay nhiều giao diện logic có thể dùng chung một cổng vật lý miễn là các luồng thông tin được giữ tách biệt về mặt logic. Nếu hai hay nhiều giao diện logic dùng chung một cổng vật lý, tài liệu do nhà cung cấp cung cấp phải quy định rõ cách thức thông tin từ các hạng mục giao diện khác nhau được giữ tách biệt về mặt logic.
Quy trình kiểm thử bắt buộc	
TE03.02.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng các giao diện mô-đun phân biệt và riêng biệt về mặt logic đối với các hạng mục giao diện được chỉ định tại khẳng định AS03.04 và, nếu áp dụng, AS03.12 và AS03.13 của mục 6.3.2. Thông tin này phải nhất quán với đặc tả và thiết kế của các giao diện logic và cổng vật lý được cung cấp tại AS03.01 ở mục 6.3.2.
TE03.02.02	Kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp cung cấp sự ánh xạ của mỗi hạng mục giao diện logic tới một cổng vật lý của mô-đun mật mã. Một giao diện logic có thể được phân bổ vật lý trên nhiều cổng vật lý, hoặc hai hay nhiều giao diện logic có thể dùng chung một cổng vật lý. Nếu hai hay nhiều giao diện dùng chung một cổng vật lý, kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp quy định rõ cách thức các luồng thông tin cho các giao diện đầu vào, đầu ra, điều khiển và trạng thái được giữ tách biệt về mặt logic.

CHÚ THÍCH Một API của một thành phần phần mềm của một mô-đun mật mã có thể được định nghĩa là một hoặc nhiều giao diện logic.

Bảng 40 - VE và TE của AS03.03

Yêu cầu chung về giao diện mô-đun mật mã - mức 1, 2, 3 và 4	
AS03.03 ISO/IEC 19790:2025, 7.3.1	Tài liệu cho các giao diện mô-đun mật mã được quy định trong ISO/IEC 19790:2025, A.2.2 phải được cung cấp.
Thông tin bắt buộc từ nhà cung cấp	
VE03.03.01	Nhà cung cấp phải cung cấp tài liệu cho các giao diện mô-đun mật mã như được quy định trong A.2.2 của ISO/IEC 19790:2025.
Quy trình kiểm thử bắt buộc	
TE03.03.01	Kiểm thử viên phải xác minh tính đầy đủ của tài liệu được quy định trong A.2.2 của ISO/IEC 19790:2025.

6.3.2 Các hạng mục giao diện

Bảng 41 - VE và TE của AS03.04

Các hạng mục giao diện - mức 1, 2, 3 và 4	
AS03.04 ISO/IEC 19790:2025, 7.3.3	Các giao diện của một mô-đun mật mã phải được phân loại thành một hoặc nhiều hạng mục trong bảy hạng mục giao diện sau đây ("đầu vào" và "đầu ra" được chỉ định từ góc độ của mô-đun):
Thông tin bắt buộc từ nhà cung cấp	
VE03.04.01	Tài liệu của nhà cung cấp phải tách các giao diện mô-đun mật mã thành các hạng mục phân biệt và riêng biệt về mặt logic bằng bảy giao diện được định nghĩa rõ ràng sau đây bên trong mô-đun mật mã ("đầu vào" và "đầu ra" được chỉ định từ góc độ của mô-đun): a) giao diện đầu vào dữ liệu (dành cho việc nhập dữ liệu như được quy định tại AS03.05); b) giao diện đầu ra dữ liệu (dành cho việc xuất dữ liệu như được quy định tại AS03.06 và AS03.07); c) giao diện đầu vào điều khiển (dành cho việc nhập các lệnh như được quy định tại AS03.08); d) giao diện đầu ra điều khiển (dành cho việc xuất các lệnh như được quy định tại AS03.09 và AS03.10); e) giao diện đầu ra trạng thái (dành cho việc xuất thông tin trạng thái như được quy định tại AS03.11); f) giao diện bảo trì (như được quy định tại AS03.12); g) giao diện nguồn điện (như được quy định tại AS03.13).
Quy trình kiểm thử bắt buộc	

TE03.04.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định rõ rằng bảy giao diện được liệt kê trong VE03.04.01 đã được thiết kế bên trong mô-đun mật mã. Nếu có, việc xác minh rằng các giao diện bên trong mô-đun mật mã hoạt động đúng như quy định phải được thực hiện theo các khẳng định từ AS03.05 đến AS03.13 tại mục 6.3.2.
------------	--

Bảng 42 - VE và TE của AS03.05

Các hạng mục giao diện - mức 1, 2, 3 và 4	
AS03.05 ISO/IEC 19790:2025, 7.3.3	Tất cả dữ liệu đầu vào phải đi vào qua giao diện đầu vào dữ liệu.
Thông tin bắt buộc từ nhà cung cấp	
VE03.05.01	Mô-đun mật mã phải có một giao diện đầu vào dữ liệu. Tất cả dữ liệu (ngoại trừ dữ liệu điều khiển đi vào qua giao diện đầu vào điều khiển) được nhập vào và xử lý bởi mô-đun mật mã phải đi vào qua giao diện đầu vào dữ liệu, bao gồm: a) dữ liệu dạng rõ; b) bản mã hoặc dữ liệu đã ký; c) các khóa mật mã và dữ liệu quản lý khóa khác (dạng rõ hoặc được mã hóa); d) dữ liệu xác thực và dữ liệu kiểm chứng (dạng rõ hoặc được mã hóa); e) thông tin trạng thái từ các nguồn bên ngoài; f) bất kỳ dữ liệu đầu vào nào khác.
VE03.05.02	Nếu áp dụng, tài liệu của nhà cung cấp phải quy định rõ bất kỳ thiết bị đầu vào bên ngoài nào được sử dụng với mô-đun mật mã để nhập dữ liệu vào giao diện đầu vào dữ liệu, chẳng hạn như thẻ thông minh, thẻ xác thực, bàn phím số, bộ nạp khóa, và các thiết bị sinh trắc học.
Quy trình kiểm thử bắt buộc	
TE03.05.01	Kiểm thử viên phải kiểm tra mô-đun để xác minh rằng mô-đun mật mã bao gồm một giao diện đầu vào dữ liệu, và giao diện đầu vào dữ liệu đó hoạt động đúng như quy định. Kiểm thử viên phải xác minh rằng tất cả dữ liệu (ngoại trừ dữ liệu điều khiển đi vào qua giao diện đầu vào điều khiển) được nhập vào và xử lý bởi mô-đun mật mã đều đi vào qua giao diện đầu vào dữ liệu, bao gồm: a) dữ liệu dạng rõ sẽ được mã hóa hoặc ký bởi mô-đun mật mã; b) dữ liệu bản mã hoặc dữ liệu đã ký sẽ được giải mã hoặc kiểm chứng bởi mô-đun; c) các khóa mật mã dạng rõ hoặc được mã hóa và dữ liệu quản lý khóa khác được nhập vào và sử dụng bởi mô-đun mật mã, bao gồm dữ liệu và vector khởi tạo, thông tin khóa phân mảnh, và thông tin kế toán khóa. CHÚ THÍCH Các yêu cầu quản lý khóa khác được đề cập trong ISO/IEC 19790:2025, 7.9.7. d) dữ liệu xác thực và kiểm chứng dạng rõ hoặc được mã hóa được nhập vào mô-đun mật mã, bao gồm mật khẩu, mã PIN, và thông tin sinh trắc học; e) thông tin trạng thái từ các nguồn bên ngoài (ví dụ: một mô-đun hoặc thiết bị mật mã khác);

	f) bất kỳ thông tin nào khác được nhập vào mô-đun mật mã để xử lý hoặc lưu trữ, ngoại trừ thông tin điều khiển được đề cập riêng ở AS03.08.
TE03.05.02	Kiểm thử viên phải xác minh xem tài liệu do nhà cung cấp cung cấp có chỉ định bất kỳ thiết bị đầu vào bên ngoài nào được sử dụng với mô-đun mật mã để nhập dữ liệu vào giao diện đầu vào dữ liệu hay không, chẳng hạn như thẻ thông minh, thẻ xác thực, bàn phím số, bộ nạp khóa, và các thiết bị sinh trắc học. Kiểm thử viên phải nhập dữ liệu vào giao diện đầu vào dữ liệu bằng các thiết bị đầu vào bên ngoài đã được xác định, và xác minh rằng việc nhập dữ liệu sử dụng thiết bị đầu vào bên ngoài hoạt động đúng như quy định.

Bảng 43 - VE và TE của AS03.06

Các hạng mục giao diện - mức 1, 2, 3 và 4	
AS03.06 ISO/IEC 19790:2025, 7.3.1	Tất cả dữ liệu đầu ra phải đi ra qua giao diện đầu ra dữ liệu.
Thông tin bắt buộc từ nhà cung cấp	
VE03.06.01	Mô-đun mật mã phải có một giao diện đầu ra dữ liệu. Tất cả dữ liệu (ngoại trừ dữ liệu trạng thái xuất ra qua giao diện đầu ra trạng thái và dữ liệu điều khiển xuất ra qua giao diện đầu ra điều khiển) đã được xử lý và xuất ra bởi mô-đun mật mã phải đi ra qua giao diện đầu ra dữ liệu, bao gồm: a) dữ liệu dạng rõ; b) dữ liệu dạng mã và chữ ký số; c) các khóa mật mã và dữ liệu quản lý khóa khác (dạng rõ hoặc được mã hóa); d) bất kỳ thông tin nào khác được xuất ra từ mô-đun mật mã sau khi xử lý hoặc lưu trữ, ngoại trừ thông tin trạng thái được đề cập riêng tại AS03.11 trong mục 6.3.2 và thông tin điều khiển được đề cập riêng tại AS03.09 và AS03.10 trong mục 6.3.2.
VE03.06.02	Nếu áp dụng, tài liệu do nhà cung cấp cung cấp phải quy định rõ bất kỳ thiết bị đầu ra bên ngoài nào được sử dụng với mô-đun mật mã để xuất dữ liệu từ giao diện đầu ra dữ liệu, chẳng hạn như thẻ thông minh, thẻ xác thực, màn hình hiển thị và các thiết bị lưu trữ khác.
VE03.06.03	Nếu các đường dẫn vật lý và logic mà dữ liệu đầu ra và thông tin SSP đi theo được dùng chung về mặt vật lý, tài liệu do nhà cung cấp cung cấp phải quy định rõ cách mô-đun mật mã thực thi sự tách biệt về mặt logic giữa dữ liệu đầu ra và thông tin SSP.
Quy trình kiểm thử bắt buộc	
TE03.06.01	Kiểm thử viên phải kiểm tra mô-đun để xác minh rằng mô-đun mật mã bao gồm một giao diện đầu ra dữ liệu, và giao diện đầu ra dữ liệu đó hoạt động đúng như quy định. Kiểm thử viên phải xác minh rằng tất cả dữ liệu đã được xử lý và xuất ra bởi mô-đun mật mã đều đi ra qua giao diện đầu ra dữ liệu. Điều này loại trừ dữ liệu trạng thái được xuất qua giao diện đầu ra trạng thái và dữ liệu điều khiển được xuất qua giao diện đầu ra điều khiển. Dữ liệu này bao gồm: a) dữ liệu dạng rõ đã được giải mã bởi mô-đun mật mã; b) dữ liệu dạng mã đã được mã hóa, và chữ ký số đã được tạo bởi mô-đun

	mật mã; c) các khóa mật mã dạng rõ hoặc được mã hóa và dữ liệu quản lý khóa khác đã được tạo nội bộ và xuất ra từ mô-đun, bao gồm dữ liệu và vector khởi tạo, thông tin chia sẻ khóa, và thông tin kế toán khóa (các yêu cầu quản lý khóa khác được đề cập trong 7.9.7 của ISO/IEC 19790:2025); d) bất kỳ thông tin nào khác được xuất ra từ mô-đun mật mã sau khi xử lý hoặc lưu trữ, ngoại trừ thông tin trạng thái được đề cập riêng tại AS03.11 trong mục 6.3.2 và thông tin điều khiển được đề cập riêng tại AS03.09 và AS03.10 trong mục 6.3.2.
TE03.06.02	Kiểm thử viên phải xác minh xem tài liệu do nhà cung cấp cung cấp có chỉ định bất kỳ thiết bị đầu ra bên ngoài nào được sử dụng với mô-đun mật mã để xuất dữ liệu từ giao diện đầu ra dữ liệu hay không, chẳng hạn như thẻ thông minh, thẻ xác thực, màn hình hiển thị, và các thiết bị lưu trữ khác. Kiểm thử viên phải xuất dữ liệu từ giao diện đầu ra dữ liệu bằng các thiết bị đầu ra bên ngoài đã được xác định, và xác minh rằng việc xuất dữ liệu sử dụng thiết bị đầu ra bên ngoài hoạt động đúng như quy định.
TE03.06.03	Nếu các đường dẫn vật lý và logic mà dữ liệu đầu ra và thông tin SSP đi theo được dùng chung về mặt vật lý, kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định rõ cách mô-đun mật mã thực thi sự tách biệt về mặt logic giữa dữ liệu đầu ra và thông tin SSP.

Bảng 44 - VE và TE của AS03.07

Các hạng mục giao diện - mức 1, 2, 3 và 4	
AS03.07 ISO/IEC 19790:2025, 7.3.3	Tất cả dữ liệu đầu ra phải bị chặn trong khi mô-đun mật mã đang ở trạng thái lỗi, và cũng bị chặn trong khi thực hiện các bài tự kiểm thử trước khi vận hành như quy định trong 7.10.3 của ISO/IEC 19790:2025, và việc xóa trắng như quy định trong 7.9.7 của ISO/IEC 19790:2025.
Thông tin bắt buộc từ nhà cung cấp	
VE03.07.01	Tài liệu do nhà cung cấp cung cấp phải quy định rõ cách mô-đun mật mã bị chặn dữ liệu đầu ra trong khi mô-đun mật mã đang ở trạng thái lỗi, và cũng chỉ định cách nó bị chặn dữ liệu đầu ra trong khi thực hiện các bài tự kiểm thử trước khi vận hành và việc xóa trắng.
VE03.07.02	Tài liệu do nhà cung cấp cung cấp phải quy định rõ cách thiết kế của mô-đun mật mã đảm bảo rằng tất cả dữ liệu đầu ra đều bị vô hiệu hóa trong khi mô-đun mật mã đang ở trạng thái lỗi, và cũng bị vô hiệu hóa trong khi thực hiện các bài tự kiểm thử trước khi vận hành và việc xóa trắng.
Quy trình kiểm thử bắt buộc	
TE03.07.01	Kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp quy định rõ tất cả dữ liệu đầu ra qua giao diện đầu ra dữ liệu đều bị vô hiệu hóa trong khi a) mô-đun mật mã đang ở trạng thái lỗi, và cả trong khi b) thực hiện: 1) các bài tự kiểm thử trước khi vận hành; 2) việc xóa trắng. Quy trình kiểm thử này có thể được phát biểu lại như sau: c) Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp rằng một

	khi điều kiện lỗi được phát hiện và trạng thái lỗi được thiết lập, tất cả dữ liệu đầu ra qua giao diện đầu ra dữ liệu đều bị chặn, cho đến khi quá trình khôi phục lỗi diễn ra. d) Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp rằng một khi mỗi dịch vụ sau đây được bắt đầu, tất cả dữ liệu đầu ra qua giao diện đầu ra dữ liệu đều bị chặn, cho đến khi dịch vụ được hoàn thành thành công:
TE03.07.02	Kiểm thử viên phải làm cho mô-đun mật mã bước vào từng trạng thái sau đây: a) mỗi trạng thái tự kiểm thử đang thực hiện các bài tự kiểm thử trước khi vận hành; b) mỗi trạng thái đang thực hiện việc xóa trắng; c) mỗi trạng thái lỗi và xác minh rằng tất cả dữ liệu đầu ra qua giao diện đầu ra dữ liệu đều bị chặn. Nếu kiểm thử viên không thể gây ra lỗi thì nhà cung cấp phải cung cấp một cơ sở lý luận cho kiểm thử viên về lý do tại sao không thể thực hiện bài kiểm thử này. Trong trường hợp đó, kiểm thử viên phải tuân theo các quy trình thay thế được tổ chức chứng nhận cho phép để đảm bảo rằng tất cả dữ liệu đầu ra qua giao diện đầu ra dữ liệu đều bị chặn. Ví dụ: Xem xét mã nguồn áp dụng. Nếu thông tin trạng thái được xuất ra từ giao diện đầu ra trạng thái để chỉ ra kết quả của các bài tự kiểm thử, kiểm thử viên phải xác minh rằng không có các CSP, dữ liệu dạng rõ, hoặc thông tin khác bị xuất ra mà nếu bị lạm dụng có thể dẫn đến sự tổn hại an toàn.
TE03.07.03	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định rõ cách thức mô-đun mật mã đảm bảo rằng tất cả dữ liệu đầu ra qua giao diện đầu ra dữ liệu đều bị chặn trong ba trạng thái được liệt kê ở TE03.07.02, tức là từ a) đến c). Kiểm thử viên cũng phải xác minh, bằng cách kiểm tra thiết kế của mô-đun mật mã, rằng giao diện đầu ra dữ liệu thực sự bị chặn về mặt logic hoặc vật lý dưới những điều kiện này.

Bảng 45 - VE và TE của AS03.08

Các hạng mục giao diện - mức 1, 2, 3 và 4	
AS03.08 ISO/IEC 19790:2025, 7.3.3	Tất cả đầu vào điều khiển phải đi vào qua giao diện đầu vào điều khiển.
Thông tin bắt buộc từ nhà cung cấp	
VE03.08.01	Mô-đun mật mã phải có một giao diện đầu vào điều khiển. Tất cả các lệnh, tín hiệu, và dữ liệu điều khiển (ngoại trừ dữ liệu đi vào qua giao diện đầu vào dữ liệu) được sử dụng để điều khiển hoạt động của mô-đun mật mã phải đi vào qua giao diện đầu vào điều khiển, bao gồm: a) các lệnh được nhập về mặt logic thông qua một API (ví dụ: cho các thành phần phần mềm và phần sụn của mô-đun mật mã); b) các tín hiệu được nhập về mặt logic hoặc vật lý qua một hoặc nhiều cổng vật lý (ví dụ: cho các thành phần phần cứng của mô-đun mật mã); c) các đầu vào điều khiển thủ công (ví dụ: sử dụng công tắc, nút bấm, hoặc

	bàn phím); bất kỳ dữ liệu điều khiển đầu vào nào khác.
VE03.08.02	Nếu áp dụng, tài liệu do nhà cung cấp cung cấp phải quy định rõ bất kỳ thiết bị đầu vào bên ngoài nào được sử dụng với mô-đun mật mã để nhập các lệnh, tín hiệu, và dữ liệu điều khiển vào giao diện đầu vào điều khiển, chẳng hạn như thẻ thông minh, thẻ xác thực, hoặc bàn phím số.
Quy trình kiểm thử bắt buộc	
TE03.08.01	Kiểm thử viên phải kiểm tra mô-đun để xác minh rằng mô-đun mật mã bao gồm một giao diện đầu vào điều khiển, và giao diện đầu vào điều khiển đó hoạt động đúng như quy định. Kiểm thử viên phải xác minh rằng tất cả các lệnh, tín hiệu, và dữ liệu điều khiển (ngoại trừ dữ liệu đi vào qua giao diện đầu vào dữ liệu) được sử dụng để điều khiển hoạt động của mô-đun mật mã đều phải đi vào qua giao diện đầu vào điều khiển, bao gồm: a) các lệnh được nhập về mặt logic thông qua một API, chẳng hạn như các lệnh gọi hàm đến một thư viện phần mềm hoặc đến một thẻ thông minh; b) các tín hiệu được nhập về mặt logic hoặc vật lý qua một hoặc nhiều cổng vật lý, chẳng hạn như các lệnh và tín hiệu được gửi qua một cổng nối tiếp hoặc một thẻ PC; c) các đầu vào điều khiển thủ công (ví dụ: sử dụng công tắc, nút bấm, hoặc bàn phím); d) bất kỳ dữ liệu điều khiển đầu vào nào khác.
TE03.08.02	Kiểm thử viên phải xác minh xem tài liệu do nhà cung cấp cung cấp có chỉ định bất kỳ thiết bị đầu vào bên ngoài nào được sử dụng với mô-đun mật mã để nhập các lệnh, tín hiệu, và dữ liệu điều khiển vào giao diện đầu vào điều khiển hay không, chẳng hạn như thẻ thông minh, thẻ xác thực, hoặc bàn phím số. Kiểm thử viên phải nhập các lệnh qua giao diện đầu vào điều khiển bằng các thiết bị đầu vào bên ngoài đã được xác định, và xác minh rằng việc nhập các lệnh sử dụng thiết bị đầu vào bên ngoài hoạt động đúng như quy định.

Bảng 46 - VE và TE của AS03.09

Các hạng mục giao diện - mức 1, 2, 3 và 4	
AS03.09 ISO/IEC 19790:2025, 7.3.3	Tất cả đầu ra điều khiển phải đi ra qua giao diện đầu ra điều khiển.
Thông tin bắt buộc từ nhà cung cấp	
VE03.09.01	Tài liệu do nhà cung cấp cung cấp phải quy định rõ rằng tất cả các lệnh, tín hiệu, và dữ liệu điều khiển đầu ra (ví dụ: các lệnh điều khiển gửi tới một mô-đun khác) được sử dụng để điều khiển hoặc chỉ ra trạng thái hoạt động của một mô-đun mật mã đều đi ra qua giao diện đầu ra điều khiển.
Quy trình kiểm thử bắt buộc	
TE03.09.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định rõ rằng tất cả các lệnh, tín hiệu, và dữ liệu điều khiển đầu ra (ví dụ: các lệnh điều khiển gửi tới một mô-đun khác) được sử dụng để điều khiển hoặc chỉ ra trạng thái hoạt động của một mô-đun mật mã đều đi ra qua giao diện đầu ra điều khiển.
TE03.09.02	Nếu giao diện đầu ra điều khiển được quy định, kiểm thử viên phải kiểm tra mô-đun để xác minh rằng giao diện đầu ra điều khiển hoạt động đúng như quy định.

Bảng 47 - VE và TE của AS03.10

Các hạng mục giao diện - mức 1, 2, 3 và 4	
AS03.10 ISO/IEC 19790:2025, 7.3.3	Tất cả đầu ra điều khiển phải bị chặn khi mô-đun mật mã đang ở trạng thái lỗi trừ khi các ngoại lệ được quy định và lập tài liệu trong chính sách an toàn.
Thông tin bắt buộc từ nhà cung cấp	
VE03.10.01	Tài liệu do nhà cung cấp cung cấp phải quy định rõ cách mô-đun mật mã đảm bảo rằng tất cả đầu ra điều khiển qua giao diện đầu ra điều khiển đều bị chặn bất cứ khi nào mô-đun đang ở trạng thái lỗi. Thông tin trạng thái có thể chỉ ra loại lỗi từ giao diện đầu ra trạng thái. CHÚ THÍCH Các trạng thái lỗi được đề cập trong 7.11 của ISO/IEC 19790:2025.
Quy trình kiểm thử bắt buộc	
TE03.10.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định rõ rằng tất cả đầu ra điều khiển qua giao diện đầu ra điều khiển đều bị chặn bất cứ khi nào mô-đun mật mã đang ở trạng thái lỗi. Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp rằng một khi điều kiện lỗi được phát hiện và trạng thái lỗi được thiết lập, tất cả đầu ra điều khiển qua giao diện đầu ra điều khiển đều bị chặn, cho đến khi quá trình khôi phục lỗi diễn ra. Kiểm thử viên cũng phải xác minh rằng các trạng thái lỗi được chỉ định để đáp ứng khẳng định này giống hệt với các trạng thái lỗi được quy định tại AS11.11.
TE03.10.02	Kiểm thử viên phải làm cho mô-đun mật mã bước vào từng trạng thái lỗi đã được quy định và xác minh rằng tất cả đầu ra điều khiển qua giao diện đầu ra điều khiển đều bị chặn. Nếu thông tin trạng thái được xuất ra từ giao diện đầu ra trạng thái để xác định loại lỗi, kiểm thử viên phải xác minh rằng thông tin xuất ra không phải là thông tin nhạy cảm. Các hành động sau đây có thể được sử dụng để làm cho mô-đun mật mã bước vào trạng thái lỗi: mở một nắp che hoặc cửa có khả năng phát hiện can thiệp; nhập các lệnh, khóa, hoặc tham số có định dạng không chính xác; giảm điện áp đầu vào, và bất kỳ hành động gây ra lỗi nào khác. Nếu kiểm thử viên không thể gây ra lỗi, thì nhà cung cấp phải cung cấp một cơ sở lý luận cho kiểm thử viên về lý do tại sao không thể thực hiện bài kiểm thử này.

Bảng 48 - VE và TE của AS03.11

Các hạng mục giao diện - mức 1, 2, 3 và 4	
AS03.11 ISO/IEC 19790:2025, 7.3.3	Tất cả đầu ra trạng thái phải đi ra qua giao diện đầu ra trạng thái.
Thông tin bắt buộc từ nhà cung cấp	
VE03.11.01	Mô-đun mật mã phải có một giao diện đầu ra trạng thái. Tất cả thông tin trạng thái, tín hiệu, chỉ báo logic, và chỉ báo vật lý được sử dụng để chỉ ra hoặc hiển thị trạng thái của mô-đun phải đi ra qua giao diện đầu ra trạng thái, bao gồm: a) thông tin trạng thái được xuất ra về mặt logic thông qua một API; b) đầu ra tín hiệu về mặt logic hoặc vật lý qua một hoặc nhiều cổng vật lý; c) chỉ báo trạng thái vật lý (ví dụ: sử dụng màn hình hiển thị, đèn báo, còi, âm

	báo, hoặc chuông); d) bất kỳ thông tin trạng thái đầu ra nào khác.
VE03.11.02	Nếu áp dụng, tài liệu do nhà cung cấp cung cấp phải quy định rõ bất kỳ thiết bị đầu ra bên ngoài nào được sử dụng với mô-đun mật mã để xuất thông tin trạng thái, tín hiệu, chỉ báo logic, và chỉ báo vật lý qua giao diện đầu ra trạng thái, chẳng hạn như thẻ thông minh, thẻ xác thực, màn hình hiển thị, và các thiết bị lưu trữ khác.
Quy trình kiểm thử bắt buộc	
TE03.11.01	Kiểm thử viên phải kiểm tra mô-đun để xác minh rằng mô-đun mật mã bao gồm một giao diện đầu ra trạng thái, và giao diện đầu ra trạng thái đó hoạt động đúng như quy định. Kiểm thử viên phải xác minh rằng tất cả thông tin trạng thái, tín hiệu, chỉ báo logic, và chỉ báo vật lý được sử dụng để chỉ ra hoặc hiển thị trạng thái của mô-đun đều phải đi ra qua giao diện đầu ra trạng thái, bao gồm: a) thông tin trạng thái được xuất ra về mặt logic thông qua một API, chẳng hạn như mã trả về từ một thư viện phần mềm hoặc một thẻ thông minh; b) đầu ra tín hiệu về mặt logic hoặc vật lý qua một hoặc nhiều cổng vật lý, chẳng hạn như thông tin trạng thái được gửi qua cổng nối tiếp hoặc cổng cắm thẻ PC; c) chỉ báo trạng thái vật lý; d) bất kỳ thông tin trạng thái đầu ra nào khác.
TE03.11.02	Kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp quy định rõ bất kỳ thiết bị đầu ra bên ngoài nào (nếu áp dụng) được sử dụng với mô-đun mật mã để xuất thông tin trạng thái, tín hiệu, chỉ báo logic, và chỉ báo vật lý qua giao diện đầu ra trạng thái.
TE03.11.03	Kiểm thử viên phải xác minh rằng thông tin trạng thái được xuất ra từ giao diện đầu ra trạng thái không được chứa bất kỳ thông tin nào có thể dẫn đến sự tổn hại an toàn của các CSP.
CHÚ THÍCH Đầu ra trạng thái có thể là ngầm định hoặc tường minh.	

Bảng 49 - VE và TE của AS03.12

Các hạng mục giao diện - mức 1, 2, 3 và 4	
AS03.12 ISO/IEC 19790:2025, 7.3.3	Tất cả các giao diện vật lý và logic với mô-đun mật mã được sử dụng khi ở vai trò bảo trì đều phải được định nghĩa.
Thông tin bắt buộc từ nhà cung cấp	
VE03.12.01	Tài liệu do nhà cung cấp cung cấp phải mô tả các giao diện bảo trì vật lý và logic được sử dụng bởi mô-đun khi ở vai trò bảo trì.
Quy trình kiểm thử bắt buộc	
TE03.12.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả tất cả các giao diện bảo trì vật lý và logic được sử dụng bởi mô-đun khi ở vai trò bảo trì.
TE03.12.02	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp và việc triển khai là nhất quán.

Bảng 50 - VE và TE của AS03.13

Các hạng mục giao diện - mức 1, 2, 3 và 4	
AS03.13 ISO/IEC 19790:2025, 7.3.3	Tất cả nguồn điện bên ngoài phải đi vào hoặc đi ra qua một giao diện nguồn điện.
Thông tin bắt buộc từ nhà cung cấp	
VE03.13.01	Nếu mô-đun mật mã yêu cầu nguồn điện từ hoặc cung cấp nguồn điện cho các thiết bị khác bên ngoài biên mật mã (ví dụ: bộ nguồn, dây nguồn, ổ cắm nguồn đầu vào/đầu ra, sạc không dây hoặc pin ngoài), tài liệu do nhà cung cấp cung cấp phải quy định rõ một giao diện nguồn điện và một cổng vật lý tương ứng.
VE03.13.02	Tất cả nguồn điện đi vào hoặc đi ra khỏi mô-đun mật mã từ hoặc tới các thiết bị khác bên ngoài biên mật mã đều phải truyền qua giao diện nguồn điện đã quy định.
Quy trình kiểm thử bắt buộc	
TE03.13.01	Kiểm thử viên phải xác minh xem tài liệu do nhà cung cấp cung cấp có chỉ định liệu mô-đun mật mã yêu cầu nguồn điện từ hoặc cung cấp nguồn điện cho các thiết bị khác bên ngoài biên mật mã hay không. Kiểm thử viên cũng phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định rõ một giao diện nguồn điện và một cổng vật lý tương ứng.
TE03.13.02	Kiểm thử viên phải xác minh, bằng cách kiểm tra mô-đun mật mã, rằng tất cả nguồn điện đi vào hoặc đi ra khỏi mô-đun từ hoặc tới các thiết bị khác bên ngoài biên mật mã đều truyền qua giao diện nguồn điện đã quy định.
CHÚ THÍCH Giao diện này không áp dụng cho các mô-đun mật mã phần mềm hoặc khi toàn bộ nguồn điện được cung cấp hoặc duy trì nội bộ bên trong biên mật mã của mô-đun mật mã (ví dụ: pin trong).	

Bảng 51 - VE và TE của AS03.14

Các hạng mục giao diện - mức 1, 2, 3 và 4	
AS03.14 ISO/IEC 19790:2025, 7.3.3	Mô-đun mật mã phải phân biệt giữa dữ liệu, thông tin điều khiển, và nguồn điện đối với đầu vào của mô-đun, và giữa dữ liệu, thông tin điều khiển, thông tin trạng thái, và nguồn điện đối với đầu ra từ mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE03.14.02	Tài liệu do nhà cung cấp cung cấp phải quy định rõ cách thức các đường dẫn vật lý và logic được sử dụng bởi dữ liệu và thông tin điều khiển đầu vào được ngắt kết nối về mặt logic hoặc vật lý khỏi các đường dẫn vật lý và logic được sử dụng bởi dữ liệu, thông tin điều khiển và thông tin trạng thái đầu ra. Nếu các đường dẫn vật lý và logic được sử dụng bởi dữ liệu và thông tin điều khiển đầu vào, cũng như dữ liệu, thông tin điều khiển và thông tin trạng thái đầu ra được dùng chung về mặt vật lý, tài liệu do nhà cung cấp cung cấp phải quy định rõ cách mô-đun mật mã thực thi sự tách biệt về mặt logic.
VE03.14.03	Tài liệu do nhà cung cấp cung cấp phải nhất quán và phải cho thấy rằng mô-đun mật mã phân biệt dữ liệu và điều khiển đối với đầu vào khỏi dữ liệu, điều khiển và trạng thái đối với đầu ra. Tài liệu của nhà cung cấp cũng phải cho thấy rằng các đường dẫn vật lý và logic mà dữ liệu và thông tin điều khiển đầu vào đi theo khi đi vào mô-đun qua các giao diện đầu vào áp dụng được ngắt kết nối về mặt logic hoặc vật lý khỏi các đường dẫn vật lý và logic mà dữ liệu, thông tin điều khiển và thông tin trạng thái đầu ra đi theo khi đi ra khỏi mô-đun qua các giao diện đầu ra áp dụng.

Quy trình kiểm thử bắt buộc	
TE03.14.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định rõ cách mô-đun mật mã phân biệt giữa dữ liệu và điều khiển đối với đầu vào và dữ liệu, điều khiển và trạng thái đối với đầu ra. Dữ liệu đầu vào được nhập từ giao diện đầu vào dữ liệu, và thông tin điều khiển được nhập từ giao diện đầu vào điều khiển phải được phân biệt về mặt logic hoặc vật lý với dữ liệu đầu ra đi ra tới giao diện đầu ra dữ liệu, điều khiển đầu ra đi ra tới giao diện đầu ra điều khiển, và thông tin trạng thái đi ra tới giao diện đầu ra trạng thái.
TE03.14.02	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định rõ cách thức các đường dẫn vật lý và logic được sử dụng bởi dữ liệu và thông tin điều khiển đầu vào được ngắt kết nối về mặt logic hoặc vật lý khỏi các đường dẫn vật lý và logic được sử dụng bởi dữ liệu, thông tin điều khiển và thông tin trạng thái đầu ra. Nếu các đường dẫn vật lý và logic được sử dụng bởi dữ liệu và thông tin điều khiển đầu vào, và các đường dẫn được sử dụng bởi dữ liệu, thông tin điều khiển và thông tin trạng thái đầu ra được dùng chung về mặt vật lý, kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định rõ cách mô-đun mật mã thực thi sự tách biệt về mặt logic.
TE03.14.03	Kiểm thử viên phải xác minh tính nhất quán của tài liệu do nhà cung cấp cung cấp, bằng cách kiểm tra mô-đun. Kiểm thử viên cũng phải xác minh rằng mô-đun mật mã phân biệt giữa dữ liệu và điều khiển đối với đầu vào và dữ liệu, điều khiển và trạng thái đối với đầu ra. Kiểm thử viên phải xác minh rằng đường dẫn A được ngắt kết nối về mặt logic hoặc vật lý khỏi đường dẫn B. Đường dẫn A bao gồm các đường dẫn vật lý và logic mà dữ liệu và thông tin điều khiển đầu vào đi theo khi đi vào mô-đun qua các giao diện đầu vào áp dụng, và đường dẫn B bao gồm các đường dẫn vật lý và logic mà dữ liệu, thông tin điều khiển và thông tin trạng thái đầu ra đi theo khi đi ra khỏi mô-đun qua các giao diện đầu ra áp dụng.

Bảng 52 - VE và TE của AS03.15

Các hạng mục giao diện - mức 1, 2, 3 và 4	
AS03.15 ISO/IEC 19790:2025, 7.3.3	Đặc tả mô-đun mật mã phải quy định một cách rõ ràng định dạng của dữ liệu và thông tin điều khiển đầu vào, bao gồm các giới hạn về độ dài đối với tất cả các đầu vào có độ dài thay đổi.
Thông tin bắt buộc từ nhà cung cấp	
VE03.15.01	Tài liệu do nhà cung cấp cung cấp phải quy định rõ các đường dẫn vật lý và logic được sử dụng bởi tất cả các hạng mục dữ liệu đầu vào chính đi vào mô-đun mật mã thông qua giao diện đầu vào dữ liệu và các cổng vật lý áp dụng. Tài liệu phải bao gồm một đặc tả về các đường dẫn áp dụng (ví dụ: bằng các bản sao được làm nổi bật hoặc chú thích của sơ đồ mạch, sơ đồ khối, hoặc thông tin khác được cung cấp theo AS02.05 và AS02.13 đến AS02.16). Tất cả dữ liệu đầu vào đi vào mô-đun mật mã thông qua giao diện đầu vào dữ liệu chỉ được sử dụng các đường dẫn đã quy định trong khi được xử lý hoặc lưu trữ bởi mỗi tiểu mục vật lý hoặc logic của mô-đun. Các đường dẫn dữ liệu đầu vào phải được quy định đủ chi tiết để đảm bảo rằng có thể xác minh được loại dữ liệu truyền qua mỗi cổng vật lý áp dụng. CHÚ THÍCH 1: Thuật ngữ "tất cả các hạng mục dữ liệu đầu vào chính" đề cập đến các mục được đề cập trong AS03.05 đối với đầu vào dữ liệu và các mục được đề cập trong AS03.08 đối với đầu vào điều khiển.

VE03.15.02	Tài liệu do nhà cung cấp cung cấp phải quy định rõ ràng tất cả dữ liệu đầu vào đi vào mô-đun mật mã thông qua giao diện đầu vào dữ liệu và các cổng vật lý áp dụng chỉ sử dụng các đường dẫn đã quy định. Tài liệu phải cho thấy rằng tất cả các luồng thông tin logic và vật lý được sử dụng bởi dữ liệu đầu vào đều nhất quán với thiết kế và hoạt động của mô-đun mật mã. Tài liệu của nhà cung cấp phải thiết lập rằng không có sự xung đột nào giữa các đường dẫn áp dụng có thể dẫn đến sự tổn hại an toàn của các CSP, dữ liệu dạng rõ, hoặc thông tin khác của mô-đun mật mã.
VE03.15.03	Tài liệu do nhà cung cấp cung cấp phải quy định một cách rõ ràng định dạng của dữ liệu và thông tin điều khiển đầu vào, bao gồm các giới hạn về độ dài đối với tất cả các đầu vào có độ dài thay đổi.
VE03.15.04	Tài liệu do nhà cung cấp cung cấp phải xác định thành phần nào bên trong biên mật mã đang kiểm chứng định dạng.
Quy trình kiểm thử bắt buộc	
TE03.15.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định các đường dẫn vật lý và logic được sử dụng bởi tất cả các hạng mục dữ liệu đầu vào chính đi vào mô-đun mật mã thông qua giao diện đầu vào dữ liệu. Kiểm thử viên cũng phải xác minh rằng các đường dẫn này phải được lập tài liệu trong đặc tả (ví dụ: bằng các bản sao được làm nổi bật hoặc chú thích của sơ đồ mạch, sơ đồ khối, hoặc thông tin khác được cung cấp theo AS02.05 và AS02.13 đến AS02.16). Kiểm thử viên phải xác minh rằng tài liệu quy định rõ loại dữ liệu truyền qua mỗi cổng vật lý áp dụng.
TE03.15.02	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun mật mã, để xác minh rằng tất cả dữ liệu đầu vào đi vào mô-đun qua giao diện đầu vào dữ liệu và các cổng vật lý áp dụng chỉ sử dụng các đường dẫn đã quy định. Kiểm thử viên phải xem xét tất cả các luồng thông tin logic và vật lý và phải xác minh rằng đặc tả về các đường dẫn được sử dụng bởi dữ liệu đầu vào là nhất quán với thiết kế và hoạt động của mô-đun mật mã. Kiểm thử viên phải xác minh rằng không có sự xung đột nào giữa các đường dẫn áp dụng có thể dẫn đến sự tổn hại an toàn của các CSP, dữ liệu dạng rõ, hoặc thông tin khác.
TE03.15.03	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng đặc tả rõ ràng được cung cấp về định dạng của dữ liệu và thông tin điều khiển đầu vào, bao gồm các giới hạn về độ dài đối với tất cả các đầu vào có độ dài thay đổi.
TE03.15.04	Kiểm thử viên phải xác minh rằng thành phần được xác định nằm bên trong biên mật mã được đặt trên đường dẫn đã chỉ định theo VE03.15.02.
TE03.15.05	Kiểm thử viên phải xem xét các mã nguồn áp dụng để đảm bảo rằng thành phần được xác định thực sự đang kiểm chứng định dạng đã được lập tài liệu.
TE03.15.06	Kiểm thử viên phải thử nhập dữ liệu và thông tin điều khiển không tuân thủ định dạng, và xác minh rằng các đầu vào dịch vụ như vậy bị mô-đun mật mã từ chối. CHÚ THÍCH 2: Nền tảng hoặc cấu hình kiểm thử có thể áp đặt một phần của định dạng/giới hạn. VÍ DỤ 1: Trình điều khiển thiết bị sử dụng mô-đun mật mã đang thực thi một phần của định dạng. VÍ DỤ 2: Một lớp trong ngăn xếp giao thức chỉ hỗ trợ gói tin có độ dài cố định. Nếu kiểm thử viên không thể nhập một số dữ liệu hoặc thông tin điều khiển nhất định không tuân thủ định dạng, thì kiểm thử viên phải yêu cầu nhà cung cấp cung cấp một cơ sở lý luận về lý do tại sao không thể thực hiện bài kiểm thử này. Trong trường hợp đó, kiểm thử viên phải tuân theo các quy trình thay thế được tổ chức chứng nhận cho phép để đảm bảo rằng mô-đun mật mã đang kiểm chứng định dạng.

Bảng 53 - VE và TE của AS03.16

Các hạng mục giao diện - mức 1, 2, 3 và 4	
AS03.16 ISO/IEC 19790:2025, 7.3.3	Mô-đun mật mã phải xác nhận rằng tất cả các đầu vào tuân thủ các đặc tả trong AS03.15.
Thông tin bắt buộc từ nhà cung cấp	
VE03.16.01	Nhà cung cấp phải cung cấp tài liệu xác định các kỹ thuật được sử dụng để xác nhận tất cả các đầu vào nhận được trên các giao diện của mô-đun.
Quy trình kiểm thử bắt buộc	
TE03.16.01	Kiểm thử viên phải xác minh rằng tài liệu được cung cấp có nêu rõ kỹ thuật dùng để xác nhận mọi đầu vào nhận được trên các giao diện của mô-đun. CHÚ THÍCH 1: Ngoài ra, khăng định này được kiểm thử như một phần của AS03.15. CHÚ THÍCH 2: Kiểm thử viên có thể sử dụng các công cụ chẩn đoán an toàn tự động do nhà cung cấp cung cấp trong AS11.30 để kiểm chứng các đầu vào.

6.3.3 Đường dẫn tin cậy dạng rõ

6.3.3.1 Mức an toàn 3

Bảng 54 - VE và TE của AS03.17

Đường dẫn tin cậy dạng rõ - mức 3 và 4	
AS03.17 ISO/IEC 19790:2025, 7.3.4.3	Đối với việc truyền các CSP dạng rõ và các thành phần khóa giữa mô-đun mật mã và điểm cuối của người gửi hoặc người nhận, mô-đun mật mã phải triển khai một đường dẫn tin cậy dạng rõ;
Thông tin bắt buộc từ nhà cung cấp	
VE03.17.01	Nhà cung cấp phải mô tả phương thức truyền các CSP dạng rõ và cách chúng được bảo vệ thông qua một đường dẫn tin cậy dạng rõ.
Quy trình kiểm thử bắt buộc	
TE03.17.01	Kiểm thử viên phải xác minh rằng đường dẫn tin cậy dạng rõ có khả năng bảo vệ các CSP dạng rõ giữa biên mật mã của mô-đun mật mã và điểm cuối của người gửi hoặc người nhận.

Bảng 55 - VE và TE của AS03.18

Đường dẫn tin cậy dạng rõ - mức 3 và 4	
AS03.18 ISO/IEC 19790:2025, 7.3.4.3	Đường dẫn tin cậy dạng rõ phải ngăn chặn sự sửa đổi, thay thế, và tiết lộ trái phép dọc theo liên kết truyền thông;
Quy trình kiểm thử bắt buộc	
Khăng định này được kiểm thử như một phần của AS03.19 và AS03.20.	

Bảng 56 - VE và TE của AS03.19

Đường dẫn tin cậy dạng rõ - mức 3 và 4	
AS03.19 ISO/IEC 19790:2025, 7.3.4.3	Các cổng vật lý được sử dụng cho đường dẫn tin cậy dạng rõ chỉ được sử dụng cho đường dẫn tin cậy dạng rõ và phải được tách biệt về mặt vật lý khỏi tất cả các cổng khác, hoặc {AS03.20 phải được thỏa mãn}.
Thông tin bắt buộc từ nhà cung cấp	

VE03.19.01	Tài liệu do nhà cung cấp cung cấp phải quy định liệu mô-đun mật mã có nhập hoặc xuất các CSP dạng rõ hay không. Các cổng vật lý được sử dụng cho việc nhập và xuất các CSP dạng rõ chỉ được sử dụng cho đường dẫn tin cậy dạng rõ và phải được tách biệt về mặt vật lý khỏi tất cả các cổng vật lý khác của mô-đun mật mã.
VE03.19.02	Nếu mô-đun mật mã nhập hoặc xuất các CSP dạng rõ, mô-đun phải đảm bảo rằng chỉ có các CSP dạng rõ đi vào hoặc đi ra khỏi mô-đun thông qua các cổng vật lý áp dụng, và không có dữ liệu nào khác, dù không được bảo vệ hay được mã hóa, đi vào hoặc đi ra khỏi mô-đun thông qua các cổng vật lý áp dụng.
VE03.19.03	Tài liệu do nhà cung cấp cung cấp phải cung cấp cơ sở lý luận về cách đường dẫn tin cậy dạng rõ ngăn chặn sự sửa đổi, thay thế, và tiết lộ trái phép dọc theo liên kết truyền thông.
Quy trình kiểm thử bắt buộc	
TE03.19.01	Kiểm thử viên phải xác minh xem tài liệu do nhà cung cấp cung cấp có quy định liệu mô-đun mật mã có nhập hoặc xuất các CSP dạng rõ hay không. Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và đồng thời kiểm tra các cổng vật lý trên mô-đun mật mã để đảm bảo rằng các cổng vật lý áp dụng được sử dụng cho việc nhập và xuất các CSP dạng rõ chỉ được sử dụng cho đường dẫn tin cậy dạng rõ và chúng được tách biệt về mặt vật lý khỏi tất cả các cổng vật lý khác của mô-đun.
TE03.19.02	Nếu mô-đun mật mã nhập hoặc xuất các CSP dạng rõ, kiểm thử viên phải xác minh rằng chỉ có các CSP dạng rõ đi vào hoặc đi ra khỏi mô-đun thông qua các cổng vật lý áp dụng, và không có dữ liệu nào khác, dù không được bảo vệ hay được mã hóa, đi vào hoặc đi ra khỏi mô-đun thông qua các cổng vật lý áp dụng.
TE03.19.03	Kiểm thử viên phải xác minh tính đúng đắn của bất kỳ cơ sở lý luận nào do nhà cung cấp cung cấp. Trách nhiệm chứng minh thuộc về nhà cung cấp; nếu có bất kỳ sự không chắc chắn hoặc mơ hồ nào, kiểm thử viên phải yêu cầu nhà cung cấp cung cấp thêm thông tin khi cần thiết.
TE03.19.04	Bằng cách thử truy cập vào liên kết truyền thông, kiểm thử viên phải xác minh rằng đường dẫn tin cậy dạng rõ ngăn chặn sự sửa đổi, thay thế, và tiết lộ trái phép dọc theo liên kết truyền thông.

Bảng 57 - VE và TE của AS03.20

Đường dẫn tin cậy dạng rõ - mức 3 và 4	
AS03.20 ISO/IEC 19790:2025, 7.3.4.3	Các giao diện logic được sử dụng cho đường dẫn tin cậy dạng rõ phải được tách biệt về mặt logic khỏi tất cả các giao diện khác; hoặc {AS03.19 phải được thỏa mãn}.
Thông tin bắt buộc từ nhà cung cấp	
VE03.20.01	Tài liệu do nhà cung cấp cung cấp phải mô tả cách các giao diện logic được sử dụng trong đường dẫn tin cậy dạng rõ để nhập và xuất các CSP dạng rõ được tách biệt về mặt logic khỏi tất cả các giao diện khác.
VE03.20.02	Nếu mô-đun mật mã nhập hoặc xuất các CSP dạng rõ, mô-đun phải đảm bảo rằng các CSP dạng rõ đi vào hoặc đi ra khỏi mô-đun thông qua giao diện logic áp dụng bằng cách sử dụng đường dẫn tin cậy dạng rõ, và không có dữ liệu nào khác, dù không được bảo vệ hay được mã hóa, đi vào hoặc đi ra khỏi mô-đun qua giao diện logic áp dụng bằng cách sử dụng đường dẫn tin cậy dạng rõ.

TCVN 12211:2026

VE03.20.03	Tài liệu do nhà cung cấp cung cấp phải cung cấp cơ sở lý luận về cách đường dẫn tin cậy dạng rõ ngăn chặn sự sửa đổi, thay thế, và tiết lộ trái phép dọc theo liên kết truyền thông.
Quy trình kiểm thử bắt buộc	
TE03.20.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun mật mã để xác minh rằng các giao diện logic áp dụng được sử dụng trong đường dẫn tin cậy dạng rõ để nhập và xuất các CSP dạng rõ được tách biệt về mặt logic khỏi tất cả các giao diện logic khác của mô-đun.
TE03.20.02	Nếu mô-đun mật mã nhập hoặc xuất các CSP dạng rõ, kiểm thử viên phải xác minh rằng các CSP dạng rõ đi vào hoặc đi ra khỏi mô-đun thông qua giao diện logic áp dụng bằng cách sử dụng đường dẫn tin cậy dạng rõ, và không có dữ liệu nào khác, dù không được bảo vệ hay được mã hóa, đi vào hoặc đi ra khỏi mô-đun qua giao diện logic áp dụng bằng cách sử dụng đường dẫn tin cậy dạng rõ.
TE03.20.03	Kiểm thử viên phải xác minh tính đúng đắn của bất kỳ cơ sở lý luận nào do nhà cung cấp cung cấp. Trách nhiệm chứng minh thuộc về nhà cung cấp; nếu có bất kỳ sự không chắc chắn hoặc mơ hồ nào, kiểm thử viên phải yêu cầu nhà cung cấp cung cấp thêm thông tin khi cần thiết.
TE03.20.04	Bằng cách thử truy cập vào liên kết truyền thông, kiểm thử viên phải xác minh rằng đường dẫn tin cậy dạng rõ ngăn chặn sự sửa đổi, thay thế, và tiết lộ trái phép dọc theo liên kết truyền thông.

Bảng 58 - VE và TE của AS03.21

Đường dẫn tin cậy dạng rõ - mức 3 và 4	
AS03.21 ISO/IEC 19790:2025, 7.3.4.3	Xác thực dựa trên danh tính phải được áp dụng cho tất cả các dịch vụ sử dụng đường dẫn tin cậy dạng rõ; và
Thông tin bắt buộc từ nhà cung cấp	
VE03.21.01	Nhà cung cấp phải cung cấp một mô tả về cơ chế xác thực được sử dụng bởi đường dẫn tin cậy dạng rõ.
Quy trình kiểm thử bắt buộc	
TE03.21.01	Kiểm thử viên phải xác minh rằng một cơ chế xác thực dựa trên danh tính được áp dụng cho tất cả các dịch vụ sử dụng đường dẫn tin cậy dạng rõ. Kiểm thử viên phải xác minh rằng các dịch vụ sử dụng đường dẫn tin cậy dạng rõ không được cung cấp nếu chưa vượt qua thành công bước xác thực người vận hành.

Bảng 59 - VE và TE của AS03.22

Đường dẫn tin cậy dạng rõ - mức 3 và 4	
AS03.22 ISO/IEC 19790:2025, 7.3.4.3	Một chỉ báo trạng thái phải được cung cấp khi đường dẫn tin cậy dạng rõ đang được sử dụng.
Thông tin bắt buộc từ nhà cung cấp	
VE03.22.01	Nhà cung cấp phải cung cấp mô tả về chỉ báo được cung cấp khi đường dẫn tin cậy dạng rõ đang được sử dụng.
Quy trình kiểm thử bắt buộc	

TE03.22.01	Kiểm thử viên phải xác minh, bằng cách vận hành mô-đun, rằng chỉ báo trạng thái được cung cấp khi đường dẫn tin cậy dạng rõ đang được sử dụng.
------------	--

6.3.3.2 Mức an toàn 4

Bảng 60 - VE và TE của AS03.23

Đường dẫn tin cậy dạng rõ - mức 4	
AS03.23 ISO/IEC 19790:2025, 7.3.4.4	Ngoài các yêu cầu của mức an toàn 3, xác thực dựa trên danh tính đa yếu tố hoặc các phương pháp xác thực khác, như được quy định cho mức an toàn 4 trong Phụ lục E của tiêu chuẩn ISO/IEC 19790:2025, phải được áp dụng cho tất cả các dịch vụ sử dụng đường dẫn tin cậy dạng rõ.
Thông tin bắt buộc từ nhà cung cấp	
VE03.23.01	Nhà cung cấp phải cung cấp mô tả về cơ chế xác thực dựa trên danh tính đa yếu tố được sử dụng bởi đường dẫn tin cậy dạng rõ.
Quy trình kiểm thử bắt buộc	
TE03.23.01	Kiểm thử viên phải xác minh rằng một cơ chế xác thực dựa trên danh tính đa yếu tố được áp dụng cho tất cả các dịch vụ sử dụng đường dẫn tin cậy dạng rõ. Kiểm thử viên phải xác minh rằng các dịch vụ sử dụng đường dẫn tin cậy dạng rõ không được cung cấp nếu chưa vượt qua thành công bước xác thực người vận hành.

6.3.4 Đường dẫn nội bộ được bảo vệ

Bảng 61 - VE và TE của AS03.24

Đường dẫn nội bộ được bảo vệ - mức 2, 3 và 4	
AS03.24 ISO/IEC 19790:2025, 7.3.4.4	Ở các mức an toàn 2, 3 và 4, các đường dẫn nội bộ được bảo vệ phải sử dụng các thuật toán mật mã được phê duyệt để cung cấp tính bảo mật và tính toàn vẹn cho dữ liệu và thông tin điều khiển liên quan đến an toàn.
Thông tin bắt buộc từ nhà cung cấp	
VE03.24.01	Nhà cung cấp phải cung cấp tài liệu quy định các đường dẫn nội bộ được bảo vệ cho tính bảo mật và tính toàn vẹn của dữ liệu và các điều khiển liên quan đến an toàn.
VE03.24.02	Tài liệu do nhà cung cấp cung cấp phải mô tả các thuật toán mật mã, cơ chế toàn vẹn và các phương pháp thiết lập khóa được sử dụng cho tất cả các đường dẫn nội bộ được bảo vệ đối với dữ liệu và điều khiển, đồng thời cung cấp chứng chỉ xác nhận nếu có hoặc cam kết của nhà cung cấp như được quy định trong VE02.18.01 và VE02.18.03.
Quy trình kiểm thử bắt buộc	
TE03.24.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định các đường dẫn nội bộ được bảo vệ cho tính bảo mật và tính toàn vẹn của dữ liệu và các điều khiển liên quan đến an toàn.
TE03.24.02	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả các thuật toán mật mã, cơ chế toàn vẹn và các phương pháp thiết lập khóa, đồng thời cung cấp một chứng chỉ xác nhận nếu có hoặc cam kết của nhà cung cấp như được quy định trong TE02.18.01 và TE02.18.03.
TE03.24.03	Đối với các phương pháp đã được lập tài liệu trong VE03.24.01 và VE03.24.02, kiểm thử viên phải xác minh bằng cách kiểm thử và kiểm tra mô-đun rằng đường dẫn nội bộ của mô-đun đang sử dụng các phương pháp đã được mô tả.

6.4 Vai trò, dịch vụ và xác thực

6.4.1 Yêu cầu chung về vai trò, dịch vụ và xác thực

Bảng 62 - VE và TE của AS04.01

Yêu cầu chung về vai trò, dịch vụ và xác thực - mức 1, 2, 3 và 4	
AS04.01 ISO/IEC 19790:2025, 7.4.1	Mô-đun mật mã phải hỗ trợ các vai trò được ủy quyền đối với người vận hành và các dịch vụ tương ứng trong từng vai trò. Một người vận hành được phép đảm nhận nhiều vai trò.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS04.11.	

Bảng 63 - VE và TE của AS04.02

Yêu cầu chung về vai trò, dịch vụ và xác thực - mức 1, 2, 3 và 4	
AS04.02 ISO/IEC 19790:2025, 7.4.1	Nếu mô-đun mật mã hỗ trợ nhiều người vận hành đồng thời, thì mô-đun đó phải duy trì trong nội bộ sự phân tách giữa các vai trò do từng người vận hành đảm nhận và các dịch vụ tương ứng
Thông tin bắt buộc từ nhà cung cấp	
VE04.02.01	Tài liệu do nhà cung cấp cung cấp phải quy định liệu có cho phép nhiều người vận hành đồng thời hay không. Tài liệu do nhà cung cấp cung cấp phải quy định phương pháp để đạt được sự phân tách các vai trò được ủy quyền và các dịch vụ được thực hiện bởi mỗi người vận hành. Tài liệu do nhà cung cấp cung cấp cũng phải mô tả bất kỳ giới hạn nào đối với người vận hành đồng thời. Ví DỤ 1: Một người vận hành ở vai trò bảo trì và một người khác ở vai trò người dùng cùng một lúc là không được chấp nhận. Ví DỤ 2: Hỗ trợ nhiều người vận hành đồng thời, lên tới 16 người vận hành ở vai trò người dùng, nhưng chỉ một dịch vụ tạo khóa RSA có thể được chạy cùng lúc trong mô-đun mật mã. Ví DỤ 3: Nhiều người vận hành đồng thời có thể đăng nhập ở vai trò chuyên viên mật mã, nhưng mỗi chuyên viên mật mã không thể thay đổi dữ liệu xác thực của những người vận hành khác cũng đang ở vai trò này.
Quy trình kiểm thử bắt buộc	
TE04.02.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả phương pháp được mô-đun triển khai để thực thi sự phân tách giữa các vai trò và dịch vụ được thực hiện bởi các người vận hành đồng thời.
TE04.02.02	Nếu mô-đun hỗ trợ nhiều hơn một vai trò thì kiểm thử viên phải đóng vai hai người vận hành độc lập: người vận hành 1 và người vận hành 2. Những người vận hành này phải đảm nhận các vai trò khác nhau. Kiểm thử viên phải xác minh rằng chỉ các dịch vụ được phân bổ cho mỗi vai trò mới có thể được thực hiện trong vai trò đó. Đối với mỗi người vận hành, kiểm thử viên cũng phải cố gắng truy cập các dịch vụ chỉ dành riêng cho vai trò do người vận hành kia đảm nhận, để xác minh rằng sự phân tách giữa các vai trò và dịch vụ được phép vẫn được duy trì ở những người vận hành đồng thời.
TE04.02.03	Nếu tài liệu do nhà cung cấp cung cấp quy định bất kỳ giới hạn nào đối với người vận hành đồng thời, kiểm thử viên phải tìm cách vi phạm các giới hạn đó bằng cách thử đảm nhận đồng thời các vai trò bị hạn chế dưới tư cách là những người vận hành độc lập và xác minh rằng mô-đun thực thi các giới hạn đó.

Bảng 64 - VE và TE của AS04.03

Yêu cầu chung về vai trò, dịch vụ và xác thực - mức 1, 2, 3 và 4	
AS04.03 ISO/IEC 19790:2025, 7.4.1	Phải cung cấp tài liệu về các vai trò, dịch vụ và xác thực được quy định tại ISO/IEC 19790:2025, Phụ lục A.2.3
Thông tin bắt buộc từ nhà cung cấp	
VE04.03.01	Nhà cung cấp phải cung cấp tài liệu về các vai trò, dịch vụ và xác thực như được mô tả trong ISO/IEC 19790:2025, A.2.3.
Quy trình kiểm thử bắt buộc	
TE04.03.01	Kiểm thử viên phải kiểm tra xem tài liệu do nhà cung cấp cung cấp có định nghĩa các vai trò, dịch vụ và xác thực tuân theo quy định trong ISO/IEC 19790:2025, A.2.3 hay không.

6.4.2 Vai trò

Bảng 65 - VE và TE của AS04.04

Vai trò - mức 1, 2, 3 và 4	
AS04.04 ISO/IEC 19790:2025, 7.4.2	Một mô-đun mật mã phải hỗ trợ tối thiểu một vai trò chuyên viên mật mã.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS04.05.	

Bảng 66 - VE và TE của AS04.05

Vai trò - mức 1, 2, 3 và 4	
AS04.05 ISO/IEC 19790:2025, 7.4.2	Vai trò chuyên viên mật mã phải được đảm nhận để thực hiện các chức năng quản lý hoặc khởi tạo mật mã, và các dịch vụ an toàn chung (ví dụ: khởi tạo mô-đun, quản lý CSP, PSP, và kiểm toán).
Thông tin bắt buộc từ nhà cung cấp	
VE04.05.01	Trong tài liệu được yêu cầu, nhà cung cấp phải bao gồm ít nhất một vai trò chuyên viên mật mã. Những vai trò này phải được quy định bằng tên và các dịch vụ được phép.
Quy trình kiểm thử bắt buộc	
TE04.05.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp định nghĩa ít nhất một vai trò chuyên viên mật mã. Kiểm thử viên phải xác minh rằng các vai trò được quy định bằng tên và các dịch vụ được phép như quy định tại AS04.05.

Bảng 67 - VE và TE của AS04.06

Vai trò - mức 1, 2, 3 và 4	
AS04.06 ISO/IEC 19790:2025, 7.4.2	Nếu mô-đun mật mã hỗ trợ một vai trò người dùng, thì vai trò người dùng phải được đảm nhận để thực hiện các dịch vụ an toàn chung, bao gồm các hoạt động mật mã và các chức năng an toàn đã phê duyệt khác.
Thông tin bắt buộc từ nhà cung cấp	
VE04.06.01	Nếu mô-đun mật mã hỗ trợ một vai trò người dùng, tài liệu do nhà cung cấp cung cấp phải (1) tuyên bố rõ ràng rằng vai trò người dùng được hỗ trợ, và (2) quy định hoàn chỉnh vai trò bằng tên và các dịch vụ được phép.
Quy trình kiểm thử bắt buộc	

TE04.06.01	Nếu mô-đun mật mã hỗ trợ một vai trò người dùng, kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp định nghĩa ít nhất một vai trò người dùng. Kiểm thử viên phải xác minh rằng vai trò người dùng được quy định bằng tên và các dịch vụ được phép như quy định tại AS04.06.
------------	--

Bảng 68 - VE và TE của AS04.07

Vai trò - mức 1, 2, 3 và 4	
AS04.07 ISO/IEC 19790:2025, 7.4.2	Tất cả các CSP dạng rõ, PSP dạng rõ, và các thành phần khóa dạng rõ phải được xóa trắng khi bước vào và khi thoát khỏi vai trò bảo trì.
Thông tin bắt buộc từ nhà cung cấp	
VE04.07.01	Nếu mô-đun mật mã có một giao diện bảo trì, tài liệu do nhà cung cấp cung cấp phải 1) tuyên bố rõ ràng một vai trò bảo trì được hỗ trợ, 2) quy định hoàn chỉnh vai trò bằng tên, mục đích và các dịch vụ được phép, và 3) quy định giao diện truy cập bảo trì theo VE03.12.01.
VE04.07.02	Tài liệu do nhà cung cấp cung cấp phải quy định cách thức các CSP dạng rõ, PSP dạng rõ, và các thành phần khóa dạng rõ của mô-đun bị xóa trắng một cách chủ động khi bước vào và thoát khỏi vai trò bảo trì.
Quy trình kiểm thử bắt buộc	
TE04.07.01	Kiểm thử viên phải xác minh xem các quy định về giao diện của mô-đun có chỉ ra một giao diện truy cập bảo trì hay không (xem AS03.12). Nếu có, kiểm thử viên phải xác minh tài liệu do nhà cung cấp cung cấp liên quan đến các vai trò được ủy quyền và xác minh rằng tài liệu đó quy định vai trò bảo trì bằng tên, mục đích và các dịch vụ được phép.
TE04.07.02	Kiểm thử viên phải xác minh xem các quy định về giao diện của mô-đun có định nghĩa một vai trò bảo trì hay không và kiểm tra việc xóa trắng tất cả các CSP dạng rõ, PSP dạng rõ, và các thành phần khóa dạng rõ như được mô tả trong đặc tả của mô-đun.
TE04.07.03	Trong khi ở vai trò bảo trì, kiểm thử viên phải nhập các giá trị đã biết cho tất cả các CSP dạng rõ, PSP dạng rõ và các thành phần khóa dạng rõ, nhằm trình diễn một cách hiệu quả việc xóa trắng các dữ liệu này. Khi thoát khỏi vai trò bảo trì, kiểm thử viên phải xác minh rằng việc xóa trắng đã diễn ra.

6.4.3 Dịch vụ

6.4.3.1 Yêu cầu chung về dịch vụ

Bảng 69 - VE và TE của AS04.08

Dịch vụ - mức 1, 2, 3 và 4	
AS04.08 ISO/IEC 19790:2025, 7.4.3.1	Dịch vụ được hiểu là bao gồm các hoạt động hoặc chức năng có thể được thực hiện bởi một mô-đun.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 70 - VE và TE của AS04.09

Dịch vụ - mức 1, 2, 3 và 4

AS04.09 ISO/IEC 19790:2025, 7.4.3.1	Đầu vào dịch vụ phải bao gồm tất cả các đầu vào dữ liệu hoặc điều khiển vào mô-đun nhằm khởi tạo hoặc thu được các dịch vụ, hoạt động, hoặc chức năng cụ thể.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 71 - VE và TE của AS04.10

Dịch vụ - mức 1, 2, 3 và 4	
AS04.10 ISO/IEC 19790:2025, 7.4.3.1	Đầu ra dịch vụ phải bao gồm tất cả các đầu ra dữ liệu, đầu ra điều khiển và đầu ra trạng thái là kết quả của các dịch vụ, hoạt động hoặc chức năng được khởi tạo hoặc thu được từ các đầu vào dịch vụ
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 72 - VE và TE của AS04.11

Dịch vụ - mức 1, 2, 3 và 4	
AS04.11 ISO/IEC 19790: 2025, 7.4.3.1	Mỗi đầu vào dịch vụ phải tạo ra một đầu ra dịch vụ.
Thông tin bắt buộc từ nhà cung cấp	
VE04.11.01	Tài liệu do nhà cung cấp cung cấp phải mô tả mục đích và chức năng của từng dịch vụ. Đối với mỗi dịch vụ, tài liệu phải xác định mục đích và chức năng của dịch vụ, các đầu vào dịch vụ, các đầu ra dịch vụ tương ứng và các vai trò được ủy quyền có thể thực hiện dịch vụ đó.
Quy trình kiểm thử bắt buộc	
TE04.11.01	Kiểm thử viên phải kiểm tra tài liệu do nhà cung cấp cung cấp và xác minh rằng mục đích và chức năng của từng dịch vụ đã được mô tả. Kiểm thử viên cũng phải kiểm tra rằng thông tin sau đây được quy định cho mỗi dịch vụ: các đầu vào dịch vụ, các đầu ra dịch vụ tương ứng, và các vai trò được ủy quyền mà trong đó dịch vụ có thể được thực hiện.
TE04.11.02	Kiểm thử viên phải thực hiện các bước sau đối với từng dịch vụ (tức là các dịch vụ liên quan đến an toàn và không liên quan đến an toàn, cả các dịch vụ đã phê duyệt và không được phê duyệt): a) Nhập mỗi đầu vào dịch vụ đã quy định và quan sát xem chúng có tạo ra các đầu ra dịch vụ đã quy định hay không. b) Đối với các dịch vụ yêu cầu người vận hành đảm nhận một vai trò, vai trò đó phải được đảm nhận để nhập mỗi đầu vào dịch vụ đã quy định và quan sát xem chúng có tạo ra các đầu ra dịch vụ đã quy định hay không. c) Đối với các dịch vụ yêu cầu người vận hành đảm nhận một vai trò, hãy đảm nhận vai trò không được quy định cho dịch vụ đó và nhập mỗi đầu vào dịch vụ đã quy định rồi quan sát xem dịch vụ có không được cung cấp hay không. d) Đối với các dịch vụ yêu cầu người vận hành đảm nhận một vai trò đã được xác thực, vai trò đó phải được đảm nhận và xác thực để nhập mỗi

	đầu vào dịch vụ đã quy định và quan sát xem chúng có tạo ra các đầu ra dịch vụ đã quy định hay không. e) Đối với các dịch vụ yêu cầu người vận hành đảm nhận một vai trò đã được xác thực, vai trò đó phải được đảm nhận nhưng dữ liệu xác thực phải bị sửa đổi để quá trình xác thực thất bại, sau đó nhập mỗi đầu vào dịch vụ đã quy định cùng dữ liệu xác thực đã sửa đổi và quan sát xem dịch vụ có không được cung cấp hay không. f) Đối với các dịch vụ cung cấp đầu ra dữ liệu qua giao diện đầu ra dữ liệu, kiểm thử viên phải xác minh kết quả so với kết quả mong đợi. Ví dụ: Nếu dịch vụ cung cấp đầu ra dữ liệu là một hàm của đầu vào dữ liệu dịch vụ, kiểm thử viên sẽ xác minh kết quả đầu ra dữ liệu như một hàm của dữ liệu đầu vào đã cung cấp.
--	---

Bảng 73 - VE và TE của AS04.12

Dịch vụ - mức 1, 2, 3 và 4	
AS04.12 ISO/IEC 19790:2025, 7.4.3.1	Một mô-đun mật mã phải cung cấp các dịch vụ sau cho người vận hành:
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 74 - VE và TE của AS04.13

Dịch vụ - mức 1, 2, 3 và 4	
AS04.13 ISO/IEC 19790:2025, 7.4.3.1	Mô-đun mật mã phải xuất ra tên hoặc định danh mô-đun, và thông tin phiên bản có thể tương quan với một hồ sơ chứng nhận (ví dụ: thông tin phiên bản phần cứng và phần mềm hoặc phần sụn).
Thông tin bắt buộc từ nhà cung cấp	
VE04.13.01	Mô-đun mật mã phải xuất ra tên hoặc định danh mô-đun, và thông tin phiên bản có thể tương quan với một hồ sơ chứng nhận (ví dụ: thông tin phiên bản phần cứng và phần mềm hoặc phần sụn).
VE04.13.02	Tài liệu do nhà cung cấp cung cấp phải xác định tên hoặc định danh mô-đun và thông tin phiên bản sẽ được đăng tải dưới dạng hồ sơ chứng nhận.
VE04.13.03	Tài liệu do nhà cung cấp cung cấp, hoặc là chính sách an toàn phi độc quyền hoặc là hướng dẫn dành cho quản trị viên, phải quy định cách tương quan đầu ra của tên và thông tin phiên bản hiện tại với một hồ sơ chứng nhận.
Quy trình kiểm thử bắt buộc	
TE04.13.01	Kiểm thử viên phải xác minh rằng các đầu ra dịch vụ (tức là tên hoặc định danh mô-đun và thông tin phiên bản) nhất quán với đặc tả và thông tin được cung cấp theo các khẳng định AS02.09, AS02.10, và AS11.04.
TE04.13.02	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp (tức là chính sách an toàn phi độc quyền hoặc hướng dẫn dành cho Quản trị viên) cung cấp đủ thông tin để nhận diện một cách rõ ràng phiên bản mô-đun.
TE04.13.03	Kiểm thử viên phải xác minh rằng đầu ra của tên hoặc định danh mô-đun và thông tin phiên bản hiện tại là đủ để người vận hành có thể tương quan mô-đun với một hồ sơ chứng nhận, với sự trợ giúp của chính sách an toàn phi độc quyền hoặc

	hướng dẫn dành cho quản trị viên.
--	-----------------------------------

Bảng 75 - VE và TE của AS04.14

Dịch vụ - mức 1, 2, 3 và 4	
AS04.14 ISO/IEC 19790:2025, 7.4.3.1	Mô-đun mật mã phải xuất trạng thái hiện tại. Điều này có thể bao gồm việc xuất các chỉ báo trạng thái để phản hồi một yêu cầu dịch vụ.
Thông tin bắt buộc từ nhà cung cấp	
VE04.14.01	Tài liệu do nhà cung cấp cung cấp phải mô tả đầu ra của trạng thái hiện tại của mô-đun.
Quy trình kiểm thử bắt buộc	
TE04.14.01	Kiểm thử viên phải xác minh tài liệu do nhà cung cấp cung cấp để đảm bảo rằng dịch vụ "hiển thị trạng thái" được phân bổ cho ít nhất một vai trò được ủy quyền. Kiểm thử viên phải xác minh rằng các dịch vụ này được mô tả như quy định tại AS04.14.
TE04.14.02	Kiểm thử viên phải xác minh rằng chỉ báo "hiển thị trạng thái" khớp với tài liệu do nhà cung cấp cung cấp.

Bảng 76 - VE và TE của AS04.15

Dịch vụ - mức 1, 2, 3 và 4	
AS04.15 ISO/IEC 19790:2025, 7.4.3.1	Mô-đun mật mã phải thực hiện các bài tự kiểm thử trước khi vận hành và các bài tự kiểm thử có điều kiện như quy định trong ISO/IEC 19790:2025, 7.10.
Thông tin bắt buộc từ nhà cung cấp	
VE04.15.01	Tài liệu do nhà cung cấp cung cấp phải mô tả việc khởi tạo và chạy các bài tự kiểm thử mà người dùng có thể gọi.
Quy trình kiểm thử bắt buộc	
TE04.15.01	Kiểm thử viên phải xác minh rằng mô-đun cung cấp khả năng khởi tạo việc chạy các bài tự kiểm thử trước khi vận hành như quy định trong ISO/IEC 19790:2025, 7.10; việc xác minh này được thực hiện trong quá trình xác minh tài liệu ở TEA.01.01.
TE04.15.02	Kiểm thử viên phải khởi tạo dịch vụ để thực hiện các bài tự kiểm thử. Kiểm thử viên phải xác minh rằng các bài tự kiểm thử trước khi vận hành như quy định trong ISO/IEC 19790:2025, 7.10 đã được thực hiện.
TE04.15.03	Kiểm thử viên phải khởi tạo dịch vụ để thực hiện các bài tự kiểm thử. Kiểm thử viên phải xác minh rằng khi mô-đun quay trở lại trạng thái vận hành, tất cả các bài tự kiểm thử thuật toán mật mã có điều kiện như quy định trong ISO/IEC 19790:2025, 7.10 đều được thực hiện trước lần sử dụng vận hành tiếp theo của thuật toán mật mã.

Bảng 77 - VE và TE của AS04.16

Dịch vụ - mức 1, 2, 3 và 4	
AS04.16 ISO/IEC	Mô-đun mật mã phải thực hiện ít nhất một chức năng an toàn đã phê duyệt như quy định trong ISO/IEC 19790:2025, 7.2.

19790:2025, 7.4.3.1	
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 78 - VE và TE của AS04.17

Dịch vụ - mức 1, 2, 3 và 4	
AS04.17 ISO/IEC 19790:2025, 7.4.3.1	Mô-đun mật mã phải thực hiện việc xóa trắng các tham số như quy định trong ISO/IEC 19790:2025, 7.9.7.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

6.4.3.2 Bỏ qua xử lý mật mã**Bảng 79 - VE và TE của AS04.18**

Dịch vụ - mức 1, 2, 3 và 4	
AS04.18 ISO/IEC 19790:2025, 7.4.3.2	Nếu mô-đun có thể xuất một mục dữ liệu hoặc mục trạng thái cụ thể dưới dạng được bảo vệ bằng mật mã, và (do cấu hình mô-đun hoặc do sự can thiệp của người vận hành) cũng có thể xuất mục đó dưới dạng không được bảo vệ, thì phải định nghĩa một khả năng bỏ qua.
Thông tin bắt buộc từ nhà cung cấp	
VE04.18.01	Nếu mô-đun triển khai một khả năng bỏ qua, tài liệu do nhà cung cấp cung cấp phải mô tả dịch vụ bỏ qua đó.
Quy trình kiểm thử bắt buộc	
TE04.18.01	Kiểm thử viên phải xác minh rằng mô-đun triển khai một khả năng bỏ qua như quy định trong tài liệu do nhà cung cấp cung cấp.

Bảng 80 - VE và TE của AS04.19

Dịch vụ - mức 1, 2, 3 và 4	
AS04.19 ISO/IEC 19790:2025, 7.4.3.2	Người vận hành phải đảm nhận một vai trò được ủy quyền trước khi định cấu hình khả năng bỏ qua;
Thông tin bắt buộc từ nhà cung cấp	
VE04.19.01	Nếu mô-đun triển khai một khả năng bỏ qua, tài liệu do nhà cung cấp cung cấp phải mô tả cách người vận hành đảm nhận một vai trò được ủy quyền trước khi định cấu hình khả năng bỏ qua.
Quy trình kiểm thử bắt buộc	
TE04.19.01	Kiểm thử viên phải xác minh từ tài liệu của nhà cung cấp rằng mô-đun yêu cầu người vận hành đảm nhận một vai trò được ủy quyền trước khi định cấu hình khả năng bỏ qua.
TE04.19.02	Kiểm thử viên phải đảm nhận vai trò đã được định nghĩa và lập tài liệu để cấu hình khả năng bỏ qua và tiến hành định cấu hình.

TE04.19.03	Người thử nghiệm phải đảm nhận một vai trò đã được xác định nhưng không được ghi trong tài liệu là có thể cấu hình khả năng bỏ qua, và tiến hành thực hiện việc cấu hình bỏ qua đó. Kiểm thử viên phải xác minh rằng lần thử này thất bại.
------------	--

Bảng 81 - VE và TE của AS04.20

Dịch vụ - mức 1, 2, 3 và 4	
AS04.20 ISO/IEC 19790:2025, 7.4.3.2	Mô-đun phải yêu cầu hai hành động nội bộ độc lập để kích hoạt khả năng bỏ qua, nhằm ngăn chặn việc vô tình xuất dữ liệu bản rõ không qua xử lý mật mã do một lỗi đơn lẻ gây ra.
Thông tin bắt buộc từ nhà cung cấp	
VE04.20.01	Nếu mô-đun triển khai một khả năng bỏ qua, tài liệu do nhà cung cấp cung cấp phải mô tả dịch vụ bỏ qua như được quy định trong AS04.20.
VE04.20.02	Mô hình trạng thái hữu hạn và tài liệu khác do nhà cung cấp cung cấp phải chỉ ra, đối với tất cả các quá trình chuyển đổi sang trạng thái bỏ qua độc quyền hoặc luân phiên, hai hành động nội bộ độc lập được yêu cầu để chuyển sang mỗi trạng thái bỏ qua.
Quy trình kiểm thử bắt buộc	
TE04.20.01	Kiểm thử viên phải xác minh xem khả năng bỏ qua có được triển khai bởi mô-đun hay không. Kiểm thử viên phải xác minh tài liệu do nhà cung cấp cung cấp để đảm bảo rằng khả năng bỏ qua được phân bổ cho ít nhất một vai trò được ủy quyền.
TE04.20.02	Kiểm thử viên phải xác minh mô hình trạng thái hữu hạn và tài liệu khác do nhà cung cấp cung cấp để đảm bảo rằng mỗi quá trình chuyển đổi sang trạng thái bỏ qua độc quyền hoặc luân phiên đều thể hiện hai hành động nội bộ độc lập. Điều này phải diễn ra để mô-đun mật mã có thể chuyển sang trạng thái bỏ qua độc quyền hoặc luân phiên.
TE04.20.03	Kiểm thử viên phải thử chuyển sang từng trạng thái bỏ qua từ mỗi trạng thái mà mô hình trạng thái hữu hạn thể hiện là có chuyển đổi như vậy và xác minh rằng phải cần đến hai hành động nội bộ để thực hiện mỗi quá trình chuyển đổi đó.

Bảng 82 - VE và TE của AS04.21

Dịch vụ - mức 1, 2, 3 và 4	
AS04.21 ISO/IEC 19790:2025, 7.4.3.2	Hai hành động nội bộ độc lập đó phải sửa đổi hành vi của phần sụn, phần mềm, hoặc phần cứng (hoặc kết hợp) được dành riêng để làm trung gian cho khả năng bỏ qua (ví dụ: hai cờ phần mềm hoặc phần cứng khác nhau được thiết lập, một trong số đó có thể do người dùng khởi tạo);
Thông tin bắt buộc từ nhà cung cấp	
VE04.21.01	Nếu mô-đun triển khai khả năng bỏ qua, tài liệu do nhà cung cấp cung cấp phải quy định cách thức hai hành động nội bộ độc lập sửa đổi hành vi phần sụn, phần mềm, hoặc phần cứng (hoặc kết hợp) được dành riêng để làm trung gian cho khả năng bỏ qua.
VE04.21.02	Tài liệu do nhà cung cấp cung cấp phải quy định cách thức hai hành động nội bộ độc lập bảo vệ chống lại việc vô tình xuất dữ liệu bản rõ do một lỗi đơn lẻ.
Quy trình kiểm thử bắt buộc	
TE04.21.01	Kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp mô tả cách thức hai hành động nội bộ độc lập ngăn chặn việc dữ liệu bản rõ vô tình được xuất ra mà

	không qua xử lý mật mã do một lỗi đơn lẻ gây ra.
TE04.21.02	Kiểm thử viên phải xác minh rằng hai hành động nội bộ độc lập có sửa đổi hành vi phần sụn, phần mềm, hoặc phần cứng (hoặc kết hợp) được dành riêng để làm trung gian cho khả năng bỏ qua, bằng cách kiểm tra mô-đun và bằng cách thử chuyển sang từng trạng thái bỏ qua từ mọi trạng thái có thể hiện sự chuyển đổi đó.

Bảng 83 - VE và TE của AS04.22

Dịch vụ - mức 1, 2, 3 và 4	
AS04.22 ISO/IEC 19790:2025, 7.4.3.2	Mô-đun phải hiển thị trạng thái của nó để chỉ ra xem khả năng bỏ qua: a) không được kích hoạt, và mô-đun đang cung cấp độc quyền các dịch vụ có xử lý mật mã (ví dụ: dữ liệu dạng rõ được mã hóa); b) được kích hoạt và mô-đun đang cung cấp độc quyền các dịch vụ không có xử lý mật mã (ví dụ: dữ liệu dạng rõ không được mã hóa); hoặc c) được kích hoạt và hủy kích hoạt luân phiên, đồng thời mô-đun đang cung cấp một số dịch vụ có xử lý mật mã và một số dịch vụ không có xử lý mật mã (ví dụ: đối với các mô-đun có nhiều kênh truyền thông, dữ liệu dạng rõ có thể được mã hóa hoặc không, tùy thuộc vào cấu hình của mỗi kênh).
Thông tin bắt buộc từ nhà cung cấp	
VE04.22.01	Tài liệu do nhà cung cấp cung cấp đối với dịch vụ "hiển thị trạng thái" phải chỉ ra trạng thái bỏ qua.
Quy trình kiểm thử bắt buộc	
TE04.22.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp đối với dịch vụ "hiển thị trạng thái" và xác minh chỉ báo của dịch vụ bỏ qua.
TE04.22.02	Kiểm thử viên phải chuyển sang từng trạng thái bỏ qua và xác minh rằng dịch vụ "hiển thị trạng thái" chỉ ra trạng thái bỏ qua tương ứng.

6.4.3.3 Bỏ qua xác thực lại**Bảng 84 - VE và TE của AS04.23**

Dịch vụ - mức 1, 2, 3 và 4	
AS04.23 ISO/IEC 19790:2025, 7.4.3.3	Tính năng bỏ qua xác thực lại chỉ được kích hoạt bởi chuyên viên mật mã. Cấu hình này cùng với bất kỳ trạng thái xác thực nào dành cho người vận hành có thể được bảo toàn khi khởi động lại, đặt lại, hoặc chu kỳ nguồn của mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE04.23.01	Nhà cung cấp phải cung cấp một mô tả về tính năng bỏ qua xác thực lại.
Quy trình kiểm thử bắt buộc	
TE04.23.01	Kiểm thử viên phải xác minh rằng tính năng bỏ qua xác thực lại chỉ có thể được kích hoạt và cấu hình bởi chuyên viên mật mã.

Bảng 85 - VE và TE của AS04.24

Dịch vụ - mức 1, 2, 3 và 4	
AS04.24 ISO/IEC 19790:2025, 7.4.3.3	Mô-đun phải yêu cầu hai hành động nội bộ độc lập nhằm ngăn chặn việc vô tình kích hoạt tính năng bỏ qua xác thực lại do một lỗi đơn lẻ.

Quy trình kiểm thử bắt buộc
Khẳng định này được kiểm thử như một phần của AS04.25.

Bảng 86 - VE và TE của AS04.25

Dịch vụ - mức 1, 2, 3 và 4	
AS04.25 ISO/IEC 19790:2025, 7.4.3.3	Hai hành động nội bộ độc lập đó phải sửa đổi hành vi phần sụn, phần mềm, hoặc phần cứng (hoặc kết hợp) được dành riêng để làm trung gian cho tính năng bỏ qua xác thực lại (ví dụ: hai cờ phần mềm, phần sụn hoặc phần cứng khác nhau được thiết lập, một trong số đó có thể do người dùng khởi tạo); và
Thông tin bắt buộc từ nhà cung cấp	
VE04.25.01	Nhà cung cấp phải định nghĩa một bộ hai hành động nội bộ cần được thực hiện độc lập với nhau nhằm kích hoạt tính năng bỏ qua xác thực lại.
VE04.25.02	Tài liệu do nhà cung cấp cung cấp phải quy định cách thức hai hành động nội bộ độc lập đó sửa đổi hành vi phần mềm hoặc phần cứng được dành riêng để làm trung gian cho tính năng bỏ qua xác thực lại.
VE04.25.03	Tài liệu do nhà cung cấp cung cấp phải quy định cách thức hai hành động nội bộ độc lập bảo vệ chống lại đầu ra vô tình do một lỗi đơn lẻ.
Quy trình kiểm thử bắt buộc	
TE04.25.01	Kiểm thử viên phải xác định xem mô-đun mật mã có triển khai tính năng bỏ qua xác thực lại hay không. Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định hai hành động nội bộ độc lập được mô-đun mật mã thực hiện trước khi kích hoạt tính năng bỏ qua xác thực lại. Kiểm thử viên cũng phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định cách thức hai hành động nội bộ độc lập bảo vệ chống lại đầu ra vô tình do một lỗi đơn lẻ.
TE04.25.02	Kiểm thử viên phải kích hoạt tính năng bỏ qua xác thực lại và xác minh rằng hai hành động nội bộ độc lập hoạt động đúng như quy định. Nếu có bất kỳ thành phần phần mềm hoặc phần sụn nào được thực thi trong quá trình kích hoạt, kiểm thử viên phải xem xét mã nguồn áp dụng để đảm bảo rằng các thành phần phần mềm hoặc phần sụn đó hỗ trợ yêu cầu phải có hai hành động nội bộ độc lập trước khi kích hoạt tính năng bỏ qua xác thực lại.
TE04.25.03	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định cách thức hai hành động nội bộ độc lập bảo vệ chống lại đầu ra vô tình do một lỗi đơn lẻ.

Bảng 87 - VE và TE của AS04.26

Dịch vụ - mức 1, 2, 3 và 4	
AS04.26 ISO/IEC 19790:2025, 7.4.3.3	Mô-đun phải hiển thị trạng thái của nó để chỉ ra xem tính năng bỏ qua xác thực lại đã được kích hoạt hay chưa.
Thông tin bắt buộc từ nhà cung cấp	
VE04.26.01	Nhà cung cấp phải lập tài liệu về chỉ báo trạng thái được sử dụng để xác nhận xem tính năng bỏ qua xác thực lại có được bật hay không.
Quy trình kiểm thử bắt buộc	

TCVN 12211:2026

TE04.26.01	Kiểm thử viên phải xác nhận rằng tài liệu do nhà cung cấp cung cấp nêu chi tiết về chỉ báo trạng thái được sử dụng để xác nhận xem tính năng bỏ qua xác thực lại có được bật hay không.
TE04.26.02	Kiểm thử viên phải bật tính năng bỏ qua xác thực lại và xác nhận rằng chỉ báo trạng thái đã được lập tài liệu hiển thị tính năng bỏ qua xác thực lại đang ở trạng thái bật.
TE04.26.03	Kiểm thử viên phải tắt tính năng bỏ qua xác thực lại và xác nhận rằng chỉ báo trạng thái đã được lập tài liệu hiển thị tính năng bỏ qua xác thực lại đang ở trạng thái tắt.

6.4.3.4 Nạp phần mềm/phần sụn**Bảng 88 - VE và TE của AS04.27**

Dịch vụ - mức 1, 2, 3 và 4	
AS04.27 ISO/IEC 19790:2025, 7.4.3.4	Nếu một mô-đun mật mã có khả năng nạp các thành phần phần mềm, phần sụn hoặc dòng bit từ một nguồn bên ngoài, thì các yêu cầu sau đây phải được áp dụng: {AS04.28 đến AS04.32}
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS04.28, AS04.29, AS04.30, AS04.31 và AS04.32.	

Bảng 89 - VE và TE của AS04.28

Dịch vụ - mức 1, 2, 3 và 4	
AS04.28 ISO/IEC 19790:2025, 7.4.3.4	Chính sách an toàn phải quy định rằng, theo chính sách, người vận hành chỉ được phép nạp phần mềm, phần sụn hoặc dòng bit đã được tổ chức chứng nhận thẩm định trước khi nạp để duy trì tính hợp lệ, ngoại trừ khi nạp vào một vùng chứa an toàn đáp ứng các yêu cầu của ISO/IEC 19790:2025, 7.5;
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	
CHÚ THÍCH 1: Khẳng định này đề cập đến ISO/IEC TS 20540.	

Bảng 90 - VE và TE của AS04.29

Dịch vụ - mức 1, 2, 3 và 4	
AS04.29 ISO/IEC 19790:2025, 7.4.3.4	Bài kiểm thử nạp phần mềm/phần sụn quy định trong ISO/IEC 19790:2025, 7.10.4.4 phải được thực hiện trước khi mã lệnh vừa nạp có thể được thực thi;
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.37, AS10.38, AS10.39, AS10.40, AS10.41 và AS10.42.	

Bảng 91 - VE và TE của AS04.30

Dịch vụ - mức 1, 2, 3 và 4	
AS04.30 ISO/IEC 19790:2025, 7.4.3.4	Mô-đun mật mã phải tạm dừng việc thực thi mọi chức năng an toàn đã phê duyệt vừa được nạp hoặc sửa đổi cho đến khi các bài tự kiểm thử trước khi vận hành quy định trong ISO/IEC 19790:2025, 7.10.3 được thực thi thành công.
Quy trình kiểm thử bắt buộc	

Khẳng định này được kiểm thử như một phần của AS10.37, AS10.38, AS10.39, AS10.40, AS10.41 và AS10.42.

Bảng 92 - VE và TE của AS04.31

Dịch vụ - mức 1, 2, 3 và 4	
AS04.31 ISO/IEC 19790:2025, 7.4.3.4	Trong trường hợp các bài tự kiểm thử trước khi vận hành chỉ bao quát mã lệnh vừa nạp hoặc sửa đổi, phải chứng minh được lý do tại sao không chạy lại các bài tự kiểm thử đã loại trừ; và
Thông tin bắt buộc từ nhà cung cấp	
VE04.31.01	Tài liệu do nhà cung cấp cung cấp phải quy định rõ lý do tại sao không cần thiết phải chạy lại các bài tự kiểm thử đã loại trừ khi mà các bài tự kiểm thử trước khi vận hành chỉ bao quát một tập con trong số các bài tự kiểm thử trước khi vận hành được mô-đun hỗ trợ.
Quy trình kiểm thử bắt buộc	
TE04.31.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định lý do tại sao các bài tự kiểm thử đã loại trừ không bắt buộc phải chạy lại, trong trường hợp các bài tự kiểm thử trước khi vận hành chỉ bao quát một tập con trong số các bài tự kiểm thử trước khi vận hành được mô-đun hỗ trợ.
TE04.31.02	Kiểm thử viên phải vận hành mô-đun mật mã và xác minh rằng mô-đun hoạt động theo đúng tài liệu.
TE04.31.03	Kiểm thử viên phải tiêm một lỗi vào mã lệnh vừa nạp hoặc sửa đổi. Kiểm thử viên phải khởi tạo bài tự kiểm thử trước khi vận hành đối với mã lệnh vừa nạp hoặc sửa đổi. Kiểm thử viên phải xác minh rằng mô-đun gặp lỗi và bước vào trạng thái lỗi.
TE04.31.04	Kiểm thử viên phải tiêm một lỗi vào mã lệnh vừa nạp hoặc sửa đổi. Kiểm thử viên phải khởi tạo bài tự kiểm thử trước khi vận hành cho tất cả các bài kiểm thử được mô-đun hỗ trợ ngoại trừ tập con các bài kiểm thử áp dụng cho mã lệnh vừa nạp hoặc sửa đổi. Kiểm thử viên phải xác minh rằng mô-đun không gặp lỗi hoặc không bước vào trạng thái lỗi.

Bảng 93 - VE và TE của AS04.32

Dịch vụ - mức 1, 2, 3 và 4	
AS04.32 ISO/IEC 19790:2025, 7.4.3.4	Thông tin phiên bản của mô-đun phải được sửa đổi để thể hiện sự bổ sung hoặc cập nhật của phần mềm hoặc phần sụn mới được nạp.
Thông tin bắt buộc từ nhà cung cấp	
VE04.32.01	Nhà cung cấp phải cung cấp các phương tiện để đọc phiên bản của phần mềm hoặc phần sụn mới được nạp.
Quy trình kiểm thử bắt buộc	
TE04.32.01	Kiểm thử viên phải nạp phần mềm/phần sụn mới vào mô-đun. Kiểm thử viên phải xác minh rằng thông tin phiên bản được sửa đổi để thể hiện sự bổ sung hoặc cập nhật của phần mềm hoặc phần sụn mới được nạp.

6.4.4 Xác thực

6.4.4.1 Yêu cầu chung về xác thực

Bảng 94 - VE và TE của AS04.33

Xác thực - mức 2, 3 và 4	
AS04.33 ISO/IEC 19790:2025, 7.4.4.1	Nếu các cơ chế xác thực dựa trên vai trò được một mô-đun mật mã hỗ trợ, mô-đun phải yêu cầu người vận hành chọn một hoặc nhiều vai trò một cách ngẫu nhiên hoặc tường minh và {phải xác thực việc đảm nhận các vai trò đã chọn (hoặc tập hợp vai trò).}
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS04.34.	

Bảng 95 - VE và TE của AS04.34

Xác thực - mức 2, 3 và 4	
AS04.34 ISO/IEC 19790:2025, 7.4.4.1	{Nếu các cơ chế xác thực dựa trên vai trò được một mô-đun mật mã hỗ trợ, mô-đun phải yêu cầu người vận hành chọn một hoặc nhiều vai trò một cách ngẫu nhiên hoặc tường minh} và phải xác thực việc đảm nhận các vai trò đã chọn (hoặc tập hợp vai trò).
Thông tin bắt buộc từ nhà cung cấp	
VE04.34.01	Nhà cung cấp phải lập tài liệu về loại hình xác thực được thực hiện đối với mô-đun. Nhà cung cấp phải lập tài liệu về các cơ chế được sử dụng để thực hiện việc lựa chọn một cách ngẫu nhiên hoặc tường minh một vai trò hay tập hợp các vai trò, và cơ chế xác thực người vận hành để đảm nhận các vai trò đó.
Quy trình kiểm thử bắt buộc	
TE04.34.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định các cơ chế được sử dụng để chọn một hay nhiều vai trò và để xác thực người vận hành khi đảm nhận một vai trò.
TE04.34.02	Kiểm thử viên phải xác minh rằng mô-đun có xác thực người vận hành đối với một vai trò đã chọn.
TE04.34.03	Kiểm thử viên phải đảm nhận từng vai trò và tạo ra một lỗi trong quá trình xác thực. Kiểm thử viên phải xác minh rằng mô-đun từ chối quyền truy cập vào từng vai trò đó.

Bảng 96 - VE và TE của AS04.35

Xác thực - mức 2, 3 và 4	
AS04.35 ISO/IEC 19790:2025, 7.4.4.1	Nếu một mô-đun mật mã cho phép người vận hành thay đổi vai trò, thì mô-đun phải xác thực việc đảm nhận bất kỳ vai trò nào chưa được xác thực trước đó cho người vận hành đó.
Thông tin bắt buộc từ nhà cung cấp	
VE04.35.01	Tài liệu do nhà cung cấp cung cấp phải mô tả khả năng người vận hành thay đổi vai trò và phải tuyên bố rằng một người vận hành phải được xác thực để đảm nhận một vai trò mới.
Quy trình kiểm thử bắt buộc	
TE04.35.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng phương pháp qua đó một người vận hành có thể thay đổi vai trò bao gồm việc xác thực người vận hành để đảm nhận một vai trò mới.
TE04.35.02	Kiểm thử viên phải xác minh rằng mô-đun thực hiện xác thực người vận hành đối với một vai trò mới.

TE04.35.03	Kiểm thử viên phải thực hiện các bài kiểm thử sau: a) Đảm nhận một vai trò, thử chuyển sang một vai trò khác mà người vận hành được ủy quyền để đảm nhận, và xác minh rằng mô-đun cho phép người vận hành yêu cầu các dịch vụ được phân bổ cho vai trò mới. b) Đảm nhận một vai trò, thử chuyển sang một vai trò khác mà người vận hành không được ủy quyền để đảm nhận, và xác minh rằng mô-đun không cho phép người vận hành yêu cầu các dịch vụ chỉ được phân bổ cho vai trò mới.
------------	--

Bảng 97 - VE và TE của AS04.36

Xác thực - mức 3 và 4	
AS04.36 ISO/IEC 19790:2025, 7.4.4.1	Nếu các cơ chế xác thực dựa trên danh tính được một mô-đun mật mã hỗ trợ, mô-đun phải yêu cầu người vận hành được nhận diện riêng biệt và duy nhất, {phải yêu cầu người vận hành chọn một hoặc nhiều vai trò một cách ngầm định hoặc tường minh,} {phải xác thực danh tính của người vận hành và xác nhận người vận hành đó được ủy quyền để đảm nhận các vai trò đã chọn hoặc tập hợp vai trò.}
Thông tin bắt buộc từ nhà cung cấp	
VE04.36.01	Tài liệu do nhà cung cấp cung cấp phải quy định loại hình xác thực được triển khai trong mô-đun. Tài liệu của nhà cung cấp phải quy định: a) các cơ chế được sử dụng để thực hiện việc nhận diện người vận hành, CHÚ THÍCH 1: Điều này liên quan đến AS04.36. b) các cơ chế được sử dụng để thực hiện việc xác thực danh tính của người vận hành, CHÚ THÍCH 2: Điều này liên quan đến AS04.38. c) các cơ chế được sử dụng để thực hiện việc chọn một cách ngầm định hoặc tường minh một vai trò hay tập hợp các vai trò, CHÚ THÍCH 3: Điều này liên quan đến AS04.37. d) các cơ chế được sử dụng để thực hiện việc kiểm chứng việc ủy quyền để người vận hành đảm nhận các vai trò, và CHÚ THÍCH 4: Điều này liên quan đến AS04.38. e) các cơ chế được sử dụng để duy trì nội bộ mối quan hệ giữa người vận hành đã được nhận diện và xác thực với vai trò hoặc tập hợp vai trò được chọn mà người vận hành được ủy quyền để đảm nhận. CHÚ THÍCH 5: Điều này liên quan đến AS04.37, AS04.38, và AS04.39.
Quy trình kiểm thử bắt buộc	
TE04.36.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có quy định: a) cách người vận hành được nhận diện duy nhất, CHÚ THÍCH 6: Điều này liên quan đến AS04.36. b) cách danh tính đó được xác thực, CHÚ THÍCH 7: Điều này liên quan đến AS04.38. c) cách người vận hành chọn một vai trò,

	CHÚ THÍCH 8: Điều này liên quan đến AS04.37. d) cách quyền ủy quyền để người vận hành đảm nhận một vai trò được thực hiện dựa trên danh tính đã xác thực, và CHÚ THÍCH 9: Điều này liên quan đến AS04.38. e) cách mối quan hệ được duy trì nội bộ giữa người vận hành đã được nhận diện và xác thực với vai trò hoặc tập hợp vai trò được chọn mà người vận hành được ủy quyền đảm nhận. CHÚ THÍCH 10: Điều này liên quan đến AS04.37, AS04.38, và AS04.39.
TE04.36.02	Kiểm thử viên phải kiểm tra mô-đun và xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng nó triển khai quy trình nhận diện và xác thực như quy định trong tài liệu do nhà cung cấp cung cấp, được cung cấp theo VE04.36.01.
TE04.36.03	Kiểm thử viên phải khởi tạo một lỗi trong quy trình xác thực và phải xác minh rằng mô-đun không cho phép kiểm thử viên tiến xa hơn bước quy trình xác thực.
TE04.36.04	Kiểm thử viên phải xác thực thành công danh tính của bản thân với mô-đun. Khi được yêu cầu chọn một hoặc nhiều vai trò, kiểm thử viên phải chọn các vai trò không tương thích với danh tính đã xác thực và phải xác minh rằng quyền ủy quyền để đảm nhận những vai trò này bị từ chối. CHÚ THÍCH 11: Quy trình kiểm thử này liên quan đến AS04.36 và AS04.38.

Bảng 98 - VE và TE của AS04.37

Xác thực - mức 3 và 4	
AS04.37 ISO/IEC 19790:2025, 7.4.4.1	{Nếu các cơ chế xác thực dựa trên danh tính được một mô-đun mật mã hỗ trợ, mô-đun phải yêu cầu người vận hành được nhận diện riêng biệt và duy nhất,} phải yêu cầu người vận hành chọn một hoặc nhiều vai trò một cách ngẫu nhiên hoặc tường minh, và {phải xác thực danh tính của người vận hành và xác nhận người vận hành đó được ủy quyền để đảm nhận các vai trò đã chọn hoặc tập hợp vai trò.}
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 99 - VE và TE của AS04.38

Xác thực - mức 3 và 4	
AS04.38 ISO/IEC 19790:2025, 7.4.4.1	{Nếu các cơ chế xác thực dựa trên danh tính được một mô-đun mật mã hỗ trợ, mô-đun phải yêu cầu người vận hành được nhận diện riêng biệt và duy nhất,} {phải yêu cầu người vận hành chọn một hoặc nhiều vai trò một cách ngẫu nhiên hoặc tường minh,} và phải xác thực danh tính của người vận hành và xác nhận người vận hành đó được ủy quyền để đảm nhận các vai trò đã chọn hoặc tập hợp vai trò.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 100 - VE và TE của AS04.39

Xác thực - mức 3 và 4	
AS04.39 ISO/IEC 19790:2025, 7.4.4.1	Nếu mô-đun mật mã cho phép người vận hành thay đổi vai trò, thì mô-đun phải xác minh việc xác thực của người vận hành đã được nhận diện để đảm nhận bất kỳ vai trò nào chưa được xác thực trước đó, và việc cấp quyền cho người vận hành đã được nhận diện để đảm nhận bất kỳ vai trò nào chưa được cấp quyền trước đó.

Thông tin bắt buộc từ nhà cung cấp	
VE04.39.01	Tài liệu do nhà cung cấp cung cấp phải quy định: a) liệu mô-đun mật mã có cho phép người vận hành thay đổi vai trò hay không; b) cách một người vận hành có thể thay đổi vai trò sau khi người vận hành đó được nhận diện và xác thực; c) cách mối quan hệ được duy trì nội bộ giữa người vận hành đã được nhận diện và xác thực với vai trò hoặc tập hợp vai trò được chọn mà người vận hành được ủy quyền (xem mục e của VE04.36.01); d) cách mô-đun mật mã thực thi việc kiểm chứng việc ủy quyền để người vận hành đã được nhận diện đảm nhận một vai trò chưa được ủy quyền trước đó; e) các điều kiện mà theo đó danh tính của người vận hành phải được xác thực lại khi thay đổi vai trò.
Quy trình kiểm thử bắt buộc	
TE04.39.01	Kiểm thử viên phải kiểm tra mô-đun và xem xét tài liệu của nhà cung cấp, để xác minh rằng mô-đun mật mã cho phép người vận hành thay đổi vai trò.
TE04.39.02	Kiểm thử viên phải xác minh trong tài liệu do nhà cung cấp cung cấp rằng phương pháp thông qua đó một người vận hành có thể sửa đổi vai trò mà không cần xác thực lại danh tính của người vận hành bao gồm cả việc kiểm chứng việc ủy quyền của người vận hành đối với một vai trò chưa được xác thực trước đó.
TE04.39.03	Kiểm thử viên phải thực hiện các bài kiểm thử sau: a) Đảm nhận từng vai trò, thử chuyển sang một vai trò khác mà kiểm thử viên được ủy quyền để đảm nhận, xác minh rằng danh tính của kiểm thử viên không bắt buộc phải được xác thực lại, và xác minh rằng kiểm thử viên có thể truy cập các dịch vụ liên kết với vai trò mới. Kiểm thử viên phải thực hiện các dịch vụ thuộc vai trò mới nhưng không thuộc vai trò trước đó nhằm xác minh rằng kiểm thử viên đã đảm nhận một vai trò khác. b) Đảm nhận từng vai trò, thử chuyển sang một vai trò khác mà người vận hành không được ủy quyền để đảm nhận, và xác minh rằng mô-đun từ chối quyền truy cập vào vai trò đó dựa trên danh tính của người vận hành.

Bảng 101 - VE và TE của AS04.40

Xác thực - mức 1, 2, 3 và 4	
AS04.40 ISO/IEC 19790:2025, 7.4.4.1	Khi một mô-đun mật mã được đặt lại, khởi động lại, tắt nguồn rồi sau đó bật nguồn lại, mô-đun phải yêu cầu người vận hành được xác thực, trừ khi tính năng bỏ qua xác thực lại được bật.
Thông tin bắt buộc từ nhà cung cấp	

VE04.40.01	Tài liệu do nhà cung cấp cung cấp phải mô tả cách kết quả của các lần xác thực trước đó bị xóa khi mô-đun bị tắt nguồn.
Quy trình kiểm thử bắt buộc	
TE04.40.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả việc xóa các lần xác thực trước đó khi tắt nguồn mô-đun.
TE04.40.02	Kiểm thử viên phải xác thực với mô-đun và đảm nhận một hoặc nhiều vai trò, tắt nguồn mô-đun, bật nguồn mô-đun, và thử thực hiện các dịch vụ trong các vai trò đó. Để đáp ứng khẳng định này, mô-đun phải từ chối quyền truy cập vào các dịch vụ sau khi bật nguồn và yêu cầu kiểm thử viên phải được xác thực lại.

Bảng 102 - VE và TE của AS04.41

Xác thực - mức 1, 2, 3 và 4	
AS04.41 ISO/IEC 19790:2025, 7.4.4.1	Dữ liệu xác thực bên trong một mô-đun mật mã phải được bảo vệ chống lại việc sử dụng, tiết lộ, sửa đổi, và thay thế trái phép.
Thông tin bắt buộc từ nhà cung cấp	
VE04.41.01	Tài liệu của nhà cung cấp phải mô tả việc bảo vệ tất cả dữ liệu xác thực bên trong mô-đun. Việc bảo vệ phải bao gồm triển khai các cơ chế bảo vệ chống lại việc sử dụng, tiết lộ, sửa đổi, và thay thế trái phép.
Quy trình kiểm thử bắt buộc	
TE04.41.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả việc bảo vệ dữ liệu xác thực. Kiểm thử viên phải xác minh rằng tài liệu mô tả cách dữ liệu sẽ được bảo vệ chống lại việc sử dụng, tiết lộ, sửa đổi, và thay thế trái phép.
TE04.41.02	Kiểm thử viên phải tìm cách truy cập (bằng cách lách qua các cơ chế bảo vệ đã được lập tài liệu) vào dữ liệu xác thực mà kiểm thử viên không được phép truy cập. Nếu mô-đun từ chối quyền truy cập hoặc chỉ cho phép truy cập vào các dạng dữ liệu đã được mã hóa hoặc được bảo vệ theo cách khác, thì yêu cầu này được đáp ứng.
CHÚ THÍCH Các chức năng an toàn đã phê duyệt có thể được sử dụng như một phần của cơ chế xác thực.	

Bảng 103 - VE và TE của AS04.42

Xác thực - mức 1, 2, 3 và 4	
AS04.42 ISO/IEC 19790:2025, 7.4.4.1	Dữ liệu của bộ kiểm chứng bên trong một mô-đun mật mã phải được bảo vệ chống lại việc sử dụng, tiết lộ, sửa đổi, và thay thế trái phép nếu nó được coi là một CSP, hoặc {phải được bảo vệ chống lại việc sửa đổi và thay thế trái phép nếu nó được coi là một PSP.}
Thông tin bắt buộc từ nhà cung cấp	
VE04.42.01	Tài liệu của nhà cung cấp phải mô tả việc bảo vệ tất cả dữ liệu của bộ kiểm chứng bên trong mô-đun. Việc bảo vệ phải bao gồm triển khai các cơ chế bảo vệ chống lại việc sử dụng, tiết lộ, sửa đổi, và thay thế trái phép.
Quy trình kiểm thử bắt buộc	
TE04.42.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả phương pháp để bảo vệ dữ liệu của bộ kiểm chứng. Kiểm thử viên phải xác minh rằng tài liệu mô tả cách dữ liệu sẽ được bảo vệ chống lại việc sử dụng, tiết lộ, sửa đổi, và thay thế trái phép.
TE04.42.02	Kiểm thử viên phải thực hiện các bài kiểm thử sau:

	a) Tìm cách truy cập (bằng cách lách qua các cơ chế bảo vệ đã được lập tài liệu) vào dữ liệu của bộ kiểm chứng mà kiểm thử viên không được phép truy cập. Nếu mô-đun từ chối quyền truy cập hoặc chỉ cho phép truy cập vào các dạng dữ liệu đã được mã hóa hoặc được bảo vệ theo cách khác, thì yêu cầu này được đáp ứng. b) Tìm cách sửa đổi hoặc thay thế dữ liệu của bộ kiểm chứng bằng cách sử dụng các giao diện của mô-đun và bất kỳ phương pháp nào không được quy định bởi tài liệu do nhà cung cấp cung cấp. Mô-đun phải ngăn chặn hoặc phát hiện sự sửa đổi hoặc thay thế dữ liệu của bộ kiểm chứng sao cho mô-đun không cho phép kiểm thử viên xác thực bằng cách sử dụng dữ liệu xác thực tương thích với dữ liệu của bộ kiểm chứng đã bị sửa đổi/thay thế, hoặc sử dụng dữ liệu của bộ kiểm chứng tương thích với dữ liệu xác thực đã bị sửa đổi/thay thế.
CHÚ THÍCH: Các chức năng an toàn đã phê duyệt có thể được sử dụng như một phần của cơ chế xác thực.	

Bảng 104 - VE và TE của AS04.43

Xác thực - mức 1, 2, 3 và 4	
AS04.43 ISO/IEC 19790:2025, 7.4.4.1	{Dữ liệu của bộ kiểm chứng bên trong một mô-đun mật mã phải được bảo vệ chống lại việc sử dụng, tiết lộ, sửa đổi, và thay thế trái phép nếu nó được coi là một CSP}, hoặc phải được bảo vệ chống lại việc sửa đổi và thay thế trái phép nếu nó được coi là một PSP.
Thông tin bắt buộc từ nhà cung cấp	
VE04.43.01	Tài liệu do nhà cung cấp cung cấp phải mô tả việc bảo vệ tất cả dữ liệu của bộ kiểm chứng bên trong mô-đun. Việc bảo vệ phải bao gồm triển khai các cơ chế bảo vệ chống lại việc sửa đổi và thay thế trái phép nếu nó được coi là một PSP.
Quy trình kiểm thử bắt buộc	
TE04.43.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả việc bảo vệ dữ liệu của bộ kiểm chứng. Kiểm thử viên phải xác minh rằng tài liệu mô tả cách dữ liệu sẽ được bảo vệ chống lại việc sửa đổi và thay thế trái phép nếu nó được coi là một PSP.
TE04.43.02	Kiểm thử viên phải thực hiện các bài kiểm thử sau: a) Tìm cách sửa đổi hoặc thay thế dữ liệu của bộ kiểm chứng bằng cách sử dụng các giao diện của mô-đun và bất kỳ phương pháp nào không được quy định bởi tài liệu do nhà cung cấp cung cấp. Mô-đun phải ngăn chặn hoặc phát hiện sự sửa đổi hoặc thay thế dữ liệu của bộ kiểm chứng sao cho mô-đun không cho phép kiểm thử viên xác thực bằng cách sử dụng dữ liệu xác thực tương thích với dữ liệu của bộ kiểm chứng đã bị sửa đổi/thay thế, hoặc sử dụng dữ liệu của bộ kiểm chứng tương thích với dữ liệu xác thực đã bị sửa đổi/thay thế.

Bảng 105 - VE và TE của AS04.44

Xác thực - mức 2, 3 và 4	
AS04.44 ISO/IEC 19790:2025, 7.4.4.1	Nếu một mô-đun mật mã không chứa dữ liệu của bộ kiểm chứng cần thiết để xác thực người vận hành trong lần đầu tiên mô-đun được truy cập, thì các phương pháp xác thực khác (ví dụ: kiểm soát thủ tục) phải được sử dụng để kiểm soát quyền truy cập vào mô-đun và khởi tạo các cơ chế xác thực.

Thông tin bắt buộc từ nhà cung cấp	
VE04.44.01	Tài liệu do nhà cung cấp cung cấp phải quy định các phương tiện để kiểm soát quyền truy cập vào mô-đun trước khi nó được khởi tạo.
Quy trình kiểm thử bắt buộc	
TE04.44.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả thủ tục mà người vận hành được xác thực khi truy cập mô-đun lần đầu tiên.
TE04.44.02	Nếu quyền truy cập vào mô-đun trước khi khởi tạo được kiểm soát bằng thủ tục, kiểm thử viên phải cố ý tạo ra một lỗi thủ tục trên một mô-đun chưa được khởi tạo và phải xác minh rằng mô-đun từ chối quyền truy cập. Kiểm thử viên phải đảm nhận vai trò được ủy quyền và xác minh rằng quá trình xác thực bắt buộc tuân thủ các thủ tục đã được lập tài liệu. Kiểm thử viên phải thử đảm nhận các vai trò khác trước khi mô-đun được khởi tạo và xác minh rằng mô-đun từ chối quyền truy cập vào các vai trò đó.

Bảng 106 - VE và TE của AS04.45

Xác thực - mức 2, 3 và 4	
AS04.45 ISO/IEC 19790:2025, 7.4.4.1	Nếu dữ liệu mặc định của bộ kiểm chứng được sử dụng để kiểm soát quyền truy cập vào các chức năng và quá trình an toàn đã phê duyệt của mô-đun, thì trong lần xác thực đầu tiên, dữ liệu mới của bộ kiểm chứng phải được cấu hình để sử dụng trong các lần xác thực tiếp theo bởi mỗi vai trò hoặc danh tính.
Thông tin bắt buộc từ nhà cung cấp	
VE04.45.01	Tài liệu do nhà cung cấp cung cấp phải quy định cách thức, trong lần xác thực đầu tiên, cách mô-đun buộc phải thiết lập dữ liệu kiểm chứng mới ngay trong lần xác thực đầu tiên để dùng cho các lần xác thực tiếp theo của từng vai trò hoặc danh tính.
VE04.45.02	Tài liệu do nhà cung cấp cung cấp phải quy định cách thức, trong các lần thử xác thực tiếp theo, mô-đun thực thi việc dữ liệu mặc định của bộ kiểm chứng không thể dẫn đến một quá trình xác thực thành công.
Quy trình kiểm thử bắt buộc	
TE04.45.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả cách thức, trong lần xác thực đầu tiên, mô-đun thực thi việc cấu hình dữ liệu mới của bộ kiểm chứng để sử dụng trong các lần thử tiếp theo bởi mỗi vai trò hoặc danh tính.
TE04.45.02	Nếu mô-đun được thiết kế để chỉ chấp nhận dữ liệu mới của bộ kiểm chứng ở lần xác thực đầu tiên, tức là sẽ không chấp nhận việc sử dụng lại dữ liệu mặc định của bộ kiểm chứng, kiểm thử viên phải nhập lại dữ liệu mặc định của bộ kiểm chứng. Nếu mô-đun không chấp nhận dữ liệu của bộ kiểm chứng này, bài kiểm thử đạt.

Bảng 107 - VE và TE của AS04.46

Xác thực - mức 2, 3 và 4	
AS04.46 ISO/IEC 19790:2025, 7.4.4.1	Yêu cầu này phải được mô-đun thực thi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS04.44 và AS04.45.	

Bảng 108 - VE và TE của AS04.47

Xác thực - mức 2, 3 và 4	
AS04.47 ISO/IEC 19790:2025, 7.4.4.1	Mô-đun phải triển khai một cơ chế xác thực đã phê duyệt như được tham chiếu trong ISO/IEC 19790:2025, Phụ lục E.
Thông tin bắt buộc từ nhà cung cấp	
VE04.47.01	Tài liệu do nhà cung cấp cung cấp phải mô tả cơ chế xác thực đã phê duyệt được sử dụng để xác thực người vận hành.
VE04.47.02	Nếu mô-đun triển khai một cơ chế xác thực đã phê duyệt, nhà cung cấp phải cung cấp chứng chỉ xác nhận hoặc cam kết của nhà cung cấp, nếu có, như quy định tại VE02.18.01 và VE02.18.03.
Quy trình kiểm thử bắt buộc	
TE04.47.01	Kiểm thử viên phải xác minh rằng cơ chế xác thực được sử dụng để xác thực người vận hành là một cơ chế đã được phê duyệt.

Bảng 109 - VE và TE của AS04.48

Xác thực - mức 2, 3 và 4	
AS04.48 ISO/IEC 19790:2025, 7.4.4.1	Độ mạnh của cơ chế xác thực đã phê duyệt phải được quy định trong chính sách an toàn tuân theo ISO/IEC 19790:2025, Phụ lục B.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	

Bảng 110 - VE và TE của AS04.49

Xác thực - mức 1, 2, 3 và 4	
AS04.49 ISO/IEC 19790:2025, 7.4.4.1	Nếu mô-đun mật mã sử dụng các chức năng an toàn để xác thực người vận hành, thì những chức năng an toàn đó phải là các chức năng an toàn đã được phê duyệt.
Thông tin bắt buộc từ nhà cung cấp	
VE04.49.01	Tài liệu do nhà cung cấp cung cấp phải quy định danh sách các chức năng an toàn được sử dụng để xác thực người vận hành.
VE04.49.02	Nhà cung cấp phải cung cấp chứng chỉ xác nhận, nếu có, cho từng chức năng an toàn đã phê duyệt như quy định tại VE02.18.01.
VE04.49.03	Nhà cung cấp phải cung cấp danh sách tất cả các chức năng an toàn theo cam kết của nhà cung cấp như quy định tại VE02.18.03.
Quy trình kiểm thử bắt buộc	
TE04.49.01	Kiểm thử viên phải xác minh rằng các chức năng an toàn được sử dụng để xác thực người vận hành đều là các chức năng an toàn đã được phê duyệt.

Bảng 111 - VE và TE của AS04.50

Xác thực - mức 2, 3 và 4	
AS04.50 ISO/IEC 19790: 2025,	Đối với mỗi lần thử sử dụng cơ chế xác thực đã phê duyệt, mô-đun phải đáp ứng độ mạnh của mục tiêu xác thực.

7.4.4.1	
Thông tin bắt buộc từ nhà cung cấp	
VE04.50.01	Tài liệu do nhà cung cấp cung cấp phải quy định mỗi cơ chế xác thực và tỷ lệ chấp nhận sai hoặc xác suất thành công của một lần truy cập ngẫu nhiên tương ứng.
Quy trình kiểm thử bắt buộc	
TE04.50.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp cho mỗi cơ chế xác thực có quy định tỷ lệ chấp nhận sai hoặc tỷ lệ truy cập ngẫu nhiên tương ứng.
TE04.50.02	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định cách thức đáp ứng mục tiêu cho mỗi cơ chế xác thực.

Bảng 112 - VE và TE của AS04.51

Xác thực - mức 2, 3 và 4	
AS04.51 ISO/IEC 19790:2025, 7.4.4.1	Đối với nhiều lần thử sử dụng cơ chế xác thực đã phê duyệt, mô-đun phải sử dụng phương pháp giới hạn tốc độ để đáp ứng độ mạnh của mục tiêu xác thực.
Thông tin bắt buộc từ nhà cung cấp	
VE04.51.01	Tài liệu do nhà cung cấp cung cấp phải quy định mỗi cơ chế xác thực và phương pháp giới hạn tốc độ tương ứng cho nhiều nỗ lực nhằm đáp ứng độ mạnh của mục tiêu xác thực.
Quy trình kiểm thử bắt buộc	
TE04.51.01	Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp đối với mỗi cơ chế xác thực rằng phương pháp giới hạn tốc độ tương ứng cho nhiều lần thử đã được quy định.
TE04.51.02	Kiểm thử viên phải xác minh rằng phương pháp giới hạn tốc độ tương ứng đang đáp ứng mục tiêu theo tài liệu do nhà cung cấp cung cấp cho mỗi cơ chế xác thực.

Bảng 113 - VE và TE của AS04.52

Xác thực - mức 2, 3 và 4	
AS04.52 ISO/IEC 19790:2025, 7.4.4.1	Cơ chế xác thực đã phê duyệt phải được đáp ứng bởi việc triển khai của mô-đun chứ không dựa vào các kiểm soát thủ tục hoặc quy tắc an toàn đã được lập tài liệu (ví dụ: các giới hạn về kích thước mật khẩu).
Thông tin bắt buộc từ nhà cung cấp	
VE04.52.01	Nhà cung cấp phải cung cấp mô tả hoàn chỉnh về các cơ chế xác thực.
Quy trình kiểm thử bắt buộc	
TE04.52.01	Kiểm thử viên phải kiểm tra mô-đun và xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng cơ chế xác thực đã phê duyệt được đáp ứng bởi việc triển khai của mô-đun và không dựa vào các kiểm soát thủ tục hoặc quy tắc an toàn đã được lập tài liệu.
TE04.52.02	Nếu mô-đun cho phép cấu hình cơ chế xác thực, kiểm thử viên phải làm theo các hướng dẫn cấu hình và sau đó thử thiết lập dữ liệu xác thực cho mô-đun bằng cách sử dụng dữ liệu của bộ kiểm chứng đáp ứng độ mạnh của mục tiêu xác thực của mô-đun, ví dụ: mật khẩu có độ dài đủ. Nếu mô-đun cho phép kiểm thử viên thiết lập

	cơ chế xác thực, bài kiểm thử đạt.
TE04.52.03	Nếu mô-đun cho phép cấu hình cơ chế xác thực, kiểm thử viên phải làm theo các hướng dẫn cấu hình và sau đó thử thiết lập dữ liệu xác thực cho mô-đun bằng cách sử dụng dữ liệu của bộ kiểm chứng không đáp ứng độ mạnh của mục tiêu xác thực của mô-đun, ví dụ: mật khẩu có độ dài không đủ. Nếu mô-đun cho phép kiểm thử viên thiết lập cơ chế xác thực ở mức độ yếu hơn, bài kiểm thử thất bại.

Bảng 114 - VE và TE của AS04.53

Xác thực - mức 2	
AS04.53 ISO/IEC 19790:2025, 7.4.4.1	Nếu hệ điều hành triển khai cơ chế xác thực, thì cơ chế xác thực đó phải đáp ứng các yêu cầu trong ISO/IEC 19790:2025, 7.4.4 áp dụng đối với mức an toàn được yêu cầu của cơ chế xác thực.
Thông tin bắt buộc từ nhà cung cấp	
VE04.53.01	Nhà cung cấp phải cung cấp đặc tả cơ chế xác thực của hệ điều hành.
Quy trình kiểm thử bắt buộc	
TE04.53.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng cơ chế xác thực đã phê duyệt được triển khai trong hệ điều hành đáp ứng các yêu cầu áp dụng.

Bảng 115 - VE và TE của AS04.54

Xác thực - mức 2, 3 và 4	
AS04.54 ISO/IEC 19790:2025, 7.4.4.1	Phản hồi của dữ liệu xác thực tới người vận hành phải được làm mờ trong quá trình xác thực đối với bất kỳ ai không phải là người vận hành (ví dụ: khi nhập mật khẩu, các ký tự riêng lẻ không được hiển thị đủ lâu để ai đó khác ngoài người vận hành có thể nhìn thấy chúng).
Thông tin bắt buộc từ nhà cung cấp	
VE04.54.01	Tài liệu do nhà cung cấp cung cấp phải quy định phương pháp được sử dụng để làm mờ phản hồi của dữ liệu xác thực đối với bất kỳ ai không phải là người vận hành trong quá trình nhập dữ liệu xác thực.
VE04.54.02	Tài liệu do nhà cung cấp cung cấp phải quy định cách thức (nếu được triển khai) nhà cung cấp cho phép người vận hành xác nhận dữ liệu xác thực tại thời điểm nhập, trong khi vẫn làm mờ bất kỳ thông tin hữu ích nào đối với tất cả những người khác.
Quy trình kiểm thử bắt buộc	
TE04.54.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng dữ liệu xác thực được làm mờ đối với bất kỳ ai không phải là người vận hành trong quá trình nhập dữ liệu.
TE04.54.02	Kiểm thử viên phải nhập dữ liệu xác thực và xác minh rằng không có sự hiển thị rõ ràng của dữ liệu xác thực đối với bất kỳ ai không phải là người vận hành trong quá trình nhập dữ liệu.
TE04.54.03	Nếu nhà cung cấp cho phép người vận hành xác nhận dữ liệu xác thực tại thời điểm nhập, kiểm thử viên phải xác minh rằng thông tin này được làm mờ đối với các thực thể khác.

Bảng 116 - VE và TE của AS04.55

Xác thực - mức 2, 3 và 4	
AS04.55 ISO/IEC 19790:2025, 7.4.4.1	Phản hồi được cung cấp cho người vận hành trong một lần thử xác thực phải ngăn chặn sự suy giảm độ mạnh của cơ chế xác thực vượt quá độ mạnh xác thực yêu cầu.
Thông tin bắt buộc từ nhà cung cấp	
VE04.55.01	Tài liệu do nhà cung cấp cung cấp phải quy định cơ chế phản hồi được sử dụng khi người vận hành đang nhập dữ liệu xác thực.
Quy trình kiểm thử bắt buộc	
TE04.55.01	Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp rằng cơ chế phản hồi không cung cấp thông tin có thể được sử dụng để đoán hoặc xác định dữ liệu xác thực.
TE04.55.02	Kiểm thử viên phải nhập dữ liệu xác thực để đảm nhận từng vai trò nhằm đảm bảo rằng cơ chế phản hồi không cung cấp thông tin hữu ích.

6.4.4.2 Mức an toàn 1**Bảng 117 - VE và TE của AS04.56**

Xác thực - mức 1	
AS04.56 ISO/IEC 19790:2025, 7.4.4.2	Đối với mức an toàn 1, một mô-đun mật mã không bắt buộc phải sử dụng các cơ chế xác thực để kiểm soát quyền truy cập vào mô-đun. Nếu một mô-đun không hỗ trợ các cơ chế xác thực, mô-đun phải yêu cầu người vận hành chọn một hoặc nhiều vai trò một cách ngầm định hoặc tường minh.
Thông tin bắt buộc từ nhà cung cấp	
VE04.56.01	Nhà cung cấp phải lập tài liệu về loại hình xác thực được thực hiện đối với mô-đun. Nhà cung cấp phải lập tài liệu về các cơ chế được sử dụng để thực hiện việc lựa chọn một cách ngầm định hoặc tường minh một vai trò hay tập hợp các vai trò, và cơ chế xác thực người vận hành để đảm nhận các vai trò đó.
VE04.56.02	Chính sách an toàn phi độc quyền do nhà cung cấp cung cấp phải cung cấp mô tả về các vai trò, ngầm định hoặc tường minh, mà người vận hành có thể đảm nhận.
VE04.56.03	Chính sách an toàn phi độc quyền do nhà cung cấp cung cấp phải cung cấp các hướng dẫn cho người vận hành để đảm nhận các vai trò ngầm định hoặc tường minh.
Quy trình kiểm thử bắt buộc	
TE04.56.01	Kiểm thử viên phải xác minh rằng chính sách an toàn phi độc quyền do nhà cung cấp cung cấp có mô tả các vai trò, ngầm định hoặc tường minh, mà người vận hành có thể đảm nhận và phương tiện để đảm nhận từng vai trò.
TE04.56.02	Kiểm thử viên phải gọi phương thức được mô tả trong chính sách an toàn phi độc quyền và xác minh rằng mỗi vai trò có thể được đảm nhận một cách ngầm định hoặc tường minh.

6.4.4.3 Mức an toàn 2**Bảng 118 - VE và TE của AS04.57**

Xác thực - mức 2

AS04.57 ISO/IEC 19790:2025, 7.4.4.3	Đối với mức an toàn 2, một mô-đun mật mã tối thiểu phải sử dụng xác thực dựa trên vai trò để kiểm soát quyền truy cập vào mô-đun.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS04.33.	

6.4.4.4 Mức an toàn 3

Bảng 119 - VE và TE của AS04.58

Xác thực - mức 3	
AS04.58 ISO/IEC 19790:2025, 7.4.4.4	Đối với mức an toàn 3, một mô-đun mật mã phải sử dụng các cơ chế xác thực dựa trên danh tính để kiểm soát quyền truy cập vào mô-đun.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS04.37 và AS04.38.	

6.4.4.5 Mức an toàn 4

Bảng 120 - VE và TE của AS04.59

Xác thực - mức 4	
AS04.59 ISO/IEC 19790:2025, 7.4.4.5	Ngoài các yêu cầu tại mức an toàn 3, một mô-đun mật mã phải sử dụng các cơ chế xác thực dựa trên danh tính đa yếu tố hoặc một phương pháp xác thực khác đáp ứng các yêu cầu mức an toàn 4 trong ISO/IEC 19790:2025, Phụ lục E.
Thông tin bắt buộc từ nhà cung cấp	
VE04.59.01	Nhà cung cấp phải cung cấp đặc tả về xác thực dựa trên danh tính đa yếu tố hoặc một phương pháp xác thực khác đáp ứng các yêu cầu của mức an toàn 4 trong ISO/IEC 19790:2025, Phụ lục E.
Quy trình kiểm thử bắt buộc	
TE04.59.01	Kiểm thử viên phải xác minh tài liệu của nhà cung cấp và đánh giá xác thực dựa trên danh tính đa yếu tố hoặc một phương pháp xác thực khác đáp ứng các yêu cầu của mức an toàn 4 trong ISO/IEC 19790:2025, Phụ lục E.
TE04.59.02	Nếu mô-đun hỗ trợ xác thực dựa trên định danh đa yếu tố, kiểm thử viên phải xác minh rằng các cơ chế xác thực yêu cầu nhiều yếu tố xác thực thuộc ít nhất hai loại yếu tố xác thực độc lập. Việc xác minh được thực hiện bằng cách phân loại từng yếu tố xác thực vào một trong các loại sau: điều mà một người biết, điều mà một người có, hoặc điều mà một người là.

6.5 An toàn phần mềm/phần sụn

6.5.1 Yêu cầu chung về an toàn phần mềm/phần sụn

Bảng 121 - VE và TE của AS05.01

Yêu cầu chung về an toàn phần mềm/phần sụn - mức 1, 2, 3 và 4	
AS05.01 ISO/IEC	Các yêu cầu của điều khoản này phải áp dụng cho các thành phần phần mềm, phần sụn, hoặc dòng bit của một mô-đun mật mã.

19790:2025, 7.5.1	
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS05.09, AS05.10, AS05.11, AS05.12, AS05.13, AS05.14, AS05.15, AS05.16, AS05.17, AS05.18, AS05.19, AS05.20, AS05.21, AS05.22, AS05.23, AS05.24, AS05.25, AS05.26, AS05.27, AS05.28 và AS05.29.	

Bảng 122 - VE và TE của AS05.02

Yêu cầu chung về an toàn phần mềm/phần sụn - mức 1	
AS05.02 ISO/IEC 19790:2025, 7.5.1	Vùng chứa an toàn phải được kiểm soát để ngăn chặn phần sụn thực thi chưa được thẩm định bên trong vùng chứa an toàn can thiệp hoặc làm tổn hại đến mô-đun mật mã. Ngoài ra, {các yêu cầu sau đây phải được áp dụng:} {AS05.04 đến AS05.08}.
Thông tin bắt buộc từ nhà cung cấp	
VE05.02.01	Nhà cung cấp phải cung cấp một mô tả về cách thức vùng chứa an toàn được kiểm soát để ngăn chặn phần sụn thực thi chưa được thẩm định bên trong vùng chứa an toàn can thiệp hoặc làm tổn hại đến mô-đun mật mã.
Quy trình kiểm thử bắt buộc	
TE05.02.01	Kiểm thử viên phải xem xét tài liệu của nhà cung cấp và kiểm tra việc triển khai để xác minh rằng vùng chứa an toàn được kiểm soát nhằm ngăn chặn phần sụn thực thi chưa được thẩm định bên trong vùng chứa an toàn can thiệp hoặc làm tổn hại đến mô-đun mật mã.
CHÚ THÍCH Khẳng định này không được áp dụng nếu nhà cung cấp mô-đun mật mã không tuyên bố về vùng chứa an toàn.	

Bảng 123 - VE và TE của AS05.03

Yêu cầu chung về an toàn phần mềm/phần sụn - mức 1	
AS05.03 ISO/IEC 19790:2025, 7.5.1	{Vùng chứa an toàn phải được kiểm soát để ngăn chặn phần sụn thực thi chưa được thẩm định bên trong vùng chứa an toàn can thiệp hoặc làm phương hại đến mô-đun mật mã.} Ngoài ra, các yêu cầu sau đây phải được áp dụng: {AS05.04 đến AS05.08}.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS05.04, AS05.05, AS05.06, AS05.07 và AS05.08.	

Bảng 124 - VE và TE của AS05.04

Yêu cầu chung về an toàn phần mềm/phần sụn - mức 1	
AS05.04 ISO/IEC 19790:2025, 7.5.1	Bài kiểm thử nạp phần mềm/phần sụn được quy định trong ISO/IEC 19790:2025, 7.10.4.4 phải được mô-đun thực hiện trước khi phần sụn được nạp vào vùng chứa an toàn có thể được thực thi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.37, AS10.38, AS10.39, AS10.40, AS10.41 và AS10.42.	

Bảng 125 - VE và TE của AS05.05

Yêu cầu chung về an toàn phần mềm/phần sụn - mức 1	
---	--

AS05.05 ISO/IEC 19790:2025, 7.5.1	Biên của mô-đun với phần sụn của vùng chứa an toàn phải được xác định.
Thông tin bắt buộc từ nhà cung cấp	
VE05.05.01	Nhà cung cấp phải cung cấp một mô tả về biên của mô-đun mật mã với phần sụn của vùng chứa an toàn.
Quy trình kiểm thử bắt buộc	
TE05.05.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp xác định rõ biên của mô-đun mật mã với phần sụn của vùng chứa an toàn.
TE05.05.02	Bằng cách nhận diện biên của mô-đun mật mã, kiểm thử viên phải xác minh rằng biên của mô-đun mật mã trong tài liệu do nhà cung cấp cung cấp là nhất quán với biên của mô-đun mật mã trong thực tế.

Bảng 126 - VE và TE của AS05.06

Yêu cầu chung về an toàn phần mềm/phần sụn - mức 1	
AS05.06 ISO/IEC 19790:2025, 7.5.1	Các giao diện được cung cấp bởi mô-đun cho phần sụn của vùng chứa an toàn phải được xác định (ví dụ: tất cả các giao diện mà mô-đun cung cấp cho vùng chứa an toàn nhằm cho phép đầu vào và đầu ra dữ liệu và điều khiển, trạng thái, v.v. đối với các giao diện bên ngoài của mô-đun từ phần sụn đang thực thi trong vùng chứa an toàn).
Thông tin bắt buộc từ nhà cung cấp	
VE05.06.01	Nhà cung cấp phải cung cấp một mô tả về các giao diện được cung cấp bởi mô-đun mật mã cho phần sụn của vùng chứa an toàn.
Quy trình kiểm thử bắt buộc	
TE05.06.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp xác định rõ các giao diện được cung cấp bởi mô-đun mật mã cho phần sụn của vùng chứa an toàn.
TE05.06.02	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và xác định các giao diện của mô-đun mật mã để kiểm tra xem việc triển khai của mô-đun mật mã có nhất quán với các giao diện của mô-đun mật mã (được mô tả) hay không.

Bảng 127 - VE và TE của AS05.07

Yêu cầu chung về an toàn phần mềm/phần sụn - mức 1, 2, 3 và 4	
AS05.07 ISO/IEC 19790:2025, 7.5.1	Các dịch vụ được cung cấp bởi mô-đun cho phần sụn của vùng chứa an toàn phải được xác định.
Thông tin bắt buộc từ nhà cung cấp	
VE05.07.01	Nhà cung cấp phải cung cấp một mô tả về các dịch vụ được cung cấp bởi mô-đun mật mã cho phần sụn của vùng chứa an toàn, bao gồm các vai trò và phương thức xác thực được yêu cầu để truy cập vào mỗi dịch vụ.
Quy trình kiểm thử bắt buộc	
TE05.07.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp xác định rõ các dịch vụ được cung cấp bởi mô-đun mật mã cho phần sụn của vùng chứa an toàn, bao gồm các vai trò và phương thức xác thực được yêu cầu để truy cập vào mỗi dịch vụ.
TE05.07.02	Từ tài liệu do nhà cung cấp cung cấp, bằng cách nhận diện các dịch vụ của mô-đun mật mã, kiểm thử viên phải xác minh rằng việc triển khai của mô-đun mật mã là nhất

	quán với các dịch vụ của mô-đun mật mã (đã nêu).
CHÚ THÍCH Việc xác thực trước khi truy cập vào các dịch vụ yêu cầu sử dụng một vai trò được xác thực sẽ được kiểm thử như một phần của AS04.56 đến AS04.59.	

Bảng 128 - VE và TE của AS05.08

Yêu cầu chung về an toàn phần mềm/phần sụn – mức 1	
AS05.08 ISO/IEC 19790:2025, 7.5.1	Tất cả các vai trò của mô-đun có quyền truy cập vào phần sụn của vùng chứa an toàn phải được xác định.
Thông tin bắt buộc từ nhà cung cấp	
VE05.08.01	Nhà cung cấp phải cung cấp một mô tả về các vai trò của mô-đun mật mã có quyền truy cập vào phần sụn của vùng chứa an toàn.
Quy trình kiểm thử bắt buộc	
TE05.08.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp xác định rõ các vai trò của mô-đun mật mã có quyền truy cập vào phần sụn của vùng chứa an toàn.
TE05.08.02	Kiểm thử viên phải xác minh tài liệu do nhà cung cấp cung cấp bằng cách nhận diện các vai trò của mô-đun mật mã nhằm đảm bảo rằng việc triển khai mô-đun mật mã là nhất quán với các vai trò của mô-đun mật mã có quyền truy cập vào phần sụn của vùng chứa an toàn.

Bảng 129 - VE và TE của AS05.09

Yêu cầu chung về an toàn phần mềm/phần sụn - mức 1, 2, 3 và 4	
AS05.09 ISO/IEC 19790:2025, 7.5.1	Tài liệu về an toàn phần mềm/phần sụn được quy định trong ISO/IEC 19790:2025, A.2.4 phải được cung cấp.
Thông tin bắt buộc từ nhà cung cấp	
VE05.09.01	Nhà cung cấp phải cung cấp tài liệu như được quy định trong ISO/IEC 19790:2025, A.2.4.
Quy trình kiểm thử bắt buộc	
TE05.09.01	Kiểm thử viên phải xác minh tính đầy đủ của tài liệu được quy định trong ISO/IEC 19790:2025, A.2.4.

6.5.2 Mức an toàn 1**Bảng 130 - VE và TE của AS05.10**

Mức an toàn 1 - mức 1, 2, 3 và 4	
AS05.10 ISO/IEC 19790:2025, 7.5.2	Các yêu cầu sau đây phải được áp dụng cho các thành phần phần mềm, phần sụn, hoặc dòng bit của một mô-đun mật mã đối với mức an toàn 1: {AS05.11 đến AS05.19}.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 131 - VE và TE của AS05.11

Mức an toàn 1 - mức 1, 2, 3 và 4	
AS05.11 ISO/IEC 19790:2025, 7.5.2	Tất cả phần mềm, phần sụn, hoặc dòng bit phải ở định dạng đáp ứng các yêu cầu của tiêu chuẩn này mà không cần sửa đổi trước khi cài đặt.
Thông tin bắt buộc từ nhà cung cấp	
VE05.11.01	Nhà cung cấp phải cung cấp đặc tả phần mềm, phần sụn, hoặc dòng bit.
Quy trình kiểm thử bắt buộc	
TE05.11.01	Kiểm thử viên phải xác minh, bằng cách kiểm tra mô-đun mật mã, rằng các đặc tả được cung cấp bởi tài liệu do nhà cung cấp cung cấp là nhất quán với thiết kế thực tế của mô-đun mật mã.

Bảng 132 - VE và TE của AS05.12

Mức an toàn 1 - mức 1, 2, 3 và 4	
AS05.12 ISO/IEC 19790:2025, 7.5.2	Một cơ chế mật mã sử dụng một kỹ thuật toàn vẹn đã được phê duyệt phải được áp dụng cho tất cả các thành phần phần mềm và phần sụn bên trong biên mật mã đã được xác định của mô-đun theo một trong các cách sau: a) bởi chính mô-đun mật mã; hoặc b) bởi một mô-đun mật mã đã được thẩm định khác sử dụng một dịch vụ đã phê duyệt.
Thông tin bắt buộc từ nhà cung cấp	
VE05.12.01	Tài liệu do nhà cung cấp cung cấp phải mô tả kỹ thuật toàn vẹn đã phê duyệt được áp dụng cho các mô-đun phần mềm và phần sụn cũng như các thành phần phần mềm hoặc phần sụn tách biệt của một mô-đun lai.
VE05.12.02	Tài liệu do nhà cung cấp cung cấp phải quy định cách thức kỹ thuật toàn vẹn được áp dụng cho các mô-đun phần mềm và phần sụn cũng như các thành phần phần mềm hoặc phần sụn tách biệt của một mô-đun lai bằng cách sử dụng: a) một chữ ký hoặc mã xác thực thông điệp bao trùm duy nhất, hoặc b) nhiều chữ ký hoặc mã rời rạc.
VE05.12.03	Tài liệu do nhà cung cấp cung cấp phải mô tả liệu kỹ thuật toàn vẹn đã phê duyệt được triển khai bởi chính mô-đun mật mã hay bởi một mô-đun mật mã đã được thẩm định khác sử dụng một dịch vụ đã phê duyệt.
VE05.12.04	Tài liệu do nhà cung cấp cung cấp phải quy định vị trí của khóa mật mã được sử dụng trong kỹ thuật toàn vẹn. Nếu chữ ký số đã phê duyệt được sử dụng làm kỹ thuật toàn vẹn, tài liệu do nhà cung cấp cung cấp cũng phải quy định vị trí của khóa ký riêng được sử dụng để tạo ra chữ ký tham chiếu.
VE05.12.05	Nhà cung cấp phải cung cấp chứng chỉ xác nhận, nếu có, hoặc cam kết của nhà cung cấp cho kỹ thuật toàn vẹn đã phê duyệt như quy định tại VE02.18.01 và VE02.18.03.
VE05.12.06	Tài liệu do nhà cung cấp cung cấp phải mô tả liệu các giá trị tạm thời được tạo ra trong quá trình kiểm tra tính toàn vẹn phần mềm hoặc phần sụn của mô-đun có bị xóa trắng khi hoàn thành quá trình kiểm tra tính toàn vẹn hay không.
Quy trình kiểm thử bắt buộc	
TE05.12.01	Kiểm thử viên phải xác minh bằng cách kiểm tra mô-đun mật mã rằng một kỹ thuật toàn vẹn đã phê duyệt được áp dụng cho các mô-đun phần mềm và phần sụn

	cũng như các thành phần phần mềm hoặc phần sụn tách biệt của một mô-đun lai.
TE05.12.02	Kiểm thử viên phải xác minh rằng nhà cung cấp đã cung cấp chứng chỉ xác nhận, nếu có, hoặc cam kết của nhà cung cấp cho kỹ thuật toàn vẹn đã phê duyệt được triển khai như quy định tại VE02.18.01 và VE02.18.03.
TE05.12.03	a) Nếu mô-đun triển khai một hàm băm hoặc MAC cho bài kiểm thử tính toàn vẹn phần mềm/phần sụn, kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp về bài kiểm thử tính toàn vẹn phần mềm/phần sụn mô tả đầy đủ quá trình mà theo đó hàm băm hoặc MAC được tính toán và kiểm chứng.
TE05.12.04	Nếu mô-đun triển khai một chữ ký số đã phê duyệt cho bài kiểm thử tính toàn vẹn phần mềm/phần sụn, kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp về bài kiểm thử tính toàn vẹn phần mềm/phần sụn bao gồm các nội dung sau: a) đặc tả về thuật toán chữ ký số đã phê duyệt được triển khai; b) nhận diện phần mềm và phần sụn được bảo vệ bằng các chữ ký số đã phê duyệt; c) xác minh rằng giá trị được tính toán trước của chữ ký số đã phê duyệt được bao gồm cùng với phần mềm hoặc phần sụn; d) kiểm chứng chữ ký số đã phê duyệt; e) bài tự kiểm thử thất bại nếu việc kiểm chứng chữ ký số đã phê duyệt thất bại.
TE05.12.05	Ngay cả khi kỹ thuật toàn vẹn đã phê duyệt được cung cấp bởi một mô-đun đã được thẩm định khác, kiểm thử viên phải xác minh rằng việc xác định đạt hay thất bại của bài kiểm thử tính toàn vẹn phần mềm/phần sụn được thực hiện như quy định tại AS10.01.
TE05.12.06	Bằng cách kiểm tra mã lệnh và tài liệu thiết kế, kiểm thử viên phải xác minh rằng việc triển khai bài kiểm thử phần mềm/phần sụn là nhất quán với thông tin được cung cấp theo AS05.12 và AS05.15.
TE05.12.07	Kiểm thử viên phải sửa đổi các thành phần phần mềm và phần sụn mật mã. Bài kiểm thử này thất bại nếu các cơ chế toàn vẹn không phát hiện ra các sửa đổi.
TE05.12.08	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả liệu các giá trị tạm thời được tạo ra trong quá trình kiểm tra tính toàn vẹn của phần mềm hoặc phần sụn của mô-đun có bị xóa trắng khi hoàn thành quá trình kiểm tra tính toàn vẹn hay không.

Bảng 133 - VE và TE của AS05.13

Mức an toàn 1 - mức 1, 2, 3 và 4	
AS05.13 ISO/IEC 19790:2025, 7.5.2	Một cơ chế mật mã sử dụng một kỹ thuật toàn vẹn đã được phê duyệt hoặc một mã phát hiện sai (EDC) phải được áp dụng cho tất cả các thành phần phần sụn hoặc dòng bit bên trong biên mật mã đã được xác định của mô-đun phần cứng hoặc bên trong các thành phần phần cứng tách biệt của mô-đun lai.
Thông tin bắt buộc từ nhà cung cấp	
VE05.13.01	Tài liệu do nhà cung cấp cung cấp phải mô tả kỹ thuật toàn vẹn đã được phê duyệt hoặc mã phát hiện sai được áp dụng cho tất cả các thành phần phần sụn hoặc dòng bit của một mô-đun mật mã phần cứng và các thành phần phần sụn hoặc dòng bit

	bên trong một thành phần phần cứng tách biệt của một mô-đun mật mã lai.
VE05.13.02	Tài liệu do nhà cung cấp cung cấp phải quy định cách thức kỹ thuật toàn vẹn đã được phê duyệt hoặc mã phát hiện sai được áp dụng cho tất cả các thành phần phần sụn hoặc dòng bit của một mô-đun mật mã phần cứng và các thành phần phần sụn hoặc dòng bit bên trong một thành phần phần cứng tách biệt của một mô-đun mật mã lai.
VE05.13.03	Nếu mô-đun triển khai một mã phát hiện sai, nhà cung cấp phải cung cấp tài liệu theo yêu cầu tại VE05.14.01.
VE05.13.04	Nếu mô-đun mật mã triển khai một kỹ thuật toàn vẹn đã được phê duyệt cho bài kiểm thử tính toàn vẹn, tài liệu do nhà cung cấp cung cấp phải cung cấp thông tin theo yêu cầu tại VE05.12.02, VE05.12.04, và VE05.12.05.
Quy trình kiểm thử bắt buộc	
TE05.13.01	Kiểm thử viên phải xác minh bằng cách kiểm tra mô-đun mật mã rằng một kỹ thuật toàn vẹn đã được phê duyệt hoặc mã phát hiện sai được áp dụng cho tất cả các thành phần phần sụn hoặc dòng bit của một mô-đun mật mã phần cứng và tất cả các thành phần phần sụn hoặc dòng bit bên trong một thành phần phần cứng tách biệt của một mô-đun mật mã lai.
TE05.13.02	Nếu mô-đun triển khai một mã phát hiện sai, kiểm thử viên phải tuân theo các quy trình được yêu cầu tại TE05.14.01.
TE05.13.03	Nếu mô-đun triển khai một hàm băm hoặc MAC cho bài kiểm thử tính toàn vẹn, kiểm thử viên phải tuân theo các quy trình được yêu cầu tại TE05.12.03.
TE05.13.04	Nếu mô-đun triển khai một chữ ký số đã được phê duyệt cho bài kiểm thử tính toàn vẹn, kiểm thử viên phải tuân theo các quy trình được yêu cầu tại TE05.12.04.
TE05.13.05	Bằng cách kiểm tra mã lệnh và tài liệu thiết kế, kiểm thử viên phải xác minh rằng việc triển khai bài kiểm thử tính toàn vẹn là nhất quán với thông tin được cung cấp từ AS05.13 đến AS05.15.
TE05.13.06	Kiểm thử viên phải sửa đổi các thành phần phần sụn hoặc dòng bit mật mã. Bài kiểm thử này thất bại nếu các cơ chế toàn vẹn không phát hiện ra các sửa đổi.

Bảng 134 - VE và TE của AS05.14

Mức an toàn 1 - mức 1, 2, 3 và 4	
AS05.14 ISO/IEC 19790:2025, 7.5.2	Nếu một EDC được sử dụng, EDC đó phải có độ dài ít nhất là 16 bit.
Thông tin bắt buộc từ nhà cung cấp	
VE05.14.01	Nhà cung cấp phải cung cấp đặc tả về mã phát hiện sai được sử dụng bên trong mô-đun. Cơ chế này phải là một mã phát hiện sai có độ dài ít nhất là 16 bit. Nhà cung cấp phải cung cấp: a) mô tả thuật toán tính toán EDC; b) tính toán các EDC khi phần sụn được cài đặt; c) mô tả quy trình kiểm chứng: 1) tính toán lại các EDC khi bài tự kiểm thử được khởi tạo; 2) so sánh EDC được lưu trữ với EDC được tính toán lại;

	3) các đầu ra dự kiến cho sự thành công hay thất bại của bài kiểm thử
Quy trình kiểm thử bắt buộc	
TE05.14.01	Kiểm thử viên phải xác minh rằng mã phát hiện sai có độ dài ít nhất là 16 bit và xác minh bằng cách kiểm tra xem thông tin sau đây có được cung cấp hay không: - việc triển khai thuật toán tính toán EDC; - quy trình kiểm chứng: - tính toán lại các EDC khi bài tự kiểm thử được khởi tạo; - so sánh EDC được lưu trữ với EDC được tính toán lại; - các đầu ra dự kiến cho sự thành công hay thất bại của bài kiểm thử

Bảng 135 - VE và TE của AS05.15

Mức an toàn 1 - mức 1, 2, 3 và 4	
AS05.15 ISO/IEC 19790:2025, 7.5.2	Nếu bài kiểm thử tính toán vẹn thất bại (tức là kết quả tính toán không được kiểm chứng thành công hoặc EDC không thể được kiểm chứng tùy thuộc vào loại mô-đun), mô-đun phải chuyển sang trạng thái lỗi.
Thông tin bắt buộc từ nhà cung cấp	
VE05.15.01	Nhà cung cấp phải cung cấp đặc tả về bài kiểm thử tính toán vẹn của phần mềm/phần sụn. Cơ chế này phải là một kỹ thuật toàn vẹn đã được phê duyệt hoặc một mã phát hiện sai tùy thuộc vào loại mô-đun (xem AS05.12 và AS05.13).
Quy trình kiểm thử bắt buộc	
TE05.15.01	Kiểm thử viên phải xác minh rằng nếu bài kiểm thử tính toán vẹn thất bại, mô-đun sẽ bước vào trạng thái lỗi.

Bảng 136 - VE và TE của AS05.16

Mức an toàn 1 - mức 1, 2, 3 và 4	
AS05.16 ISO/IEC 19790:2025, 7.5.2	Bài kiểm thử tính toán vẹn có thể bao gồm một mã xác thực thông điệp bao trùm duy nhất; EDC; chữ ký; hoặc nhiều mã xác thực, EDC hoặc chữ ký rời rạc mà nếu bất kỳ mã xác thực, EDC hoặc chữ ký rời rạc nào bị lỗi đều sẽ khiến mô-đun bước vào trạng thái lỗi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS05.12, AS05.13 và AS05.15.	

Bảng 137 - VE và TE của AS05.17

Mức an toàn 1 - mức 1, 2, 3 và 4	
AS05.17 ISO/IEC 19790:2025, 7.5.2	Người vận hành phải có khả năng thực hiện bài kiểm thử tính toán vẹn theo yêu cầu.
Thông tin bắt buộc từ nhà cung cấp	
VE05.17.01	Tài liệu do nhà cung cấp cung cấp phải mô tả cách thực hiện bài kiểm thử tính toán vẹn theo yêu cầu thông qua một dịch vụ, quá trình đặt lại, khởi động lại, hoặc chu kỳ nguồn.
Quy trình kiểm thử bắt buộc	
TE05.17.01	Kiểm thử viên phải xác minh rằng bài kiểm thử tính toán vẹn có thể được thực hiện

	theo yêu cầu thông qua một dịch vụ, quá trình đặt lại, khởi động lại, hoặc chu kỳ nguồn.
TE05.17.02	Kiểm thử viên phải xác minh bằng cách kiểm tra mô-đun rằng tính toàn vẹn của tất cả các thành phần phần mềm và phần sụn bên trong mô-đun được kiểm tra trong suốt bài kiểm thử tính toàn vẹn có thể gọi được theo yêu cầu thông qua một dịch vụ, quá trình đặt lại, khởi động lại, hoặc chu kỳ nguồn.

Bảng 138 - VE và TE của AS05.18

Mức an toàn 1 - mức 1, 2, 3 và 4	
AS05.18 ISO/IEC 19790:2025, 7.5.2	Tất cả các đầu vào dữ liệu và điều khiển, cũng như các đầu ra dữ liệu, điều khiển và trạng thái của mô-đun mật mã và các dịch vụ đều phải được định tuyến thông qua một giao diện mô-đun đã được định nghĩa.
Thông tin bắt buộc từ nhà cung cấp	
VE05.18.01	Yêu cầu về tài liệu do nhà cung cấp cung cấp được quy định tại VE05.22.01 và 6.3.1, 6.3.2 và 6.4.3.
Quy trình kiểm thử bắt buộc	
TE05.18.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có quy định những nội dung sau: a) toàn bộ tập hợp các lệnh được sử dụng để yêu cầu các dịch vụ của mô-đun mật mã, bao gồm cả các tham số đi vào hoặc đi ra khỏi biên mật mã của mô-đun như một phần của dịch vụ được yêu cầu.
TE05.18.02	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng tất cả các đầu vào dữ liệu và điều khiển, cũng như các đầu ra dữ liệu, điều khiển và trạng thái của mô-đun mật mã và các dịch vụ chỉ truyền qua giao diện mô-đun đã được định nghĩa.

Bảng 139 - VE và TE của AS05.19

Mức an toàn 1 - mức 1, 2, 3 và 4	
AS05.19 ISO/IEC 19790:2025, 7.5.2	Nếu phần mềm, phần sụn, hoặc dòng bit được nạp và được liên kết, ràng buộc với, sửa đổi hoặc là một điều kiện thực thi bắt buộc của mô-đun đã được thẩm định, thì bài kiểm thử nạp phần mềm/phần sụn là có thể áp dụng và phải được thực hiện bởi mô-đun đã được thẩm định.
Thông tin bắt buộc từ nhà cung cấp	
VE05.19.01	Nhà cung cấp phải cung cấp một đặc tả về các quy trình nạp phần mềm/phần sụn, bao gồm: a) các loại quy trình nạp phần mềm hoặc phần sụn: 1) thêm các thành phần phần mềm, phần sụn, hoặc dòng bit; 2) cập nhật các thành phần phần mềm, phần sụn, hoặc dòng bit hiện có; b) vị trí lưu trữ các thành phần phần mềm, phần sụn, hoặc dòng bit mới được nạp; c) các thành phần phần mềm, phần sụn, dòng bit hoặc phần cứng hiện có để thực thi việc nạp phần mềm, phần sụn hoặc dòng bit; d) các thành phần phần mềm/phần sụn/dòng bit hiện có sẽ bị ảnh hưởng,

	sửa đổi, hoặc thay thế do kết quả của việc nạp phần mềm/phần sụn/dòng bit; e) các thành phần phần mềm/phần sụn/dòng bit hiện có sẽ không bị ảnh hưởng, không bị sửa đổi, và cũng không bị thay thế do kết quả của việc nạp phần mềm/phần sụn/dòng bit.
VE05.19.02	Nhà cung cấp phải cung cấp đặc tả về bài kiểm thử nạp phần mềm/phần sụn được thực hiện bởi mô-đun đã được thẩm định.
Quy trình kiểm thử bắt buộc	
TE05.19.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác định xem mô-đun mật mã có khả năng nạp phần mềm, phần sụn, hoặc dòng bit hay không.
TE05.19.02	Nếu mô-đun mật mã có khả năng nạp bất kỳ thành phần phần mềm, phần sụn, hoặc dòng bit nào, kiểm thử viên phải xem xét tài liệu của nhà cung cấp và kiểm tra mô-đun theo các loại nạp phần mềm/phần sụn/dòng bit nhằm xác định xem các thành phần phần mềm, phần sụn và dòng bit bổ sung có được nạp hay không, hoặc các thành phần phần mềm, phần sụn, và dòng bit hiện có có được cập nhật hay không.
TE05.19.03	Nếu các thành phần phần mềm, phần sụn, và dòng bit bổ sung được nạp, kiểm thử viên phải xác minh rằng bài kiểm thử nạp phần mềm/phần sụn/dòng bit được thực hiện cùng với quá trình nạp phần mềm/phần sụn/dòng bit đó.
TE05.19.04	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng vai trò chuyên viên mật mã đã được đảm nhận để thực hiện quá trình nạp phần mềm/phần sụn/dòng bit.
TE05.19.05	Bằng cách kiểm tra mã lệnh và tài liệu thiết kế, kiểm thử viên phải xác minh rằng việc triển khai quá trình nạp phần mềm/phần sụn là nhất quán với thông tin được cung cấp theo VE05.19.01.

6.5.3 Mức an toàn 2

Bảng 140 - VE và TE của AS05.20

Mức an toàn 2 - mức 2, 3 và 4	
AS05.20 ISO/IEC 19790:2025, 7.5.3	Ngoài các yêu cầu của mức an toàn 1, các yêu cầu sau đây phải được áp dụng cho các mô-đun phần mềm và phần sụn hoặc các thành phần phần mềm và phần sụn tách biệt của một mô-đun lai đối với mức an toàn 2: {AS05.21 đến AS05.24}.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS05.21, AS05.22, AS05.23 và AS05.24.	

Bảng 141 - VE và TE của AS05.21

Mức an toàn 2 - mức 2, 3 và 4	
AS05.21 ISO/IEC 19790:2025, 7.5.3	Mã lệnh chỉ được ở định dạng có thể thực thi.
Thông tin bắt buộc từ nhà cung cấp	
VE05.21.01	Nhà cung cấp phải cung cấp mô tả về phần mềm và phần sụn cùng với định dạng có thể thực thi được sử dụng.
Quy trình kiểm thử bắt buộc	

TE05.21.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng định dạng có thể thực thi đã được lập tài liệu không yêu cầu biên dịch thêm và không có mã lệnh nào bị sửa đổi động.
TE05.21.02	Kiểm thử viên phải kiểm tra mô-đun mật mã và xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng định dạng có thể thực thi đã được lập tài liệu được sử dụng cho mỗi thành phần phần mềm/phần sụn.

Bảng 142 - VE và TE của AS05.22

Mức an toàn 2 - mức 2, 3 và 4	
AS05.22 ISO/IEC 19790:2025, 7.5.3	Không được có dịch vụ hoặc thiết lập điều khiển nào thông qua giao diện mô-đun cho phép người vận hành khởi tạo hoặc thực hiện các kỹ thuật gỡ lỗi khi đang vận hành.
Thông tin bắt buộc từ nhà cung cấp	
VE05.22.01	Nhà cung cấp phải cung cấp đặc tả về các dịch vụ giao diện hoặc thiết lập điều khiển của mô-đun.
Quy trình kiểm thử bắt buộc	
TE05.22.01	Kiểm thử viên phải xác minh đặc tả đã được nhà cung cấp lập tài liệu về các dịch vụ hoặc thiết lập điều khiển.
TE05.22.02	Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp rằng các dịch vụ hoặc thiết lập điều khiển không cho phép người vận hành khởi tạo hoặc thực hiện các kỹ thuật gỡ lỗi.
TE05.22.03	Kiểm thử viên phải kiểm tra các dịch vụ hoặc thiết lập điều khiển để xác minh rằng người vận hành không thể khởi tạo hoặc thực hiện các kỹ thuật gỡ lỗi.

Bảng 143 - VE và TE của AS05.23

Mức an toàn 2 - mức 2, 3 và 4	
AS05.23 ISO/IEC 19790:2025, 7.5.3	Một chữ ký số đã phê duyệt hoặc mã xác thực thông điệp có khóa phải được áp dụng cho tất cả phần mềm và phần sụn bên trong biên mật mã đã được xác định của mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE05.23.01	Nhà cung cấp phải cung cấp tài liệu xác định kỹ thuật được sử dụng để duy trì tính toàn vẹn của các thành phần phần mềm và phần sụn mật mã.
Quy trình kiểm thử bắt buộc	
TE05.23.01	Kiểm thử viên phải xác minh rằng thông tin quy định tại VE05.23.01 được bao gồm.
TE05.23.02	Kiểm thử viên phải tìm cách làm hỏng các thành phần phần mềm và phần sụn mật mã. Nếu mô-đun xác định rằng tính toàn vẹn được duy trì, bài kiểm thử này thất bại.

Bảng 144 - VE và TE của AS05.24

Mức an toàn 2 - mức 2, 3 và 4	
AS05.24 ISO/IEC 19790:2025, 7.5.3	Nếu kết quả tính toán không được kiểm chứng thành công, bài kiểm thử thất bại, và mô-đun phải chuyển sang trạng thái lỗi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS05.15 và AS05.23.	

6.5.4 Mức an toàn 3 và 4

Bảng 145 - VE và TE của AS05.25

Mức an toàn 3 và 4 - mức 3 và 4	
AS05.25 ISO/IEC 19790:2025, 7.5.4	Ngoài các yêu cầu của mức an toàn 1 và 2, các yêu cầu sau đây phải được áp dụng cho các mô-đun phần mềm và phần sụn hoặc các thành phần phần mềm và phần sụn rời rạc của một mô-đun lai đối với mức an toàn 3 và 4: {AS05.26 đến AS05.29}.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS05.26, AS05.27, AS05.28 và AS05.29.	

Bảng 146 - VE và TE của AS05.26

Mức an toàn 3 và 4 - mức 3 và 4	
AS05.26 ISO/IEC 19790:2025, 7.5.4	Một cơ chế mật mã sử dụng chữ ký số đã phê duyệt phải được áp dụng cho tất cả các thành phần phần mềm và phần sụn bên trong biên mật mã đã được xác định của mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE05.26.01	Nhà cung cấp phải cung cấp tài liệu về cơ chế chữ ký số đã phê duyệt.
Quy trình kiểm thử bắt buộc	
TE05.26.01	Kiểm thử viên phải xác minh bằng cách kiểm tra mô-đun mật mã rằng một cơ chế mật mã sử dụng cơ chế chữ ký số đã phê duyệt được áp dụng cho tất cả các thành phần phần mềm và phần sụn bên trong biên mật mã đã được xác định của mô-đun.

Bảng 147 - VE và TE của AS05.27

Mức an toàn 3 và 4 - mức 3 và 4	
AS05.27 ISO/IEC 19790:2025, 7.5.4	Nếu kết quả tính toán không được kiểm chứng thành công, bài kiểm thử thất bại, và mô-đun phải chuyển sang trạng thái lỗi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS05.23.	

Bảng 148 - VE và TE của AS05.28

Mức an toàn 3 và 4 - mức 3 và 4	
AS05.28 ISO/IEC 19790:2025, 7.5.4	Sự thất bại trong việc kiểm chứng chữ ký duy nhất hoặc bất kỳ chữ ký rời rạc nào đều phải khiến mô-đun bước vào trạng thái lỗi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS05.12.	

Bảng 149 - VE và TE của AS05.29

Mức an toàn 3 và 4 - mức 3 và 4	
AS05.29 ISO/IEC 19790:2025, 7.5.4	Khóa ký riêng phải nằm bên ngoài mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE05.29.01	Yêu cầu về tài liệu do nhà cung cấp cung cấp được quy định tại VE05.12.04. Thiết kế của nhà cung cấp phải đảm bảo rằng khóa ký riêng để tạo chữ ký tham chiếu không nằm bên trong biên mật mã của mô-đun mật mã.
Quy trình kiểm thử bắt buộc	

TE05.29.01	Kiểm thử viên phải kiểm tra mô-đun mật mã và xem xét tài liệu của nhà cung cấp để xác minh rằng khóa ký riêng không nằm bên trong biên mật mã.
------------	--

6.6 Môi trường hoạt động

6.6.1 Yêu cầu chung về môi trường hoạt động

Bảng 150 - VE và TE của AS06.01

Yêu cầu chung về môi trường hoạt động - mức 1	
AS06.01 ISO/IEC 19790:2025, 7.6.1	Các mô-đun phần cứng, phần sụn và phần sụn lai ghép phải sử dụng một môi trường hoạt động không thể sửa đổi hoặc bị giới hạn.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS06.03 và AS06.04.	

Bảng 151 - VE và TE của AS06.02

Yêu cầu chung về môi trường hoạt động - mức 1 và 2	
AS06.02 ISO/IEC 19790:2025, 7.6.1	Các mô-đun phần mềm và mô-đun phần mềm lai ghép phải sử dụng một môi trường hoạt động có thể sửa đổi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS06.07, AS06.08, AS06.09, AS06.10, AS06.11, AS06.12, AS06.13, AS06.14, AS06.15, AS06.16, AS06.17, AS06.18, AS06.19, AS06.20, AS06.21, AS06.22, AS06.23, AS06.24, AS06.25, AS06.26, AS06.27, AS06.28, AS06.29, AS06.30, AS06.31, AS06.32 và AS06.33.	

6.6.2 Khả năng áp dụng của điều khoản

CHÚ THÍCH Các yêu cầu từ AS06.07 đến AS06.33 áp dụng cho hệ điều hành hoặc các môi trường hoạt động khi có liên quan

Bảng 152 - VE và TE của AS06.03

Khả năng áp dụng của điều khoản - mức 1	
AS06.03 ISO/IEC 19790:2025, 7.6.2	Nếu môi trường hoạt động là không thể sửa đổi và mô-đun ở mức an toàn 1 theo ISO/IEC 19790:2025, 7.7, thì các yêu cầu về hệ điều hành trong ISO/IEC 19790:2025, 7.6.3 mức an toàn 1 phải được áp dụng.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS06.07, AS06.08, AS06.09, AS06.10 và AS06.11.	

Bảng 153 - VE và TE của AS06.04

Khả năng áp dụng của điều khoản - mức 1	
AS06.04 ISO/IEC 19790:2025, 7.6.2	Nếu môi trường hoạt động là một môi trường hoạt động bị giới hạn và mô-đun ở mức an toàn 1 theo ISO/IEC 19790:2025, 7.7 thì các yêu cầu về hệ điều hành trong ISO/IEC 19790:2025, 7.6.3 mức an toàn 1 phải được áp dụng.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS06.07, AS06.08, AS06.09, AS06.10 và AS06.11.	

Bảng 154 - VE và TE của AS06.05

Khả năng áp dụng của điều khoản - mức 1 và 2	
--	--

AS06.05 ISO/IEC 19790:2025, 7.6.2	Nếu môi trường hoạt động là một môi trường hoạt động có thể sửa đổi, các yêu cầu trong ISO/IEC 19790:2025, 7.6.3 phải được áp dụng.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS06.07, AS06.08, AS06.09, AS06.10, AS06.11, AS06.12, AS06.13, AS06.14, AS06.15, AS06.16, AS06.17, AS06.18, AS06.19, AS06.20, AS06.21, AS06.22, AS06.23, AS06.24, AS06.25, AS06.26, AS06.27, AS06.28, AS06.29, AS06.30, AS06.31, AS06.32 và AS06.33.	

Bảng 155 - VE và TE của AS06.06

Khả năng áp dụng của điều khoản - mức 1 và 2	
AS06.06 ISO/IEC 19790:2025, 7.6.2	Các yêu cầu về tài liệu đối với môi trường hoạt động được quy định trong ISO/IEC 19790:2025, A.2.5 phải được cung cấp.
Thông tin bắt buộc từ nhà cung cấp	
VE06.06.01	Nhà cung cấp phải cung cấp các yêu cầu về tài liệu như được quy định trong ISO/IEC 19790:2025, A.2.5.
Quy trình kiểm thử bắt buộc	
TE06.06.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu như quy định trong ISO/IEC 19790:2025, A.2.5.

6.6.3 Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi**6.6.3.1 Mức an toàn 1****Bảng 156 - VE và TE của AS06.07**

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 1 và 2	
AS06.07 ISO/IEC 19790:2025, 7.6.3.1	Mỗi phiên bản của một mô-đun mật mã phải có quyền kiểm soát đối với các SSP của chính nó.
Thông tin bắt buộc từ nhà cung cấp	
VE06.07.01	Nhà cung cấp phải cung cấp một mô tả về cơ chế hệ điều hành được sử dụng để đảm bảo rằng mỗi phiên bản của một mô-đun mật mã có quyền kiểm soát đối với các SSP của chính nó trong khi quá trình mật mã đang được sử dụng.
Quy trình kiểm thử bắt buộc	
TE06.07.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra hệ điều hành để xác minh rằng mỗi phiên bản của một mô-đun mật mã có quyền kiểm soát đối với các SSP của chính nó trong khi mô-đun mật mã đang được sử dụng.
TE06.07.02	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra hệ điều hành để xác minh rằng yêu cầu này được thực thi bởi chính mô-đun mật mã.
TE06.07.03	Kiểm thử viên phải thực hiện các chức năng mật mã như được mô tả trong tài liệu hướng dẫn dành cho người dùng và chuyên viên mật mã. Trong khi các chức năng mật mã đang thực thi, cùng một kiểm thử viên hoặc một kiểm thử viên khác phải tìm cách để giành quyền truy cập trái phép vào các khóa bí mật và khóa riêng tư, các giá trị tạo khóa trung gian, và các SSP khác đang nằm dưới sự kiểm soát của mô-đun mật mã. Nếu kiểm thử viên có thể giành được quyền truy cập trái phép, bài kiểm thử thất bại.

CHÚ THÍCH 1: Mỗi phiên bản của một mô-đun mật mã kiểm soát các SSP của chính nó và không bị sở hữu hoặc kiểm soát bởi các quá trình/người vận hành bên ngoài.

CHÚ THÍCH 2: Yêu cầu này không được thực thi bởi tài liệu và quy trình hành chính mà bởi chính mô-đun mật mã.

Bảng 157 - VE và TE của AS06.08

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 1 và 2	
AS06.08 ISO/IEC 19790:2025, 7.6.3.1	Hệ điều hành phải cung cấp khả năng tách biệt các quá trình ứng dụng riêng lẻ khỏi nhau nhằm ngăn chặn quyền truy cập không được kiểm soát vào các CSP và các sửa đổi không được kiểm soát đối với các SSP bất kể dữ liệu này nằm trong bộ nhớ của quá trình hay được lưu trữ trên bộ nhớ liên tục bên trong môi trường hoạt động.
Thông tin bắt buộc từ nhà cung cấp	
VE06.08.01	Nhà cung cấp phải cung cấp một mô tả về cơ chế hệ điều hành được sử dụng để cung cấp khả năng tách biệt các quá trình ứng dụng riêng lẻ khỏi nhau nhằm ngăn chặn quyền truy cập không được kiểm soát vào các CSP và các sửa đổi không được kiểm soát đối với các SSP bất kể dữ liệu này nằm trong bộ nhớ của quá trình hay được lưu trữ trên bộ nhớ liên tục bên trong môi trường hoạt động.
Quy trình kiểm thử bắt buộc	
TE06.08.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra cơ chế hệ điều hành được sử dụng để xác minh rằng nó cung cấp khả năng tách biệt các quá trình ứng dụng riêng lẻ khỏi nhau nhằm ngăn chặn quyền truy cập không được kiểm soát vào các CSP và các sửa đổi không được kiểm soát đối với các SSP bất kể dữ liệu này nằm trong bộ nhớ của quá trình hay được lưu trữ trên bộ nhớ liên tục bên trong môi trường hoạt động.
TE06.08.02	Kiểm thử viên phải thực hiện các chức năng mật mã như được mô tả trong tài liệu hướng dẫn dành cho người dùng và chuyên viên mật mã. Trong khi các chức năng mật mã đang thực thi, cùng một kiểm thử viên hoặc một kiểm thử viên khác phải nỗ lực để giành quyền truy cập vào các CSP và thực hiện các sửa đổi đối với các SSP bất kể dữ liệu này nằm trong bộ nhớ của quá trình hay được lưu trữ trên bộ nhớ liên tục bên trong môi trường hoạt động. Nếu kiểm thử viên có thể giành được quyền truy cập, bài kiểm thử thất bại.

Bảng 158 - VE và TE của AS06.09

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 1 và 2	
AS06.09 ISO/IEC 19790:2025, 7.6.3.1	Các giới hạn đối với cấu hình của hệ điều hành phải được lập tài liệu trong chính sách an toàn của mô-đun mật mã.
Thông tin bắt buộc từ nhà cung cấp	
VE06.09.01	Nhà cung cấp phải cung cấp tài liệu mô tả về bất kỳ giới hạn nào đối với cấu hình của hệ điều hành.
Quy trình kiểm thử bắt buộc	
TE06.09.01	Kiểm thử viên phải xác minh rằng bất kỳ giới hạn nào đối với cấu hình của hệ điều hành đều được lập tài liệu trong chính sách an toàn.

Bảng 159 - VE và TE của AS06.10

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 1 và 2	
AS06.10 ISO/IEC 19790:2025, 7.6.3.1	Các quá trình được sinh ra bởi mô-đun mật mã phải thuộc sở hữu của mô-đun và không thuộc sở hữu của các quá trình/người vận hành bên ngoài.
Thông tin bắt buộc từ nhà cung cấp	
VE06.10.01	Nhà cung cấp phải cung cấp một mô tả về cơ chế hệ điều hành được sử dụng để đảm bảo rằng các quá trình được sinh ra bởi mô-đun mật mã thuộc sở hữu của mô-đun và không thuộc sở hữu của các quá trình/người vận hành bên ngoài.
Quy trình kiểm thử bắt buộc	
TE06.10.01	Kiểm thử viên phải xác minh tài liệu do nhà cung cấp cung cấp và kiểm tra hệ điều hành để đảm bảo rằng các quá trình được sinh ra bởi mô-đun mật mã thuộc sở hữu của mô-đun và không thuộc sở hữu của các quá trình/người vận hành bên ngoài.
TE06.10.02	Kiểm thử viên phải xác minh tài liệu do nhà cung cấp cung cấp và kiểm tra hệ điều hành để đảm bảo rằng yêu cầu này phải được thực thi bởi chính mô-đun mật mã.
TE06.10.03	Kiểm thử viên phải thực hiện các chức năng mật mã như được mô tả trong tài liệu hướng dẫn dành cho người dùng và chuyên viên mật mã. Trong khi các chức năng mật mã đang thực thi, cùng một kiểm thử viên hoặc một kiểm thử viên khác phải tìm cách giành quyền sở hữu một quá trình mật mã được sinh ra thuộc sở hữu của mô-đun mật mã từ một quá trình hoặc người vận hành bên ngoài độc lập. Nếu kiểm thử viên có thể giành được quyền sở hữu của một quá trình mật mã được sinh ra, bài kiểm thử thất bại.
CHÚ THÍCH Yêu cầu này không thể được thực thi bằng các thủ tục và tài liệu hành chính mà phải bởi chính mô-đun mật mã.	

Bảng 160 - VE và TE của AS06.11

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 1 và 2	
AS06.11 ISO/IEC 19790:2025, 7.6.3.1	Các yêu cầu này không thể được thực thi bằng các tài liệu và thủ tục hành chính và phải được thực thi bởi chính hệ điều hành. {AS06.07 đến AS06.10}
Thông tin bắt buộc từ nhà cung cấp	
VE06.11.01	Nhà cung cấp phải cung cấp tài liệu mô tả về cách thức các yêu cầu từ ISO/IEC 19790:2025, 7.6.3 được thực thi bởi hệ điều hành.
Quy trình kiểm thử bắt buộc	
TE06.11.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có mô tả về cách thức các yêu cầu từ ISO/IEC 19790:2025, 7.6.3 được thực thi bởi hệ điều hành.
TE06.11.02	Kiểm thử viên phải kiểm tra hệ điều hành và xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng các yêu cầu được thực thi bởi hệ điều hành.

6.6.3.2 Mức an toàn 2**Bảng 161 - VE và TE của AS06.12**

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2
--

AS06.12 ISO/IEC 19790:2025, 7.6.3.2	Ngoài các yêu cầu của mức an toàn 1, đối với mức an toàn 2, một hệ điều hành phải đáp ứng các yêu cầu sau đây hoặc theo như được tổ chức chứng nhận cho phép: {AS06.13 đến AS06.33}.
Thông tin bắt buộc từ nhà cung cấp	
VE06.12.01	Nhà cung cấp phải cung cấp tài liệu mô tả về hệ điều hành.
VE06.12.02	Nhà cung cấp phải cung cấp tài liệu so sánh hệ điều hành hiện tại với hệ điều hành được tổ chức chứng nhận cho phép.
Quy trình kiểm thử bắt buộc	
TE06.12.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có mô tả về hệ điều hành.
TE06.12.02	Kiểm thử viên phải kiểm tra hệ điều hành để xác minh rằng nó khớp với mô tả do nhà cung cấp cung cấp.
TE06.12.03	Kiểm thử viên phải kiểm tra hệ điều hành và xem xét mô tả do nhà cung cấp cung cấp để xác minh rằng hệ điều hành đó được tổ chức chứng nhận cho phép.
CHÚ THÍCH 1: Nếu các yêu cầu về hệ điều hành không được quy định bởi một tổ chức chứng nhận, khẳng định này sẽ được kiểm thử trong AS06.12 đến AS06.33.	
CHÚ THÍCH 2: Nếu các yêu cầu về hệ điều hành được quy định bởi một tổ chức chứng nhận, khẳng định này sẽ được kiểm thử như quy định trong AS06.12.	

Bảng 162 - VE và TE của AS06.13

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.13 ISO/IEC 19790:2025, 7.6.3.2	Tất cả phần mềm mật mã, các SSP, thông tin điều khiển và trạng thái phải nằm dưới sự kiểm soát của một hệ điều hành có triển khai các kiểm soát truy cập dựa trên vai trò hoặc, tối thiểu là một kiểm soát truy cập tùy ý với cơ chế mạnh mẽ để định nghĩa các nhóm mới và gán các quyền hạn chế, ví dụ như thông qua danh sách kiểm soát truy cập (ACL), và có khả năng chỉ định mỗi người dùng vào nhiều hơn một nhóm.
Thông tin bắt buộc từ nhà cung cấp	
VE06.13.01	Nhà cung cấp phải cung cấp tài liệu về hệ điều hành, trong đó mô tả các cơ chế kiểm soát của hệ điều hành thực thi hoặc kiểm soát truy cập dựa trên vai trò hoặc, tối thiểu là, một kiểm soát truy cập tùy ý với cơ chế mạnh mẽ để định nghĩa các nhóm mới và gán các quyền hạn chế. Ví dụ, cơ chế này có thể bao gồm danh sách kiểm soát truy cập (ACL) và có khả năng gán mỗi người dùng vào nhiều hơn một nhóm.
Quy trình kiểm thử bắt buộc	
TE06.13.01	Kiểm thử viên phải xác minh, từ tài liệu do nhà cung cấp cung cấp và thông qua việc kiểm tra các cơ chế kiểm soát của hệ điều hành, rằng hệ điều hành triển khai các kiểm soát truy cập dựa trên vai trò hoặc, tối thiểu là, một kiểm soát truy cập tùy ý với một cơ chế mạnh mẽ để định nghĩa các nhóm mới và gán các quyền hạn chế, ví dụ như thông qua danh sách kiểm soát truy cập (ACL) và với khả năng gán mỗi người dùng vào nhiều hơn một nhóm.
TE06.13.02	Kiểm thử viên phải cấu hình các kiểm soát truy cập dựa trên vai trò hoặc các kiểm soát truy cập tùy ý của hệ điều hành để cấp quyền cho một người dùng hoặc nhóm cụ thể. Kiểm thử viên, với tư cách đảm nhận một vai trò người dùng hoặc nhóm được phép, phải thử thực thi, sửa đổi, hoặc đọc các SSP, dữ liệu điều khiển hoặc

	trạng thái mà kiểm thử viên được ủy quyền truy cập.
TE06.13.03	Kiểm thử viên phải cấu hình các kiểm soát truy cập dựa trên vai trò hoặc các kiểm soát truy cập tùy ý của hệ điều hành để cấp quyền cho một người dùng hoặc nhóm cụ thể. Kiểm thử viên, với tư cách đảm nhận một vai trò người dùng hoặc nhóm khác, phải thử thực thi, sửa đổi, hoặc đọc các SSP, dữ liệu điều khiển hoặc trạng thái mà kiểm thử viên không có quyền truy cập.

Bảng 163 - VE và TE của AS06.14

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.14 ISO/IEC 19790:2025, 7.6.3.2	Hệ điều hành phải được cấu hình để bảo vệ chống lại việc thực thi trái phép, sửa đổi trái phép, và đọc trái phép các SSP, dữ liệu điều khiển và dữ liệu trạng thái;
Thông tin bắt buộc từ nhà cung cấp	
VE06.14.01	Nhà cung cấp phải cung cấp tài liệu về hệ điều hành, trong đó mô tả các cơ chế kiểm soát của hệ điều hành có thể được cấu hình để bảo vệ chống lại việc thực thi trái phép, sửa đổi trái phép, và đọc trái phép các SSP, dữ liệu điều khiển và dữ liệu trạng thái.
Quy trình kiểm thử bắt buộc	
TE06.14.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra các cơ chế kiểm soát của hệ điều hành để xác minh rằng hệ điều hành có thể được cấu hình để bảo vệ chống lại việc thực thi trái phép, sửa đổi trái phép, và đọc trái phép các SSP, dữ liệu điều khiển và dữ liệu trạng thái.
TE06.14.02	Kiểm thử viên phải cấu hình hệ điều hành để bảo vệ chống lại việc thực thi trái phép, sửa đổi trái phép, và đọc trái phép các SSP, dữ liệu điều khiển và dữ liệu trạng thái. Trong khi thực thi một quá trình mật mã, kiểm thử viên phải thử thực thi, sửa đổi hoặc đọc các SSP, dữ liệu điều khiển hoặc trạng thái mà kiểm thử viên được ủy quyền truy cập.
TE06.14.03	Kiểm thử viên phải cấu hình hệ điều hành để bảo vệ chống lại việc thực thi trái phép, sửa đổi trái phép, và đọc trái phép các SSP, dữ liệu điều khiển và dữ liệu trạng thái. Trong quá trình thực thi một quá trình mật mã, kiểm thử viên phải thử thực thi, sửa đổi hoặc đọc các SSP, dữ liệu điều khiển hoặc trạng thái mà kiểm thử viên không có quyền truy cập.

Bảng 164 - VE và TE của AS06.15

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.15 ISO/IEC 19790:2025, 7.6.3.2	{Để bảo vệ dữ liệu ở dạng bản rõ, phần mềm mật mã và các SSP,} các cơ chế kiểm soát truy cập của hệ điều hành phải được cấu hình để xác định và thực thi tập hợp các vai trò, hoặc các nhóm cùng các quyền hạn giới hạn tương ứng của chúng, có quyền đọc quyền để thực thi phần mềm mật mã đã được lưu trữ;
Thông tin bắt buộc từ nhà cung cấp	
VE06.15.01	Nhà cung cấp phải cung cấp tài liệu về hệ điều hành, trong đó mô tả cách các cơ chế kiểm soát truy cập của hệ điều hành được cấu hình để xác định và thực thi tập hợp các vai trò, hoặc các nhóm cùng các quyền hạn giới hạn tương ứng của chúng, có quyền đọc quyền để thực thi phần mềm mật mã đã được lưu trữ.
Quy trình kiểm thử bắt buộc	

TE06.15.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra các cơ chế kiểm soát của hệ điều hành để xác minh rằng hệ điều hành được cấu hình để xác định và thực thi tập hợp các vai trò, hoặc các nhóm cùng các quyền hạn giới hạn tương ứng của chúng, có quyền độc quyền để thực thi phần mềm mật mã đã được lưu trữ.
TE06.15.02	Kiểm thử viên phải cấu hình các cơ chế kiểm soát của hệ điều hành để xác định và thực thi tập hợp các vai trò, hoặc các nhóm cùng các quyền hạn giới hạn tương ứng của chúng, nhằm cấp quyền độc quyền để thực thi phần mềm mật mã đã được lưu trữ. Kiểm thử viên phải xác minh rằng họ có quyền độc quyền để thực thi phần mềm mật mã đã được lưu trữ.
TE06.15.03	Kiểm thử viên phải cấu hình các cơ chế kiểm soát của hệ điều hành để định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ nhằm không cấp quyền thực thi phần mềm mật mã được lưu trữ. Kiểm thử viên phải xác minh rằng họ không có quyền thực thi phần mềm mật mã được lưu trữ.

Bảng 165 - VE và TE của AS06.16

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.16 ISO/IEC 19790:2025, 7.6.3.2	{Để bảo vệ dữ liệu dạng rõ, phần mềm mật mã và các SSP, các cơ chế kiểm soát truy cập của hệ điều hành} phải được cấu hình để định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ, vốn có quyền độc quyền sửa đổi (tức là ghi, thay thế, và xóa) phần mềm mô-đun mật mã sau đây được lưu trữ bên trong biên mật mã: các chương trình mật mã, dữ liệu mật mã (ví dụ: dữ liệu kiểm toán mật mã), các SSP, và dữ liệu dạng rõ;
Thông tin bắt buộc từ nhà cung cấp	
VE06.16.01	Nhà cung cấp phải cung cấp tài liệu về hệ điều hành, trong đó mô tả cách các cơ chế kiểm soát truy cập của hệ điều hành được cấu hình để định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ, vốn có quyền độc quyền sửa đổi (tức là ghi, thay thế, và xóa) phần mềm mô-đun mật mã sau đây được lưu trữ bên trong biên mật mã: các chương trình mật mã, dữ liệu mật mã (ví dụ: dữ liệu kiểm toán mật mã), các SSP, và dữ liệu dạng rõ.
Quy trình kiểm thử bắt buộc	
TE06.16.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra các cơ chế kiểm soát của hệ điều hành để xác minh rằng hệ điều hành được cấu hình nhằm định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ, vốn có quyền độc quyền sửa đổi (tức là ghi, thay thế, và xóa) phần mềm mô-đun mật mã sau đây được lưu trữ bên trong biên mật mã: các chương trình mật mã, dữ liệu mật mã (ví dụ: dữ liệu kiểm toán mật mã), các SSP, và dữ liệu dạng rõ.
TE06.16.02	Kiểm thử viên phải cấu hình các cơ chế kiểm soát của hệ điều hành để định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ nhằm cấp quyền độc quyền sửa đổi (tức là ghi, thay thế, và xóa) phần mềm mô-đun mật mã sau đây được lưu trữ bên trong biên mật mã: các chương trình mật mã, dữ liệu mật mã (ví dụ: dữ liệu kiểm toán mật mã), các SSP, và dữ liệu dạng rõ. Kiểm thử viên phải xác minh rằng họ có quyền độc quyền sửa đổi (tức là ghi, thay thế, và xóa) phần mềm mô-đun mật mã sau đây được lưu trữ bên trong biên mật mã: các chương trình mật mã, dữ liệu mật mã (ví dụ: dữ liệu kiểm toán mật mã), các SSP, và dữ liệu dạng rõ.

TE06.16.03	Kiểm thử viên phải cấu hình các cơ chế kiểm soát của hệ điều hành để định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ nhằm không cấp quyền sửa đổi (tức là ghi, thay thế, và xóa) phần mềm mô-đun mật mã sau đây được lưu trữ bên trong biên mật mã: các chương trình mật mã, dữ liệu mật mã (ví dụ: dữ liệu kiểm toán mật mã), các SSP, và dữ liệu dạng rõ. Kiểm thử viên phải xác minh rằng họ không có quyền sửa đổi (tức là ghi, thay thế, và xóa) phần mềm mô-đun mật mã sau đây được lưu trữ bên trong biên mật mã: các chương trình mật mã, dữ liệu mật mã (ví dụ: dữ liệu kiểm toán mật mã), các SSP, và dữ liệu dạng rõ.
------------	---

Bảng 166 - VE và TE của AS06.17

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.17 ISO/IEC 19790:2025, 7.6.3.2	{Để bảo vệ dữ liệu dạng rõ, phần mềm mật mã và các SSP, các cơ chế kiểm soát truy cập của hệ điều hành} phải được cấu hình để định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ, vốn có quyền độc quyền đọc dữ liệu mật mã (ví dụ: dữ liệu kiểm toán mật mã), các CSP, và dữ liệu dạng rõ;
Thông tin bắt buộc từ nhà cung cấp	
VE06.17.01	Nhà cung cấp phải cung cấp tài liệu về hệ điều hành, trong đó mô tả cách các cơ chế kiểm soát truy cập của hệ điều hành được cấu hình để định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ, vốn có quyền độc quyền đọc dữ liệu mật mã (ví dụ: dữ liệu kiểm toán mật mã), các CSP, và dữ liệu dạng rõ.
Quy trình kiểm thử bắt buộc	
TE06.17.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra các cơ chế kiểm soát của hệ điều hành để xác minh rằng hệ điều hành được cấu hình nhằm định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ, vốn có quyền độc quyền đọc dữ liệu mật mã (ví dụ: dữ liệu kiểm toán mật mã), các CSP, và dữ liệu dạng rõ.
TE06.17.02	Kiểm thử viên phải cấu hình các cơ chế kiểm soát của hệ điều hành để định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ nhằm cấp quyền độc quyền đọc dữ liệu mật mã (ví dụ: dữ liệu kiểm toán mật mã), các CSP, và dữ liệu dạng rõ. Kiểm thử viên phải xác minh rằng họ có quyền độc quyền đọc dữ liệu mật mã (ví dụ: dữ liệu kiểm toán mật mã), các CSP, và dữ liệu dạng rõ.
TE06.17.03	Kiểm thử viên phải cấu hình các cơ chế kiểm soát của hệ điều hành để định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ nhằm không cấp quyền đọc dữ liệu mật mã (ví dụ: dữ liệu kiểm toán mật mã), các CSP, và dữ liệu dạng rõ. Kiểm thử viên phải xác minh rằng họ không có quyền độc quyền đọc dữ liệu mật mã (ví dụ: dữ liệu kiểm toán mật mã), các CSP, và dữ liệu dạng rõ.

Bảng 167 - VE và TE của AS06.18

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.18 ISO/IEC 19790:2025, 7.6.3.2	{Để bảo vệ dữ liệu dạng rõ, phần mềm mật mã và các SSP, các cơ chế kiểm soát truy cập của hệ điều hành} phải được cấu hình để định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ, vốn có quyền độc quyền nhập các SSP.
Thông tin bắt buộc từ nhà cung cấp	

VE06.18.01	Nhà cung cấp phải cung cấp tài liệu về hệ điều hành, trong đó mô tả cách các cơ chế kiểm soát truy cập của hệ điều hành được cấu hình để định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ, vốn có quyền độc quyền nhập các SSP.
Quy trình kiểm thử bắt buộc	
TE06.18.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra các cơ chế kiểm soát của hệ điều hành để xác minh rằng hệ điều hành được cấu hình nhằm định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ, vốn có quyền độc quyền nhập các SSP.
TE06.18.02	Kiểm thử viên phải cấu hình các cơ chế kiểm soát của hệ điều hành để định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ nhằm cấp quyền độc quyền nhập các SSP. Kiểm thử viên phải xác minh rằng họ có quyền độc quyền nhập các SSP.
TE06.18.03	Kiểm thử viên phải cấu hình các cơ chế kiểm soát của hệ điều hành để định nghĩa và thực thi tập hợp các vai trò hoặc các nhóm và các quyền hạn chế tương ứng của họ nhằm không cấp quyền nhập các SSP. Kiểm thử viên phải xác minh rằng họ không có quyền nhập các SSP.

Bảng 168 - VE và TE của AS06.19

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.19 ISO/IEC 19790:2025, 7.6.3.2	Các đặc tả sau đây phải nhất quán với quyền và dịch vụ của các vai trò hoặc các nhóm được chỉ định như định nghĩa trong chính sách an toàn:
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS06.20, AS06.21, AS06.22 và AS06.23.	

Bảng 169 - VE và TE của AS06.20

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.20 ISO/IEC 19790:2025, 7.6.3.2	Khi không hỗ trợ vai trò bảo trì, hệ điều hành phải ngăn tất cả người vận hành và các quá trình đang chạy sửa đổi các quá trình mật mã đang chạy (tức là các bản sao chương trình mật mã đã được nạp và đang thực thi). Trong trường hợp này, các quá trình đang chạy đề cập đến tất cả các quá trình, dù là mật mã hay không, không thuộc sở hữu hoặc không do hệ điều hành khởi tạo (tức là do người vận hành khởi tạo);
Thông tin bắt buộc từ nhà cung cấp	
VE06.20.01	Nhà cung cấp phải cung cấp tài liệu về hệ điều hành, trong đó mô tả cách hệ điều hành ngăn tất cả người vận hành và các quá trình đang chạy sửa đổi các quá trình mật mã đang chạy (tức là các bản sao chương trình mật mã đã được nạp và đang thực thi) khi không ở vai trò bảo trì.
VE06.20.02	Các đặc tả về cách hệ điều hành ngăn tất cả người vận hành và các quá trình đang chạy sửa đổi các quá trình mật mã đang chạy (tức là các bản sao chương trình mật mã đã được nạp và đang thực thi) khi không ở vai trò bảo trì phải nhất quán với quyền và dịch vụ của các vai trò hoặc các nhóm được chỉ định như định nghĩa trong chính sách an toàn.
Quy trình kiểm thử bắt buộc	

TE06.20.01	Kiểm thử viên phải xác minh, từ tài liệu do nhà cung cấp cung cấp và thông qua kiểm tra các cơ chế kiểm soát của hệ điều hành, rằng hệ điều hành được cấu hình để ngăn tất cả người vận hành và các quá trình đang chạy sửa đổi các quá trình mật mã đang chạy (tức là các bản sao chương trình mật mã đã được nạp và đang thực thi) khi không ở vai trò bảo trì.
TE06.20.02	Kiểm thử viên phải xác minh rằng quyền và dịch vụ của các vai trò hoặc các nhóm được chỉ định như định nghĩa trong chính sách an toàn là nhất quán với cách hệ điều hành được cấu hình để ngăn tất cả người vận hành và các quá trình đang chạy sửa đổi các quá trình mật mã đang chạy (tức là các bản sao chương trình mật mã đã được nạp và đang thực thi) khi không ở vai trò bảo trì.
TE06.20.03	Kiểm thử viên phải cấu hình các cơ chế kiểm soát của hệ điều hành để ngăn tất cả người vận hành và các quá trình đang chạy sửa đổi các quá trình mật mã đang chạy (tức là các bản sao chương trình mật mã đã được nạp và đang thực thi) khi không ở vai trò bảo trì. Kiểm thử viên phải đảm nhận vai trò người vận hành và xác minh rằng họ bị ngăn không cho sửa đổi các quá trình mật mã đang chạy khi không ở vai trò bảo trì. Kiểm thử viên phải xác minh rằng các quá trình đang chạy bị ngăn không cho sửa đổi các quá trình mật mã đang chạy khi không ở vai trò bảo trì.

Bảng 170 - VE và TE của AS06.21

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.21 ISO/IEC 19790:2025, 7.6.3.2	Hệ điều hành phải ngăn các quá trình của người dùng giành được quyền truy cập đọc hoặc ghi vào các SSP thuộc sở hữu của các quá trình khác và vào các SSP của hệ thống;
Thông tin bắt buộc từ nhà cung cấp	
VE06.21.01	Nhà cung cấp phải cung cấp tài liệu về hệ điều hành, trong đó mô tả cách hệ điều hành ngăn các quá trình thuộc các vai trò người dùng hoặc nhóm người dùng giành được quyền truy cập đọc hoặc ghi vào các SSP thuộc sở hữu của các quá trình khác và vào các SSP của hệ thống.
VE06.21.02	Các đặc tả về cách hệ điều hành ngăn các quá trình thuộc các vai trò người dùng hoặc nhóm người dùng giành được quyền truy cập đọc hoặc ghi vào các SSP thuộc sở hữu của các quá trình khác và vào các SSP của hệ thống phải nhất quán với quyền và dịch vụ của các vai trò hoặc các nhóm được chỉ định như định nghĩa trong chính sách an toàn.
Quy trình kiểm thử bắt buộc	
TE06.21.01	Kiểm thử viên phải xác minh, từ tài liệu do nhà cung cấp cung cấp và thông qua kiểm tra các cơ chế kiểm soát của hệ điều hành, rằng hệ điều hành được cấu hình để ngăn các quá trình thuộc các vai trò người dùng hoặc nhóm người dùng giành được quyền truy cập đọc hoặc ghi vào các SSP thuộc sở hữu của các quá trình khác và vào các SSP của hệ thống.
TE06.21.02	Kiểm thử viên phải xác minh rằng quyền và dịch vụ của các vai trò hoặc các nhóm được chỉ định như định nghĩa trong chính sách an toàn là nhất quán với cách hệ điều hành được cấu hình để ngăn các quá trình thuộc các vai trò người dùng hoặc nhóm người dùng giành được quyền truy cập đọc hoặc ghi vào các SSP thuộc sở hữu của các quá trình khác và vào các SSP của hệ thống.

TE06.21.03	Kiểm thử viên phải cấu hình các cơ chế kiểm soát của hệ điều hành để ngăn các quá trình thuộc các vai trò người dùng hoặc nhóm người dùng giành được quyền truy cập đọc hoặc ghi vào các SSP thuộc sở hữu của các quá trình khác và vào các SSP của hệ thống. Kiểm thử viên phải xác minh rằng các quá trình đang chạy thuộc các vai trò người dùng hoặc nhóm người dùng bị ngăn không cho giành quyền truy cập đọc hoặc ghi vào các SSP thuộc sở hữu của các quá trình khác và vào các SSP của hệ thống.
------------	---

Bảng 171 - VE và TE của AS06.22

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.22 ISO/IEC 19790:2025, 7.6.3.2	Cấu hình của hệ điều hành đáp ứng AS06.20 và AS06.21 phải được quy định trong tài liệu hướng dẫn dành cho quản trị viên.
Thông tin bắt buộc từ nhà cung cấp	
VE06.22.01	Nhà cung cấp phải cung cấp các tài liệu hướng dẫn dành cho quản trị viên, trong đó mô tả cách hệ điều hành được cấu hình để đáp ứng các yêu cầu từ AS06.13 đến AS06.18.
Quy trình kiểm thử bắt buộc	
TE06.22.01	Kiểm thử viên phải xác minh rằng các tài liệu hướng dẫn dành cho quản trị viên do nhà cung cấp cung cấp có mô tả về cách hệ điều hành được cấu hình để đáp ứng các yêu cầu từ AS06.13 đến AS06.18.

Bảng 172 - VE và TE của AS06.23

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.23 ISO/IEC 19790:2025, 7.6.3.2	Hướng dẫn dành cho quản trị viên phải tuyên bố rằng hệ điều hành phải được cấu hình như quy định để nội dung của mô-đun được coi là đã được bảo vệ.
Thông tin bắt buộc từ nhà cung cấp	
VE06.23.01	Nhà cung cấp phải cung cấp các tài liệu hướng dẫn dành cho quản trị viên tuyên bố rằng hệ điều hành phải được cấu hình như quy định từ AS06.13 đến AS06.18 để nội dung của mô-đun được coi là đã được bảo vệ.
Quy trình kiểm thử bắt buộc	
TE06.23.01	Kiểm thử viên phải xác minh rằng các tài liệu hướng dẫn dành cho quản trị viên do nhà cung cấp cung cấp có tuyên bố rằng hệ điều hành phải được cấu hình như quy định từ AS06.13 đến AS06.18 để nội dung của mô-đun được coi là đã được bảo vệ.

Bảng 173 - VE và TE của AS06.24

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.24 ISO/IEC 19790:2025, 7.6.3.2	Cơ chế nhận diện và xác thực đối với hệ điều hành phải đáp ứng các yêu cầu của ISO/IEC 19790:2025, 7.4.4 ở mức an toàn 2, 3 hoặc 4, và được quy định trong chính sách an toàn của mô-đun.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS06.27, AS06.28, AS06.29, AS06.30, AS06.31,	

Bảng 174 - VE và TE của AS06.25

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.25 ISO/IEC 19790:2025, 7.6.3.2	Tất cả phần mềm mật mã, các SSP, thông tin điều khiển và trạng thái phải nằm dưới sự kiểm soát của một hệ điều hành.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS06.27, AS06.28, AS06.29, AS06.30, AS06.31, AS06.32 và AS06.33.	

Bảng 175 - VE và TE của AS06.26

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.26 ISO/IEC 19790:2025, 7.6.3.2	Hệ điều hành tối thiểu phải có các thuộc tính sau:
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS06.27, AS06.28, AS06.29, AS06.30, AS06.31, AS06.32 và AS06.33.	

Bảng 176 - VE và TE của AS06.27

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.27 ISO/IEC 19790:2025, 7.6.3.2	Hệ điều hành phải cung cấp một cơ chế kiểm toán với ngày và giờ của từng sự kiện được kiểm toán.
Thông tin bắt buộc từ nhà cung cấp	
VE06.27.01	Nhà cung cấp phải cung cấp tài liệu về hệ điều hành mô tả cơ chế kiểm toán do hệ điều hành cung cấp và cách mỗi sự kiện được đánh dấu bằng ngày và giờ.
Quy trình kiểm thử bắt buộc	
TE06.27.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra hệ điều hành để xác minh rằng cơ chế kiểm toán được cung cấp và mỗi sự kiện được đánh dấu bằng ngày và giờ.

Bảng 177 - VE và TE của AS06.28

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.28 ISO/IEC 19790:2025, 7.6.3.2	Mô-đun mật mã không được bao gồm các SSP như một phần của bất kỳ hồ sơ kiểm toán nào;
Thông tin bắt buộc từ nhà cung cấp	
VE06.28.01	Nhà cung cấp phải cung cấp tài liệu về hệ điều hành mô tả các dịch vụ của mô-đun mật mã cung cấp hồ sơ kiểm toán cho cơ chế kiểm toán của hệ điều hành.
Quy trình kiểm thử bắt buộc	

TE06.28.01	Kiểm thử viên phải xác minh, từ tài liệu do nhà cung cấp cung cấp và thông qua việc kiểm tra các dịch vụ của mô-đun mật mã cung cấp hồ sơ kiểm toán cho cơ chế kiểm toán của hệ điều hành, rằng không có SSP nào được cung cấp trong các hồ sơ kiểm toán.
TE06.28.02	Kiểm thử viên phải thực thi các dịch vụ của mô-đun cung cấp hồ sơ kiểm toán và kiểm tra các bản ghi kiểm toán của hệ điều hành để xác minh rằng không có SSP nào được cung cấp.

Bảng 178 - VE và TE của AS06.29

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.29 ISO/IEC 19790:2025, 7.6.3.2	Mô-đun mật mã phải cung cấp các sự kiện sau đây để cơ chế kiểm toán của hệ điều hành ghi lại: a) việc sửa đổi, truy cập, xóa, và thêm mới dữ liệu mật mã và các SSP; b) việc thêm hoặc xóa một người vận hành vào hoặc khỏi vai trò chuyên viên mật mã (nếu các vai trò đó được quản lý bởi mô-đun mật mã); c) việc sử dụng một chức năng chuyên viên mật mã liên quan đến an toàn; d) các yêu cầu truy cập dữ liệu của bộ kiểm chứng liên quan đến mô-đun mật mã; e) việc sử dụng cơ chế xác thực (ví dụ: đăng nhập) liên quan đến mô-đun mật mã; và f) các yêu cầu tường minh để đảm nhận vai trò chuyên viên mật mã.
Thông tin bắt buộc từ nhà cung cấp	
VE06.29.01	Nhà cung cấp phải cung cấp tài liệu về hệ điều hành mô tả các sự kiện của mô-đun mật mã được cung cấp và được ghi lại bởi cơ chế kiểm toán của hệ điều hành.
VE06.29.02	Nhà cung cấp phải cung cấp tài liệu xác định bất kỳ sự kiện nào cần thiết để đáp ứng các yêu cầu trong AS06.29 mà được ghi lại bởi mô-đun mật mã, và trong trường hợp các sự kiện này không được ghi lại một cách riêng biệt bởi hệ điều hành.
Quy trình kiểm thử bắt buộc	
TE06.29.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra các dịch vụ của mô-đun mật mã (cung cấp hồ sơ sự kiện kiểm toán cho cơ chế kiểm toán của hệ điều hành hoặc của mô-đun mật mã) để xác minh rằng danh sách các sự kiện được quy định trong AS06.29 được cung cấp bởi mô-đun mật mã để ghi lại sự kiện.
TE06.29.02	Kiểm thử viên phải thực thi các dịch vụ của mô-đun cung cấp hồ sơ sự kiện kiểm toán và kiểm tra các bản ghi kiểm toán của hệ điều hành hoặc mô-đun mật mã để xác minh rằng các sự kiện trong AS06.29 đã được ghi lại. CHÚ THÍCH 1: Kiểm thử viên không bắt buộc phải kiểm tra cơ chế kiểm toán do hệ điều hành cung cấp và được nhà cung cấp xác định. CHÚ THÍCH 2: Các sự kiện kiểm toán có thể được ghi lại và lưu trữ song song bởi cả hệ điều hành và mô-đun mật mã. Mục đích của TE06.29.02 là để xác nhận rằng hệ điều hành hoặc mô-đun mật mã báo cáo một sự kiện cụ thể, nhưng không phải là cả hai.

Bảng 179 - VE và TE của AS06.30

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2
--

AS06.30 ISO/IEC 19790:2025, 7.6.3.2	Mô-đun mật mã có thể ghi lại một số hoặc tất cả các sự kiện được quy định trong ISO/IEC 19790:2025, 7.6.3.2 e) bằng cơ chế kiểm toán của chính nó; bất kể thế nào, tất cả các yêu cầu kiểm toán trong AS06.29 phải được ghi lại, bởi hệ điều hành, bởi mô-đun hoặc bởi sự kết hợp của cả hai.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS06.29.	

Bảng 180 - VE và TE của AS06.31

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.31 ISO/IEC 19790:2025, 7.6.3.2	Cơ chế kiểm toán của hệ điều hành phải có khả năng kiểm toán các sự kiện liên quan đến hệ điều hành sau đây: a) tất cả các lượt truy cập đọc hoặc ghi của người vận hành vào dữ liệu kiểm toán được lưu trong vết kiểm toán; b) quyền truy cập vào các tệp được mô-đun mật mã sử dụng để lưu trữ dữ liệu mật mã hoặc các SSP; c) việc thêm hoặc xóa một người vận hành vào hoặc khỏi vai trò chuyên viên mật mã (nếu các vai trò đó được quản lý bởi hệ điều hành); d) các yêu cầu sử dụng cơ chế quản lý dữ liệu của bộ kiểm chứng (nếu dữ liệu của bộ kiểm chứng liên quan đến mô-đun mật mã được quản lý bởi hệ điều hành); e) các lần cố thử sử dụng chức năng đường dẫn tin cậy dạng rõ và liệu yêu cầu đó có được cấp phép hay không, khi đường dẫn tin cậy dạng rõ được hỗ trợ ở mức an toàn này; và f) nhận diện phía khởi tạo và phía đích của đường dẫn tin cậy dạng rõ, khi đường dẫn tin cậy dạng rõ được hỗ trợ ở mức an toàn này.
Thông tin bắt buộc từ nhà cung cấp	
VE06.31.01	Nhà cung cấp phải cung cấp tài liệu về hệ điều hành mô tả các sự kiện của hệ điều hành được cung cấp và được ghi lại bởi cơ chế kiểm toán của hệ điều hành.
Quy trình kiểm thử bắt buộc	
TE06.31.01	Kiểm thử viên phải xác minh, từ tài liệu của nhà cung cấp và thông qua việc kiểm tra tài liệu về hệ điều hành, rằng hệ điều hành cung cấp danh sách các sự kiện được quy định trong AS06.31 dưới dạng hồ sơ sự kiện kiểm toán cho cơ chế kiểm toán của hệ điều hành.
TE06.31.02	Kiểm thử viên phải thực thi các dịch vụ của mô-đun mật mã để xác minh rằng các sự kiện của hệ điều hành trong AS06.31 đã được ghi lại. CHÚ THÍCH: Kiểm thử viên không bắt buộc phải kiểm tra cơ chế kiểm toán do hệ điều hành cung cấp và được nhà cung cấp xác định.

Bảng 181 - VE và TE của AS06.32

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.32 ISO/IEC 19790:2025, 7.6.3.2	Hệ điều hành phải được cấu hình để ngăn những người vận hành khác không có các đặc quyền được xác định trong chính sách an toàn sửa đổi phần mềm mô-đun mật mã và dữ liệu kiểm toán được lưu trữ bên trong môi trường hoạt động của mô-đun mật mã.
Thông tin bắt buộc từ nhà cung cấp	

VE06.32.01	Nhà cung cấp phải cung cấp tài liệu về hệ điều hành quy định cách hệ điều hành được cấu hình để ngăn những người vận hành khác không có các đặc quyền được xác định trong chính sách an toàn sửa đổi phần mềm mô-đun mật mã và dữ liệu kiểm toán được lưu trữ bên trong môi trường hoạt động của mô-đun mật mã.
Quy trình kiểm thử bắt buộc	
TE06.32.01	Kiểm thử viên phải xác minh, từ tài liệu do nhà cung cấp cung cấp và thông qua việc kiểm tra các kiểm soát cấu hình của hệ điều hành, rằng hệ điều hành được cấu hình để ngăn những người vận hành khác không có các đặc quyền được xác định trong chính sách an toàn sửa đổi phần mềm mô-đun mật mã và dữ liệu kiểm toán được lưu trữ bên trong môi trường hoạt động của mô-đun mật mã.
TE06.32.02	Kiểm thử viên phải cấu hình các kiểm soát của hệ điều hành để ngăn những người vận hành khác không có các đặc quyền được xác định trong chính sách an toàn sửa đổi phần mềm mô-đun mật mã và dữ liệu kiểm toán được lưu trữ bên trong môi trường hoạt động của mô-đun mật mã.
TE06.32.03	Kiểm thử viên phải đảm nhận các đặc quyền được xác định trong chính sách an toàn cho phép sửa đổi phần mềm mô-đun mật mã và dữ liệu kiểm toán được lưu trữ bên trong môi trường hoạt động của mô-đun mật mã. Và sau đó, kiểm thử viên phải xác minh rằng việc sửa đổi có thể được thực hiện.
TE06.32.04	Kiểm thử viên phải đảm nhận các đặc quyền được xác định trong chính sách an toàn không cho phép sửa đổi phần mềm mô-đun mật mã và dữ liệu kiểm toán được lưu trữ bên trong môi trường hoạt động của mô-đun mật mã. Sau đó, kiểm thử viên phải xác minh rằng việc sửa đổi không thể được thực hiện.

Bảng 182 - VE và TE của AS06.33

Yêu cầu về hệ điều hành đối với môi trường hoạt động có thể sửa đổi - mức 2	
AS06.33 ISO/IEC 19790:2025, 7.6.3.2	Chỉ những hệ điều hành được cấu hình để đáp ứng các yêu cầu quy định tại ISO/IEC 19790:2025, 7.6.3.2 mới được phép sử dụng ở mức an toàn 2.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS06.07, AS06.08, AS06.09, AS06.10, AS06.11, AS06.12, AS06.13, AS06.14, AS06.15, AS06.16, AS06.17, AS06.18, AS06.19, AS06.20, AS06.21, AS06.22, AS06.23, AS06.24, AS06.25, AS06.26, AS06.27, AS06.28, AS06.29, AS06.30, AS06.31 và AS06.32.	

6.7 An toàn vật lý

6.7.1 Các hình thái an toàn vật lý

Bảng 183 - VE và TE của AS07.01

Các hình thái an toàn vật lý - mức 1, 2, 3 và 4	
AS07.01 ISO/IEC 19790:2025, 7.7.1	Một mô-đun mật mã phải sử dụng các cơ chế an toàn vật lý nhằm hạn chế quyền truy cập vật lý trái phép vào nội dung của mô-đun và răn đe việc sử dụng hoặc sửa đổi trái phép mô-đun khi đã được cài đặt.
Thông tin bắt buộc từ nhà cung cấp	
VE07.01.01	Tài liệu do nhà cung cấp cung cấp phải mô tả các cơ chế an toàn vật lý có thể áp dụng được sử dụng bởi mô-đun. Nội dung của mô-đun, bao gồm tất cả phần cứng, phần sụn, và dữ liệu (bao gồm cả các CSP không được bảo vệ) đều phải được bảo

	vệ.
Quy trình kiểm thử bắt buộc	
TE07.01.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả các cơ chế an toàn vật lý có thể áp dụng được sử dụng bởi mô-đun.
TE07.01.02	Kiểm thử viên phải xác minh rằng các cơ chế an toàn vật lý được lập tài liệu đã được triển khai.

Bảng 184 - VE và TE của AS07.02

Các hình thái an toàn vật lý - mức 1, 2, 3 và 4	
AS07.02 ISO/IEC 19790:2025, 7.7.1	Tất cả phần cứng, phần sụn, các phần tử dữ liệu và các SSP bên trong biên mặt mã phải được bảo vệ vật lý như quy định đối với mức an toàn vật lý mục tiêu.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 185 - VE và TE của AS07.03

Các hình thái an toàn vật lý - mức 1, 2, 3 và 4	
AS07.03 ISO/IEC 19790:2025, 7.7.1	Các yêu cầu của ISO/IEC 19790:2025, 7.7 phải được áp dụng cho các mô-đun phần cứng và phần sụn, cũng như các thành phần phần cứng và phần sụn của các mô-đun lại.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 186 - VE và TE của AS07.04

Các hình thái an toàn vật lý - mức 1, 2, 3 và 4	
AS07.04 ISO/IEC 19790:2025, 7.7.1	Tài liệu về an toàn vật lý quy định tại ISO/IEC 19790:2025, A.2.6 phải được cung cấp.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

6.7.2 Yêu cầu chung về an toàn vật lý**6.7.2.1 Yêu cầu chung về an toàn vật lý cho mọi mức an toàn****Bảng 187 - VE và TE của AS07.05**

Yêu cầu chung về an toàn vật lý - mức 1, 2, 3 và 4	
AS07.05 ISO/IEC 19790:2025, 7.7.2.1	Các yêu cầu sau đây phải được áp dụng cho tất cả các hình thái vật lý: {AS07.06 đến AS07.37}
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.06, AS07.07, AS07.08, AS07.09, AS07.10, AS07.11, AS07.12, AS07.13, AS07.14, AS07.15, AS07.16, AS07.17, AS07.18, AS07.19, AS07.20, AS07.21, AS07.22, AS07.23, AS07.24, AS07.25, AS07.26, AS07.27, AS07.28, AS07.29, AS07.30, AS07.31, AS07.32 và AS07.33.	

Bảng 188 - VE và TE của AS07.06

Yêu cầu chung về an toàn vật lý - mức 1, 2, 3 và 4	
AS07.06 ISO/IEC 19790:2025, 7.7.2.1	Tài liệu phải quy định hình thái vật lý của mô-đun mật mã;
Thông tin bắt buộc từ nhà cung cấp	
VE07.06.01	Tài liệu của nhà cung cấp phải quy định hình thái vật lý của mô-đun: mô-đun mật mã đơn chip hoặc mô-đun mật mã đa chip như định nghĩa tại ISO/IEC 19790:2025, 7.7.1. Hình thái vật lý được quy định phải nhất quán với thiết kế vật lý của mô-đun. Tài liệu do nhà cung cấp cung cấp cũng phải tuyên bố mô-đun dự kiến đáp ứng mức an toàn nào (từ 1 đến 4).
Quy trình kiểm thử bắt buộc	
TE07.06.01	Kiểm thử viên phải xác minh rằng nhà cung cấp đã xác định mô-đun mật mã là mô-đun đơn chip hay mô-đun mật mã đa chip như định nghĩa tại ISO/IEC 19790:2025, 7.7.1. Kiểm thử viên phải thực hiện một quá trình xác định độc lập rằng hình thái vật lý đáp ứng một trong hai tiêu chí được quy định dưới đây. Các đặc tính quyết định cơ bản của hai hình thái vật lý và một số ví dụ phổ biến được tóm tắt dưới đây. a) Mô-đun mật mã đơn chip. Đặc điểm: Một chip mạch tích hợp (IC) duy nhất, được sử dụng như một thiết bị độc lập hoặc được nhúng vật lý bên trong một mô-đun hoặc vỏ bọc khác có thể không có bảo vệ vật lý. Mô-đun đơn chip sẽ bao gồm một khối khuôn (die) có thể được bao phủ bằng một vật liệu bên ngoài đồng nhất như nhựa hoặc gốm, và các đầu nối đầu vào/đầu ra bên ngoài. - Ví dụ: Các chip IC đơn lẻ, thẻ thông minh có một chip IC duy nhất, hoặc các hệ thống khác có một chip IC duy nhất để triển khai các chức năng mật mã và các chức năng liên quan đến an toàn. b) Mô-đun mật mã đa chip. Đặc điểm: Hai hoặc nhiều chip IC được kết nối với nhau và được nhúng vật lý bên trong một sản phẩm hoặc vỏ bọc khác có thể không có bảo vệ vật lý hoặc nhúng vật lý vào một vỏ bọc được bảo vệ vật lý hoàn toàn.
TE07.06.02	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có tuyên bố về mức an toàn mà mô-đun dự kiến đáp ứng. Kiểm thử viên phải thực hiện một quá trình xác định độc lập về mức an toàn mà mô-đun thực sự đáp ứng.

Bảng 189 - VE và TE của AS07.07

Yêu cầu chung về an toàn vật lý - mức 1, 2, 3 và 4	
AS07.07 ISO/IEC 19790:2025, 7.7.2.1	Bất cứ khi nào việc xóa trắng được thực hiện vì mục đích an toàn vật lý, việc xóa trắng phải diễn ra trong một khoảng thời gian đủ ngắn để ngăn chặn việc khôi phục các SSP đã bị xóa trắng trong khoảng thời gian từ lúc phát hiện ra đến lúc việc xóa trắng thực sự diễn ra.
Thông tin bắt buộc từ nhà cung cấp	
VE07.07.01	Tài liệu do nhà cung cấp cung cấp phải quy định thời gian phản hồi của việc xóa trắng sau khi phát hiện có sự can thiệp trái phép.
Quy trình kiểm thử bắt buộc	

TE07.07.01	Kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp có mô tả thời gian phản hồi xóa trắng sau khi phát hiện có sự can thiệp trái phép.
TE07.07.02	Kiểm thử viên phải xác minh rằng cơ chế phản hồi xóa trắng được triển khai như quy định.
TE07.07.03	Kiểm thử viên phải tìm cách ngăn chặn mô-đun thực hiện việc xóa trắng sau khi mô-đun phát hiện có sự can thiệp. Nếu kiểm thử viên thành công, bài kiểm thử phải được xác định là thất bại.

Bảng 190 - VE và TE của AS07.08

Yêu cầu chung về an toàn vật lý - mức 1, 2, 3 và 4	
AS07.08 ISO/IEC 19790:2025, 7.7.2.1	{Nếu một mô-đun bao gồm một vai trò bảo trì đòi hỏi quyền truy cập vật lý vào nội dung của mô-đun hoặc nếu mô-đun được thiết kế để cho phép truy cập vật lý (ví dụ: bởi nhà cung cấp mô-đun hoặc cá nhân được ủy quyền khác), thì} một giao diện bảo trì phải được xác định.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS03.12.	

Bảng 191 - VE và TE của AS07.09

Yêu cầu chung về an toàn vật lý - mức 1, 2, 3 và 4	
AS07.09 ISO/IEC 19790:2025, 7.7.2.1	{Nếu một mô-đun bao gồm một vai trò bảo trì đòi hỏi quyền truy cập vật lý vào nội dung của mô-đun hoặc nếu mô-đun được thiết kế để cho phép truy cập vật lý (ví dụ: bởi nhà cung cấp mô-đun hoặc cá nhân được ủy quyền khác), thì}: giao diện bảo trì phải bao gồm tất cả các đường dẫn truy cập vật lý vào nội dung của mô-đun mật mã, bao gồm mọi nắp hoặc cửa có thể tháo rời.
Thông tin bắt buộc từ nhà cung cấp	
VE07.09.01	Tài liệu do nhà cung cấp cung cấp phải quy định giao diện bảo trì, bao gồm mọi nắp hoặc cửa có thể tháo rời.
Quy trình kiểm thử bắt buộc	
TE07.09.01	Kiểm thử viên phải xác minh trong tài liệu của nhà cung cấp rằng một giao diện bảo trì được cung cấp, bao gồm mọi nắp hoặc cửa có thể tháo rời.

Bảng 192 - VE và TE của AS07.10

Yêu cầu chung về an toàn vật lý - mức 1, 2, 3 và 4	
AS07.10 ISO/IEC 19790:2025, 7.7.2.1	{Nếu một mô-đun bao gồm một vai trò bảo trì đòi hỏi quyền truy cập vật lý vào nội dung của mô-đun hoặc nếu mô-đun được thiết kế để cho phép truy cập vật lý (ví dụ: bởi nhà cung cấp mô-đun hoặc cá nhân được ủy quyền khác), thì}: bất kỳ nắp hoặc cửa nào có thể tháo rời được bao gồm trong giao diện bảo trì đều phải được bảo vệ bằng các cơ chế an toàn vật lý thích hợp.
Thông tin bắt buộc từ nhà cung cấp	
VE07.10.01	Tài liệu do nhà cung cấp cung cấp phải quy định một biện pháp bảo vệ vật lý sao cho mọi nắp hoặc cửa có thể tháo rời được bao gồm trong giao diện bảo trì đều được bảo vệ bằng các cơ chế an toàn vật lý thích hợp.
Quy trình kiểm thử bắt buộc	
TE07.10.01	Kiểm thử viên phải xác minh rằng mọi nắp hoặc cửa có thể tháo rời được bao gồm trong giao diện bảo trì đều được bảo vệ bằng các cơ chế an toàn vật lý thích hợp.

6.7.2.2 Mức an toàn 1

Bảng 193 - VE và TE của AS07.11

Yêu cầu chung về an toàn vật lý - mức 1, 2, 3 và 4	
AS07.11 ISO/IEC 19790:2025, 7.7.2.2	Các yêu cầu sau đây phải được áp dụng cho tất cả các mô-đun mật mã đối với mức an toàn 1: {AS07.12 đến AS07.13}
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.12 và AS07.13.	

Bảng 194 - VE và TE của AS07.12

Yêu cầu chung về an toàn vật lý - mức 1, 2, 3 và 4	
AS07.12 ISO/IEC 19790:2025, 7.7.2.2	Mô-đun mật mã phải được cấu thành từ các phần tử cấp độ sản xuất có áp dụng các kỹ thuật thụ động hóa tiêu chuẩn (ví dụ: một lớp phủ bảo vệ mạch hoặc một lớp phủ niêm phong được phủ lên mạch điện của mô-đun để bảo vệ chống lại hư hỏng do môi trường hoặc các hư hỏng vật lý khác).
Thông tin bắt buộc từ nhà cung cấp	
VE07.12.01	Tài liệu do nhà cung cấp cung cấp phải cung cấp bằng chứng về việc sử dụng các sản phẩm hoặc phần tử cấp độ sản xuất, bao gồm bằng chứng về cách thức các hạng mục này đã được kiểm tra để đáp ứng các thông số kỹ thuật hoạt động.
VE07.12.02	Tài liệu do nhà cung cấp cung cấp phải đề cập đến các kỹ thuật thụ động hóa được sử dụng trong quá trình sản xuất mô-đun.
Quy trình kiểm thử bắt buộc	
TE07.12.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng mô-đun chứa các sản phẩm hoặc phần tử đã được thiết kế nhằm đáp ứng các thông số kỹ thuật hoạt động.
TE07.12.02	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng một quy trình thụ động hóa tiêu chuẩn đã được áp dụng cho mô-đun. Quy trình thụ động hóa phải là một lớp phủ niêm phong được phủ lên mạch điện của chip để bảo vệ nó khỏi hư hỏng do môi trường hoặc các hư hỏng vật lý khác. Nếu không sử dụng quy trình thụ động hóa tiêu chuẩn, thì tài liệu phải cung cấp thông tin để chỉ ra lý do tại sao phương pháp này tương đương với một phương pháp tiếp cận thụ động hóa tiêu chuẩn.

Bảng 195 - VE và TE của AS07.13

Yêu cầu chung về an toàn vật lý - mức 1, 2, 3 và 4	
AS07.13 ISO/IEC 19790:2025, 7.7.2.2	Khi thực hiện bảo trì vật lý, việc xóa trắng phải được thực hiện tự động bởi mô-đun mật mã hoặc được người vận hành khởi tạo.
Thông tin bắt buộc từ nhà cung cấp	
VE07.13.01	Nếu mô-đun hỗ trợ vai trò bảo trì, tài liệu do nhà cung cấp cung cấp phải xác định liệu việc xóa trắng được thực hiện tự động bởi mô-đun hay do người vận hành khởi tạo.

VE07.13.02	Nếu các CSP, PSP và các thành phần khóa dạng rõ bị xóa trắng bằng thủ tục trong khi nằm dưới sự kiểm soát của người vận hành (tức là người vận hành có mặt để quan sát việc xóa trắng hoàn tất thành công, hoặc kiểm soát việc đó qua một phiên quản trị từ xa), tài liệu do nhà cung cấp cung cấp và chính sách an toàn của mô-đun phải quy định cách thức thực hiện các phương pháp này.
VE07.13.03	Nếu các CSP, PSP và các thành phần khóa dạng rõ bị xóa trắng một cách tự động khi đảm nhận vai trò bảo trì, tài liệu do nhà cung cấp cung cấp phải quy định cách các phương pháp xóa trắng được sử dụng để những kẻ tấn công không thể lấy được các CSP dạng rõ, PSP dạng rõ và các thành phần khóa dạng rõ bên trong mô-đun.
Quy trình kiểm thử bắt buộc	
TE07.13.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có xác định liệu việc xóa trắng được thực hiện tự động bởi mô-đun hay được người vận hành khởi tạo.
TE07.13.02	Nếu sử dụng các phương pháp xóa trắng theo thủ tục, kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp, bao gồm cả chính sách an toàn, quy định rằng thủ tục này phải được thực hiện dưới sự kiểm soát của người vận hành.
TE07.13.03	Nếu việc xóa trắng được người vận hành khởi tạo, kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp và chính sách an toàn có quy định quy trình cho việc xóa trắng.
TE07.13.04	Nếu việc xóa trắng diễn ra tự động, kiểm thử viên phải xác minh xem có những CSP, PSP và thành phần khóa dạng rõ nào trong mô-đun, sau đó đảm nhận vai trò bảo trì. Kiểm thử viên sau đó phải thử thực hiện các hoạt động mật mã bằng cách sử dụng từng CSP dạng rõ, PSP dạng rõ và thành phần khóa dạng rõ đã được lưu trữ trong mô-đun. Kiểm thử viên phải xác minh rằng không thể truy cập vào mọi SSP không được bảo vệ.
TE07.13.05	Kiểm thử viên phải xác minh rằng tất cả các CSP dạng rõ, PSP dạng rõ, và các thành phần khóa dạng rõ không bị xóa trắng bởi lệnh xóa trắng đều được 1) mã hóa bằng một thuật toán đã phê duyệt, hoặc 2) được bảo vệ về mặt vật lý hoặc logic bên trong một mô-đun mật mã được nhúng đã được thẩm định (được thẩm định là tuân thủ ISO/IEC 19790: 2025).

6.7.2.3 Mức an toàn 2

Bảng 196 - VE và TE của AS07.14

Yêu cầu chung về an toàn vật lý - mức 2, 3 và 4	
AS07.14 ISO/IEC 19790: 2025, 7.7.2.2	Ngoài các yêu cầu chung đối với mức an toàn 1, các yêu cầu sau đây phải được áp dụng cho tất cả các mô-đun mật mã đối với mức an toàn 2: {AS07.15 đến AS07.20}
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.15, AS07.16, AS07.17, AS07.18, AS07.19 và AS07.20.	

Bảng 197 - VE và TE của AS07.15

Yêu cầu chung về an toàn vật lý - mức 2, 3 và 4	
AS07.15 ISO/IEC	Mô-đun mật mã phải:

19790: 2025, 7.7.2.3	a) được bao phủ hoàn toàn bằng một vật liệu có bằng chứng bị can thiệp (ngoại trừ các đường dẫn nội bộ được bảo vệ); hoặc b) bao gồm một vỏ bọc có thể bao gồm các nắp hoặc cửa có thể tháo rời (ngoại trừ các đường dẫn nội bộ được bảo vệ). VÍ DỤ 1: Các lớp phủ phù hợp bao gồm nhựa epoxy và nhựa cứng. VÍ DỤ 2: Các vật liệu chứa phù hợp bao gồm kim loại và nhựa cứng
Thông tin bắt buộc từ nhà cung cấp	
VE07.15.01	Tài liệu do nhà cung cấp cung cấp phải xác định rằng mô-đun được bao phủ hoàn toàn bằng một vật liệu có bằng chứng bị can thiệp (ngoại trừ các đường dẫn nội bộ được bảo vệ) hoặc rằng mô-đun được đóng kín trong một hộp chứa có thể bao gồm các nắp hoặc cửa có thể tháo rời (ngoại trừ các đường dẫn nội bộ được bảo vệ).
Quy trình kiểm thử bắt buộc	
TE07.15.01	Kiểm thử viên phải kiểm tra mô-đun và xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng mô-đun hoặc được bao phủ hoàn toàn bằng một vật liệu có bằng chứng bị can thiệp (ngoại trừ các đường dẫn nội bộ được bảo vệ) hoặc rằng mô-đun được đóng kín trong một hộp chứa có thể bao gồm các cửa hoặc nắp có thể tháo rời (ngoại trừ các đường dẫn nội bộ được bảo vệ). Các yêu cầu sau đây phải được đáp ứng: a) Lớp vỏ bọc hoặc lớp phủ phải bao bọc hoàn toàn toàn bộ mô-đun (ngoại trừ các đường dẫn nội bộ được bảo vệ). b) Vật liệu vỏ bọc hoặc lớp phủ phải có thành phần được xác định trong tài liệu do nhà cung cấp cung cấp. Vỏ bọc phải ở cấp độ sản xuất. Tài liệu của nhà cung cấp phải chỉ ra rằng một vỏ bọc cùng chất liệu đã được sử dụng thương mại hoặc cung cấp dữ liệu chứng minh rằng nó tương đương với một sản phẩm thương mại.

Bảng 198 - VE và TE của AS07.16

Yêu cầu chung về an toàn vật lý - mức 2, 3 và 4	
AS07.16 ISO/IEC 19790: 2025, 7.7.2.3	Nếu mô-đun nằm trong một vỏ bọc chứa các cửa hoặc nắp có thể tháo rời, thì các cửa hoặc nắp này phải được khóa bằng các khóa cơ khí có khả năng chống mở khóa, sử dụng khóa vật lý hoặc khóa logic.
Thông tin bắt buộc từ nhà cung cấp	
VE07.16.01	Các cửa hoặc nắp đi kèm theo vỏ bọc phải được khóa bằng ổ khóa cơ học chống phá khóa sử dụng khóa vật lý hoặc khóa logic. Tài liệu do nhà cung cấp cung cấp phải mô tả các khóa và các khóa vật lý hoặc khóa logic được sử dụng,
Quy trình kiểm thử bắt buộc	
TE07.16.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng các cửa hoặc nắp được khóa bằng ổ khóa chống phá khóa, yêu cầu một khóa vật lý hoặc một khóa logic.
TE07.16.02	Kiểm thử viên phải thử mở nắp hoặc cửa đã bị khóa mà không sử dụng khóa và xác minh rằng nắp hoặc cửa sẽ không mở được mà không có dấu hiệu bị hư hỏng.

Bảng 199 - VE và TE của AS07.17

Yêu cầu chung về an toàn vật lý - mức 2, 3 và 4	
AS07.17 ISO/IEC 19790:2025, 7.7.2.3	{Nếu mô-đun nằm trong một vỏ bọc chứa các cửa hoặc nắp có thể tháo rời, thì các cửa hoặc nắp này phải được khóa bằng các ổ khóa cơ học chống phá khóa sử dụng khóa vật lý hoặc khóa logic} hoặc phải được bảo vệ bằng các tem niêm phong có bằng chứng bị can thiệp (ví dụ: băng keo niêm phong bằng chứng hoặc tem toàn ảnh).
Thông tin bắt buộc từ nhà cung cấp	
VE07.17.01	Tài liệu do nhà cung cấp cung cấp phải mô tả các tem niêm phong có bằng chứng bị can thiệp.
Quy trình kiểm thử bắt buộc	
TE07.17.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng nắp hoặc cửa được bảo vệ bằng một tem niêm phong có bằng chứng bị can thiệp chẳng hạn như băng keo niêm phong bằng chứng hoặc tem toàn ảnh.
TE07.17.02	Kiểm thử viên phải xác minh rằng nắp hoặc cửa không thể bị mở nếu không phá vỡ hoặc gỡ bỏ tem niêm phong, và tem niêm phong đó không thể bị gỡ ra và sau đó dán lại.

Bảng 200 - VE và TE của AS07.18

Yêu cầu chung về an toàn vật lý - mức 2, 3 và 4	
AS07.18 ISO/IEC 19790:2025, 7.7.2.3	Mô-đun mật mã phải cung cấp các dấu vết có thể nhìn thấy được (ví dụ: trên nắp đậy, vỏ bọc, lớp phủ, bao bì đóng gói, hoặc tem niêm phong) nhằm cung cấp bằng chứng có thể phát hiện được về các nỗ lực sửa đổi hoặc truy cập mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE07.18.01	Tài liệu do nhà cung cấp cung cấp phải xác định thiết kế có bằng chứng bị can thiệp của mô-đun bao gồm mọi đặc tính liên quan cần thiết để đảm bảo có bằng chứng bị can thiệp.
Quy trình kiểm thử bắt buộc	
TE07.18.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng mô-đun có bao gồm các dấu vết bị can thiệp. Việc kiểm tra phải xác minh rằng thiết kế có bằng chứng bị can thiệp sẽ dẫn đến việc để lại dấu vết sau mọi nỗ lực nhằm sửa đổi, thăm dò trực tiếp hoặc thao túng các thành phần bên trong của mô-đun.

Bảng 201 - VE và TE của AS07.19

Yêu cầu chung về an toàn vật lý - mức 2, 3 và 4	
AS07.19 ISO/IEC 19790:2025, 7.7.2.3	Vật liệu có bằng chứng bị can thiệp, lớp phủ, vỏ bọc hoặc bao bì đóng gói phải đục hoặc mờ trong phạm vi quang phổ nhìn thấy được (tức là ánh sáng có dải bước sóng từ 400 nm đến 750 nm) nhằm ngăn chặn việc thu thập thông tin về các hoạt động bên trong của các khu vực trọng yếu của mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE07.19.01	Tài liệu do nhà cung cấp cung cấp phải quy định rằng vật liệu có bằng chứng bị can thiệp, lớp phủ, hoặc vỏ bọc là đục hoặc mờ trong quang phổ nhìn thấy được.
Quy trình kiểm thử bắt buộc	

TE07.19.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng vật liệu có bằng chứng bị can thiệp, lớp phủ, hoặc vỏ bọc là đục hoặc mờ trong quang phổ nhìn thấy được.
TE07.19.02	Kiểm thử viên phải chiếu sáng mô-đun trong toàn bộ dải quang phổ nhìn thấy được để xác minh rằng vật liệu có bằng chứng bị can thiệp là đục hoặc mờ.

Bảng 202 - VE và TE của AS07.20

Yêu cầu chung về an toàn vật lý - mức 2, 3 và 4	
AS07.20 ISO/IEC 19790:2025, 7.7.2.3	Nếu mô-đun mật mã có chứa các lỗ thông gió hoặc khe hở, thì mô-đun phải được cấu trúc theo cách thức để ngăn chặn việc thu thập thông tin về cấu trúc bên trong hoặc các thành phần của mô-đun thông qua việc quan sát bằng mắt trực tiếp sử dụng các nguồn sáng nhân tạo trong quang phổ nhìn thấy được đối với cấu trúc bên trong hoặc các thành phần của mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE07.20.01	Nếu mô-đun nằm trong một nắp đậy hoặc vỏ bọc có chứa bất kỳ lỗ thông gió hoặc khe hở nào, thì chúng phải được cấu trúc theo cách thức nhằm ngăn chặn việc thu thập thông tin về cấu trúc bên trong hoặc các thành phần của mô-đun thông qua quan sát bằng mắt trực tiếp sử dụng các nguồn sáng nhân tạo trong quang phổ nhìn thấy được đối với cấu trúc bên trong hoặc các thành phần của mô-đun. Tài liệu do nhà cung cấp cung cấp phải mô tả cách tiếp cận thiết kế vật lý nhằm ngăn chặn sự quan sát như vậy.
Quy trình kiểm thử bắt buộc	
TE07.20.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh xem mô-đun có nắp đậy hoặc vỏ bọc với các lỗ thông gió, khe hở, hoặc khe hở khác hay không, và nếu có, liệu chúng có được cấu trúc để ngăn chặn việc thu thập thông tin về cấu trúc bên trong hoặc các thành phần của mô-đun thông qua quan sát bằng mắt trực tiếp sử dụng các nguồn sáng nhân tạo trong quang phổ nhìn thấy được đối với cấu trúc bên trong hoặc các thành phần của mô-đun hay không.

6.7.2.4 Mức an toàn 3**Bảng 203 - VE và TE của AS07.21**

Yêu cầu chung về an toàn vật lý - mức 3 và 4	
AS07.21 ISO/IEC 19790:2025, 7.7.2.4	Ngoài các yêu cầu chung đối với mức an toàn 1 và 2, các yêu cầu sau đây phải được áp dụng cho tất cả các mô-đun mật mã đối với mức an toàn 3: {AS07.22 đến AS07.30}.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.22, AS07.23, AS07.24, AS07.25, AS07.26, AS07.27, AS07.28, AS07.29 và AS07.30.	

Bảng 204 - VE và TE của AS07.22

Yêu cầu chung về an toàn vật lý - mức 3 và 4

AS07.22 ISO/IEC 19790:2025, 7.7.2.4	Mô-đun phải được bao phủ (ngoại trừ các đường dẫn nội bộ được bảo vệ) bằng một lớp phủ, vỏ bọc hoặc bao bì đóng gói cứng, đục, có bằng chứng bị can thiệp, {nhằm đảm bảo rằng các nỗ lực cố gỡ bỏ hoặc xuyên thủng vật lý lớp phủ đó bằng các phương pháp phi hóa học phải có xác suất cao gây ra hư hỏng nghiêm trọng cho mô-đun mật mã}
Thông tin bắt buộc từ nhà cung cấp	
VE07.22.01	Tài liệu do nhà cung cấp cung cấp phải xác định lớp phủ, vỏ bọc hoặc bao bì đóng gói có bằng chứng bị can thiệp, cứng, đục được sử dụng.
VE07.22.02	Tài liệu do nhà cung cấp cung cấp phải cung cấp thông tin thiết kế hỗ trợ cho mô-đun khi được bao phủ bằng lớp phủ, vỏ bọc hoặc bao bì đóng gói có bằng chứng bị can thiệp, cứng, đục. Vật liệu đó phải đục trong quang phổ nhìn thấy được.
Quy trình kiểm thử bắt buộc	
TE07.22.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng mô-đun được bao phủ bằng một vỏ bọc, lớp phủ hoặc bao bì đóng gói có bằng chứng bị can thiệp, cứng, đục.
TE07.22.02	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng vật liệu đồ keo không thể bị gỡ bỏ hoặc xuyên thủng mà không có xác suất cao gây ra hư hỏng nghiêm trọng cho mô-đun. Kiểm thử viên phải xác minh các đặc tính chống tháo dỡ của lớp phủ, vỏ bọc hoặc bao bì đóng gói của mô-đun. Kiểm thử viên phải thử bóc hoặc cạy vật liệu đó ra khỏi mô-đun và xác minh rằng, với một lực tác động hợp lý, không thể bóc hoặc cạy vật liệu ra mà không làm mô-đun ngừng hoạt động hoặc làm mạch điện của mô-đun bị phá hủy vật lý rõ rệt.

Bảng 205 - VE và TE của AS07.23

Yêu cầu chung về an toàn vật lý - mức 3 và 4	
AS07.23 ISO/IEC 19790:2025, 7.7.2.4	{Mô-đun phải được bao phủ (ngoại trừ các đường dẫn nội bộ được bảo vệ) bằng một lớp phủ, vỏ bọc hoặc bao bì đóng gói cứng, đục, có bằng chứng bị can thiệp} nhằm đảm bảo rằng các nỗ lực cố gỡ bỏ hoặc xuyên thủng vật lý lớp phủ đó bằng các phương pháp phi hóa học phải có xác suất cao gây ra hư hỏng nghiêm trọng cho mô-đun mật mã.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.22.	

Bảng 206 - VE và TE của AS07.24

Yêu cầu chung về an toàn vật lý - mức 3 và 4	
AS07.24 ISO/IEC 19790:2025, 7.7.2.4	Nếu mô-đun mật mã có chứa bất kỳ cửa hoặc nắp có thể tháo rời nào hoặc nếu một giao diện truy cập bảo trì được định nghĩa, thì mô-đun phải có khả năng phản hồi can thiệp trái phép và xóa trắng.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.25.	

Bảng 207 - VE và TE của AS07.25

Yêu cầu chung về an toàn vật lý - mức 3 và 4	
AS07.25 ISO/IEC 19790:2025,	Bất kỳ khả năng phản hồi can thiệp trái phép và xóa trắng nào đều phải xóa trắng ngay lập tức tất cả các CSP dạng rõ, các PSP dạng rõ và các thành phần khóa dạng rõ khi phát hiện một sự kiện can thiệp (ví dụ: một cánh cửa bị mở, một nắp

7.7.2.4	đậy bị tháo, một cảm biến can thiệp bên trong bị kích hoạt chẳng hạn như vi phạm vỏ bọc phát hiện can thiệp, hoặc khi giao diện bảo trì bị truy cập).
Thông tin bắt buộc từ nhà cung cấp	
VE07.25.01	Tài liệu do nhà cung cấp cung cấp phải cung cấp tài liệu thiết kế hỗ trợ cho vỏ bọc của mô-đun, các cảm biến can thiệp trái phép hoặc giao diện bảo trì, nếu được định nghĩa.
VE07.25.02	Tài liệu do nhà cung cấp cung cấp phải xác định bất kỳ cửa hoặc nắp có thể tháo rời nào hoặc giao diện bảo trì và phải lập tài liệu về mạch phản hồi can thiệp và mạch xóa trắng của mô-đun.
VE07.25.03	Tài liệu do nhà cung cấp cung cấp phải xác định bất kỳ cảm biến phát hiện can thiệp nào (ví dụ: vỏ bọc phát hiện can thiệp) và phải lập tài liệu về mạch phản hồi can thiệp và mạch xóa trắng của mô-đun liên kết với các cảm biến này.
Quy trình kiểm thử bắt buộc	
TE07.25.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định: a) tất cả các cửa, nắp đậy có thể tháo rời và liệu một giao diện bảo trì có được chỉ định hay không; b) mạch phản hồi can thiệp và mạch xóa trắng được liên kết với các cửa, nắp đậy có thể tháo rời và giao diện bảo trì; c) tất cả các cảm biến can thiệp cần thiết để đáp ứng các yêu cầu hiện hành của ISO/IEC 19790: 2025, 7.7; và d) mạch phản hồi can thiệp và mạch xóa trắng được liên kết với tất cả các cảm biến can thiệp cần thiết để đáp ứng các yêu cầu hiện hành của ISO/IEC 19790: 2025, 7.7.
TE07.25.02	Nếu mô-đun hỗ trợ phát hiện can thiệp và phản hồi, thì kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng mô-đun sẽ xóa trắng tất cả các CSP dạng rõ, PSP dạng rõ và các thành phần khóa dạng rõ.
TE07.25.03	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng mạch phản hồi can thiệp và mạch xóa trắng, nếu được hỗ trợ, vẫn duy trì hoạt động trong khi các CSP dạng rõ, PSP dạng rõ và các thành phần khóa dạng rõ đang được chứa bên trong mô-đun.
TE07.25.04	Nếu mô-đun hỗ trợ phát hiện can thiệp và phản hồi, kiểm thử viên phải kiểm tra xem mô-đun có xóa trắng tất cả các CSP dạng rõ, PSP dạng rõ và các thành phần khóa dạng rõ khi một nắp đậy hoặc cửa bị tháo gỡ hoặc nếu giao diện bảo trì bị truy cập hay không.

Bảng 208 - VE và TE của AS07.26

Yêu cầu chung về an toàn vật lý - mức 3 và 4	
AS07.26 ISO/IEC 19790: 2025, 7.7.2.4	Nếu một mô-đun hỗ trợ khả năng phản hồi can thiệp và xóa trắng, khả năng phản hồi can thiệp và xóa trắng đó phải duy trì hoạt động trong khi các CSP dạng rõ, PSP dạng rõ và các thành phần khóa dạng rõ đang được chứa bên trong mô-đun mật mã.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.25.	

Bảng 209 - VE và TE của AS07.27

Yêu cầu chung về an toàn vật lý - mức 3 và 4	
AS07.27 ISO/IEC 19790:2025, 7.7.2.4	Việc xóa trắng được kích hoạt bởi việc phát hiện sự kiện can thiệp phải được thực hiện bởi mô-đun mà không cần nguồn điện bên ngoài mô-đun và trước khi nguồn điện bên trong mô-đun không đủ để mạch xóa trắng của mô-đun hoạt động;
Thông tin bắt buộc từ nhà cung cấp	
VE07.27.01	Nếu mô-đun chứa khả năng phản hồi can thiệp và xóa trắng, tài liệu do nhà cung cấp cung cấp phải lập tài liệu về cách thức việc xóa trắng có thể được hoàn thành sau khi phát hiện một sự kiện can thiệp mà không cần nguồn điện bên ngoài mô-đun và trước khi nguồn điện bên trong mô-đun không đủ để mạch xóa trắng của mô-đun hoạt động.
Quy trình kiểm thử bắt buộc	
TE07.27.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp một lời giải trình về cách thức thiết kế phản hồi can thiệp và xóa trắng của các mô-đun có thể đáp ứng AS07.27.
TE07.27.02	Kiểm thử viên phải ngắt kết nối tất cả nguồn điện bên ngoài và phá vỡ rào cản vỏ bọc phát hiện can thiệp, sau đó xác minh rằng mô-đun xóa trắng tất cả các CSP dạng rõ và các PSP dạng rõ của người vận hành. Dựa trên lời giải trình do nhà cung cấp đưa ra, kiểm thử viên phải thực hiện các bài kiểm thử nhằm xác nhận AS07.27 được đáp ứng. Điều này phải được thực hiện dựa trên sự kết hợp giữa việc kiểm tra mô-đun để xác nhận thiết kế của mô-đun và bài kiểm thử tiếp theo. CHÚ THÍCH Trong trường hợp mô-đun không lưu trữ bất kỳ CSP dạng rõ hoặc PSP dạng rõ của người vận hành nào trong trạng thái tắt nguồn của nó, AS07.27 được ngầm hiểu là đã được đáp ứng và không cần kiểm tra thêm.

Bảng 210 - VE và TE của AS07.28

Yêu cầu chung về an toàn vật lý - mức 3 và 4	
AS07.28 ISO/IEC 19790:2025, 7.7.2.4	Nếu mô-đun mật mã có chứa các lỗ thông gió hoặc khe hở, thì mô-đun phải được cấu trúc theo cách thức nhằm ngăn chặn việc thăm dò vật lý mà không bị phát hiện bên trong vỏ bọc (ví dụ: ngăn chặn việc thăm dò bằng một đầu dò khớp nối đơn).
Thông tin bắt buộc từ nhà cung cấp	
VE07.28.01	Nếu mô-đun nằm trong một nắp đậy hoặc vỏ bọc có chứa bất kỳ lỗ thông gió hoặc khe hở nào, thì chúng phải được cấu trúc theo cách thức nhằm ngăn chặn việc thăm dò vật lý mà không bị phát hiện bên trong vỏ bọc. Tài liệu do nhà cung cấp cung cấp phải mô tả phương pháp thiết kế vật lý của lỗ thông gió.
Quy trình kiểm thử bắt buộc	
TE07.28.01	Kiểm thử viên phải xem xét tài liệu của nhà cung cấp và kiểm tra mô-đun để xác minh xem mô-đun có nắp đậy hoặc vỏ bọc với các lỗ thông gió, khe hở, hoặc khe hở khác hay không, và nếu có, liệu chúng có được cấu trúc để ngăn việc thăm dò không bị phát hiện vào bên trong nắp đậy hoặc vỏ bọc hay không.

Bảng 211 - VE và TE của AS07.29

Yêu cầu chung về an toàn vật lý - mức 3 và 4

AS07.29 ISO/IEC 19790: 2025, 7.7.2.4	Các vỏ bọc, lớp phủ hoặc vật liệu đổ keo vững chắc hoặc cứng, dù phủ bám theo biên dạng hay không bám theo biên dạng phải duy trì các đặc tính về độ bền và độ cứng trong suốt dải nhiệt độ hoạt động, lưu trữ và phân phối dự kiến của mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE07.29.01	Tài liệu của nhà cung cấp phải mô tả độ bền hoặc độ cứng của vỏ bọc, lớp phủ hoặc vật liệu đổ keo cứng, phủ bám theo biên dạng hoặc không bám theo biên dạng, và phải cung cấp cơ sở hợp lý chứng minh rằng độ bền hoặc độ cứng đó là phù hợp với thiết kế của mô-đun.
VE07.29.02	Chính sách an toàn do nhà cung cấp cung cấp phải quy định nhiệt độ cao nhất và thấp nhất trong dải nhiệt độ.
Quy trình kiểm thử bắt buộc	
TE07.29.01	Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp và việc kiểm thử mô-đun rằng độ bền hoặc độ cứng của vỏ bọc, lớp phủ, hoặc vật liệu đổ keo cứng, phủ bám theo biên dạng hoặc không bám theo biên dạng được triển khai như quy định. Kiểm thử viên phải xác minh độ cứng của mô-đun tại các nhiệt độ sau: a) nhiệt độ thấp nhất trong dải nhiệt độ hoạt động, lưu trữ và phân phối dự kiến của mô-đun; b) nhiệt độ cao nhất trong dải nhiệt độ hoạt động, lưu trữ và phân phối dự kiến của mô-đun.
TE07.29.02	Kiểm thử viên phải xác minh rằng chính sách an toàn do nhà cung cấp cung cấp có quy định dải nhiệt độ cao và thấp.

Bảng 212 - VE và TE của AS07.30

Yêu cầu chung về an toàn vật lý - mức 3 và 4	
AS07.30 ISO/IEC 19790: 2025, 7.7.2.4	Nếu các tem niêm phong có bằng chứng bị can thiệp được sử dụng, chúng phải được đánh số duy nhất hoặc có thể nhận diện độc lập (ví dụ: băng keo niêm phong bằng chứng được đánh số duy nhất hoặc tem toàn ảnh có thể nhận diện duy nhất).
Thông tin bắt buộc từ nhà cung cấp	
VE07.30.01	Nhà cung cấp phải cung cấp đặc tả về tem niêm phong có bằng chứng bị can thiệp.
Quy trình kiểm thử bắt buộc	
TE07.30.01	Kiểm thử viên phải xác minh rằng các tem niêm phong có bằng chứng bị can thiệp được đánh số duy nhất hoặc có thể nhận diện độc lập như đã lập tài liệu.

6.7.2.5 Mức an toàn 4**Bảng 213 - VE và TE của AS07.31**

Yêu cầu chung về an toàn vật lý - mức 4	
AS07.31 ISO/IEC 19790: 2025, 7.7.2.5	Ngoài các yêu cầu chung đối với mức an toàn 1, 2, và 3, yêu cầu sau đây phải được áp dụng cho tất cả các mô-đun mật mã đối với mức an toàn 4: {AS07.32 và AS07.33}.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.32 và AS07.33.	

Bảng 214 - VE và TE của AS07.32

Yêu cầu chung về an toàn vật lý - mức 4	
AS07.32 ISO/IEC 19790: 2025, 7.7.2.5	Mô-đun mật mã phải cung cấp sự bảo vệ chống lại việc tiêm lỗi.
Thông tin bắt buộc từ nhà cung cấp	
VE07.32.01	Tài liệu do nhà cung cấp cung cấp phải quy định cơ chế bảo vệ chống lại việc tiêm lỗi.
Quy trình kiểm thử bắt buộc	
TE07.32.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng các cơ chế bảo vệ chống tiêm lỗi đã được quy định.
TE07.32.02	Kiểm thử viên phải tiêm các lỗi tại biên mô-đun bao gồm cả các giao diện và xác định rằng chức năng liên quan đến an toàn của mô-đun không bị tổn hại.
CHÚ THÍCH Việc tiêm lỗi có thể có bản chất là điện, quang, hoặc cơ học.	

Bảng 215 - VE và TE của AS07.33

Yêu cầu chung về an toàn vật lý - mức 4	
AS07.33 ISO/IEC 19790: 2025, 7.7.2.5	Các kỹ thuật giảm nhẹ tiêm lỗi và các số liệu giảm nhẹ được sử dụng phải được lập tài liệu như quy định tại ISO/IEC 19790: 2025, Phụ lục B.
Thông tin bắt buộc từ nhà cung cấp	
VE07.33.01	Tài liệu do nhà cung cấp cung cấp phải quy định các kỹ thuật giảm nhẹ tiêm lỗi và các số liệu giảm nhẹ được mô-đun sử dụng.
Quy trình kiểm thử bắt buộc	
TE07.33.01	Kiểm thử viên phải xác minh rằng các kỹ thuật giảm nhẹ tiêm lỗi và các số liệu giảm nhẹ được mô-đun sử dụng đã được lập tài liệu như quy định.

6.7.3 Yêu cầu an toàn vật lý đối với từng hình thái an toàn vật lý**6.7.3.1 Mô-đun mật mã đơn chip****Bảng 216 - VE và TE của AS07.34**

Yêu cầu an toàn vật lý đối với từng hình thái an toàn vật lý - mức 4	
AS07.34 ISO/IEC 19790: 2025, 7.7.3.1	Ngoài các yêu cầu chung về an toàn vật lý đối với các mức an toàn 1, 2, 3 và 4, các yêu cầu sau đây phải được áp dụng cho các mô-đun mật mã đơn chip đối với mức an toàn 4.
Thông tin bắt buộc từ nhà cung cấp	
VE07.34.01	Tài liệu do nhà cung cấp cung cấp phải quy định rằng (AS07.35) hoặc (AS07.36 đến AS07.37) được đáp ứng.
Quy trình kiểm thử bắt buộc	
TE07.34.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có bao gồm một lời tuyên bố về tùy chọn nào đã được thực hiện để đáp ứng các yêu cầu của mức 4 đối với các mô-đun mật mã đơn chip.

Bảng 217 - VE và TE của AS07.35

Yêu cầu an toàn vật lý đối với từng hình thái an toàn vật lý - mức 4	
AS07.35 ISO/IEC 19790:2025, 7.7.3.1	Lớp phủ chống tháo dỡ hoặc vỏ bọc vững chắc phải có các đặc tính hòa tan sao cho việc hòa tan lớp phủ hoặc vỏ bọc vững chắc đó có xác suất cao gây ra hư hỏng nghiêm trọng cho mô-đun (tức là mô-đun sẽ không hoạt động và bị hư hỏng không thể sửa chữa); hoặc {AS07.36 đến AS07.37}.
Thông tin bắt buộc từ nhà cung cấp	
VE07.35.01	Tài liệu do nhà cung cấp cung cấp phải mô tả các đặc tính hòa tan của lớp phủ chống tháo dỡ. Các đặc tính hòa tan của vật liệu phải sao cho việc hòa tan vật liệu để gỡ bỏ nó sẽ có xác suất cao làm hòa tan hoặc gây ra hư hỏng nghiêm trọng cho mô-đun.
Quy trình kiểm thử bắt buộc	
TE07.35.01	Kiểm thử viên phải xác minh tài liệu do nhà cung cấp cung cấp để xác định các thuộc tính hòa tan của lớp phủ chống tháo dỡ của mô-đun.
TE07.35.02	Kiểm thử viên phải kiểm tra các thuộc tính hòa tan của lớp phủ chống tháo dỡ của mô-đun. Dựa trên tài liệu được cung cấp tại VE07.35.01, kiểm thử viên phải xác minh xem loại dung môi nào sẽ được yêu cầu để làm tổn hại đến lớp phủ chống tháo dỡ.

Bảng 218 - VE và TE của AS07.36

Yêu cầu an toàn vật lý đối với từng hình thái an toàn vật lý - mức 4	
AS07.36 ISO/IEC 19790:2025, 7.7.3.1	{Lớp phủ chống tháo dỡ hoặc vỏ bọc vững chắc phải có các đặc tính hòa tan sao cho việc hòa tan lớp phủ hoặc vỏ bọc vững chắc đó có xác suất cao gây ra hư hỏng nghiêm trọng cho mô-đun (tức là mô-đun sẽ không hoạt động và bị hư hỏng không thể sửa chữa);} hoặc mô-đun phải cung cấp một vỏ bọc phát hiện can thiệp cùng với mạch phát hiện can thiệp mà {sẽ phát hiện sự can thiệp bằng các phương pháp như cắt, khoan, phay, mài, đốt cháy, làm nóng chảy, hoặc hòa tan lớp phủ hoặc bao bì đóng gói của mô-đun đơn chip tới một mức độ đủ để cho phép truy cập hoặc sửa đổi các SSP, hoặc sẽ dẫn đến việc sử dụng hoặc sửa đổi trái phép mô-đun.}
Thông tin bắt buộc từ nhà cung cấp	
VE07.36.01	Vỏ bọc hoặc vật liệu đồ keo phải được bao bọc bởi một vỏ bọc phát hiện can thiệp cùng với mạch phát hiện can thiệp thông qua việc sử dụng các cơ chế phát hiện can thiệp. Tài liệu do nhà cung cấp cung cấp phải mô tả thiết kế của vỏ bọc phát hiện can thiệp hoặc mạch phát hiện can thiệp.
Quy trình kiểm thử bắt buộc	
TE07.36.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng vỏ bọc của mô-đun hoặc vật liệu đồ keo có chứa các cơ chế phát hiện can thiệp. Điều này phải tạo thành một vỏ bọc phát hiện can thiệp với mạch phát hiện can thiệp nhằm bảo vệ các thành phần của mô-đun. Các cơ chế này phải được thiết kế sao cho bất kỳ sự phá vỡ vỏ bọc hoặc vật liệu đồ keo nào nhằm truy cập vào các thành phần của mô-đun đều có thể bị phát hiện.

Bảng 219 - VE và TE của AS07.37

Yêu cầu an toàn vật lý đối với từng hình thái an toàn vật lý - mức 4
--

AS07.37 ISO/IEC 19790: 2025, 7.7.3.1	{Lớp phủ chống tháo dỡ hoặc vỏ bọc vững chắc phải có các đặc tính hòa tan sao cho việc hòa tan lớp phủ hoặc vỏ bọc vững chắc đó có xác suất cao gây ra hư hỏng nghiêm trọng cho mô-đun (tức là mô-đun sẽ không hoạt động và bị hư hỏng không thể sửa chữa);} hoặc {mô-đun phải cung cấp một vỏ bọc phát hiện can thiệp cùng với mạch phát hiện can thiệp} phải phát hiện sự can thiệp bằng các phương pháp như cắt, khoan, phay, mài, đốt cháy, làm nóng chảy, hoặc hòa tan lớp phủ hoặc bao bì đóng gói của mô-đun đơn chip tới một mức độ đủ để cho phép truy cập hoặc sửa đổi các SSP, hoặc sẽ dẫn đến việc sử dụng hoặc sửa đổi trái phép mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE07.37.01	Tài liệu do nhà cung cấp cung cấp phải mô tả thiết kế phát hiện can thiệp.
Quy trình kiểm thử bắt buộc	
TE07.37.01	Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp rằng mô-đun có chứa mạch phát hiện can thiệp liên tục giám sát vỏ bọc phát hiện can thiệp; phát hiện bất kỳ sự phá vỡ nào bằng các phương pháp như khoan, phay, mài, hoặc hòa tan bất kỳ phần nào của vỏ bọc; và sau đó xóa trắng tất cả các CSP dạng rõ, các PSP dạng rõ và các thành phần khóa dạng rõ.
TE07.37.02	Kiểm thử viên phải phá vỡ vỏ bọc phát hiện can thiệp bằng cách sử dụng các cuộc tấn công liên quan đến thiết kế của nó và xác minh rằng mô-đun phát hiện được nỗ lực xâm nhập và xóa trắng tất cả các CSP dạng rõ và các PSP dạng rõ của người vận hành.

6.7.3.2 Mô-đun mật mã đa chip

Bảng 220 - VE và TE của AS07.38

Yêu cầu an toàn vật lý đối với từng hình thái an toàn vật lý - mức 4	
AS07.38 ISO/IEC 19790: 2025, 7.7.3.2	Ngoài các yêu cầu chung về an toàn vật lý đối với các mức an toàn 1, 2, 3 và 4 được quy định tại ISO/IEC 19790:2025, 7.7.2, các yêu cầu sau đây phải được áp dụng cho các mô-đun mật mã đa chip đối với mức an toàn 4:
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.39, AS07.40, AS07.41, AS07.42, AS07.43, AS07.44 và AS07.45.	

Bảng 221 - VE và TE của AS07.39

Yêu cầu an toàn vật lý đối với từng hình thái an toàn vật lý - mức 4	
AS07.39 ISO/IEC 19790: 2025, 7.7.3.2	Tất cả các giao diện giữa các thành phần mang dữ liệu và kiểm soát liên quan đến an toàn phải là một đường dẫn nội bộ được bảo vệ, hoặc được đóng kín hoàn toàn trong một vỏ bọc phát hiện can thiệp cùng với mạch phát hiện can thiệp.
Thông tin bắt buộc từ nhà cung cấp	
VE07.39.01	Tài liệu của nhà cung cấp phải quy định cách thức tất cả các giao diện giữa các thành phần mang dữ liệu và kiểm soát liên quan đến an toàn hoặc là một đường dẫn nội bộ được bảo vệ, hoặc được đóng kín hoàn toàn trong một vỏ bọc phát hiện can thiệp cùng với mạch phát hiện can thiệp.
Quy trình kiểm thử bắt buộc	

TE07.39.01	Kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp có quy định cách thức tắt cả các giao diện giữa các thành phần mang dữ liệu và kiểm soát liên quan đến an toàn hoặc là một đường dẫn nội bộ được bảo vệ, hoặc được đóng kín hoàn toàn trong một vỏ bọc phát hiện can thiệp cùng với mạch phát hiện can thiệp.
TE07.39.02	Kiểm thử viên phải xác minh bằng cách kiểm tra mô-đun rằng tất cả các giao diện giữa các thành phần hoặc là một đường dẫn nội bộ được bảo vệ, hoặc được đóng kín hoàn toàn trong một vỏ bọc phát hiện can thiệp cùng với mạch phát hiện can thiệp.

Bảng 222 - VE và TE của AS07.40

Yêu cầu an toàn vật lý đối với từng hình thái an toàn vật lý - mức 4	
AS07.40 ISO/IEC 19790:2025, 7.7.3.1	Tất cả các thành phần phải được bao phủ bằng một lớp phủ chống tháo dỡ cứng, đục, một vỏ bọc vững chắc, hoặc được đóng kín hoàn toàn trong một vỏ bọc phát hiện can thiệp.
Thông tin bắt buộc từ nhà cung cấp	
VE07.40.01	Tài liệu do nhà cung cấp cung cấp phải mô tả cách thức tắt cả các thành phần được bao phủ bằng một lớp phủ chống tháo dỡ cứng, đục, vỏ bọc vững chắc, hoặc được đóng kín hoàn toàn trong một vỏ bọc phát hiện can thiệp.
Quy trình kiểm thử bắt buộc	
TE07.40.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và xác minh rằng nó có mô tả cách thức tắt cả các thành phần được bao phủ bằng một lớp phủ chống tháo dỡ cứng, đục, vỏ bọc vững chắc, hoặc được đóng kín hoàn toàn trong một vỏ bọc phát hiện can thiệp.
TE07.40.02	Kiểm thử viên phải kiểm tra mô-đun để xác minh rằng tất cả các thành phần đều được bao phủ bằng một lớp phủ chống tháo dỡ cứng, đục, vỏ bọc vững chắc, hoặc được đóng kín hoàn toàn trong một vỏ bọc phát hiện can thiệp.

Bảng 223 - VE và TE của AS07.41

Yêu cầu an toàn vật lý đối với từng hình thái an toàn vật lý - mức 4	
AS07.41 ISO/IEC 19790:2025, 7.7.3.2	Khi vỏ bọc phát hiện can thiệp được sử dụng, nó phải phát hiện sự can thiệp bằng các phương pháp như cắt, khoan, phay, mài, đốt cháy, làm nóng chảy, hoặc hòa tan vỏ bọc của mô-đun tới một mức độ đủ để cho phép truy cập hoặc sửa đổi các SSP, hoặc sẽ dẫn đến việc sử dụng hoặc sửa đổi trái phép mô-đun.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.45.	

Bảng 224 - VE và TE của AS07.42

Yêu cầu an toàn vật lý đối với từng hình thái an toàn vật lý - mức 4	
AS07.42 ISO/IEC 19790:2025, 7.7.3.2	Khi sử dụng một lớp phủ chống tháo dỡ cứng, đục hoặc một vỏ bọc vững chắc, vật liệu phải có các đặc tính về độ cứng và độ bám dính sao cho việc cố bóc hoặc cạy lớp phủ hoặc vỏ bọc vững chắc đó ra khỏi mô-đun sẽ có xác suất cao dẫn đến hư hỏng nghiêm trọng cho mô-đun (tức là mô-đun sẽ không hoạt động và bị hư hỏng không thể sửa chữa).
Thông tin bắt buộc từ nhà cung cấp	

VE07.42.01	Tài liệu do nhà cung cấp cung cấp phải trình bày chi tiết về các đặc tính độ cứng và độ bám dính sao cho nỗ lực bóc hoặc cạy lớp phủ hoặc vỏ bọc vững chắc đó ra khỏi mô-đun sẽ có xác suất cao dẫn đến hư hỏng nghiêm trọng cho mô-đun.
Quy trình kiểm thử bắt buộc	
TE07.42.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có trình bày chi tiết về các đặc tính độ cứng và độ bám dính sao cho việc cố bóc hoặc cạy lớp phủ hoặc vỏ bọc vững chắc đó ra khỏi mô-đun sẽ có xác suất cao dẫn đến hư hỏng nghiêm trọng cho mô-đun.
TE07.42.02	Kiểm thử viên phải xác minh các đặc tính chống tháo dỡ của lớp phủ hoặc vỏ bọc vững chắc của mô-đun. Kiểm thử viên phải thử bóc hoặc cạy vật liệu đó ra khỏi mô-đun và xác minh rằng, với một lực tác động hợp lý, không thể bóc hoặc cạy vật liệu ra mà không làm mô-đun ngừng hoạt động hoặc làm mạch điện của mô-đun bị phá hủy vật lý rõ rệt.

Bảng 225 - VE và TE của AS07.43

Yêu cầu an toàn vật lý đối với từng hình thái an toàn vật lý - mức 4	
AS07.43 ISO/IEC 19790:2025, 7.7.3.2	Khi sử dụng một lớp phủ chống tháo dỡ cứng, đục hoặc một vỏ bọc vững chắc, vật liệu phải có các đặc tính hòa tan sao cho việc hòa tan lớp phủ hoặc vỏ bọc vững chắc đó sẽ có xác suất cao làm hòa tan hoặc gây ra hư hỏng nghiêm trọng cho mô-đun (tức là mô-đun sẽ không hoạt động và bị hư hỏng không thể sửa chữa).
Thông tin bắt buộc từ nhà cung cấp	
VE07.43.01	Tài liệu do nhà cung cấp cung cấp phải xác định lớp phủ chống tháo dỡ cứng, đục hoặc vỏ bọc vững chắc được sử dụng. Tài liệu phải mô tả cách lớp phủ hoặc vỏ bọc vững chắc có các đặc tính hòa tan sao cho việc hòa tan lớp phủ hoặc vỏ bọc vững chắc đó sẽ có xác suất cao làm hòa tan hoặc gây ra hư hỏng nghiêm trọng cho mô-đun (tức là mô-đun sẽ không hoạt động và bị hư hỏng không thể sửa chữa).
Quy trình kiểm thử bắt buộc	
TE07.43.01	Kiểm thử viên phải xác minh bằng việc kiểm tra và từ tài liệu do nhà cung cấp cung cấp rằng mô-đun được bao phủ bằng một lớp phủ chống tháo dỡ cứng, đục hoặc một vỏ bọc vững chắc.
TE07.43.02	Kiểm thử viên phải xác minh bằng kiểm tra thực tế rằng lớp phủ chống tháo dỡ hoặc vỏ bọc vững chắc hoặc là: a) có khả năng chống lại các hóa chất thông thường mà người ta có thể kỳ vọng một cách hợp lý là sẽ tấn công cấu trúc của lớp phủ hoặc vỏ bọc; hoặc b) bị hư hỏng nghiêm trọng do sự tấn công của hóa chất (tức là mô-đun sẽ không hoạt động và bị hư hỏng không thể sửa chữa).

Bảng 226 - VE và TE của AS07.44

Yêu cầu an toàn vật lý đối với từng hình thái an toàn vật lý - mức 4	
AS07.44 ISO/IEC 19790:2025, 7.7.3.2	Khi vỏ bọc phát hiện can thiệp được sử dụng, mô-đun mật mã phải có khả năng phản hồi can thiệp và xóa trắng để liên tục giám sát vỏ bọc phát hiện can thiệp.
Quy trình kiểm thử bắt buộc	

Khẳng định này được kiểm thử như một phần của AS07.45.

Bảng 227 - VE và TE của AS07.45

Yêu cầu an toàn vật lý đối với từng hình thái an toàn vật lý - mức 4	
AS07.45 ISO/IEC 19790:2025, 7.7.3.2	Khi vỏ bọc phát hiện can thiệp được sử dụng, mô-đun mật mã khi phát hiện có sự can thiệp, phải xóa trắng ngay lập tức tất cả các CSP dạng rõ, các PSP dạng rõ và các thành phần khóa dạng rõ.
Thông tin bắt buộc từ nhà cung cấp	
VE07.45.01	Tài liệu của nhà cung cấp phải mô tả nếu có bất kỳ vỏ bọc phát hiện can thiệp nào được sử dụng. Nếu được sử dụng, tài liệu đó sau đó phải mô tả: a) cách thức nó phát hiện sự can thiệp bằng các phương pháp như cắt, khoan, phay, mài, đốt cháy, làm nóng chảy, hoặc hòa tan vỏ bọc của mô-đun tới một mức độ đủ để cho phép truy cập hoặc sửa đổi các SSP, hoặc sẽ dẫn đến việc sử dụng hoặc sửa đổi trái phép mô-đun; b) cách khả năng phản hồi can thiệp và xóa trắng liên tục giám sát vỏ bọc phát hiện can thiệp; và c) cách mô-đun mật mã khi phát hiện có sự can thiệp, xóa trắng ngay lập tức tất cả các CSP dạng rõ, các PSP dạng rõ và các thành phần khóa dạng rõ.
Quy trình kiểm thử bắt buộc	
TE07.45.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và xác minh rằng tài liệu đó có mô tả nếu bất kỳ vỏ bọc phát hiện can thiệp nào được sử dụng. Nếu được sử dụng, kiểm thử viên phải xem xét và xác nhận rằng tài liệu có mô tả: a) cách thức nó phát hiện sự can thiệp bằng các phương pháp như cắt, khoan, phay, mài, đốt cháy, làm nóng chảy, hoặc hòa tan vỏ bọc của mô-đun tới một mức độ đủ để cho phép truy cập hoặc sửa đổi các SSP, hoặc sẽ dẫn đến việc sử dụng hoặc sửa đổi trái phép mô-đun; b) cách khả năng phản hồi can thiệp và xóa trắng liên tục giám sát vỏ bọc phát hiện can thiệp; và c) cách mô-đun mật mã khi phát hiện có sự can thiệp, xóa trắng ngay lập tức tất cả các CSP dạng rõ, các PSP dạng rõ và các thành phần khóa dạng rõ.
TE07.45.02	Kiểm thử viên phải xem xét bằng việc kiểm tra thực tế để đảm bảo rằng việc triển khai mô-đun khớp với thiết kế vỏ bọc phát hiện can thiệp đã được lập tài liệu.
TE07.45.03	Đối với mỗi hướng tấn công (cắt, khoan, phay, mài, đốt cháy, làm nóng chảy, hoặc hòa tan vỏ bọc của mô-đun), kiểm thử viên phải tìm cách vô hiệu hóa thiết kế vỏ bọc phát hiện can thiệp của mô-đun và xác nhận rằng trong mỗi trường hợp: a) vỏ bọc phát hiện can thiệp có phát hiện được các nỗ lực truy cập hoặc gỡ bỏ vỏ bọc phát hiện can thiệp; và b) sau khi phát hiện có sự can thiệp, mô-đun sẽ xóa trắng ngay lập tức tất cả các CSP dạng rõ, các PSP dạng rõ và các thành phần khóa dạng rõ. CHÚ THÍCH: Có thể sử dụng một bài kiểm thử duy nhất để xác minh sự bảo vệ chống lại nhiều đường hướng tấn công ở nơi mà điều này có thể được chứng minh là hợp lý dựa trên thiết kế của vỏ bọc can thiệp VÍ DỤ: Trong một số thiết kế, một bài kiểm thử duy nhất tập trung vào các cuộc tấn công bằng phương pháp khoan có thể là đủ để kiểm tra luôn cả khả năng chống cắt và phay.

TE07.45.04	Kiểm thử viên phải xem xét việc triển khai các cơ chế phát hiện can thiệp để xác nhận rằng chúng cung cấp khả năng giám sát liên tục vỏ bọc phát hiện can thiệp đủ để phát hiện mọi hành vi truy cập hoặc sửa đổi các SSP, vốn sẽ dẫn đến việc sử dụng hoặc sửa đổi trái phép mô-đun. Trong thực tế, một mô-đun có thể định kỳ thăm dò các cảm biến được sử dụng để phát hiện sự can thiệp. Trong trường hợp tính năng này được triển khai, bài kiểm thử phải xác nhận rằng điều này được thực hiện với tần suất đủ dày đặc nhằm tránh việc kẻ tấn công có khả năng phá vỡ vỏ bọc phát hiện can thiệp và vô hiệu hóa các cơ chế phản hồi can thiệp trước khi các CSP dạng rõ, các PSP dạng rõ và các thành phần khóa dạng rõ bị truy cập.

6.7.4 Bảo vệ chống/Thử nghiệm sự cố môi trường

6.7.4.1 Mức an toàn 3

CHÚ THÍCH 1: Một mô-đun mật mã không bắt buộc phải sử dụng các tính năng bảo vệ chống sự cố môi trường hoặc trải qua thử nghiệm sự cố môi trường đối với mức an toàn 1 và 2.

Bảng 228 - VE và TE của AS07.46

Bảo vệ chống/thử nghiệm sự cố môi trường - mức 3	
AS07.46 ISO/IEC 19790:2025, 7.7.4.3	Mô-đun hoặc phải sử dụng các tính năng EFP hoặc phải trải qua quá trình EFT.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.48, AS07.49, AS07.50, AS07.51, AS07.52, AS07.53, AS07.54, AS07.56, AS07.57, AS07.58, AS07.59 và AS07.60.	

6.7.4.2 Mức an toàn 4

Bảng 229 - VE và TE của AS07.47

Bảo vệ chống/thử nghiệm sự cố môi trường - mức 4	
AS07.47 ISO/IEC 19790:2025, 7.7.4.4	Mô-đun phải sử dụng các tính năng EFP.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.48, AS07.49 và AS07.50.	

6.7.5 Các tính năng bảo vệ chống sự cố môi trường

Bảng 230 - VE và TE của AS07.48

Các tính năng bảo vệ chống sự cố môi trường - mức 3 và 4	
AS07.48 ISO/IEC 19790:2025, 7.7.5	Các tính năng EFP phải bảo vệ mô-đun mật mã chống lại các điều kiện môi trường bất thường (vô tình hoặc do chủ đích gây ra) khi nằm ngoài dải hoạt động bình thường của mô-đun, vốn có thể làm tổn hại đến tính an toàn của mô-đun mật mã.

Quy trình kiểm thử bắt buộc

Khẳng định này được kiểm thử như một phần của AS07.50.

Bảng 231 - VE và TE của AS07.49

Các tính năng bảo vệ chống sự cố môi trường - mức 3 và 4	
AS07.49 ISO/IEC 19790:2025, 7.7.5	Mô-đun mật mã phải theo dõi và phản hồi chính xác khi nhiệt độ và điện áp hoạt động nằm ngoài các dải hoạt động bình thường đã được quy định.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.50.	

Bảng 232 - VE và TE của AS07.50

Các tính năng bảo vệ chống sự cố môi trường - mức 3 và 4	
AS07.50 ISO/IEC 19790:2025, 7.7.5	Nếu nhiệt độ hoặc điện áp rơi ra ngoài dải hoạt động bình thường của mô-đun mật mã, khả năng bảo vệ hoặc phải: a) tắt mô-đun để ngăn chặn các hoạt động tiếp theo; hoặc b) ngay lập tức xóa trắng tất cả các CSP dạng rõ, các PSP dạng rõ và các thành phần khóa dạng rõ.
Thông tin bắt buộc từ nhà cung cấp	
VE07.50.01	Nếu EFP được chọn cho một điều kiện cụ thể, mô-đun phải theo dõi và phản hồi chính xác với các biến động về nhiệt độ hoặc điện áp hoạt động nằm ngoài dải hoạt động bình thường của mô-đun đối với điều kiện đó. Các tính năng bảo vệ phải liên tục đo lường các điều kiện môi trường này. Nếu xác định một điều kiện nằm ngoài dải hoạt động bình thường của mô-đun, mạch bảo vệ hoặc phải: a) tắt mô-đun, hoặc b) xóa trắng tất cả các CSP dạng rõ, PSP dạng rõ và các thành phần khóa dạng rõ. Tài liệu phải tuyên bố cách tiếp cận nào trong số này đã được chọn và cung cấp mô tả đặc tả về các tính năng EFP được triển khai bên trong mô-đun.
VE07.50.02	Chính sách an toàn phải đề cập đến việc liệu tính năng EFP được sử dụng sẽ buộc mô-đun tắt máy hay xóa trắng tất cả các CSP dạng rõ, PSP dạng rõ và các thành phần khóa dạng rõ, đồng thời phải quy định dải nhiệt độ được đáp ứng.
Quy trình kiểm thử bắt buộc	
TE07.50.01	Kiểm thử viên phải cấu hình điều kiện môi trường (nhiệt độ môi trường xung quanh và điện áp) gần với mức cực hạn thích hợp của dải hoạt động bình thường được quy định cho mô-đun và xác minh rằng mô-đun tiếp tục hoạt động theo các tham số hoạt động bình thường.
TE07.50.02	Kiểm thử viên phải mở rộng nhiệt độ và điện áp ra ngoài dải bình thường đã được quy định và xác minh rằng mô-đun hoặc tự tắt để ngăn chặn các hoạt động tiếp theo, hoặc xóa trắng tất cả các CSP dạng rõ, PSP dạng rõ và các thành phần khóa dạng rõ.
TE07.50.03	Nếu mô-đun được thiết kế để xóa trắng tất cả các CSP dạng rõ, PSP dạng rõ và thành phần khóa dạng rõ, và mô-đun vẫn còn hoạt động sau khi trở về dải môi trường bình thường, kiểm thử viên phải thực hiện các dịch vụ yêu cầu sử dụng các CSP, PSP dạng rõ và các thành phần khóa dạng rõ và xác minh rằng mô-đun không thực hiện các dịch vụ này.

TE07.50.04	Kiểm thử viên phải xác minh rằng chính sách an toàn quy định dải điện áp và nhiệt độ hoạt động bình thường. Kiểm thử viên cũng phải xác minh liệu mô-đun tự tắt hay xóa trắng tất cả các CSP dạng rõ, PSP dạng rõ và thành phần khóa dạng rõ nếu điện áp hoặc nhiệt độ hoạt động rơi ra ngoài dải hoạt động bình thường của mô-đun.
------------	---

6.7.6 Các thủ tục thử nghiệm sự cố môi trường

Bảng 233 - VE và TE của AS07.51

Các thủ tục thử nghiệm sự cố môi trường - mức 3	
AS07.51 ISO/IEC 19790:2025, 7.7.6	EFT phải bao gồm sự kết hợp giữa phân tích, mô phỏng và thử nghiệm một mô-đun mật mã để cung cấp sự đảm bảo hợp lý rằng các điều kiện môi trường (vô tình hoặc do chủ đích gây ra) khi nằm ngoài các dải hoạt động bình thường của mô-đun về nhiệt độ và điện áp sẽ không làm tổn hại đến tính an toàn của mô-đun mật mã.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.54.	

Bảng 234 - VE và TE của AS07.52

Các thủ tục thử nghiệm sự cố môi trường – mức 3	
AS07.52 ISO/IEC 19790:2025, 7.7.6	EFT phải chứng minh rằng, nếu điện áp hoặc nhiệt độ hoạt động rơi ra ngoài dải hoạt động bình thường của mô-đun dẫn đến một lỗi, {tính an toàn của mô-đun mật mã không được bị phương hại tại bất kỳ thời điểm nào.}
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.54.	

Bảng 235 - VE và TE của AS07.53

Các thủ tục thử nghiệm sự cố môi trường – mức 3	
AS07.53 ISO/IEC 19790:2025, 7.7.6	{EFT phải chứng minh rằng, nếu điện áp hoặc nhiệt độ hoạt động rơi ra ngoài dải hoạt động bình thường của mô-đun dẫn đến một lỗi,} tính an toàn của mô-đun mật mã không được bị phương hại tại bất kỳ thời điểm nào.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.54.	

Bảng 236 - VE và TE của AS07.54

Các thủ tục thử nghiệm sự cố môi trường – mức 3	
AS07.54 ISO/IEC 19790:2025, 7.7.6	Dải nhiệt độ cần thử nghiệm phải bắt đầu từ một nhiệt độ nằm trong dải nhiệt độ hoạt động bình thường đến nhiệt độ thấp nhất (tức là lạnh nhất) nằm ngoài dải hoạt động bình thường mà dẫn đến việc mô-đun gặp lỗi hoặc bước vào trạng thái lỗi.
Thông tin bắt buộc từ nhà cung cấp	
VE07.54.01	Nếu EFT được chọn cho một điều kiện cụ thể, mô-đun phải được thử nghiệm trong dải nhiệt độ quy định tại AS07.54 và các dải điện áp quy định tại AS07.59 và AS07.60. Mô-đun hoặc phải: a) tiếp tục hoạt động bình thường, hoặc b) gặp lỗi và tắt máy, hoặc c) bước vào trạng thái lỗi.

	Tài liệu phải tuyên bố cách tiếp cận nào trong sổ này đã được chọn và cung cấp một mô tả đặc tả về EFT.
VE07.54.02	Chính sách an toàn phải đề cập đến việc liệu tính năng EFT được sử dụng sẽ khiến mô-đun tiếp tục hoạt động bình thường, gặp lỗi hay bước vào trạng thái lỗi, đồng thời phải quy định dải nhiệt độ được đáp ứng.
Quy trình kiểm thử bắt buộc	
TE07.54.01	Kiểm thử viên phải cấu hình điều kiện môi trường (tức là điện áp và nhiệt độ môi trường xung quanh) như quy định trong AS07.54, AS07.59, và AS07.60 và xác minh rằng mô-đun hoặc tiếp tục hoạt động bình thường, hoặc tự tắt để ngăn chặn các hoạt động tiếp theo, hoặc bước vào trạng thái lỗi.
TE07.54.02	Nếu mô-đun được thiết kế để bước vào trạng thái lỗi, và mô-đun vẫn còn hoạt động sau khi trở về dải môi trường bình thường, kiểm thử viên phải xác minh rằng mô-đun đang ở trong trạng thái lỗi.
TE07.54.03	Kiểm thử viên phải xác minh rằng chính sách an toàn phi độc quyền có quy định dải nhiệt độ và điện áp hoạt động bình thường, và liệu mô-đun tự tắt hoặc bước vào trạng thái lỗi nếu nhiệt độ hoặc điện áp hoạt động rơi ra ngoài dải hoạt động bình thường của mô-đun hay không.

Bảng 237 - VE và TE của AS07.55

Các thủ tục thử nghiệm sự cố môi trường – mức 3	
AS07.55 ISO/IEC 19790:2025, 7.7.6	Dải nhiệt độ cũng phải bắt đầu từ một nhiệt độ nằm trong dải nhiệt độ hoạt động bình thường đến nhiệt độ cao nhất (tức là nóng nhất) nằm ngoài dải hoạt động bình thường mà dẫn đến việc mô-đun gặp lỗi hoặc bước vào trạng thái lỗi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.54.	

Bảng 238 - VE và TE của AS07.56

Các thủ tục thử nghiệm sự cố môi trường - mức 3	
AS07.56 ISO/IEC 19790: 2025, 7.7.6	Dải nhiệt độ cần thử nghiệm phải từ 100 °C đến 200 °C; tuy nhiên, {bài thử nghiệm phải bị gián đoạn ngay khi mô-đun gặp lỗi hoặc mô-đun bước vào trạng thái lỗi.}
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.54.	

Bảng 239 - VE và TE của AS07.57

Các thủ tục thử nghiệm sự cố môi trường – mức 3	
AS07.57 ISO/IEC 19790:2025, 7.7.6	{Dải nhiệt độ cần thử nghiệm phải từ 100 °C đến 200 °C;} tuy nhiên, bài thử nghiệm phải bị gián đoạn ngay khi mô-đun gặp lỗi hoặc mô-đun bước vào trạng thái lỗi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.54.	

Bảng 240 - VE và TE của AS07.58

Các thủ tục thử nghiệm sự cố môi trường - mức 3	
AS07.58 ISO/IEC	Nhiệt độ phải được theo dõi nội bộ tại các thành phần nhạy cảm và các thiết bị trọng yếu, chứ không chỉ theo dõi ở biên mật mã của mô-đun.

19790:2025, 7.7.6	
Thông tin bắt buộc từ nhà cung cấp	
VE07.58.01	Nhà cung cấp phải lập tài liệu về các thành phần nhạy cảm và các thiết bị trọng yếu liên quan đến AS07.58.
Quy trình kiểm thử bắt buộc	
TE07.58.01	Kiểm thử viên phải lập tài liệu về cách thức nhiệt độ được theo dõi khi thực hiện thử nghiệm EFT nhằm đảm bảo rằng dải nhiệt độ được ghi nhận trong bài kiểm thử tương ứng với nhiệt độ đo được bên trong các thiết bị trọng yếu và thành phần nhạy cảm do nhà cung cấp xác định, chứ không chỉ ở biên mật mã của mô-đun.

Bảng 241 - VE và TE của AS07.59

Các thủ tục thử nghiệm sự cố môi trường - mức 3	
AS07.59 ISO/IEC 19790:2025, 7.7.6	Dải điện áp được thử nghiệm phải được giảm dần từ một điện áp nằm trong dải điện áp hoạt động bình thường xuống một điện áp thấp hơn nằm ngoài dải điện áp bình thường mà dẫn đến việc mô-đun gặp lỗi hoặc bước vào trạng thái lỗi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.54.	

Bảng 242 - VE và TE của AS07.60

Các thủ tục thử nghiệm sự cố môi trường - mức 3	
AS07.60 ISO/IEC 19790:2025, 7.7.6	Dải điện áp được thử nghiệm cũng phải được tăng dần từ một điện áp nằm trong dải điện áp hoạt động bình thường lên một điện áp cao hơn nằm ngoài dải điện áp bình thường mà dẫn đến việc mô-đun gặp lỗi hoặc bước vào trạng thái lỗi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS07.54.	

6.8 An toàn không xâm lấn

6.8.1 Yêu cầu chung về an toàn không xâm lấn

Bảng 243 - VE và TE của AS08.01

Yêu cầu chung về an toàn không xâm lấn - mức 1, 2, 3 và 4	
AS08.01 ISO/IEC 19790:2025, 7.8.1	Các kỹ thuật giảm thiểu tấn công không xâm lấn được triển khai bởi mô-đun mật mã để bảo vệ các SSP của mô-đun mà không được tham chiếu trong ISO/IEC 19790:2025, Phụ lục F phải đáp ứng các yêu cầu trong ISO/IEC 19790:2025, 7.12.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS12.01, AS12.02, AS12.03 và AS12.04.	

Bảng 244 - VE và TE của AS08.02

Yêu cầu chung về an toàn không xâm lấn - mức 1, 2, 3 và 4	
AS08.02 ISO/IEC 19790:2025, 7.8.1	Tài liệu về an toàn không xâm lấn được quy định trong ISO/IEC 19790:2025, A.2.7 phải được cung cấp.
Thông tin bắt buộc từ nhà cung cấp	
VE08.02.01	Nhà cung cấp phải cung cấp các yêu cầu về tài liệu như được quy định trong ISO/IEC 19790:2025, A.2.7.

Quy trình kiểm thử bắt buộc	
TE08.02.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu như quy định trong ISO/IEC 19790: 2025, A.2.7.

6.8.2 Mức an toàn 1 và 2

Bảng 245 - VE và TE của AS08.03

Mức an toàn 1 và 2 - mức 1, 2, 3 và 4	
AS08.03 ISO/IEC 19790:2025, 7.8.2	Đối với mức an toàn 1 và 2, tài liệu phải quy định tất cả các kỹ thuật giảm thiểu được sử dụng để bảo vệ các SSP của mô-đun khỏi các cuộc tấn công không xâm lấn được tham chiếu trong ISO/IEC 19790:2025, Phụ lục F.
Thông tin bắt buộc từ nhà cung cấp	
VE08.03.01	Nhà cung cấp phải cung cấp tài liệu hỗ trợ quy định tất cả các kỹ thuật giảm thiểu được sử dụng để bảo vệ các SSP của mô-đun khỏi các cuộc tấn công không xâm lấn được quy định trong ISO/IEC 19790:2025, Phụ lục F.
Quy trình kiểm thử bắt buộc	
TE08.03.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu hỗ trợ quy định tất cả các kỹ thuật giảm thiểu được sử dụng để bảo vệ các SSP của mô-đun khỏi các cuộc tấn công không xâm lấn được quy định trong ISO/IEC 19790:2025, Phụ lục F.

Bảng 246 - VE và TE của AS08.04

Mức an toàn 1 và 2 - mức 1, 2, 3 và 4	
AS08.04 ISO/IEC 19790:2025, 7.8.2	Tài liệu phải bao gồm bằng chứng về tính hiệu quả của từng kỹ thuật giảm thiểu tấn công.
Thông tin bắt buộc từ nhà cung cấp	
VE08.04.01	Nhà cung cấp phải quy định trong tài liệu về tính hiệu quả của các kỹ thuật giảm thiểu.
Quy trình kiểm thử bắt buộc	
TE08.04.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu quy định tính hiệu quả của các kỹ thuật giảm thiểu.

6.8.3 Mức an toàn 3

Bảng 247 - VE và TE của AS08.05

Mức an toàn 3 - mức 3	
AS08.05 ISO/IEC 19790:2025, 7.8.3	Ngoài các yêu cầu đối với mức an toàn 1 và 2, mô-đun mật mã phải được kiểm thử để đáp ứng các số liệu kiểm thử giảm thiểu tấn công không xâm lấn đã phê duyệt đối với mức an toàn 3 như được tham chiếu trong ISO/IEC 19790:2025, Phụ lục F.
Thông tin bắt buộc từ nhà cung cấp	
VE08.05.01	Nhà cung cấp phải cung cấp tài liệu chứng minh rằng mô-đun đáp ứng các số liệu kiểm thử giảm thiểu tấn công không xâm lấn đã phê duyệt đối với mức an toàn 3.
Quy trình kiểm thử bắt buộc	
TE08.05.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu chứng minh rằng mô-đun đáp ứng các số liệu kiểm thử giảm thiểu tấn công không xâm lấn đã phê duyệt đối với mức an toàn 3.
TE08.05.02	Mô-đun phải được kiểm thử theo bất kỳ quy trình kiểm thử nào được quy định trong ISO/IEC 20085-1 và ISO/IEC 20085-2.

6.8.4 Mức an toàn 4

Bảng 248 - VE và TE của AS08.06

Mức an toàn 4 - mức 4	
AS08.06 ISO/IEC 19790:2025, 7.8.4	Ngoài các yêu cầu đối với mức an toàn 1 và 2, mô-đun mật mã phải được kiểm thử để đáp ứng các số liệu kiểm thử giảm thiểu tấn công không xâm lấn đã phê duyệt đối với mức an toàn 4 như được tham chiếu trong ISO/IEC 19790:2025, Phụ lục F.
Thông tin bắt buộc từ nhà cung cấp	
VE08.06.01	Nhà cung cấp phải cung cấp tài liệu chứng minh rằng mô-đun đáp ứng các số liệu kiểm thử giảm thiểu tấn công không xâm lấn đã phê duyệt đối với mức an toàn 4.
Quy trình kiểm thử bắt buộc	
TE08.06.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu chứng minh rằng mô-đun đáp ứng các số liệu kiểm thử giảm thiểu tấn công không xâm lấn đã phê duyệt đối với mức an toàn 4.
TE08.06.02	Mô-đun phải được kiểm thử theo bất kỳ thủ tục kiểm thử nào được quy định trong ISO/IEC 20085-1 và ISO/IEC 20085-2.

6.9 Quản lý tham số an toàn nhạy cảm

6.9.1 Yêu cầu chung về quản lý tham số an toàn nhạy cảm

Bảng 249 - VE và TE của AS09.01

Yêu cầu chung về quản lý tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.01 ISO/IEC 19790:2025, 7.9.1	Các CSP phải được bảo vệ bên trong mô-đun nhằm chống lại việc truy cập, sử dụng, tiết lộ, sửa đổi, và thay thế trái phép.
Thông tin bắt buộc từ nhà cung cấp	
VE09.01.01	Tài liệu do nhà cung cấp cung cấp phải mô tả việc bảo vệ tất cả các CSP bên trong mô-đun. Việc bảo vệ phải bao gồm việc triển khai các cơ chế nhằm bảo vệ chống lại việc truy cập, sử dụng, tiết lộ, sửa đổi, và thay thế trái phép.
Quy trình kiểm thử bắt buộc	
TE09.01.01	Kiểm thử viên phải kiểm tra tài liệu do nhà cung cấp cung cấp mô tả việc bảo vệ các CSP. Kiểm thử viên phải xác minh rằng tài liệu có mô tả cách thức những CSP này được bảo vệ nhằm chống lại việc truy cập, sử dụng, tiết lộ, sửa đổi, và thay thế trái phép.
TE09.01.02	Kiểm thử viên phải nỗ lực truy cập (bằng cách vượt qua các cơ chế bảo vệ đã được lập tài liệu) vào các CSP mà kiểm thử viên không có thẩm quyền truy cập. Để đáp ứng khẳng định này, mô-đun bắt buộc phải từ chối truy cập.
TE09.01.03	Kiểm thử viên phải nỗ lực sửa đổi các CSP bằng bất kỳ phương pháp nào không được quy định bởi tài liệu do nhà cung cấp cung cấp. CHÚ THÍCH Các CSP được mã hóa bằng một thuật toán không được phê duyệt hoặc thuật toán hay phương pháp độc quyền được coi là ở dạng không được bảo vệ trong phạm vi của tiêu chuẩn này.

Bảng 250 - VE và TE của AS09.02

Yêu cầu chung về quản lý tham số an toàn nhạy cảm - mức 1, 2, 3 và 4
--

AS09.02 ISO/IEC 19790:2025, 7.9.1	Các PSP phải được bảo vệ bên trong mô-đun nhằm chống lại việc sửa đổi và thay thế trái phép.
Thông tin bắt buộc từ nhà cung cấp	
VE09.02.01	Tài liệu do nhà cung cấp cung cấp phải mô tả việc bảo vệ tất cả các PSP nhằm chống lại việc sửa đổi và thay thế trái phép.
Quy trình kiểm thử bắt buộc	
TE09.02.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có mô tả cách các PSP được bảo vệ nhằm chống lại việc sửa đổi và thay thế trái phép.
TE09.02.02	Kiểm thử viên phải tìm cách sửa đổi tất cả các PSP bằng bất kỳ phương pháp nào không được quy định bởi tài liệu do nhà cung cấp cung cấp và phải thử nhập chúng vào mô-đun.

Bảng 251 - VE và TE của AS09.03

Yêu cầu chung về quản lý tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.03 ISO/IEC 19790:2025, 7.9.1	Một mô-đun phải liên kết một SSP được tạo ra, được nhập vào, hoặc được xuất ra từ mô-đun với thực thể (tức là người, nhóm, vai trò, hoặc quá trình) mà SSP đó được gán cho.
Thông tin bắt buộc từ nhà cung cấp	
VE09.03.01	Các thủ tục liên quan đến SSP đã được lập tài liệu phải mô tả các cơ chế hoặc thủ tục được sử dụng để đảm bảo rằng mỗi SSP được liên kết với đúng thực thể.
Quy trình kiểm thử bắt buộc	
TE09.03.01	Kiểm thử viên phải xác minh rằng các thủ tục nhập/xuất SSP đã được lập tài liệu có đề cập đến cách một SSP được nhập vào hoặc xuất ra được liên kết với đúng thực thể.
TE09.03.02	Đối với mỗi SSP có thể được nhập vào, đầu tiên kiểm thử viên phải nhập SSP đó trong khi đảm nhận đúng thực thể. Kiểm thử viên sau đó phải xác minh rằng việc nhập là không thể khi đảm nhận một thực thể không chính xác.
TE09.03.03	Đối với mỗi SSP có thể được xuất ra, đầu tiên kiểm thử viên phải xuất SSP đó trong khi đảm nhận đúng thực thể. Kiểm thử viên sau đó phải xác minh rằng việc xuất là không thể khi đảm nhận một thực thể không chính xác.

Bảng 252 - VE và TE của AS09.04

Yêu cầu chung về quản lý tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.04 ISO/IEC 19790:2025, 7.9.1	Dữ liệu xác thực, dữ liệu của bộ kiểm chứng vốn không phải là các PSP, thông tin trạng thái của RBG, và các giá trị tạo khóa trung gian phải được coi là các CSP.
Thông tin bắt buộc từ nhà cung cấp	
VE09.04.01	Nhà cung cấp phải cung cấp tài liệu xác nhận rằng dữ liệu xác thực và dữ liệu của bộ kiểm chứng, vốn không phải là các PSP, thông tin trạng thái của RBG, và các giá trị tạo khóa trung gian được định nghĩa là các CSP.
Quy trình kiểm thử bắt buộc	
TE09.04.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu rằng dữ liệu xác thực và dữ liệu của bộ kiểm chứng vốn không phải là các PSP, thông tin trạng thái của RBG, và các giá trị tạo khóa trung gian được định nghĩa là các CSP.

TE09.04.02	Kiểm thử viên phải xác minh rằng chính sách an toàn do nhà cung cấp cung cấp có định nghĩa bất kỳ dữ liệu xác thực và dữ liệu của bộ kiểm chứng nào vốn không phải là các PSP, thông tin trạng thái của RBG, và các giá trị tạo khóa trung gian là các CSP.
------------	---

Bảng 253 - VE và TE của AS09.05

Yêu cầu chung về quản lý tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.05 ISO/IEC 19790:2025, 7.9.1	Các giá trị băm của mật khẩu phải được coi là các CSP trừ khi chúng được tạo ra bằng một phương pháp bảo vệ mật khẩu đã phê duyệt (ví dụ: salt và băm) như được quy định trong ISO/IEC 19790:2025, Phụ lục E, trong trường hợp đó {các giá trị băm của mật khẩu phải được coi là các PSP.}
Thông tin bắt buộc từ nhà cung cấp	
VE09.05.01	Nhà cung cấp phải cung cấp tài liệu chứng minh rằng các giá trị băm của mật khẩu vốn không được tạo ra bằng một phương pháp bảo vệ mật khẩu đã phê duyệt (ví dụ: salt và băm) như được quy định trong ISO/IEC 19790:2025, Phụ lục E, được định nghĩa là các CSP.
Quy trình kiểm thử bắt buộc	
TE09.05.01	Kiểm thử viên phải xác minh rằng nhà cung cấp đã cung cấp tài liệu xác nhận rằng bất kỳ giá trị băm nào của mật khẩu đều được định nghĩa là CSP.
TE09.05.02	Kiểm thử viên phải xác minh rằng chính sách an toàn do nhà cung cấp cung cấp có định nghĩa bất kỳ giá trị băm nào của mật khẩu là các CSP.

Bảng 254 - VE và TE của AS09.06

Yêu cầu chung về quản lý tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.06 ISO/IEC 19790:2025, 7.9.1	{Các giá trị băm của mật khẩu phải được coi là các CSP trừ khi chúng được tạo ra bằng một phương pháp bảo vệ mật khẩu đã phê duyệt (ví dụ: salt và băm) như được quy định trong ISO/IEC 19790:2025, Phụ lục E,} trong trường hợp đó các giá trị băm của mật khẩu phải được coi là các PSP.
Thông tin bắt buộc từ nhà cung cấp	
VE09.06.01	Nhà cung cấp phải cung cấp tài liệu chứng minh rằng các giá trị băm của mật khẩu vốn được tạo ra bằng một phương pháp bảo vệ mật khẩu đã phê duyệt (ví dụ: salt và băm) như được quy định trong ISO/IEC 19790:2025, Phụ lục E, được định nghĩa là các PSP.
Quy trình kiểm thử bắt buộc	
TE09.06.01	Kiểm thử viên phải xác minh rằng nhà cung cấp đã cung cấp tài liệu xác nhận rằng bất kỳ giá trị băm nào của mật khẩu đều được định nghĩa là PSP.
TE09.06.02	Kiểm thử viên phải xác minh rằng chính sách an toàn do nhà cung cấp cung cấp có định nghĩa bất kỳ giá trị băm nào của mật khẩu là các PSP.

Bảng 255 - VE và TE của AS09.07

Yêu cầu chung về quản lý tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.07 ISO/IEC 19790:2025, 7.9.1	Khi một hàm băm được sử dụng trên mật khẩu/Mã PIN (PINs), cho dù nó được sử dụng độc lập hay như một phần của phương pháp bảo vệ mật khẩu đã phê duyệt theo ISO/IEC 19790:2025, Phụ lục E, thì một thuật toán băm đã phê duyệt như được liệt kê trong ISO/IEC 19790:2025, Phụ lục C phải được sử dụng.
Thông tin bắt buộc từ nhà cung cấp	

VE09.07.01	Tài liệu do nhà cung cấp cung cấp phải mô tả thuật toán băm đã phê duyệt được sử dụng để tạo ra các giá trị băm của mật khẩu/Mã PIN.
VE09.07.02	Nhà cung cấp phải cung cấp một chứng chỉ xác nhận nếu có sẵn như được quy định trong VE02.18.01, hoặc cam kết của nhà cung cấp như được quy định trong VE02.18.03.
Quy trình kiểm thử bắt buộc	
TE09.07.01	Kiểm thử viên phải xác minh bằng cách kiểm tra mô-đun mật mã rằng một thuật toán băm đã phê duyệt được sử dụng để tạo ra các giá trị băm của mật khẩu/Mã PIN.
TE09.07.02	Kiểm thử viên phải xác minh rằng nhà cung cấp đã cung cấp một chứng chỉ xác nhận nếu có sẵn đối với thuật toán băm đã phê duyệt được triển khai như quy định trong VE02.18.01, hoặc cam kết của nhà cung cấp như quy định trong VE02.18.03.

Bảng 256 - VE và TE của AS09.08

Yêu cầu chung về quản lý tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.08 ISO/IEC 19790:2025, 7.9.1	Tài liệu về quản lý tham số an toàn nhạy cảm được quy định trong ISO/IEC 19790:2025, A.2.8 phải được cung cấp.
Thông tin bắt buộc từ nhà cung cấp	
VE09.08.01	Nhà cung cấp phải cung cấp các yêu cầu về tài liệu như được quy định trong ISO/IEC 19790:2025, A.2.8.
Quy trình kiểm thử bắt buộc	
TE09.08.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu như quy định trong ISO/IEC 19790:2025, A.2.8.

6.9.2 Các bộ tạo bit ngẫu nhiên

CHÚ THÍCH: Một mô-đun mật mã có thể chứa các bộ tạo bit ngẫu nhiên (RBG), một chuỗi các bộ tạo bit ngẫu nhiên, hoặc có thể chỉ đơn thuần là một bộ tạo bit ngẫu nhiên.

Bảng 257 - VE và TE của AS09.09

Các bộ tạo bit ngẫu nhiên - mức 1, 2, 3 và 4	
AS09.09 ISO/IEC 19790:2025, 7.9.2	Nếu một chức năng an toàn đã phê duyệt yêu cầu các giá trị ngẫu nhiên, thì một RBG đã phê duyệt phải được sử dụng để cung cấp các giá trị này.
Thông tin bắt buộc từ nhà cung cấp	
VE09.09.01	Nhà cung cấp phải cung cấp danh sách tất cả các RBG được sử dụng trong các chức năng an toàn đã phê duyệt bên trong mô-đun mật mã cùng với mục đích sử dụng chính xác của chúng.
VE09.09.02	Nhà cung cấp phải cung cấp tài liệu chứng minh rằng bất kỳ giá trị ngẫu nhiên nào được sử dụng bởi các chức năng an toàn đã phê duyệt đều được cung cấp từ một RBG đã phê duyệt.
VE09.09.03	Nhà cung cấp phải cung cấp tài liệu chứng minh rằng tất cả các RBG được sử dụng trong các chức năng an toàn đã phê duyệt đều được kiểm thử theo phương pháp được quy định trong ISO/IEC 20543.
Quy trình kiểm thử bắt buộc	
TE09.09.01	Kiểm thử viên phải xác minh rằng tất cả các RBG được sử dụng bởi các chức năng an toàn đã phê duyệt đều được lập tài liệu và định nghĩa rõ mục đích sử dụng.

TE09.09.02	Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp rằng các RBG được triển khai dùng trong các chức năng an toàn đã phê duyệt là tuân thủ các RBG đã phê duyệt được liệt kê tại ISO/IEC 19790:2025, Phụ lục C.
TE09.09.03	Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp rằng mọi giá trị ngẫu nhiên được sử dụng bởi các chức năng an toàn đã phê duyệt đều được cung cấp từ một RBG đã phê duyệt.
TE09.09.04	Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp rằng tất cả các RBG được sử dụng trong các chức năng an toàn đã phê duyệt đều được kiểm thử theo phương pháp quy định trong ISO/IEC 20543.
CHÚ THÍCH Các RBG đã phê duyệt được liệt kê trong ISO/IEC 19790:2025, Phụ lục C.	

Bảng 258 - VE và TE của AS09.10

Các bộ tạo bit ngẫu nhiên - mức 1, 2, 3 và 4	
AS09.10 ISO/IEC 19790:2025, 7.9.2	Đầu vào entropy được sử dụng làm giá trị mầm cho một RBG đã phê duyệt phải được coi là một CSP.
Thông tin bắt buộc từ nhà cung cấp	
VE09.10.01	Nhà cung cấp phải cung cấp tài liệu chứng minh rằng đầu vào entropy được sử dụng giá trị mầm cho một RBG đã phê duyệt được định nghĩa là một CSP.
Quy trình kiểm thử bắt buộc	
TE09.10.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu chứng minh rằng đầu vào entropy được sử dụng giá trị mầm cho một RBG đã phê duyệt được định nghĩa là một CSP.

6.9.3 Tạo tham số an toàn nhạy cảm**Bảng 259 - VE và TE của AS09.11**

Tạo tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.11 ISO/IEC 19790:2025, 7.9.3	Việc làm tổn hại đến tính an toàn của phương pháp tạo SSP sử dụng đầu ra của một RBG đã phê duyệt (ví dụ: đoán giá trị mầm để khởi tạo bộ tạo bit ngẫu nhiên tất định) phải yêu cầu ít nhất số lượng phép toán bằng với số lượng phép toán cần thiết để xác định giá trị của SSP đã được tạo.
Thông tin bắt buộc từ nhà cung cấp	
VE09.11.01	Nhà cung cấp phải cung cấp tài liệu bao gồm lý do chứng minh làm thế nào việc phương hại đến tính an toàn của phương pháp tạo SSP (ví dụ: đoán giá trị mầm để khởi tạo RBG tất định) lại yêu cầu số lượng phép toán ít nhất bằng với số lượng phép toán cần thiết để xác định giá trị của SSP đã được tạo.
Quy trình kiểm thử bắt buộc	
TE09.11.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có bao gồm lý do chứng minh làm thế nào việc phương hại đến tính an toàn của phương pháp tạo SSP (ví dụ: đoán giá trị mầm để khởi tạo RBG tất định) lại yêu cầu số lượng phép toán ít nhất bằng với số lượng phép toán cần thiết để xác định giá trị của SSP đã được tạo.
TE09.11.02	Kiểm thử viên phải xác minh tính chính xác của bất kỳ lý do nào do nhà cung cấp đưa ra. Trách nhiệm chứng minh thuộc về nhà cung cấp; nếu có bất kỳ sự không chắc chắn hoặc mơ hồ nào, kiểm thử viên phải yêu cầu nhà cung cấp cung cấp thêm thông tin.

Bảng 260 - VE và TE của AS09.12

Tạo tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.12 ISO/IEC 19790:2025, 7.9.3	Các SSP được mô-đun tạo ra từ đầu ra của một RBG đã phê duyệt hoặc bắt nguồn từ một SSP được nhập vào mô-đun và được sử dụng bởi một chức năng an toàn đã phê duyệt phải được tạo bằng cách sử dụng các phương pháp tạo tham số an toàn nhạy cảm đã phê duyệt liệt kê trong ISO/IEC 19790:2025, Phụ lục D.
Thông tin bắt buộc từ nhà cung cấp	
VE09.12.01	Nhà cung cấp phải cung cấp danh sách tất cả các SSP được mô-đun tạo ra, được sử dụng trong mô-đun mật mã và mục đích sử dụng chính xác của chúng. Những SSP này được tạo ra từ đầu ra của một RBG đã phê duyệt hoặc bắt nguồn từ một SSP được nhập vào mô-đun và được sử dụng bởi một chức năng an toàn đã phê duyệt.
VE09.12.02	Nhà cung cấp phải cung cấp tài liệu chứng minh rằng các SSP do mô-đun tạo ra được tạo bằng phương pháp tạo SSP đã phê duyệt. Những SSP này được tạo ra từ đầu ra của một RBG đã phê duyệt hoặc bắt nguồn từ một SSP được nhập vào mô-đun và được sử dụng bởi một chức năng an toàn đã phê duyệt.
Quy trình kiểm thử bắt buộc	
TE09.12.01	Kiểm thử viên phải xác minh rằng tất cả các SSP được mô-đun tạo ra đều được lập tài liệu và được định nghĩa mục đích sử dụng. Những SSP này được tạo ra từ đầu ra của một RBG đã phê duyệt hoặc bắt nguồn từ một SSP được nhập vào mô-đun và được sử dụng bởi một chức năng an toàn đã phê duyệt.
TE09.12.02	Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp rằng các SSP được triển khai và tạo ra bởi mô-đun là tuân thủ các phương pháp tạo SSP đã phê duyệt liệt kê trong ISO/IEC 19790:2025, Phụ lục D. Những SSP này được tạo ra từ đầu ra của một RBG đã phê duyệt hoặc bắt nguồn từ một SSP được nhập vào mô-đun và được sử dụng bởi một chức năng an toàn đã phê duyệt.

6.9.4 Thiết lập tham số an toàn nhạy cảm tự động

CHÚ THÍCH Việc thiết lập tham số an toàn nhạy cảm tự động có thể bao gồm việc truyền tải SSP tự động hoặc các phương pháp thỏa thuận SSP.

Bảng 261 - VE và TE của AS09.13

Thiết lập tham số an toàn nhạy cảm tự động - mức 1, 2, 3 và 4	
AS09.13 ISO/IEC 19790:2025, 7.9.4	Việc thiết lập SSP tự động phải sử dụng một phương pháp đã phê duyệt được liệt kê trong ISO/IEC 19790:2025, Phụ lục D.
Thông tin bắt buộc từ nhà cung cấp	
VE09.13.01	Nhà cung cấp phải cung cấp danh sách tất cả các phương pháp thiết lập SSP tự động được sử dụng trong mô-đun mật mã và mục đích sử dụng chính xác của chúng.
Quy trình kiểm thử bắt buộc	
TE09.13.01	Kiểm thử viên phải xác minh rằng tất cả các phương pháp thiết lập SSP tự động đều được lập tài liệu và mục đích sử dụng của chúng được xác định rõ.
TE09.13.02	Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp rằng các phương pháp thiết lập SSP tự động được triển khai là tuân thủ các phương pháp thiết lập SSP tự động đã phê duyệt được liệt kê trong ISO/IEC 19790:2025, Phụ lục D.

6.9.5 Nhập và xuất tham số an toàn nhạy cảm

6.9.5.1 Yêu cầu chung về nhập và xuất tham số an toàn nhạy cảm

Các tham số an toàn nhạy cảm có thể được nhập vào hoặc xuất ra thủ công khỏi một mô-đun một cách trực tiếp (ví dụ: nhập qua bàn phím hoặc bàn phím số, hoặc xuất qua màn hình hiển thị trực quan) hoặc bằng phương thức điện tử (ví dụ: thông qua thẻ thông minh/token, thẻ PC, thiết bị nạp khóa điện tử khác, hoặc môi trường hoạt động của mô-đun).

Bảng 262 - VE và TE của AS09.14

Nhập và xuất tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.14 ISO/IEC 19790:2025, 7.9.5.1	Nếu các SSP được nhập hoặc xuất thủ công khỏi một mô-đun, việc nhập hoặc xuất phải được thực hiện thông qua các giao diện mô-đun đã được định nghĩa.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS03.04, AS03.05, AS03.06, AS03.07, AS03.08, AS03.09, AS03.10, AS03.11, AS03.12, AS03.13 và AS03.14.	

Bảng 263 - VE và TE của AS09.15

Nhập và xuất tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.15 ISO/IEC 19790:2025, 7.9.5.1	Tất cả các SSP được bảo vệ bằng mật mã, được nhập vào hoặc xuất ra khỏi mô-đun phải được bảo vệ bằng cách sử dụng một chức năng an toàn đã phê duyệt, như quy định tại ISO/IEC 19790:2025, Phụ lục C.
Thông tin bắt buộc từ nhà cung cấp	
VE09.15.01	Tài liệu do nhà cung cấp cung cấp phải quy định tất cả các SSP được bảo vệ bằng mật mã vốn được nhập vào hoặc xuất ra khỏi mô-đun mật mã.
VE09.15.02	Tài liệu do nhà cung cấp cung cấp phải nêu rõ phương pháp được sử dụng để bảo vệ bằng mật mã các SSP vốn được nhập vào hoặc xuất ra khỏi mô-đun mật mã.
Quy trình kiểm thử bắt buộc	
TE09.15.01	Kiểm thử viên phải xác minh rằng nhà cung cấp đã cung cấp tài liệu quy định tất cả các SSP được bảo vệ bằng mật mã vốn được nhập vào và xuất ra khỏi mô-đun mật mã.
TE09.15.02	Kiểm thử viên phải xác minh rằng nhà cung cấp đã cung cấp tài liệu quy định phương pháp được sử dụng để bảo vệ bằng mật mã các SSP vốn được nhập vào hoặc xuất ra khỏi mô-đun mật mã.
TE09.15.03	Kiểm thử viên phải xác minh rằng phương pháp được sử dụng để bảo vệ bằng mật mã các SSP vốn được nhập vào hoặc xuất ra khỏi mô-đun mật mã được thực hiện bằng cách sử dụng một chức năng an toàn đã phê duyệt.

Bảng 264 - VE và TE của AS09.16

Nhập và xuất tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.16 ISO/IEC 19790:2025, 7.9.5.1	Nếu các SSP đã được mã hóa được nhập thủ công một cách trực tiếp vào mô-đun, thì các giá trị dạng rõ của các SSP đó không được hiển thị.
Thông tin bắt buộc từ nhà cung cấp	
VE09.16.01	Các cơ chế nhập SSP đã được lập tài liệu đối với các SSP được mã hóa phải ngăn chặn việc hiển thị các giá trị dạng rõ của chúng.

Quy trình kiểm thử bắt buộc	
TE09.16.01	Kiểm thử viên phải xác minh rằng các cơ chế nhập SSP đã được lập tài liệu đối với các SSP được mã hóa có tác dụng ngăn chặn việc hiển thị các giá trị dạng rõ của chúng trong suốt quá trình nhập SSP được mã hóa.
TE09.16.02	Kiểm thử viên phải nhập tất cả các SSP đã mã hóa và giám sát các giao diện đầu ra của mô-đun để xác minh rằng bất kỳ giá trị SSP dạng rõ nào phát sinh đều không được hiển thị. CHÚ THÍCH Đối với các SSP được nhập trực tiếp, các giá trị được nhập có thể được hiển thị tạm thời để cho phép xác minh bằng mắt nhằm cải thiện độ chính xác.

Bảng 265 - VE và TE của AS09.17

Nhập và xuất tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.17 ISO/IEC 19790:2025, 7.9.5.1	Ngoại trừ dữ liệu xác thực, các SSP được nhập thủ công một cách trực tiếp (ở dạng rõ hoặc dạng mã hóa) phải được kiểm chứng trong quá trình nhập vào mô-đun về độ chính xác bằng cách sử dụng bài kiểm thử nhập thủ công có điều kiện được quy định tại ISO/IEC 19790:2025, 7.10.4.5.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.44, AS10.45, AS10.46 và AS10.47.	

Bảng 266 - VE và TE của AS09.18

Nhập và xuất tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.18 ISO/IEC 19790:2025, 7.9.5.1	Để ngăn chặn việc vô tình xuất thông tin nhạy cảm, mô-đun phải yêu cầu hai hành động nội bộ độc lập nhằm xuất ra bất kỳ CSP dạng rõ nào;
Thông tin bắt buộc từ nhà cung cấp	
VE09.18.01	Nếu mô-đun xuất bất kỳ CSP dạng rõ nào, tài liệu do nhà cung cấp cung cấp phải mô tả các dịch vụ đầu ra đó.
VE09.18.02	Mô hình trạng thái hữu hạn và các tài liệu khác do nhà cung cấp cung cấp phải chỉ ra rằng, đối với việc xuất các CSP dạng rõ, bắt buộc phải có hai hành động nội bộ độc lập.
Quy trình kiểm thử bắt buộc	
TE09.18.01	Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp hoặc từ mô hình trạng thái hữu hạn rằng mô-đun cho phép xuất các CSP dạng rõ.
TE09.18.02	Kiểm thử viên phải xác minh từ mô hình trạng thái hữu hạn và các tài liệu khác do nhà cung cấp cung cấp rằng việc xuất các CSP dạng rõ yêu cầu hai hành động nội bộ độc lập để mô-đun mật mã có thể xuất các CSP dạng rõ.
TE09.18.03	Kiểm thử viên phải thử xuất các CSP dạng rõ mà không để mô-đun thực hiện hai hành động nội bộ độc lập. Mô-đun sẽ bị đánh giá là thất bại nếu nó cho phép xuất các CSP dạng rõ mà không có hai hành động nội bộ độc lập.

Bảng 267 - VE và TE của AS09.19

Nhập và xuất tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.19 ISO/IEC 19790:2025, 7.9.5.1	Đối với việc nhập hoặc xuất điện tử thông qua kết nối không dây, các CSP và các thành phần khóa phải được mã hóa.

Thông tin bắt buộc từ nhà cung cấp	
VE09.19.01	Nếu mô-đun nhập hoặc xuất các CSP, và các thành phần khóa thông qua các giao diện không dây, tài liệu do nhà cung cấp cung cấp phải mô tả các dịch vụ không dây đó.
VE09.19.02	Nếu mô-đun nhập hoặc xuất các CSP, và các thành phần khóa thông qua các giao diện không dây, tài liệu do nhà cung cấp cung cấp phải mô tả các phương pháp mã hóa được sử dụng để mã hóa các CSP và các thành phần khóa.
Quy trình kiểm thử bắt buộc	
TE09.19.01	Kiểm thử viên phải xác minh xem mô-đun có nhập hoặc xuất các CSP và thành phần khóa thông qua các giao diện không dây hay không.
TE09.19.02	Kiểm thử viên phải xác minh rằng các phương pháp mã hóa được sử dụng để mã hóa các CSP và các thành phần khóa là các phương pháp mã hóa đã phê duyệt. CHÚ THÍCH Đối với mức an toàn 1 và 2, các CSP và thành phần khóa dạng rõ có thể được nhập và xuất thông qua các cổng vật lý và các giao diện logic được chia sẻ với các cổng vật lý và giao diện logic khác của mô-đun mật mã.

Bảng 268 - VE và TE của AS09.20

Nhập và xuất tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.20 ISO/IEC 19790:2025, 7.9.5.1	Các khóa mật mã được thiết lập không dây bằng các phương pháp tự động phải sử dụng một phương pháp đã phê duyệt được liệt kê trong ISO/IEC 19790:2025, Phụ lục D.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS09.13.	

Bảng 269 - VE và TE của AS09.21

Nhập và xuất tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.21 ISO/IEC 19790:2025, 7.9.5.1	Nếu mô-đun mật mã sử dụng các thủ tục phân chia thông tin để nhập hoặc xuất các khóa mật mã, mô-đun phải yêu cầu ít nhất hai thành phần khóa để tái tạo lại khóa mật mã ban đầu.
Thông tin bắt buộc từ nhà cung cấp	
VE09.21.01	Tài liệu do nhà cung cấp cung cấp phải quy định số lượng thành phần được yêu cầu để xây dựng lại CSP ban đầu.
VE09.21.02	Nếu yêu cầu phải biết về số lượng thành phần khóa để tái tạo lại khóa ban đầu, tài liệu do nhà cung cấp cung cấp phải bao gồm cơ sở hợp lý tuyên bố việc biết bất kỳ số lượng thành phần khóa nào ít hơn tổng số lượng thành phần khóa sẽ không cung cấp thông tin nào về khóa ban đầu ngoài độ dài của nó.
Quy trình kiểm thử bắt buộc	
TE09.21.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả cách thức thủ tục phân chia thông tin yêu cầu ít nhất hai thành phần để xây dựng lại CSP ban đầu.
TE09.21.02	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả cách thức việc xuất các CSP theo thủ tục phân chia thông tin sẽ không dẫn đến việc xuất ra một thành phần duy nhất có thể được sử dụng để xây dựng lại CSP ban đầu.

TE09.21.03	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có cung cấp cơ sở hợp lý chứng minh rằng không có thông tin nào được thu thập nếu không biết tất cả các thành phần khóa cần thiết, và việc xuất các CSP theo thủ tục phân chia thông tin không dẫn đến việc xuất ra một thành phần duy nhất có thể được sử dụng để xây dựng lại CSP ban đầu.
TE09.21.04	Kiểm thử viên phải xác minh tính chính xác của bất kỳ cơ sở hợp lý nào do nhà cung cấp đưa ra. Trách nhiệm chứng minh thuộc về nhà cung cấp; nếu có bất kỳ sự không chắc chắn hoặc mơ hồ nào, kiểm thử viên phải yêu cầu nhà cung cấp cung cấp thêm thông tin.

6.9.5.2 Mức an toàn 1 và 2

Bảng 270 - VE và TE của AS09.22

Nhập và xuất tham số an toàn nhạy cảm - mức 1 và 2	
AS09.22 ISO/IEC 19790:2025, 7.9.5.2	Đối với các mô-đun phần mềm hoặc các thành phần phần mềm của một mô-đun phần mềm lai ghép, các CSP và các thành phần khóa có thể được nhập hoặc xuất khỏi mô-đun dưới định dạng rõ; trong trường hợp này, mô-đun không được xuất các CSP và thành phần khóa ra khỏi môi trường hoạt động.
Thông tin bắt buộc từ nhà cung cấp	
VE09.22.01	Đối với các mô-đun phần mềm hoặc các thành phần phần mềm của một mô-đun phần mềm lai ghép, nhà cung cấp phải cung cấp tài liệu chứng minh rằng các CSP và các thành phần khóa được nhập vào hoặc xuất ra khỏi mô-đun dưới định dạng rõ được duy trì bên trong môi trường hoạt động và các CSP và thành phần khóa dưới định dạng rõ không được xuất ra khỏi môi trường hoạt động.
Quy trình kiểm thử bắt buộc	
TE09.22.01	Đối với các mô-đun phần mềm hoặc các thành phần phần mềm của một mô-đun phần mềm lai ghép, kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu chứng minh rằng các CSP và thành phần khóa được nhập hoặc xuất khỏi mô-đun dưới định dạng rõ được duy trì bên trong môi trường hoạt động và các CSP và thành phần khóa dưới định dạng rõ không được xuất ra khỏi môi trường hoạt động.

6.9.5.3 Mức an toàn 3

Bảng 271 - VE và TE của AS09.23

Nhập và xuất tham số an toàn nhạy cảm - mức 3	
AS09.23 ISO/IEC 19790:2025, 7.9.5.3	Các khóa mật mã, các thành phần khóa từ các thủ tục phân chia thông tin, và các CSP không phải khóa được nhập vào hoặc xuất ra khỏi mô-đun mật mã bằng các phương pháp nhập trực tiếp hoặc điện tử hoặc phải được mã hóa hoặc sử dụng một đường dẫn tin cậy dạng rõ đáp ứng các yêu cầu của mức an toàn 3 trong ISO/IEC 19790:2025, 7.3.4.
Thông tin bắt buộc từ nhà cung cấp	
VE09.23.01	Nhà cung cấp phải cung cấp tài liệu mô tả liệu các khóa mật mã, các thành phần khóa từ các thủ tục phân chia thông tin, và các CSP không phải khóa được nhập vào hoặc xuất ra khỏi mô-đun mật mã dưới dạng mã hóa hay sử dụng một đường dẫn tin cậy dạng rõ.
VE09.23.02	Đối với các khóa được mã hóa khi nhập vào hoặc xuất ra khỏi mô-đun, tài liệu do nhà cung cấp cung cấp phải mô tả phương pháp mã hóa và cung cấp chứng chỉ

	xác nhận nếu có hoặc cam kết của nhà cung cấp như được quy định tại VE02.18.01 và VE02.18.03.
VE09.23.03	Đối với các khóa được nhập vào hoặc xuất ra khỏi mô-đun bằng cách sử dụng các thủ tục phân chia thông tin, tài liệu do nhà cung cấp cung cấp phải mô tả các phương pháp phân chia thông tin được sử dụng như quy định từ VE09.21.01 đến VE09.21.02.
VE09.23.04	Đối với các khóa được nhập vào hoặc xuất ra khỏi một mô-đun bằng cách sử dụng một đường dẫn tin cậy dạng rõ, tài liệu do nhà cung cấp cung cấp phải mô tả đường dẫn tin cậy dạng rõ như quy định từ AS03.17 đến AS03.22.
Quy trình kiểm thử bắt buộc	
TE09.23.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có quy định rằng các khóa mật mã, các thành phần khóa từ các thủ tục phân chia thông tin, và các CSP không phải khóa được nhập vào hoặc xuất ra khỏi mô-đun mật mã dưới dạng mã hóa hoặc sử dụng một đường dẫn tin cậy dạng rõ.
TE09.23.02	Đối với các khóa được mã hóa khi nhập vào hoặc xuất ra khỏi một mô-đun, kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có mô tả phương pháp mã hóa. Kiểm thử viên phải xác minh rằng nhà cung cấp cung cấp một chứng chỉ xác nhận nếu có hoặc cam kết của nhà cung cấp như quy định trong TE02.18.01 và TE02.18.03.
TE09.23.03	Đối với các khóa được nhập vào hoặc xuất ra khỏi một mô-đun bằng cách sử dụng các thủ tục phân chia thông tin, kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả các phương pháp phân chia thông tin được sử dụng như quy định từ TE09.21.01 đến TE09.21.04.
TE09.23.04	Đối với các khóa được nhập vào hoặc xuất ra khỏi một mô-đun bằng cách sử dụng một đường dẫn tin cậy dạng rõ, kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả đường dẫn tin cậy dạng rõ được sử dụng như quy định từ AS03.17 đến AS03.22.
TE09.23.05	Đối với các phương pháp đã được lập tài liệu trong TE09.23.01 đến TE09.23.04, kiểm thử viên phải xác minh bằng kiểm tra thực tế và xem xét mô-đun để đảm bảo rằng các khóa được nhập đang sử dụng các phương pháp đã mô tả.

Bảng 272 - VE và TE của AS09.24

Nhập và xuất tham số an toàn nhạy cảm - mức 3	
AS09.24 ISO/IEC 19790:2025, 7.9.5.3	Khi nhập hoặc xuất các thành phần khóa từ các thủ tục phân chia thông tin, mô-đun phải xác thực từng người vận hành (tức là từng bên nhập hoặc xuất thành phần khóa riêng biệt) một cách độc lập bằng phương thức xác thực đáp ứng các yêu cầu mức an toàn 3 trong ISO/IEC 19790:2025, 7.4.4.
Thông tin bắt buộc từ nhà cung cấp	
VE09.24.01	Tài liệu do nhà cung cấp cung cấp phải quy định cách thức phương pháp xác thực dựa trên danh tính được sử dụng và kiểm tra trước khi nhập từng thành phần khóa riêng biệt.
Quy trình kiểm thử bắt buộc	
TE09.24.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có quy định cách thức phương pháp xác thực dựa trên danh tính được sử dụng và kiểm tra trước khi nhập từng thành phần khóa riêng biệt.
TE09.24.02	Bài kiểm thử phải thực hiện việc nhập khóa phân mảnh vào mô-đun và xác nhận

	ràng cần phải có quá trình xác thực dựa trên danh tính riêng biệt để nhập mỗi thành phần khóa.
--	--

6.9.5.4 Mức an toàn 4

Bảng 273 - VE và TE của AS09.25

Nhập và xuất tham số an toàn nhạy cảm - mức 4	
AS09.25 ISO/IEC 19790:2025, 7.9.5.4	Các khóa mật mã được nhập vào hoặc xuất ra khỏi mô-đun mật mã phải được mã hóa hoặc được nhập bằng cách sử dụng các thủ tục phân chia thông tin.
Thông tin bắt buộc từ nhà cung cấp	
VE09.25.01	Nhà cung cấp phải cung cấp tài liệu mô tả liệu các khóa mật mã được nhập vào hoặc xuất ra khỏi mô-đun dưới dạng mã hóa hay sử dụng các thủ tục phân chia thông tin.
VE09.25.02	Đối với các khóa được mã hóa khi nhập vào hoặc xuất ra khỏi mô-đun, tài liệu do nhà cung cấp cung cấp phải mô tả phương pháp mã hóa và cung cấp chứng chỉ xác nhận nếu có hoặc cam kết của nhà cung cấp như quy định tại VE02.18.01 và VE02.18.03.
VE09.25.03	Đối với các khóa được nhập vào hoặc xuất ra khỏi một mô-đun bằng cách sử dụng các thủ tục phân chia thông tin, tài liệu do nhà cung cấp cung cấp phải mô tả các phương pháp phân chia thông tin được sử dụng như quy định từ VE09.21.01 đến VE09.21.02.
Quy trình kiểm thử bắt buộc	
TE09.25.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả liệu các khóa mật mã được nhập hoặc xuất khỏi mô-đun dưới dạng mã hóa hay sử dụng các thủ tục phân chia thông tin.
TE09.25.02	Đối với các khóa được mã hóa khi nhập vào hoặc xuất ra khỏi một mô-đun, kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có mô tả phương pháp mã hóa và cung cấp chứng chỉ xác nhận nếu có hoặc cam kết của nhà cung cấp như quy định tại TE02.18.01 và VE02.18.03.
TE09.25.03	Đối với các khóa được nhập vào hoặc xuất ra khỏi một mô-đun bằng cách sử dụng các thủ tục phân chia thông tin, kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả các phương pháp phân chia thông tin được sử dụng như quy định từ TE09.21.01 đến TE09.21.04.
TE09.25.04	Đối với các phương pháp đã được lập tài liệu trong TE09.25.01 đến TE09.25.03, kiểm thử viên phải xác minh bằng kiểm tra thực tế và xem xét mô-đun để đảm bảo rằng các khóa được nhập đang sử dụng các phương pháp đã mô tả.

Bảng 274 - VE và TE của AS09.26

Nhập và xuất tham số an toàn nhạy cảm - mức 4	
AS09.26 ISO/IEC 19790:2025, 7.9.5.4	Các thành phần khóa từ các thủ tục phân chia thông tin và các CSP không phải khóa phải được nhập vào hoặc xuất ra khỏi mô-đun dưới dạng mã hóa hoặc thông qua một đường dẫn tin cậy dạng rõ đáp ứng các yêu cầu của mức an toàn 4 trong ISO/IEC 19790:2025, 7.3.4.
Thông tin bắt buộc từ nhà cung cấp	
VE09.26.01	Nhà cung cấp phải cung cấp tài liệu mô tả liệu các thành phần khóa từ các thủ tục

	phân chia thông tin và các CSP không phải khóa được nhập vào hoặc xuất ra khỏi mô-đun dưới dạng mã hóa hay sử dụng các thủ tục phân chia thông tin.
VE09.26.02	Đối với các thành phần khóa từ các thủ tục phân chia thông tin và các CSP không phải khóa được mã hóa khi nhập vào hoặc xuất ra khỏi một mô-đun, tài liệu do nhà cung cấp cung cấp phải mô tả phương pháp mã hóa và cung cấp chứng chỉ xác nhận nếu có hoặc cam kết của nhà cung cấp như quy định tại VE02.18.01 và VE02.18.03.
VE09.26.03	Đối với các thành phần khóa từ các thủ tục phân chia thông tin và các CSP không phải khóa được nhập vào hoặc xuất ra khỏi một mô-đun bằng cách sử dụng các thủ tục phân chia thông tin, tài liệu do nhà cung cấp cung cấp phải mô tả các phương pháp phân chia thông tin được sử dụng.
Quy trình kiểm thử bắt buộc	
TE09.26.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có mô tả liệu các thành phần khóa từ các thủ tục phân chia thông tin và các CSP không phải khóa được nhập vào hay xuất ra khỏi mô-đun dưới dạng mã hóa hay sử dụng các thủ tục phân chia thông tin.
TE09.26.02	Đối với các thành phần khóa từ các thủ tục phân chia thông tin và các CSP không phải khóa được mã hóa khi nhập vào hoặc xuất ra khỏi một mô-đun, kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp có mô tả phương pháp mã hóa. Kiểm thử viên phải xác minh rằng nhà cung cấp cung cấp chứng chỉ xác nhận nếu có hoặc cam kết của nhà cung cấp như quy định tại TE02.18.01 và VE02.18.03.
TE09.26.03	Đối với các thành phần khóa từ các thủ tục phân chia thông tin và các CSP không phải khóa được nhập vào hoặc xuất ra khỏi một mô-đun bằng cách sử dụng các thủ tục phân chia thông tin, kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp mô tả các phương pháp phân chia thông tin được sử dụng.
TE09.26.04	Đối với các phương pháp đã được lập tài liệu trong TE09.26.01 đến TE09.26.03, kiểm thử viên phải xác minh bằng kiểm tra thực tế và xem xét mô-đun để đảm bảo rằng các khóa được nhập đang sử dụng các phương pháp đã mô tả.

Bảng 275 - VE và TE của AS09.27

Nhập và xuất tham số an toàn nhạy cảm - mức 4	
AS09.27 ISO/IEC 19790:2025, 7.9.5.4	Đối với các thành phần khóa được nhập hoặc xuất ra như một phần của các thủ tục phân chia thông tin, mô-đun phải xác thực từng người vận hành (tức là từng bên nhập/xuất thành phần khóa riêng biệt) một cách độc lập bằng phương thức xác thực đáp ứng các yêu cầu mức an toàn 4 trong ISO/IEC 19790:2025, 7.4.4.
Thông tin bắt buộc từ nhà cung cấp	
VE09.27.01	Tài liệu do nhà cung cấp cung cấp phải quy định rằng xác thực dựa trên danh tính đa yếu tố hoặc một phương thức khác đáp ứng các yêu cầu mức an toàn 4 trong ISO/IEC 19790:2025, 7.4.4 được sử dụng cho từng thành phần khóa riêng biệt.
Quy trình kiểm thử bắt buộc	
TE09.27.01	Kiểm thử viên phải xác minh rằng xác thực dựa trên danh tính đa yếu tố hoặc phương thức khác đáp ứng các yêu cầu mức an toàn 4 trong ISO/IEC 19790:2025, 7.4.4 được sử dụng cho từng thành phần khóa riêng biệt.
TE09.27.02	Kiểm thử viên phải xác minh phương pháp xác thực đa yếu tố hoặc phương thức khác theo AS04.59.

6.9.6 Lưu trữ tham số an toàn nhạy cảm

Bảng 276 - VE và TE của AS09.28

Lưu trữ tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.28 ISO/IEC 19790:2025, 7.9.6	Một mô-đun phải liên kết mỗi SSP được lưu trữ bên trong mô-đun với thực thể (ví dụ: người vận hành, vai trò, hoặc quá trình) mà SSP đó được gán cho.
Thông tin bắt buộc từ nhà cung cấp	
VE09.28.01	Tài liệu do nhà cung cấp cung cấp về lưu trữ khóa phải mô tả các cơ chế hoặc thủ tục được sử dụng để đảm bảo rằng mỗi khóa được liên kết với đúng thực thể.
Quy trình kiểm thử bắt buộc	
TE09.28.01	Kiểm thử viên phải xác minh tài liệu về lưu trữ khóa để đảm bảo rằng các thủ tục có giải quyết cách một khóa được lưu trữ được liên kết với đúng thực thể.
TE09.28.02	Kiểm thử viên phải sửa đổi mối liên kết giữa khóa và thực thể. Sau đó, kiểm thử viên phải thử thực hiện các chức năng mật mã với tư cách là một trong những thực thể đó và phải xác minh rằng các chức năng này thất bại.

6.9.7 Xóa trắng tham số an toàn nhạy cảm

6.9.7.1 Yêu cầu chung về xóa trắng tham số an toàn nhạy cảm

Bảng 277 - VE và TE của AS09.29

Xóa trắng tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.29 ISO/IEC 19790:2025, 7.9.7.1	Một mô-đun phải cung cấp các phương pháp để xóa trắng tất cả các CSP dạng rõ, các PSP dạng rõ, và các thành phần khóa dạng rõ bên trong mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE09.29.01	Tài liệu do nhà cung cấp cung cấp phải quy định các thông tin xóa trắng sau đây đối với các CSP của người vận hành và các PSP của người vận hành: a) các kỹ thuật xóa trắng; b) các hạn chế đối với thời điểm các CSP dạng rõ, PSP dạng rõ, và thành phần khóa dạng rõ có thể bị xóa trắng; c) các CSP dạng rõ, PSP dạng rõ, và thành phần khóa dạng rõ nào bị xóa trắng; d) các CSP dạng rõ, PSP dạng rõ, và thành phần khóa dạng rõ nào không bị xóa trắng và cơ sở hợp lý; e) cơ sở hợp lý giải thích cách kỹ thuật xóa trắng được thực hiện trong khoảng thời gian đủ nhanh để không bị khai thác đến các CSP dạng rõ, PSP dạng rõ và thành phần khóa dạng rõ.
VE09.29.02	Tài liệu do nhà cung cấp cung cấp phải quy định cách thức các phương pháp xóa trắng được sử dụng sao cho kẻ tấn công không thể chiếm đoạt các CSP dạng rõ, PSP dạng rõ và thành phần khóa dạng rõ bên trong mô-đun.
VE09.29.03	Nếu các CSP dạng rõ, PSP dạng rõ và thành phần khóa dạng rõ bị xóa trắng bằng thủ tục dưới sự kiểm soát của người vận hành (tức là có mặt để quan sát phương pháp đã hoàn tất thành công hoặc được kiểm soát thông qua một phiên quản lý

	từ xa), tài liệu do nhà cung cấp cung cấp và chính sách an toàn của mô-đun phải quy định cách thức các phương pháp đó được thực hiện.
Quy trình kiểm thử bắt buộc	
TE09.29.01	Kiểm thử viên phải xác minh tài liệu của nhà cung cấp có bao gồm thông tin được quy định trong VE09.29.01. Kiểm thử viên phải xác minh tính chính xác của mọi cơ sở hợp lý do nhà cung cấp cung cấp. Trách nhiệm chứng minh thuộc về nhà cung cấp; nếu có sự không chắc chắn hoặc mơ hồ, kiểm thử viên phải yêu cầu nhà cung cấp cung cấp thêm thông tin khi cần thiết.
TE09.29.02	Kiểm thử viên phải xác minh xem những CSP dạng rõ, PSP dạng rõ và thành phần khóa dạng rõ nào có trong mô-đun và kích hoạt lệnh xóa trắng. Sau khi lệnh xóa trắng hoàn tất, kiểm thử viên phải thử thực hiện các hoạt động mật mã sử dụng từng CSP dạng rõ, PSP dạng rõ và thành phần khóa dạng rõ từng được lưu trữ trong mô-đun. Kiểm thử viên phải xác minh rằng không thể truy cập vào từng SSP không được bảo vệ đó.
TE09.29.03	Kiểm thử viên phải khởi tạo quá trình xóa trắng và xác minh rằng phương pháp hủy SSP được thực hiện trong khoảng thời gian không đủ dài để gây tổn hại đến các CSP ở dạng bản rõ, các PSP ở dạng bản rõ, và các thành phần khóa ở dạng bản rõ
TE09.29.04	Kiểm thử viên phải xác minh rằng tất cả các CSP dạng rõ, PSP dạng rõ, và thành phần khóa dạng rõ không bị xóa trắng bởi lệnh xóa trắng thì hoặc phải 1) được mã hóa bằng một thuật toán đã phê duyệt, hoặc 2) được bảo vệ vật lý hoặc logic bên trong một mô-đun mật mã được nhúng đã được thẩm định (được thẩm định là tuân thủ ISO/IEC 19790:2025).
TE09.29.05	Nếu các phương pháp xóa trắng thủ tục được sử dụng, kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp, bao gồm cả chính sách an toàn, có quy định rằng thủ tục phải được thực hiện dưới sự kiểm soát của người vận hành.
TE09.29.06	Nếu phương pháp xóa trắng thủ tục không nằm dưới sự kiểm soát trực tiếp của người vận hành, kiểm thử viên phải xác minh tính chính xác của mọi cơ sở hợp lý do nhà cung cấp cung cấp về lý do tại sao kẻ tấn công không thể lấy được các CSP dạng rõ, PSP dạng rõ và thành phần khóa dạng rõ bên trong mô-đun. Trách nhiệm chứng minh thuộc về nhà cung cấp; nếu có sự không chắc chắn hoặc mơ hồ, kiểm thử viên phải yêu cầu nhà cung cấp cung cấp thêm thông tin. CHÚ THÍCH Các CSP dạng rõ, PSP dạng rõ, thành phần khóa dạng rõ được lưu trữ tạm thời, và các giá trị lưu trữ khác thuộc sở hữu của mô-đun sẽ bị xóa trắng khi chúng không còn cần thiết cho việc sử dụng trong tương lai.

Bảng 278 - VE và TE của AS09.30

Xóa trắng tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
AS09.30 ISO/IEC 19790:2025, 7.9.7.1	Một SSP hoặc thành phần khóa đã bị xóa trắng không được có khả năng truy xuất lại hay tái sử dụng, kể cả để phản hồi lại sự can thiệp.
Thông tin bắt buộc từ nhà cung cấp	
VE09.30.01	Tài liệu do nhà cung cấp cung cấp phải quy định cách một SSP hoặc thành phần khóa đã bị xóa trắng không thể bị truy xuất lại hay tái sử dụng.
Quy trình kiểm thử bắt buộc	

TE09.30.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có quy định cách một SSP hoặc thành phần khóa đã bị xóa trắng không thể bị truy xuất lại hay tái sử dụng.
TE09.30.02	Kiểm thử viên phải xác minh tính chính xác của mọi cơ sở hợp lý do nhà cung cấp đưa ra. Trách nhiệm chứng minh thuộc về nhà cung cấp; nếu có bất kỳ sự không chắc chắn hoặc mơ hồ nào, kiểm thử viên phải yêu cầu nhà cung cấp cung cấp thêm thông tin. Không đòi hỏi xóa trắng các PSP được bảo vệ, các CSP được mã hóa, hoặc các CSP được bảo vệ vật lý hoặc logic theo cách khác bên trong một mô-đun nhúng bổ sung đã được thẩm định (đáp ứng các yêu cầu của ISO/IEC 19790:2025). Các SSP không bắt buộc phải đáp ứng các yêu cầu xóa trắng này nếu chúng được sử dụng duy nhất để tiết lộ dữ liệu dạng rõ cho các quá trình đóng vai trò proxy xác thực (ví dụ: một CSP là khóa khởi tạo mô-đun). CHÚ THÍCH 1: Không đòi hỏi xóa trắng các PSP được bảo vệ, các CSP được mã hóa, hoặc các CSP được bảo vệ vật lý hoặc logic theo cách khác bên trong một mô-đun nhúng bổ sung đã được thẩm định (đáp ứng các yêu cầu của ISO/IEC 19790:2025). CHÚ THÍCH 2: Các SSP không bắt buộc phải đáp ứng các yêu cầu xóa trắng này nếu chúng được sử dụng duy nhất để tiết lộ dữ liệu dạng rõ cho các quá trình đóng vai trò proxy xác thực (ví dụ: một CSP là khóa khởi tạo mô-đun).

6.9.7.2 Mức an toàn 1

Bảng 279 - VE và TE của AS09.31

Xóa trắng tham số an toàn nhạy cảm - mức 1	
AS09.31 ISO/IEC 19790:2025, 7.9.7.2	Nếu việc xóa trắng được thực hiện theo thủ tục, chính sách an toàn phải cung cấp hướng dẫn về cách thực hiện thủ tục đó, sao cho tất cả các CSP dạng rõ, các PSP dạng rõ và các thành phần khóa dạng rõ đều bị xóa trắng.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	

6.9.7.3 Mức an toàn 2 và 3

Bảng 280 - VE và TE của AS09.32

Xóa trắng tham số an toàn nhạy cảm - mức 2, 3 và 4	
AS09.32 ISO/IEC 19790:2025, 7.9.7.3	Mô-đun mật mã phải thực hiện việc xóa trắng các CSP dạng rõ, các PSP dạng rõ và các thành phần khóa dạng rõ (ví dụ: ghi đè bằng toàn bộ số không, hoặc toàn bộ số một, hoặc bằng dữ liệu ngẫu nhiên).
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS09.29.	

Bảng 281 - VE và TE của AS09.33

Xóa trắng tham số an toàn nhạy cảm - mức 2, 3 và 4	
AS09.33 ISO/IEC 19790:2025, 7.9.7.3	Khi xóa trắng các CSP dạng rõ hoặc các PSP dạng rõ, hoặc cả hai để phản hồi lại yêu cầu của người dùng hoặc phản hồi lại sự can thiệp, mô-đun không được ghi đè chúng bằng các CSP dạng rõ hoặc PSP của người dùng khác, kể cả trong quá trình phản hồi can thiệp.

Thông tin bắt buộc từ nhà cung cấp	
VE09.33.01	Tài liệu do nhà cung cấp cung cấp phải quy định rằng quá trình xóa trắng loại trừ việc ghi đè một SSP dạng rõ bằng một SSP dạng rõ khác.
Quy trình kiểm thử bắt buộc	
TE09.33.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có quy định rằng quá trình xóa trắng loại trừ việc ghi đè một SSP dạng rõ bằng một SSP dạng rõ khác.

Bảng 282 - VE và TE của AS09.34

Xóa trắng tham số an toàn nhạy cảm - mức 2, 3 và 4	
AS09.34 ISO/IEC 19790:2025, 7.9.7.3	Các SSP tạm thời phải bị xóa trắng khi chúng không còn cần thiết nữa, tuy nhiên, trong trường hợp này AS09.35 và AS03.07 sẽ không được áp dụng.
Thông tin bắt buộc từ nhà cung cấp	
VE09.34.01	Tài liệu do nhà cung cấp cung cấp phải quy định rằng các SSP tạm thời sẽ bị xóa trắng khi chúng không còn cần thiết nữa.
Quy trình kiểm thử bắt buộc	
TE09.34.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có quy định rằng các SSP tạm thời sẽ bị xóa trắng khi chúng không còn cần thiết nữa.

Bảng 283 - VE và TE của AS09.35

Xóa trắng tham số an toàn nhạy cảm - mức 2, 3 và 4	
AS09.35 ISO/IEC 19790:2025, 7.9.7.3	Mô-đun phải cung cấp một chỉ báo trạng thái đầu ra khi việc xóa trắng các CSP dạng rõ, PSP dạng rõ và các thành phần khóa dạng rõ hoàn tất, kể cả khi phản hồi lại sự can thiệp.
Thông tin bắt buộc từ nhà cung cấp	
VE09.35.01	Tài liệu do nhà cung cấp cung cấp phải quy định rằng mô-đun cung cấp chỉ báo trạng thái đầu ra khi quá trình xóa trắng hoàn tất (AS03.11).
Quy trình kiểm thử bắt buộc	
TE09.35.01	Kiểm thử viên phải xác minh rằng nhà cung cấp cung cấp tài liệu quy định việc mô-đun đưa ra một chỉ báo trạng thái đầu ra khi quá trình xóa trắng hoàn tất.
TE09.35.02	Kiểm thử viên phải thực hiện việc xóa trắng và xác minh bộ chỉ báo trạng thái đầu ra.

6.9.7.4 Mức an toàn 4

Bảng 284 - VE và TE của AS09.36

Xóa trắng tham số an toàn nhạy cảm - mức 4	
AS09.36 ISO/IEC 19790:2025, 7.9.7.4	Ngoài các yêu cầu của mức an toàn 2 và 3, các yêu cầu sau đây cũng phải được đáp ứng: {AS09.37 đến AS09.39}
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS09.37, AS09.38 và AS09.39.	

Bảng 285 - VE và TE của AS09.37

Xóa trắng tham số an toàn nhạy cảm - mức 4	
AS09.37 ISO/IEC 19790:2025, 7.9.7.4	Việc xóa trắng phải diễn ra ngay lập tức và không thể bị gián đoạn; và {phải diễn ra trong một khoảng thời gian đủ ngắn để ngăn chặn việc khôi phục SSP đang bị xóa trắng giữa thời điểm quá trình xóa trắng được khởi tạo và khi việc xóa trắng thực tế hoàn tất, kể cả khi phản hồi lại sự can thiệp}.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS09.38.	

Bảng 286 - VE và TE của AS09.38

Xóa trắng tham số an toàn nhạy cảm - mức 4	
AS09.38 ISO/IEC 19790:2025, 7.9.7.4	{Việc xóa trắng phải diễn ra ngay lập tức và không thể bị gián đoạn;} và phải diễn ra trong một khoảng thời gian đủ ngắn để ngăn chặn việc khôi phục SSP đang bị xóa trắng giữa thời điểm quá trình xóa trắng được khởi tạo và khi việc xóa trắng thực tế hoàn tất, kể cả khi phản hồi lại sự can thiệp.
Thông tin bắt buộc từ nhà cung cấp	
VE09.38.01	Nhà cung cấp phải cung cấp tài liệu chứng minh rằng việc xóa trắng mô-đun là ngay lập tức, không thể bị gián đoạn và diễn ra trong một khoảng thời gian đủ ngắn để ngăn chặn việc khôi phục dữ liệu nhạy cảm sau thời điểm quá trình xóa trắng được khởi tạo và trước khi việc xóa trắng thực tế hoàn tất.
Quy trình kiểm thử bắt buộc	
TE09.38.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu chứng minh rằng việc xóa trắng mô-đun là ngay lập tức, không thể bị gián đoạn và diễn ra trong một khoảng thời gian đủ ngắn để ngăn chặn việc khôi phục dữ liệu nhạy cảm giữa thời điểm khi quá trình xóa trắng được khởi tạo và khi quá trình xóa trắng thực tế hoàn tất.
TE09.38.02	Kiểm thử viên phải thực hiện việc xóa trắng mô-đun. Kiểm thử viên phải tìm cách làm gián đoạn quá trình xóa trắng để ngăn chặn sự hoàn tất toàn phần hoặc một phần của quá trình này.

Bảng 287 - VE và TE của AS09.39

Xóa trắng tham số an toàn nhạy cảm - mức 4	
AS09.39 ISO/IEC 19790:2025, 7.9.7.4	Tất cả các SSP phải bị xóa trắng, kể cả khi phản hồi lại sự can thiệp, sao cho mô-đun được trả về trạng thái xuất xưởng.
Thông tin bắt buộc từ nhà cung cấp	
VE09.39.01	Nhà cung cấp phải cung cấp tài liệu chứng minh rằng tất cả các CSP và PSP đều bị xóa trắng sao cho mô-đun được trả về trạng thái xuất xưởng.
Quy trình kiểm thử bắt buộc	
TE09.39.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu chứng minh rằng tất cả các CSP và PSP đều bị xóa trắng sao cho mô-đun được trả về trạng thái xuất xưởng.
TE09.39.02	Kiểm thử viên phải thực hiện việc xóa trắng mô-đun. Kiểm thử viên phải xác minh rằng mô-đun đã trở về trạng thái xuất xưởng.

6.10 Tự kiểm thử

6.10.1 Yêu cầu chung về tự kiểm thử

Bảng 288 - VE và TE của AS10.01

Yêu cầu chung về tự kiểm thử - mức 1, 2, 3 và 4	
AS10.01 ISO/IEC 19790:2025, 7.10.1	Tất cả các quá trình tự kiểm thử phải được mô-đun thực hiện mà không cần có các kiểm soát bên ngoài, các véc-tơ kiểm thử đầu vào được cung cấp từ bên ngoài, các kết quả đầu ra dự kiến, hoặc sự can thiệp của người vận hành, và bất kể việc mô-đun sẽ vận hành một dịch vụ đã phê duyệt hay không được phê duyệt.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 289 - VE và TE của AS10.02

Yêu cầu chung về tự kiểm thử - mức 1, 2, 3 và 4	
AS10.02 ISO/IEC 19790:2025, 7.10.1	Việc xác định đạt hay không đạt phải do mô-đun thực hiện, mà không cần có các kiểm soát bên ngoài, các véc-tơ kiểm thử đầu vào được cung cấp từ bên ngoài, các kết quả đầu ra dự kiến, hoặc sự can thiệp của người vận hành, và bất kể việc mô-đun sẽ vận hành một dịch vụ đã phê duyệt hay không được phê duyệt.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	
CHÚ THÍCH Mục đích của khẳng định này là việc xác định đạt hay không đạt sẽ do mô-đun thực hiện, mà không cần có các kiểm soát bên ngoài, chủ yếu dành cho các quá trình tự kiểm thử trước khi vận hành và quá trình tự kiểm thử thuật toán mật mã (có điều kiện). Cần lưu ý rằng bài kiểm thử nạp phần mềm/phần sụn vào một mô-đun đã được thẩm định có liên quan đến việc phần mềm hoặc phần sụn đó được nạp từ một nguồn bên ngoài, còn bài kiểm thử nhập thủ công có liên quan đến các SSP hoặc thành phần khóa được do vận hành nhập vào thủ công; tuy nhiên, bản chất của nó là giống nhau.	

Bảng 290 - VE và TE của AS10.03

Yêu cầu chung về tự kiểm thử - mức 1, 2, 3 và 4	
AS10.03 ISO/IEC 19790:2025, 7.10.1	Các quá trình tự kiểm thử trước khi vận hành phải được thực hiện và vượt qua thành công trước khi mô-đun cung cấp bất kỳ dữ liệu đầu ra nào thông qua giao diện đầu ra dữ liệu.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.14.	

Bảng 291 - VE và TE của AS10.04

Yêu cầu chung về tự kiểm thử - mức 1, 2, 3 và 4	
AS10.04 ISO/IEC 19790:2025, 7.10.1	Các quá trình tự kiểm thử có điều kiện phải được thực hiện khi một thuật toán mật mã hoặc quá trình có thể áp dụng được gọi (tức là các thuật toán mật mã bắt buộc phải trải qua quá trình tự kiểm thử).
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.25.	

Bảng 292 - VE và TE của AS10.05

Yêu cầu chung về tự kiểm thử - mức 1, 2, 3 và 4	
AS10.05 ISO/IEC 19790:2025,	Tất cả các quá trình tự kiểm thử được xác định trong các tiêu chuẩn cơ sở ở ISO/IEC 19790:2025, Phụ lục C, D và E phải được triển khai nếu có thể áp dụng.

7.10.1	
Thông tin bắt buộc từ nhà cung cấp	
VE10.05.01	Tài liệu do nhà cung cấp cung cấp phải cung cấp danh sách các bài tự kiểm thử bao gồm các bài sau: a) các bài tự kiểm thử trước khi vận hành: 1) kiểm tra tính toàn vẹn phần mềm/phần sụn trước khi vận hành; 2) kiểm tra bỏ qua trước khi vận hành; 3) kiểm tra các chức năng trọng yếu trước khi vận hành; 4) các bài tự kiểm thử có điều kiện; b) kiểm tra thuật toán mật mã có điều kiện: 1) kiểm tra tính nhất quán theo cặp có điều kiện; 2) kiểm tra nạp phần mềm/phần sụn có điều kiện; 3) kiểm tra nhập thủ công có điều kiện; 4) kiểm tra bỏ qua có điều kiện; 5) kiểm tra các chức năng trọng yếu có điều kiện.
VE10.05.02	Tài liệu do nhà cung cấp cung cấp phải quy định rằng các bài kiểm thử được xác định trong các tiêu chuẩn cơ sở (như quy định trong ISO/IEC 19790:2025, Phụ lục C, D và E) được triển khai nếu có thể áp dụng, hoặc theo quy định của tổ chức chứng nhận, bên cạnh các bài kiểm thử được quy định trong ISO/IEC 19790:2025.
Quy trình kiểm thử bắt buộc	
TE10.05.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu chứng minh rằng các bài kiểm thử được xác định trong các tiêu chuẩn cơ sở quy định tại ISO/IEC 19790:2025, Phụ lục C, D và E được triển khai nếu có thể áp dụng, hoặc theo quy định của tổ chức chứng nhận, bên cạnh các bài kiểm thử được quy định trong ISO/IEC 19790:2025.

Bảng 293 - VE và TE của AS10.06

Yêu cầu chung về tự kiểm thử - mức 1, 2, 3 và 4	
AS10.06 ISO/IEC 19790:2025, 7.10.1	Tất cả các quá trình tự kiểm thử được xác định ngoài hoặc thay cho những quá trình được quy định trong các tiêu chuẩn cơ sở ở ISO/IEC 19790:2025, Phụ lục C, D và E phải được triển khai như được tham chiếu trong ISO/IEC 19790:2025, Phụ lục C, D và E đối với từng chức năng an toàn đã phê duyệt.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.01, AS10.02, AS10.03 và AS10.04.	

Bảng 294 - VE và TE của AS10.07

Yêu cầu chung về tự kiểm thử - mức 1, 2, 3 và 4	
AS10.07 ISO/IEC 19790:2025, 7.10.1	Nếu một mô-đun mật mã không vượt qua một bài tự kiểm thử, mô-đun đó: phải bước vào một trạng thái lỗi; hoặc {phải hoạt động theo quy định của tổ chức chứng nhận đối với sự cố tự kiểm thử cụ thể đó, nếu bài tự kiểm thử đó được xác định trong các tiêu chuẩn cơ sở ở ISO/IEC 19790:2025, Phụ lục C, D và E.}

Thông tin bắt buộc từ nhà cung cấp	
VE10.07.01	Đối với mỗi điều kiện lỗi, tài liệu do nhà cung cấp cung cấp phải cung cấp tên điều kiện, mô tả về điều kiện, các sự kiện có thể sinh ra điều kiện đó, và các hành động cần thiết để xóa điều kiện đó và tiếp tục hoạt động bình thường.
Quy trình kiểm thử bắt buộc	
TE10.07.01	Kiểm thử viên phải xác minh danh sách các tự kiểm thử để kiểm tra mô-đun trong ISO/IEC 19790:2025, Phụ lục C, D và E.
TE10.07.02	Kiểm thử viên phải kiểm tra để đảm bảo rằng thông tin được cung cấp ở trên đã được quy định cho mỗi điều kiện lỗi.
TE10.07.03	Kiểm thử viên phải khiến cho từng điều kiện lỗi xảy ra và phải thử xóa điều kiện lỗi đó. Kiểm thử viên phải xác minh rằng các hành động cần thiết để xóa điều kiện lỗi là nhất quán với tài liệu do nhà cung cấp cung cấp. Nếu kiểm thử viên không thể khiến từng điều kiện lỗi xảy ra, kiểm thử viên phải xác minh danh sách mã lệnh hoặc tài liệu thiết kế để kiểm tra xem các hành động cần thiết để xóa từng điều kiện lỗi có nhất quán với những mô tả trong tài liệu do nhà cung cấp cung cấp hay không.
TE10.07.04	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng việc xác định đạt hay không đạt của mỗi bài tự kiểm thử được thực hiện bởi mô-đun, mà không cần có các kiểm soát bên ngoài, các véc-tơ kiểm thử đầu vào được cung cấp từ bên ngoài, các kết quả đầu ra dự kiến, hoặc sự can thiệp của người vận hành.

Bảng 295 - VE và TE của AS10.08

Yêu cầu chung về tự kiểm thử - mức 1, 2, 3 và 4	
AS10.08 ISO/IEC 19790:2025, 7.10.1	{Nếu một mô-đun mật mã không vượt qua một bài tự kiểm thử, mô-đun đó: phải bước vào một trạng thái lỗi; hoặc} phải hoạt động theo quy định của tổ chức chứng nhận đối với sự cố tự kiểm thử cụ thể đó, nếu bài tự kiểm thử đó được xác định trong các tiêu chuẩn cơ sở ở ISO/IEC 19790:2025, Phụ lục C, D và E.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 296 - VE và TE của AS10.09

Yêu cầu chung về tự kiểm thử - mức 1, 2, 3 và 4	
AS10.09 ISO/IEC 19790:2025, 7.10.1	Nếu một mô-đun mật mã không vượt qua được bài kiểm thử nhập thủ công có điều kiện hoặc bài kiểm thử nạp phần mềm/phần sụn có điều kiện, và trong một số trường hợp là bài kiểm thử chức năng trọng yếu có điều kiện, mô-đun phải chỉ ra rằng bài kiểm thử đã thất bại, nhưng mô-đun không bắt buộc phải bước vào một trạng thái lỗi, ngăn chặn dữ liệu đầu ra, hoặc ngừng việc xử lý mật mã.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.07.	

Bảng 297 - VE và TE của AS10.10

Yêu cầu chung về tự kiểm thử - mức 1, 2, 3 và 4	
AS10.10 ISO/IEC 19790:2025, 7.10.1	Người vận hành mô-đun phải có khả năng xác định xem mô-đun đã bước vào một trạng thái lỗi hay chưa, thông qua một chỉ báo lỗi do mô-đun xuất ra hoặc một cách ngầm định thông qua một thủ tục rõ ràng được lập tài liệu trong chính sách an toàn.
Thông tin bắt buộc từ nhà cung cấp	

VE10.10.01	Nhà cung cấp phải lập tài liệu về tất cả các trạng thái lỗi liên quan đến mỗi quá trình tự kiểm thử và phải chỉ ra chỉ báo lỗi dự kiến đối với mỗi trạng thái lỗi.
VE10.10.02	Nếu mô-đun đã bước vào một trạng thái lỗi thông qua một chỉ báo lỗi được xuất ra một cách ngẫu nhiên, chính sách an toàn phi độc quyền do nhà cung cấp cung cấp phải mô tả một cách rõ ràng thủ tục để xác định xem mô-đun mật mã đã bước vào một trạng thái lỗi hay chưa.
Quy trình kiểm thử bắt buộc	
TE10.10.01	Kiểm thử viên phải xác minh tài liệu do nhà cung cấp cung cấp, kiểm tra để đảm bảo rằng nó liệt kê mọi trạng thái lỗi mà mô-đun bước vào khi gặp sự cố tự kiểm thử, và chỉ ra chỉ báo lỗi liên kết với mỗi trạng thái lỗi đó. Kiểm thử viên phải so sánh danh sách các trạng thái lỗi với những trạng thái lỗi được định nghĩa trong mô hình trạng thái hữu hạn (xem AS11.11) để xác minh rằng chúng khớp với nhau.
TE10.10.02	Bằng cách kiểm tra tài liệu do nhà cung cấp cung cấp có quy định cách mỗi tự kiểm thử xử lý lỗi, kiểm thử viên phải xác minh rằng: a) mô-đun bước vào trạng thái lỗi khi thất bại một bài tự kiểm thử; b) trạng thái lỗi nhất quán với tài liệu và mô hình trạng thái hữu hạn; c) mô-đun đưa ra một chỉ báo lỗi; d) chỉ báo lỗi đó nhất quán với chỉ báo lỗi đã được lập tài liệu.
TE10.10.03	Kiểm thử viên phải chạy từng bài tự kiểm thử và khiến mô-đun bước vào mọi trạng thái lỗi. Kiểm thử viên phải so sánh chỉ báo lỗi được quan sát với chỉ báo được quy định trong tài liệu do nhà cung cấp cung cấp. Nếu chúng không giống nhau, bài kiểm thử này bị coi là thất bại.
TE10.10.04	Nếu mô-đun đã bước vào một trạng thái lỗi thông qua một chỉ báo lỗi được xuất ra một cách ngẫu nhiên, kiểm thử viên phải xác minh rằng mô-đun đã bước vào trạng thái lỗi một cách ngẫu nhiên thông qua thủ tục được lập tài liệu trong chính sách an toàn phi độc quyền.

Bảng 298 - VE và TE của AS10.11

Yêu cầu chung về tự kiểm thử - mức 1, 2, 3 và 4	
AS10.11 ISO/IEC 19790:2025, 7.10.1	Mô-đun mật mã không được thực hiện bất kỳ hoạt động mật mã nào hoặc xuất dữ liệu và thông tin điều khiển qua giao diện đầu ra dữ liệu và đầu ra điều khiển khi đang ở trong trạng thái lỗi.
Thông tin bắt buộc từ nhà cung cấp	
VE10.11.01	Các yêu cầu về tài liệu do nhà cung cấp cung cấp được quy định tại VE03.07.01, VE03.07.02, VE03.09.01, và VE03.10.01. Thiết kế của nhà cung cấp cũng phải đảm bảo rằng không thể thực hiện các hoạt động mật mã trong khi mô-đun đang ở trong trạng thái lỗi.
Quy trình kiểm thử bắt buộc	
TE10.11.01	Kiểm thử viên phải xác minh rằng việc chặn đầu ra dữ liệu và kiểm soát đã được thực hiện theo quy định tại TE03.07.01, TE03.07.02, TE03.10.01 và TE03.10.02. Các kết quả của việc xác minh phải chỉ ra rằng: a) tài liệu do nhà cung cấp cung cấp chứng minh rằng mọi hoạt động xuất dữ liệu và thông tin điều khiển thông qua giao diện đầu ra dữ liệu và điều khiển

	đều bị chặn bất cứ khi nào mô-đun đang ở trong trạng thái lỗi; b) mô-đun chặn mọi hoạt động xuất dữ liệu và thông tin điều khiển khi mô-đun đang ở trong trạng thái lỗi.
TE10.11.02	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có quy định rằng các chức năng mật mã bị chặn trong khi mô-đun đang ở trong trạng thái lỗi.
TE10.11.03	Kiểm thử viên phải khiến mô-đun bước vào trạng thái lỗi và xác minh rằng bất kỳ hoạt động mật mã nào mà kiểm thử viên thử khởi tạo đều bị ngăn chặn.

Bảng 299 - VE và TE của AS10.12

Yêu cầu chung về tự kiểm thử - mức 1, 2, 3 và 4	
AS10.12 ISO/IEC 19790:2025, 7.10.1	Mô-đun mật mã không được sử dụng bất kỳ chức năng nào dựa trên một chức năng hoặc thuật toán đã không vượt qua một bài tự kiểm thử cho đến khi bài tự kiểm thử tương ứng đó được lặp lại và vượt qua thành công.
Thông tin bắt buộc từ nhà cung cấp	
VE10.12.01	Nhà cung cấp phải cung cấp tài liệu thiết kế tuyên bố rằng mô-đun mật mã không thể sử dụng bất kỳ chức năng nào dựa trên một chức năng hoặc thuật toán đã thất bại trong quá trình tự kiểm thử cho đến khi quá trình tự kiểm thử tương ứng đó được lặp lại và vượt qua thành công.
Quy trình kiểm thử bắt buộc	
TE10.12.01	Kiểm thử viên phải gây ra lỗi trong một chức năng hoặc thuật toán để kích hoạt trạng thái thất bại tự kiểm thử và khởi tạo một tính năng có sử dụng chức năng hoặc thuật toán đó. Kiểm thử viên phải xác minh rằng mô-đun không thể sử dụng tính năng này.
TE10.12.02	Kiểm thử viên phải chạy từng bài tự kiểm thử và khiến mô-đun bước vào mọi trạng thái lỗi hoặc trạng thái vận hành suy giảm. Kiểm thử viên phải thử sử dụng mô-đun mật mã, và xác minh rằng chức năng đó không thể được sử dụng cho đến khi bài tự kiểm thử tương ứng được lặp lại và vượt qua thành công.

6.10.2 Mức an toàn 3 và 4**Bảng 300 - VE và TE của AS10.13**

Mức an toàn 3 và 4 - mức 3 và 4	
AS10.13 ISO/IEC 19790:2025, 7.10.2	Ở mức an toàn 3 và 4, mô-đun phải duy trì một bản ghi lỗi có chứa ít nhất là sự kiện lỗi gần đây nhất (tức là bài tự kiểm thử nào đã thất bại).
Thông tin bắt buộc từ nhà cung cấp	
VE10.13.01	Tài liệu của nhà cung cấp phải quy định chức năng ghi nhận lỗi của mô-đun bao gồm các loại thông tin được ghi lại trong bản ghi lỗi (ví dụ: bài tự kiểm thử nào đã thất bại, lỗi xảy ra khi nào).
Quy trình kiểm thử bắt buộc	
TE10.13.01	Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp rằng chức năng ghi nhận lỗi cung cấp thông tin, tối thiểu là về sự kiện lỗi gần đây nhất.
TE10.13.02	Kiểm thử viên phải khiến mô-đun mật mã bước vào trạng thái lỗi và xác minh rằng mô-đun tạo ra bản ghi lỗi, tối thiểu là đối với sự kiện lỗi gần đây nhất.

Bảng 301 - VE và TE của AS10.14

Mức an toàn 3 và 4 - mức 3 và 4	
AS10.14 ISO/IEC 19790:2025, 7.10.2	Bản ghi lỗi phải được bảo vệ khỏi sự sửa đổi và thay thế trái phép.
Thông tin bắt buộc từ nhà cung cấp	
VE10.14.01	Tài liệu do nhà cung cấp cung cấp phải mô tả cơ chế bảo vệ khỏi sự sửa đổi và thay thế trái phép.
Quy trình kiểm thử bắt buộc	
TE10.14.01	Kiểm thử viên phải xác minh từ tài liệu do nhà cung cấp cung cấp rằng bản ghi lỗi được bảo vệ khỏi sự sửa đổi và thay thế trái phép.
TE10.14.02	Kiểm thử viên phải thử sử dụng mô-đun mật mã và xác minh rằng bản ghi lỗi được bảo vệ khỏi sự sửa đổi và thay thế trái phép.

Bảng 302 - VE và TE của AS10.15

Mức an toàn 3 và 4 - mức 1, 2, 3 và 4	
AS10.15 ISO/IEC 19790:2025, 7.10.2	Tài liệu về tự kiểm thử quy định tại ISO/IEC 19790:2025, A.2.9 phải được cung cấp.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

6.10.3 Tự kiểm thử trước khi vận hành**6.10.3.1 Yêu cầu chung về tự kiểm thử trước khi vận hành****Bảng 303 - VE và TE của AS10.16**

Tự kiểm thử trước khi vận hành - mức 1, 2, 3 và 4	
AS10.16 ISO/IEC 19790:2025, 7.10.3.1	Các bài tự kiểm thử trước khi vận hành phải được thực hiện và vượt qua thành công bởi một mô-đun mật mã: a) sau khi một mô-đun mật mã được bật nguồn hoặc khởi tạo (sau khi bị tắt nguồn, thiết lập lại, khởi động lại, khởi động lạnh, gián đoạn nguồn điện, v.v.); b) trước khi nguồn điện chính, phụ, hoặc dự phòng được cấp cho mô-đun; và c) trước khi mô-đun chuyển sang trạng thái hoạt động.
Thông tin bắt buộc từ nhà cung cấp	
VE10.16.01	Tài liệu do nhà cung cấp cung cấp phải cung cấp thông tin cho mỗi bài tự kiểm thử trước khi vận hành.
VE10.16.02	Nhà cung cấp phải cung cấp trình tự các bài tự kiểm thử trước khi vận hành sau khi mô-đun được bật nguồn hoặc khởi tạo và trước khi mô-đun chuyển sang trạng thái hoạt động.
Quy trình kiểm thử bắt buộc	
TE10.16.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có quy định cụ thể từng bài tự kiểm thử trước khi vận hành. Kiểm thử viên phải xác minh rằng các quá trình tự kiểm thử trước khi vận hành được thực hiện đúng như quy định.

TE10.16.02	Bằng cách kiểm tra mã lệnh và tài liệu thiết kế, kiểm thử viên phải xác minh rằng mỗi bài kiểm thử trước khi vận hành được thực hiện và vượt qua thành công sau khi một mô-đun mật mã được bật nguồn hoặc khởi tạo và trước khi mô-đun chuyển sang trạng thái hoạt động.
------------	--

Bảng 304 - VE và TE của AS10.17

Tự kiểm thử trước khi vận hành - mức 1, 2, 3 và 4	
AS10.17 ISO/IEC 19790:2025, 7.10.3.1	Một mô-đun mật mã phải thực hiện các bài tự kiểm thử trước khi vận hành sau đây, nếu có thể áp dụng: a) kiểm tra tính toàn vẹn phần mềm/phần sụn trước khi vận hành; b) kiểm tra bỏ qua trước khi vận hành; và c) kiểm tra các chức năng trọng yếu trước khi vận hành.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.18, AS10.19, AS10.20, AS10.21, AS10.22, AS10.23 và AS10.24.	

6.10.3.2 Kiểm tra tính toàn vẹn phần mềm/phần sụn trước khi vận hành

Bảng 305 - VE và TE của AS10.18

Tự kiểm thử trước khi vận hành - mức 1, 2, 3 và 4	
AS10.18 ISO/IEC 19790:2025, 7.10.3.2	Tất cả các thành phần phần mềm, phần sụn, và dòng bit bên trong biên mật mã phải được xác minh bằng cách sử dụng một kỹ thuật toàn vẹn đã phê duyệt hoặc EDC đáp ứng các yêu cầu được định nghĩa trong ISO/IEC 19790:2025, Điều 7.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS05.12, AS05.13, AS05.14, AS05.15, AS05.16, AS05.17, AS05.18, AS05.19, AS05.20, AS05.21, AS05.22, AS05.23, AS05.24, AS05.25, AS05.26, AS05.27, AS05.28 và AS05.29.	

Bảng 306 - VE và TE của AS10.19

Tự kiểm thử trước khi vận hành - mức 1, 2, 3 và 4	
AS10.19 ISO/IEC 19790:2025, 7.10.3.2	Nếu việc xác minh thất bại, bài kiểm thử tính toàn vẹn phần mềm/phần sụn trước khi vận hành sẽ bị đánh giá là không đạt.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 307 - VE và TE của AS10.20

Tự kiểm thử trước khi vận hành - mức 1, 2, 3 và 4	
AS10.20 ISO/IEC 19790:2025, 7.10.3.2	Nếu một mô-đun phần cứng không chứa phần sụn hoặc dòng bit, mô-đun tối thiểu phải triển khai một bài tự kiểm thử thuật toán mật mã có điều kiện như được quy định trong ISO/IEC 19790:2025, 7.10.4.2 để đóng vai trò như một bài tự kiểm thử trước khi vận hành.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

6.10.3.3 Kiểm thử việc bỏ qua trước khi vận hành

Bảng 308 - VE và TE của AS10.21

Tự kiểm thử trước khi vận hành - mức 1, 2, 3 và 4	
AS10.21 ISO/IEC 19790:2025, 7.10.3.3	Nếu một mô-đun mật mã triển khai khả năng bỏ qua, thì mô-đun đó phải đảm bảo hoạt động chính xác của logic chi phối việc kích hoạt khả năng bỏ qua thông qua việc thử nghiệm logic đó.
Thông tin bắt buộc từ nhà cung cấp	
VE10.21.01	Tài liệu do nhà cung cấp cung cấp phải quy định cách thức mô-đun mật mã đảm bảo hoạt động chính xác của logic chi phối việc kích hoạt khả năng bỏ qua.
Quy trình kiểm thử bắt buộc	
TE10.21.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng logic chi phối việc kích hoạt khả năng bỏ qua được triển khai đúng như quy định.
TE10.21.02	Kiểm thử viên phải kiểm tra mô-đun và xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng bài kiểm thử bỏ qua trước khi vận hành được triển khai nhằm thử nghiệm logic chi phối việc kích hoạt khả năng bỏ qua.
TE10.21.03	Kiểm thử viên phải khiến cho từng điều kiện lỗi của bài kiểm thử bỏ qua trước khi vận hành xảy ra và phải xác minh rằng việc chặn đầu ra được thực hiện khi nằm trong trạng thái lỗi tương ứng.
TE10.21.04	Kiểm thử viên phải chạy bài kiểm thử bỏ qua trước khi vận hành và phải xác minh rằng bất kỳ tính năng nào dựa vào logic chi phối việc kích hoạt khả năng bỏ qua sẽ không thể được sử dụng theo như quy định tại TE10.12.01 và TE10.12.02.

Bảng 309 - VE và TE của AS10.22

Tự kiểm thử trước khi vận hành - mức 1, 2, 3 và 4	
AS10.22 ISO/IEC 19790:2025, 7.10.3.3	Mô-đun cũng phải xác minh đường truyền dữ liệu bằng cách: a) đặt công tắc bỏ qua ở trạng thái cung cấp quá trình xử lý mật mã và xác minh rằng dữ liệu truyền qua cơ chế bỏ qua đã được xử lý bằng mật mã; và b) đặt công tắc bỏ qua ở trạng thái không cung cấp quá trình xử lý mật mã và xác minh rằng dữ liệu truyền qua cơ chế bỏ qua chưa được xử lý bằng mật mã.
Thông tin bắt buộc từ nhà cung cấp	
VE10.22.01	Tài liệu do nhà cung cấp cung cấp phải quy định cách đặt công tắc bỏ qua để cung cấp quá trình xử lý mật mã.
VE10.22.02	Tài liệu do nhà cung cấp cung cấp phải mô tả cách cơ chế bỏ qua được thiết kế để bắt buộc việc truyền tải dữ liệu đã được xử lý bằng mật mã thông qua đường truyền dữ liệu, bằng cách đặt công tắc bỏ qua ở trạng thái cung cấp quá trình xử lý mật mã.
VE10.22.03	Tài liệu do nhà cung cấp cung cấp phải quy định cách đặt công tắc bỏ qua sao cho không cung cấp quá trình xử lý mật mã.
VE10.22.04	Tài liệu do nhà cung cấp cung cấp phải mô tả cách cơ chế bỏ qua được thiết kế để bắt buộc việc truyền tải dữ liệu chưa được xử lý bằng mật mã thông qua đường truyền dữ liệu, bằng cách đặt công tắc bỏ qua ở trạng thái không cung cấp quá

	trình xử lý mật mã.
Quy trình kiểm thử bắt buộc	
TE10.22.01	Kiểm thử viên phải xác minh thông qua việc kiểm tra mô-đun rằng mô-đun không cung cấp khả năng bỏ qua khi đặt công tắc bỏ qua ở trạng thái cung cấp quá trình xử lý mật mã.
TE10.22.02	Bằng cách kiểm tra mã lệnh hoặc tài liệu thiết kế, hoặc cả hai, kiểm thử viên phải xác minh rằng việc triển khai cơ chế bỏ qua là nhất quán với tài liệu do nhà cung cấp cung cấp.
TE10.22.03	Bằng cách kiểm tra mã lệnh hoặc tài liệu thiết kế, hoặc cả hai, kiểm thử viên phải xác minh rằng mô-đun thực hiện bài kiểm thử bỏ qua trước khi vận hành, trong đó xác minh rằng dữ liệu truyền qua đường truyền dữ liệu đã được xử lý bằng mật mã khi đặt công tắc bỏ qua ở trạng thái cung cấp quá trình xử lý mật mã.
TE10.22.04	Kiểm thử viên phải xác minh thông qua việc kiểm tra mô-đun rằng mô-đun cung cấp khả năng bỏ qua khi đặt công tắc bỏ qua ở trạng thái không cung cấp quá trình xử lý mật mã.
TE10.22.05	Bằng cách kiểm tra mã lệnh hoặc tài liệu thiết kế, hoặc cả hai, kiểm thử viên phải xác minh rằng mô-đun thực hiện bài kiểm thử bỏ qua trước khi vận hành, trong đó xác minh rằng dữ liệu truyền qua đường truyền dữ liệu chưa được xử lý bằng mật mã khi đặt công tắc bỏ qua ở trạng thái không cung cấp quá trình xử lý mật mã.

6.10.3.4 Kiểm thử chức năng trọng yếu trước khi vận hành

Bảng 310 - VE và TE của AS10.23

Tự kiểm thử trước khi vận hành - mức 1, 2, 3 và 4	
AS10.23 ISO/IEC 19790:2025, 7.10.3.4	Có thể có các chức năng an toàn khác mang tính trọng yếu đối với hoạt động an toàn của mô-đun mật mã mà bắt buộc phải được thử nghiệm như một bài kiểm thử trước khi vận hành.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.24.	

Bảng 311 - VE và TE của AS10.24

Tự kiểm thử trước khi vận hành - mức 1, 2, 3 và 4	
AS10.24 ISO/IEC 19790:2025, 7.10.3.4	Tài liệu phải quy định các chức năng trọng yếu được kiểm thử trước vận hành.
Thông tin bắt buộc từ nhà cung cấp	
VE10.24.01	Nhà cung cấp phải cung cấp tài liệu về tất cả các chức năng trọng yếu. Đối với mỗi chức năng trọng yếu được kiểm tra, nhà cung cấp phải chỉ ra: a) mục đích của chức năng trọng yếu đó; b) các chức năng trọng yếu nào được thử nghiệm bởi các bài tự kiểm thử trước khi vận hành nào; c) các chức năng trọng yếu nào được thử nghiệm bởi các bài tự kiểm thử có

	điều kiện nào.
Quy trình kiểm thử bắt buộc	
TE10.24.01	Kiểm thử viên phải xác minh tài liệu do nhà cung cấp cung cấp về các chức năng trọng yếu (trước khi vận hành và có điều kiện) được thử nghiệm và các tự kiểm thử được thiết kế để thử nghiệm chúng. Tài liệu này phải bao gồm các thông tin sau: a) việc xác định và mô tả về tất cả các chức năng trọng yếu; b) việc xác định ít nhất một quá trình tự kiểm thử cho mỗi chức năng trọng yếu.
TE10.24.02	Bằng cách kiểm tra mã lệnh và tài liệu thiết kế, kiểm thử viên phải xác minh rằng mô-đun thực hiện các tự kiểm thử được chỉ định đối với mỗi chức năng trọng yếu.
CHÚ THÍCH Các chức năng trọng yếu được định nghĩa là các chức năng không được định nghĩa ở nơi khác trong ISO/IEC 19790:2025, mà khi gặp sự cố, có thể dẫn đến việc truy cập, sử dụng, tiết lộ, sửa đổi, và thay thế các SSP trái phép. Các ví dụ về chức năng trọng yếu bao gồm nhưng không giới hạn ở: tạo bit ngẫu nhiên, sự vận hành của chức năng an toàn, và sự bỏ qua mật mã.	

6.10.4 Tự kiểm thử có điều kiện

6.10.4.1 Yêu cầu chung về tự kiểm thử có điều kiện

Bảng 312 - VE và TE của AS10.25

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.25 ISO/IEC 19790:2025, 7.10.4.1	Các bài tự kiểm thử có điều kiện phải được thực hiện bởi một mô-đun mật mã khi các điều kiện được quy định cho các bài kiểm thử sau đây xảy ra: tự kiểm thử thuật toán mật mã, kiểm tra tính nhất quán theo cặp, kiểm tra nạp phần mềm/phần sụn, kiểm tra nhập thủ công, kiểm tra bỏ qua có điều kiện và kiểm tra chức năng trọng yếu có điều kiện.
Thông tin bắt buộc từ nhà cung cấp	
VE10.25.01	Tài liệu do nhà cung cấp cung cấp phải cung cấp thông tin về các bài tự kiểm thử có điều kiện.
Quy trình kiểm thử bắt buộc	
TE10.25.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có quy định cụ thể về các bài tự kiểm thử có điều kiện.
TE10.25.02	Kiểm thử viên phải xác minh rằng các bài tự kiểm thử có điều kiện được thực hiện theo đúng những gì được quy định trong tài liệu do nhà cung cấp cung cấp.

6.10.4.2 Tự kiểm thử thuật toán mật mã có điều kiện

Bảng 313 - VE và TE của AS10.26

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.26 ISO/IEC 19790:2025, 7.10.4.2	Một bài tự kiểm thử thuật toán mật mã phải được tiến hành đối với tất cả các thuật toán mật mã đã phê duyệt như được tham chiếu trong ISO/IEC 19790:2025, Phụ lục C, D và E.
Thông tin bắt buộc từ nhà cung cấp	
VE10.26.01	Tài liệu do nhà cung cấp cung cấp phải cung cấp đặc tả về các tự kiểm thử thuật toán mật mã có điều kiện.
VE10.26.02	Nhà cung cấp phải cung cấp tài liệu bao gồm lý do chứng minh làm thế nào mỗi bài tự kiểm thử thuật toán mật mã có điều kiện lại được thực hiện trước lần sử dụng

	phục vụ hoạt động đầu tiên của thuật toán mật mã đó.
VE10.26.03	Nhà cung cấp phải quy định việc một bài kiểm thử biết trước kết quả, một bài kiểm thử so sánh, hay bài kiểm thử phát hiện lỗi được sử dụng để kiểm tra thuật toán mật mã của mô-đun. Nếu một bài kiểm thử so sánh hoặc một bài kiểm thử phát hiện lỗi, hoặc cả hai, được sử dụng, nhà cung cấp phải lập tài liệu về thực tế này.
Quy trình kiểm thử bắt buộc	
TE10.26.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng mô-đun có tiến hành một bài tự kiểm thử thuật toán mật mã có điều kiện trước lần sử dụng phục vụ hoạt động đầu tiên của mỗi thuật toán mật mã.

Bảng 314 - VE và TE của AS10.27

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.27 ISO/IEC 19790:2025, 7.10.4.2	Tự kiểm thử thuật toán mật mã có điều kiện phải được thực thi trước lần sử dụng phục vụ hoạt động đầu tiên của thuật toán mật mã sau khi bật nguồn, một quá trình khởi tạo mô-đun mới, hoặc theo yêu cầu tự kiểm thử định kỳ.
Thông tin bắt buộc từ nhà cung cấp	
VE10.27.01	Tài liệu do nhà cung cấp cung cấp phải quy định thời điểm mô-đun thực hiện các tự kiểm thử mật mã có điều kiện.
Quy trình kiểm thử bắt buộc	
TE10.27.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng các tự kiểm thử mật mã có điều kiện được mô-đun thực hiện: a) trước lần sử dụng phục vụ hoạt động đầu tiên của thuật toán mật mã sau khi bật nguồn; b) vào một lần khởi tạo mô-đun mới; c) do được kích hoạt bởi yêu cầu tự kiểm thử định kỳ.

Bảng 315 - VE và TE của AS10.28

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.28 ISO/IEC 19790:2025, 7.10.4.2	Nếu kết quả đầu ra được tính toán không bằng với kết quả đã biết trước, bài tự kiểm thử thuật toán mật mã dựa trên kết quả đã biết trước sẽ thất bại.
Thông tin bắt buộc từ nhà cung cấp	
VE10.28.01	Tài liệu do nhà cung cấp cung cấp phải quy định phương pháp được sử dụng để so sánh kết quả đầu ra được tính toán với kết quả đã biết trước.
VE10.28.02	Tài liệu phải trình bày sự chuyển đổi sang một trạng thái lỗi và sự xuất hiện của một chỉ báo lỗi khi hai kết quả đầu ra không bằng nhau.
Quy trình kiểm thử bắt buộc	
TE10.28.01	Kiểm thử viên phải xác minh rằng tài liệu nhất quán với việc triển khai thực tế của mô-đun mật mã.
TE10.28.02	Khẳng định này được kiểm thử theo TE10.07.02, TE10.10.01, TE10.10.02, và TE10.10.03.

Bảng 316 - VE và TE của AS10.29

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.29 ISO/IEC 19790:2025, 7.10.4.2	Một bài tự kiểm thử thuật toán mật mã do mô-đun hỗ trợ, tối thiểu phải sử dụng bất kỳ độ dài khóa, độ dài modulo, số nguyên tố DSA, hoặc đường cong đã được phê duyệt nào mà mô-đun có hỗ trợ.
Thông tin bắt buộc từ nhà cung cấp	
VE10.29.01	Tài liệu do nhà cung cấp cung cấp phải cung cấp đặc tả của từng bài tự kiểm thử thuật toán mật mã có điều kiện được triển khai bởi mô-đun.
Quy trình kiểm thử bắt buộc	
TE10.29.01	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng mỗi bài kiểm thử thuật toán mật mã có điều kiện, tối thiểu, sử dụng ít nhất một trong các độ dài khóa, độ dài modulo, số nguyên tố DSA, hoặc các đường cong đã phê duyệt được hỗ trợ bởi mô-đun.

Bảng 317 - VE và TE của AS10.30

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.30 ISO/IEC 19790:2025, 7.10.4.2	Nếu một thuật toán mật mã quy định nhiều chế độ (ví dụ: ECB, CBC, v.v.), tối thiểu phải chọn một chế độ cho bài tự kiểm thử được mô-đun hỗ trợ.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.29.	

Bảng 318 - VE và TE của AS10.31

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.31 ISO/IEC 19790:2025, 7.10.4.2	Các hàm một chiều: (Các) vector kiểm thử đầu vào phải tạo ra đầu ra giống hệt với đầu ra mong đợi [ví dụ: hàm băm, hàm băm có khóa, xác thực thông điệp, RBG (đầu vào entropy cố định), thỏa thuận SSP].
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.28.	

Bảng 319 - VE và TE của AS10.32

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.32 ISO/IEC 19790:2025, 7.10.4.2	Đối với các hàm khả nghịch: Hàm chiều thuận và chiều nghịch phải được tự kiểm thử trước khi mỗi hàm được sử dụng riêng biệt (ví dụ: mã hóa và giải mã khóa đối xứng, mã hóa và giải mã nhằm truyền tải tham số an toàn nhạy cảm, tạo và xác minh chữ ký số).
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.28.	

Bảng 320 - VE và TE của AS10.33

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
--	--

TCVN 12211:2026

AS10.33 ISO/IEC 19790:2025, 7.10.4.2	Nếu các kết quả đầu ra không bằng nhau, bài tự kiểm thử thuật toán mật mã theo hình thức so sánh sẽ thất bại.
Thông tin bắt buộc từ nhà cung cấp	
VE10.33.01	Nhà cung cấp phải mô tả bài tự kiểm thử thuật toán mật mã theo hình thức so sánh đã được triển khai.
VE10.33.02	Yêu cầu do nhà cung cấp cung cấp được quy định theo VE10.28.01 dành cho yêu cầu của nhà cung cấp.
Quy trình kiểm thử bắt buộc	
TE10.33.01	Kiểm thử viên phải xác minh xem tài liệu của bài kiểm thử so sánh có bao gồm: a) việc sử dụng hai hoặc nhiều bản triển khai thuật toán mật mã độc lập; b) việc liên tục so sánh các kết quả đầu ra của bản triển khai thuật toán mật mã; c) sự chuyển đổi sang một trạng thái lỗi và xuất ra một chỉ báo lỗi khi hai kết quả đầu ra không bằng nhau.
TE10.33.02	Bằng cách kiểm tra mã lệnh và tài liệu thiết kế, kiểm thử viên phải xác minh rằng mô-đun có thực hiện các bước đã được lập tài liệu để thực hiện bài kiểm thử so sánh.

Bảng 321 - VE và TE của AS10.34

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.34 ISO/IEC 19790:2025, 7.10.4.2	Nếu phát hiện một lỗi, bài tự kiểm thử thuật toán mật mã nhằm phát hiện lỗi sẽ thất bại. VÍ DỤ: Bài kiểm thử phát hiện lỗi của RBG sẽ xử lý một lỗi xảy ra ở nguồn entropy bên trong phần triển khai của RBG.
Thông tin bắt buộc từ nhà cung cấp	
VE10.34.01	Nhà cung cấp phải quy định xem một bài kiểm thử phát hiện lỗi có được sử dụng để thử nghiệm thuật toán mật mã của mô-đun nhằm bổ sung cho một bài kiểm thử biết trước kết quả hay một bài kiểm thử so sánh hay không.
Quy trình kiểm thử bắt buộc	
TE10.34.01	Kiểm thử viên phải xác minh rằng tài liệu của bài kiểm thử phát hiện lỗi có bao gồm: a) mô tả từng điều kiện lỗi trong phần đặc tả/triển khai thuật toán mật mã; b) đặc tả về chỉ báo lỗi (nội bộ) tương ứng đối với từng điều kiện lỗi; c) lý do khẳng định mỗi điều kiện lỗi đều được thử nghiệm trong bài kiểm thử phát hiện lỗi.
TE10.34.02	Kiểm thử viên phải xác minh rằng tài liệu là nhất quán với việc triển khai thực tế của mô-đun mật mã.
TE10.34.03	Khẳng định này được kiểm thử theo TE10.07.02, TE10.07.03, TE10.11.02, TE10.11.03, TE10.12.01, và TE10.12.02.

6.10.4.3 Kiểm thử tính nhất quán theo cặp có điều kiện

Bảng 322 - VE và TE của AS10.35

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4
--

AS10.35 ISO/IEC 19790:2025, 7.10.4.3	Nếu một mô-đun mật mã tạo ra các cặp khóa phi đối xứng, một bài kiểm thử tính nhất quán theo cặp phải được thực hiện đối với mỗi cặp khóa phi đối xứng được tạo ra như tham chiếu trong ISO/IEC 19790:2025, Phụ lục C đối với thuật toán mật mã áp dụng tương ứng.
Thông tin bắt buộc từ nhà cung cấp	
VE10.35.01	Nếu các cặp khóa công khai hoặc khóa riêng được sử dụng để thực hiện việc truyền tải khóa đã phê duyệt, hoặc một mật mã phi đối xứng, tài liệu do nhà cung cấp cung cấp phải mô tả bài kiểm thử tính nhất quán theo cặp. Bài kiểm thử này bao gồm việc áp dụng khóa công khai vào một giá trị dạng rõ hoặc vào một thông điệp đã được mã hóa. Bản mã thu được phải được so sánh với bản rõ ban đầu để xác minh rằng chúng khác nhau. a) Nếu hai giá trị này bằng nhau, thì mô-đun mật mã phải bước vào một trạng thái lỗi và xuất ra một chỉ báo lỗi thông qua giao diện trạng thái. b) Nếu hai giá trị này khác nhau, thì khóa bí mật phải được áp dụng vào bản mã. Nếu kết quả không bằng với bản rõ ban đầu, thì bài kiểm thử tính nhất quán theo cặp sẽ thất bại.
VE10.35.02	Nếu các cặp khóa công khai hoặc khóa riêng chỉ được sử dụng cho việc tính toán hoặc xác minh chữ ký số, tài liệu do nhà cung cấp cung cấp phải mô tả bài kiểm thử tính nhất quán theo cặp thông qua việc tính toán và xác minh một chữ ký. Nếu không thể xác minh được chữ ký, bài kiểm thử tính nhất quán theo cặp sẽ thất bại.
VE10.35.03	Nếu các cặp khóa công khai hoặc khóa riêng được sử dụng để thực hiện thỏa thuận SSP, tài liệu do nhà cung cấp cung cấp phải mô tả bài kiểm thử tính nhất quán theo cặp. Tài liệu do nhà cung cấp cung cấp phải xác định các thuật toán tiên quyết của thỏa thuận SSP đó. Bài kiểm thử này phải bao gồm việc áp dụng cặp khóa để xem liệu nó có vượt qua bài kiểm thử tính nhất quán theo cặp hay không bằng cách thử nghiệm các thuật toán tiên quyết đã được triển khai. Ví dụ: Thỏa thuận khóa Diffie-Hellman sử dụng nguyên thủy mật mã trường hữu hạn vốn phổ biến đối với Thuật toán chữ ký số (DSA).
Quy trình kiểm thử bắt buộc	
TE10.35.01	Nếu các cặp khóa công khai hoặc khóa riêng được sử dụng để thực hiện một phương pháp truyền tải khóa đã phê duyệt, hoặc một mật mã phi đối xứng, kiểm thử viên phải xác minh rằng việc triển khai bài kiểm thử tính nhất quán theo cặp, như quy định tại VE10.35.01, là nhất quán với tài liệu do nhà cung cấp cung cấp bằng cách kiểm tra mã lệnh và tài liệu thiết kế.
TE10.35.02	Nếu các cặp khóa công khai hoặc khóa riêng được sử dụng cho việc tính toán hoặc xác minh chữ ký số, thì kiểm thử viên phải xác minh rằng việc triển khai bài kiểm thử tính nhất quán theo cặp như định nghĩa tại VE10.35.02 là nhất quán với tài liệu do nhà cung cấp cung cấp bằng cách kiểm tra mã lệnh và tài liệu thiết kế.
TE10.35.03	Nếu các cặp khóa công khai hoặc khóa riêng được sử dụng để thực hiện thỏa thuận SSP, thì kiểm thử viên phải xác minh rằng việc triển khai bài kiểm thử tính nhất quán theo cặp như định nghĩa tại VE10.35.03 là nhất quán với tài liệu do nhà cung cấp cung cấp bằng cách kiểm tra mã lệnh và tài liệu thiết kế.
TE10.35.04	Nếu có thể, kiểm thử viên phải sửa đổi một trong các khóa của các cặp khóa trước khi bài kiểm thử tính nhất quán theo cặp được thực hiện. Bài kiểm thử bị coi là thất bại nếu bài kiểm thử tính nhất quán theo cặp không phát hiện ra sự sửa đổi đó.

6.10.4.4 Kiểm thử nạp phần mềm/phần sụn có điều kiện

Bảng 323 - VE và TE của AS10.36

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.36 ISO/IEC 19790:2025, 7.10.4.4	Nếu một mô-đun mật mã có khả năng nạp phần mềm, phần sụn, hoặc dòng bit từ một nguồn bên ngoài, thì các yêu cầu sau đây, bên cạnh những yêu cầu trong ISO/IEC 19790:2025, 7.4.3.4, phải được thực hiện:
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 324 - VE và TE của AS10.37

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.37 ISO/IEC 19790:2025, 7.10.4.4	Mô-đun mật mã phải triển khai một kỹ thuật xác thực dữ liệu đã phê duyệt để kiểm chứng tính xác thực của phần mềm, phần sụn, hoặc dòng bit được nạp vào;
Thông tin bắt buộc từ nhà cung cấp	
VE10.37.01	Tài liệu do nhà cung cấp cung cấp phải mô tả kỹ thuật xác thực đã phê duyệt được sử dụng để bảo vệ tính toàn vẹn của tất cả các thành phần phần mềm, phần sụn và dòng bit được nạp từ bên ngoài.
VE10.37.02	Nếu mô-đun triển khai một kỹ thuật xác thực đã phê duyệt, nhà cung cấp phải cung cấp chứng chỉ xác nhận nếu có hoặc cam kết của nhà cung cấp như quy định tại VE02.18.01 và VE02.18.03.
VE10.37.03	Nhà cung cấp phải cung cấp tài liệu quy định cách khóa xác thực tham chiếu được nạp độc lập vào mô-đun trước quá trình nạp phần mềm, phần sụn hoặc dòng bit.
VE10.37.04	Tài liệu do nhà cung cấp cung cấp phải mô tả các cơ chế nhằm đảm bảo rằng phần mềm, phần sụn, hoặc dòng bit đã được nạp sẽ không thể được sử dụng nếu bài kiểm thử nạp phần mềm/phần sụn thất bại.
Quy trình kiểm thử bắt buộc	
TE10.37.01	Kiểm thử viên phải xác định, từ tài liệu do nhà cung cấp cung cấp, xem kỹ thuật xác thực đã phê duyệt nào được sử dụng cho bài kiểm thử nạp phần mềm/phần sụn.
TE10.37.02	Kiểm thử viên phải xác minh rằng nếu một kỹ thuật xác thực đã phê duyệt được triển khai, nhà cung cấp đã cung cấp chứng chỉ xác nhận nếu có hoặc cam kết của nhà cung cấp như quy định tại VE02.18.01 và VE02.18.03.
TE10.37.03	Nếu mô-đun triển khai một kỹ thuật xác thực đã phê duyệt cho bài kiểm thử nạp phần mềm/phần sụn, kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp về bài kiểm thử nạp phần mềm/phần sụn bao gồm: a) đặc tả của kỹ thuật xác thực đã phê duyệt được triển khai; b) việc nhận diện phần mềm và phần sụn được bảo vệ bằng kỹ thuật xác thực đã phê duyệt; c) việc tính toán kỹ thuật xác thực đã phê duyệt khi phần mềm và phần sụn được nạp; d) việc xác minh kỹ thuật xác thực đã phê duyệt khi bài kiểm thử nạp được khởi tạo; e) sự thất bại của quá trình tự kiểm thử khi quá trình kiểm chứng kỹ thuật

	xác thực đã phê duyệt thất bại.
TE10.37.04	Bằng cách kiểm tra mã lệnh và tài liệu thiết kế, kiểm thử viên phải xác minh rằng việc triển khai bài kiểm thử nạp phần mềm/phần sụn là nhất quán với TE10.37.01, TE10.37.02, và TE10.37.03.
TE10.37.05	Kiểm thử viên phải thử nghiệm mô-đun bằng cách sửa đổi phần mềm hoặc phần sụn dự kiến nạp, hoặc bằng cách sửa đổi cơ chế xác thực được triển khai và kích hoạt quá trình tự kiểm thử. Sau đó, kiểm thử viên phải quan sát đầu ra từ giao diện đầu ra trạng thái hoặc thông qua thủ tục được lập tài liệu trong chính sách an toàn phi độc quyền để xác định xem mô-đun có bước vào một trạng thái lỗi hay không. Nếu không có chỉ báo nào được xuất ra, dù là trực tiếp hay ngầm định, cho thấy rằng bài kiểm thử nạp phần mềm/phần sụn đã thất bại, thì khẳng định này bị coi là thất bại. Nếu kiểm thử viên không thể sửa đổi phần mềm hoặc phần sụn dự kiến nạp, hoặc cơ chế xác thực được triển khai, thì nhà cung cấp phải cung cấp một cơ sở hợp lý cho kiểm thử viên về lý do tại sao bài kiểm thử này không thể được thực hiện.
TE10.37.06	Kiểm thử viên phải dùng thử mô-đun mật mã, với việc sửa đổi phần mềm hoặc phần sụn dự kiến nạp, sửa đổi khóa xác thực tham chiếu, hoặc nỗ lực vượt qua cơ chế xác thực được triển khai, và phải khởi tạo bài kiểm thử nạp phần mềm/phần sụn. Sau khi bài tự kiểm thử thất bại, kiểm thử viên phải xác minh rằng phần mềm hoặc phần sụn đã nạp không thể được sử dụng và thông tin về phiên bản của mô-đun không bị thay đổi.
TE10.37.07	Bằng cách kiểm tra mã lệnh và tài liệu thiết kế, kiểm thử viên phải xác minh rằng khóa xác thực tham chiếu được nạp hoàn toàn độc lập với quá trình nạp phần mềm hoặc phần sụn.
TE10.37.08	Bằng cách kiểm tra mã lệnh và tài liệu thiết kế, kiểm thử viên phải xác minh rằng bài kiểm thử nạp phần mềm/phần sụn sẽ thất bại nếu không nạp khóa xác thực tham chiếu trước khi nạp phần mềm hoặc phần sụn.
TE10.37.09	Nếu mô-đun cho phép người vận hành nạp khóa xác thực tham chiếu, kiểm thử viên phải dùng thử mô-đun mật mã, mà không cần nạp trước khóa xác thực tham chiếu đó, và phải khởi tạo bài kiểm thử nạp phần mềm/phần sụn. Nếu bài kiểm thử nạp phần mềm/phần sụn đạt, khẳng định này bị coi là thất bại. Nếu khóa được nạp từ nhà máy không thể bị thay thế, khẳng định này đạt.

Bảng 325 - VE và TE của AS10.38

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.38 ISO/IEC 19790:2025, 7.10.4.4	Khóa xác thực tham chiếu phải được nạp độc lập vào mô-đun trước khi tiến hành nạp phần mềm, phần sụn, hoặc dòng bit;
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.37.	

Bảng 326 - VE và TE của AS10.39

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.39 ISO/IEC 19790:2025,	Kỹ thuật xác thực dữ liệu đã phê duyệt được áp dụng phải được kiểm chứng thành công hoặc {bài kiểm thử nạp phần mềm/phần sụn sẽ thất bại.}

7.10.4.4	
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.37.	

Bảng 327 - VE và TE của AS10.40

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.40 ISO/IEC 19790:2025, 7.10.4.4	{bài kiểm thử nạp phần mềm/phần sụn sẽ thất bại.} hoặc bài kiểm thử nạp phần mềm/phần sụn sẽ thất bại.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.37.	

Bảng 328 - VE và TE của AS10.41

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.41 ISO/IEC 19790:2025, 7.10.4.4	Phần mềm, phần sụn, hoặc dòng bit đã được nạp sẽ không được sử dụng nếu bài kiểm thử nạp phần mềm/phần sụn thất bại.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.37.	

Bảng 329 - VE và TE của AS10.42

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.42 ISO/IEC 19790:2025, 7.10.4.4	Bài kiểm thử nạp phần mềm/phần sụn phải được thực hiện và vượt qua thành công trước lần thực thi đầu tiên của bất kỳ thành phần phần mềm, phần sụn hoặc dòng bit mới nào.
Thông tin bắt buộc từ nhà cung cấp	
VE10.42.01	Nhà cung cấp phải cung cấp tài liệu quy định cách bài kiểm thử nạp phần mềm/phần sụn được thực hiện và vượt qua thành công trước lần thực thi đầu tiên của bất kỳ thành phần phần mềm, phần sụn hoặc dòng bit mới nào.
Quy trình kiểm thử bắt buộc	
TE10.42.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định cách bài kiểm thử nạp phần mềm/phần sụn được thực hiện và vượt qua thành công trước lần thực thi đầu tiên của bất kỳ thành phần phần mềm, phần sụn hoặc dòng bit mới nào.
TE10.42.02	Kiểm thử viên phải kiểm tra mô-đun để xác minh rằng bài kiểm thử nạp phần mềm/phần sụn được thực hiện và vượt qua thành công trước lần thực thi đầu tiên của bất kỳ thành phần phần mềm, phần sụn hoặc dòng bit mới nào.

6.10.4.5 Kiểm thử nhập thủ công có điều kiện**Bảng 330 - VE và TE của AS10.43**

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4
--

AS10.43 ISO/IEC 19790:2025, 7.10.4.5	Nếu các SSP hoặc thành phần khóa được nhập thủ công trực tiếp vào một mô-đun mật mã hoặc nếu một lỗi từ phía người vận hành con người có thể dẫn đến việc nhập sai giá trị dự kiến, thì các bài kiểm thử nhập thủ công sau đây phải được thực hiện:
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	

Bảng 331 - VE và TE của AS10.44

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.44 ISO/IEC 19790:2025, 7.10.4.5	SSP hoặc các thành phần khóa phải được áp dụng một mã phát hiện sai (EDC), hoặc {phải được nhập bằng cách sử dụng các mục nhập trùng lặp}.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.47.	

Bảng 332 - VE và TE của AS10.45

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.45 ISO/IEC 19790:2025, 7.10.4.5	{SSP hoặc các thành phần khóa phải được áp dụng một mã phát hiện sai (EDC),} hoặc phải được nhập bằng cách sử dụng các mục nhập trùng lặp.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.47.	

Bảng 333 - VE và TE của AS10.46

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.46 ISO/IEC 19790:2025, 7.10.4.5	Nếu một EDC được sử dụng, EDC phải có độ dài ít nhất là 16 bit.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.47.	

Bảng 334 - VE và TE của AS10.47

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.47 ISO/IEC 19790:2025, 7.10.4.5	Nếu không thể xác minh EDC, hoặc các mục nhập trùng lặp không khớp với nhau, bài kiểm thử sẽ thất bại.
Thông tin bắt buộc từ nhà cung cấp	
VE10.47.01	Nhà cung cấp phải lập tài liệu về bài kiểm thử nhập thủ công. Tùy thuộc vào việc sử dụng mã phát hiện sai hay các mục nhập trùng lặp của các SSP hoặc thành phần khóa, bài kiểm thử nhập thủ công phải bao gồm các nội dung sau: a) mã phát hiện sai (EDC): 1) mô tả về thuật toán tính toán EDC;

	2) mô tả về quá trình xác minh; 3) các kết quả đầu ra dự kiến cho sự thành công hoặc thất bại của bài kiểm thử; b) các mục nhập trùng lặp: 1) mô tả về quá trình xác minh; 2) các kết quả đầu ra dự kiến cho sự thành công hoặc thất bại của bài kiểm thử.
VE10.47.02	Nếu EDC được liên kết với SSP hoặc các thành phần khóa, thì tài liệu do nhà cung cấp cung cấp mô tả định dạng của SSP hoặc các thành phần khóa (xem AS09.03) phải bao gồm các trường dành cho EDC.
Quy trình kiểm thử bắt buộc	
TE10.47.01	Kiểm thử viên phải xác minh từ tài liệu của nhà cung cấp xem phương pháp nào được sử dụng cho bài kiểm thử nhập thủ công (mã phát hiện sai hay các mục nhập trùng lặp). Dựa trên phương pháp được sử dụng, kiểm thử viên phải kiểm tra tài liệu, mã lệnh, hoặc tài liệu thiết kế do nhà cung cấp cung cấp có quy định việc triển khai bài kiểm thử nhập thủ công để xác minh xem các thông tin sau có được bao gồm hay không: a) mã phát hiện sai: 1) định dạng SSP hoặc thành phần khóa cho tất cả các SSP hoặc thành phần khóa được nhập thủ công, bao gồm các trường dành cho EDC (xem AS09.03); 2) mô tả thuật toán EDC; 3) mô tả quá trình xác minh EDC; 4) tất cả các kết quả đầu ra dự kiến cho sự thành công hoặc thất bại của bài kiểm thử; b) các mục nhập trùng lặp của SSP hoặc thành phần khóa: 1) các mục nhập trùng lặp đối với tất cả các SSP và thành phần khóa được nhập thủ công; 2) mô tả quá trình xác minh mục nhập trùng lặp; 3) tất cả các kết quả đầu ra dự kiến cho sự thành công hoặc thất bại của bài kiểm thử.
TE10.47.02	Đối với các bài kiểm thử nhập thủ công sử dụng một EDC, kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp và kiểm tra mô-đun để xác minh rằng định dạng của SSP hoặc các thành phần khóa có bao gồm các trường dành cho EDC và EDC đó có độ dài ít nhất là 16 bit.

TE10.47.03	Đối với các bài kiểm thử nhập thủ công sử dụng một EDC, kiểm thử viên phải thực hiện các bài kiểm thử sau: a) Kiểm thử viên phải nhập từng SSP được nhập thủ công và xác minh rằng thủ tục được sử dụng để nhập từng SSP tuân thủ đúng với thủ tục đã được lập tài liệu, bao gồm cả hình thức của các SSP tại thời điểm chúng được nhập vào. b) Kiểm thử viên phải nhập từng loại SSP được nhập thủ công mà không mắc bất kỳ lỗi nào và phải xác minh giao diện đầu ra trạng thái. Nếu không có chỉ báo nào được xuất ra, hoặc nếu chỉ báo đó không khớp với chỉ báo đã được lập tài liệu cho sự thành công của bài kiểm thử nhập thủ công, bài kiểm thử đó đã thất bại. c) Kiểm thử viên phải thử thực hiện các hoạt động mật mã với mỗi SSP đã được nhập để xác minh rằng nó đã được nhập chính xác. d) Kiểm thử viên phải sửa đổi hoặc là EDC liên kết với mỗi SSP được nhập thủ công hoặc là chính SSP đó và phải nhập chúng vào mô-đun. Kiểm thử viên phải xác minh chỉ báo được xuất ra từ giao diện đầu ra trạng thái; nếu không có chỉ báo nào được xuất ra, hoặc chỉ báo đó không khớp với chỉ báo đã được lập tài liệu cho sự thất bại của bài kiểm thử nhập thủ công, bài kiểm thử đó đã thất bại. e) Kiểm thử viên phải thử thực hiện các hoạt động mật mã với mỗi SSP chưa được nhập thành công. Mọi hoạt động sử dụng từng SSP đều bắt buộc phải thất bại, qua đó xác minh rằng SSP đó chưa được nhập vào.
TE10.47.04	Đối với các bài kiểm thử nhập thủ công sử dụng các mục nhập trùng lặp của các SSP hoặc thành phần khóa, kiểm thử viên phải thực hiện các bài kiểm thử sau: a) Kiểm thử viên phải nhập từng loại SSP được nhập thủ công mà không mắc bất kỳ lỗi nào và phải xác minh giao diện đầu ra trạng thái. Nếu không có chỉ báo nào được xuất ra, hoặc nếu chỉ báo đó không khớp với chỉ báo đã được lập tài liệu cho sự thành công của bài kiểm thử nhập thủ công, bài kiểm thử đó đã thất bại. b) Kiểm thử viên phải thử thực hiện các hoạt động mật mã với mỗi SSP đã được nhập để xác minh rằng nó đã được nhập chính xác. c) Kiểm thử viên phải sửa đổi một trong các SSP được nhập thủ công, hoặc là mục nhập trùng lặp thứ nhất hoặc thứ hai, và phải nhập chúng vào mô-đun. Kiểm thử viên phải xác minh chỉ báo được xuất ra từ giao diện đầu ra trạng thái; nếu không có chỉ báo nào được xuất ra, hoặc chỉ báo đó không khớp với chỉ báo đã được lập tài liệu cho sự thất bại của bài kiểm thử nhập thủ công, bài kiểm thử đó đã thất bại. d) Kiểm thử viên phải thử thực hiện các hoạt động mật mã với mỗi SSP chưa được nhập thành công. Mọi hoạt động sử dụng từng SSP đều bắt buộc phải thất bại, qua đó xác minh rằng SSP đó chưa được nhập vào.

6.10.4.6 Kiểm thử việc bỏ qua có điều kiện

Bảng 335 - VE và TE của AS10.48

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.48 ISO/IEC 19790:2025, 7.10.4.6	Nếu một mô-đun mật mã triển khai một khả năng bỏ qua nơi các dịch vụ có thể được cung cấp mà không cần quá trình xử lý mật mã (ví dụ: truyền tải dữ liệu dạng rõ thông qua mô-đun), thì bộ các bài kiểm thử bỏ qua sau đây phải được thực hiện nhằm đảm bảo rằng một điểm lỗi duy nhất của các thành phần mô-đun sẽ không dẫn đến việc vô tình xuất ra dữ liệu dạng rõ:
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.49, AS10.50, AS10.51 và AS10.52.	

Bảng 336 - VE và TE của AS10.49

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.49 ISO/IEC 19790:2025, 7.10.4.6	Một mô-đun mật mã phải kiểm tra sự hoạt động chính xác của các dịch vụ cung cấp quá trình xử lý mật mã khi có sự chuyển đổi giữa một dịch vụ bỏ qua độc quyền và một dịch vụ mật mã độc quyền;
Thông tin bắt buộc từ nhà cung cấp	
VE10.49.01	Nếu mô-đun mật mã triển khai một dịch vụ bỏ qua, thì nhà cung cấp phải triển khai một bài kiểm thử bỏ qua để xác minh sự hoạt động chính xác của dịch vụ mật mã khi có sự chuyển đổi giữa một dịch vụ bỏ qua độc quyền và một dịch vụ mật mã độc quyền.
VE10.49.02	Nhà cung cấp phải cung cấp một mô tả về bài kiểm thử bỏ qua. Bài kiểm thử bỏ qua phải chứng minh được rằng, khi chuyển sang một dịch vụ mật mã độc quyền, mô-đun không xuất ra thông tin dạng rõ.
Quy trình kiểm thử bắt buộc	
TE10.49.01	Kiểm thử viên phải xác minh rằng mô-đun có triển khai một bài kiểm thử bỏ qua để xác minh sự hoạt động chính xác của dịch vụ mật mã khi có sự chuyển đổi giữa một dịch vụ bỏ qua độc quyền và một dịch vụ mật mã độc quyền.
TE10.49.02	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp là nhất quán với việc triển khai bài kiểm thử bỏ qua thông qua việc xem xét mã nguồn và tài liệu thiết kế.
TE10.49.03	Kiểm thử viên phải chuyển đổi mô-đun từ dịch vụ bỏ qua độc quyền sang dịch vụ mật mã độc quyền và xác minh rằng thông tin dạng rõ không bị xuất ra.

Bảng 337 - VE và TE của AS10.50

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.50 ISO/IEC 19790:2025, 7.10.4.6	Nếu một mô-đun mật mã có thể tự động luân phiên giữa một dịch vụ bỏ qua và một dịch vụ mật mã, cung cấp một số dịch vụ có kèm quá trình xử lý mật mã và một số dịch vụ không kèm quá trình xử lý mật mã, thì mô-đun phải kiểm tra sự hoạt động chính xác của các dịch vụ cung cấp quá trình xử lý mật mã khi cơ chế chi phối thủ tục chuyển đổi bị sửa đổi (ví dụ: một bảng nguồn/dịch địa chỉ IP);
Thông tin bắt buộc từ nhà cung cấp	
VE10.50.01	Nếu mô-đun mật mã được thiết kế để tự động luân phiên giữa một dịch vụ bỏ qua và một dịch vụ mật mã, thì nhà cung cấp phải triển khai một bài kiểm thử bỏ qua để xác minh sự hoạt động chính xác của dịch vụ mật mã khi cơ chế chi phối thủ tục chuyển đổi bị sửa đổi.
VE10.50.02	Nhà cung cấp phải cung cấp một mô tả về bài kiểm thử đó. Bài kiểm thử bỏ qua phải đảm bảo rằng khi cơ chế chi phối thủ tục chuyển đổi bị sửa đổi:

	a) cơ chế được xác minh là chưa bị thay đổi kể từ lần sửa đổi cuối cùng. Nếu cơ chế đã bị thay đổi, mô-đun mật mã phải bước vào một trạng thái lỗi và xuất ra một chỉ báo lỗi tới giao diện trạng thái; b) sự hoạt động chính xác của dịch vụ mật mã được xác minh bằng cách chứng minh rằng mô-đun không xuất ra thông tin dạng rõ. Bài kiểm thử bỏ qua thất bại nếu dữ liệu lẽ ra phải được xử lý bằng mật mã lại bị xuất ra ở dạng rõ.
Quy trình kiểm thử bắt buộc	
TE10.50.01	Kiểm thử viên phải xác minh rằng mô-đun có triển khai một bài kiểm thử bỏ qua để xác minh sự hoạt động chính xác của dịch vụ mật mã khi cơ chế chi phối thủ tục chuyển đổi bị sửa đổi.
TE10.50.02	Kiểm thử viên phải xác minh rằng mô tả về bài kiểm thử là nhất quán với việc triển khai bài kiểm thử bỏ qua thông qua việc xem xét mã nguồn và tài liệu thiết kế.
TE10.50.03	Kiểm thử viên phải xác minh sự hoạt động chính xác của bài kiểm thử bỏ qua bằng cách: a) xác minh rằng cơ chế chi phối thủ tục chuyển đổi có kiểm tra nhằm đảm bảo rằng không có sự thay đổi nào đối với cơ chế diễn ra kể từ lần sửa đổi cuối cùng. Kiểm thử viên sẽ lập tài liệu về phương pháp được sử dụng. Nếu thiết kế cho phép, kiểm thử viên phải sửa đổi cơ chế để thử nghiệm phương pháp được sử dụng; b) sửa đổi cơ chế chi phối thủ tục chuyển đổi nhằm xác minh sự hoạt động chính xác của cơ chế đó và xác minh sự hoạt động chính xác của dịch vụ mật mã thông qua việc xác minh rằng thông tin dạng rõ không bị xuất ra.

Bảng 338 - VE và TE của AS10.51

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.51 ISO/IEC 19790:2025, 7.10.4.6	Nếu một mô-đun mật mã duy trì thông tin nội bộ chi phối khả năng bỏ qua, thì mô-đun phải xác minh tính toàn vẹn của thông tin chi phối đó thông qua một kỹ thuật toàn vẹn đã phê duyệt ngay trước khi sửa đổi thông tin chi phối đó, và {Ngoài các yêu cầu tại mức an toàn 1 và 2, mô-đun phải thực hiện các quá trình tự kiểm thử thuật toán mật mã trước khi vận hành hoặc có điều kiện một cách lặp lại và tự động, theo một khoảng thời gian xác định, mà không cần đầu vào hay kiểm soát từ bên ngoài.}
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.52.	

Bảng 339 - VE và TE của AS10.52

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.52 ISO/IEC 19790:2025, 7.10.4.6	Nếu một mô-đun mật mã duy trì thông tin nội bộ chi phối khả năng bỏ qua, thì {Nếu khoảng thời gian vận hành của một mô-đun giữa việc thiết lập lại, khởi động lại, hoặc chu kỳ nguồn là đủ ngắn, các yêu cầu tự kiểm thử định kỳ có thể được bỏ qua; trong trường hợp này, chính sách an toàn phải quy định khoảng thời gian vận hành dự kiến của mô-đun, và do đó các tự kiểm thử định kỳ là không bắt buộc.} và phải tạo ra một giá trị toàn vẹn mới sử dụng kỹ thuật toàn vẹn đã phê duyệt ngay sau khi sửa đổi.
Thông tin bắt buộc từ nhà cung cấp	

VE10.52.01	Tài liệu do nhà cung cấp cung cấp phải quy định phương pháp sửa đổi thông tin nội bộ chi phối khả năng bỏ qua.
VE10.52.02	Nhà cung cấp phải cung cấp một đặc tả chi tiết về thông tin nội bộ chi phối khả năng bỏ qua, trình tự nội bộ để cập nhật thông tin đó, và cơ chế để duy trì tính toàn vẹn của thông tin đó sử dụng một kỹ thuật toàn vẹn đã phê duyệt.
Quy trình kiểm thử bắt buộc	
TE10.52.01	Bằng cách kiểm tra mã lệnh và tài liệu thiết kế, kiểm thử viên phải xác minh rằng thông tin chi phối được duy trì trong mô-đun mật mã là nhất quán với tài liệu do nhà cung cấp cung cấp.
TE10.52.02	Bằng cách kiểm tra mã lệnh và tài liệu thiết kế, kiểm thử viên phải xác minh rằng trình tự nội bộ để cập nhật thông tin chi phối là nhất quán với tài liệu do nhà cung cấp cung cấp.
TE10.52.03	Bằng cách kiểm tra mã lệnh và tài liệu thiết kế, kiểm thử viên phải xác minh rằng cơ chế duy trì tính toàn vẹn của thông tin chi phối là nhất quán với tài liệu do nhà cung cấp cung cấp.

6.10.4.7 Kiểm thử chức năng trọng yếu có điều kiện

Bảng 340 - VE và TE của AS10.53

Tự kiểm thử có điều kiện - mức 1, 2, 3 và 4	
AS10.53 ISO/IEC 19790:2025, 7.10.4.7	Có thể có các chức năng an toàn khác mang tính trọng yếu đối với sự hoạt động an toàn của mô-đun mật mã mà bắt buộc phải được thử nghiệm thông qua một bài tự kiểm thử có điều kiện.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.23.	

6.10.4.8 Tự kiểm thử định kỳ

6.10.4.8.1 Mức an toàn 1 và 2

Bảng 341 - VE và TE của AS10.54

Tự kiểm thử có điều kiện - mức 1 và 2	
AS10.54 ISO/IEC 19790:2025, 7.10.4.8.1	Một mô-đun mật mã phải cho phép người vận hành kích hoạt các quá trình tự kiểm thử thuật toán mật mã trước khi vận hành hoặc có điều kiện theo yêu cầu nhằm phục vụ cho việc thử nghiệm mô-đun định kỳ.
Thông tin bắt buộc từ nhà cung cấp	
VE10.54.01	Nhà cung cấp phải mô tả thủ tục thông qua đó người vận hành có thể kích hoạt các quá trình tự kiểm thử trước khi vận hành theo yêu cầu nhằm phục vụ cho việc thử nghiệm mô-đun định kỳ. Tất cả các quá trình tự kiểm thử trước khi vận hành đều phải được bao gồm.
VE10.54.02	Nhà cung cấp phải mô tả thủ tục thông qua đó người vận hành có thể kích hoạt các quá trình tự kiểm thử thuật toán mật mã có điều kiện theo yêu cầu nhằm phục vụ cho việc thử nghiệm mô-đun định kỳ. Tối thiểu, các bài tự kiểm thử thuật toán mật mã có điều kiện phải được bao gồm.
Quy trình kiểm thử bắt buộc	
TE10.54.01	Kiểm thử viên phải kiểm tra tài liệu do nhà cung cấp cung cấp để xác minh rằng

	việc kích hoạt các bài tự kiểm thử trước khi vận hành theo yêu cầu đã được quy định cho tất cả các quá trình tự kiểm thử trước khi vận hành.
TE10.54.02	Kiểm thử viên phải kích hoạt các quá trình tự kiểm thử trước khi vận hành theo yêu cầu để xác minh rằng việc kích hoạt các quá trình tự kiểm thử trước khi vận hành theo yêu cầu là nhất quán với tài liệu do nhà cung cấp cung cấp.
TE10.54.03	Kiểm thử viên phải kích hoạt các quá trình tự kiểm thử thuật toán mật mã có điều kiện theo yêu cầu để xác minh rằng việc kích hoạt các quá trình tự kiểm thử thuật toán mật mã có điều kiện theo yêu cầu là nhất quán với tài liệu do nhà cung cấp cung cấp.

6.10.4.8.2 Mức an toàn 3 và 4

Bảng 342 - VE và TE của AS10.55

Tự kiểm thử có điều kiện - mức 3 và 4	
AS10.55 ISO/IEC 19790:2025, 7.10.4.8.2	Ngoài các yêu cầu tại mức an toàn 1 và 2, mô-đun phải thực hiện các quá trình tự kiểm thử thuật toán mật mã trước khi vận hành hoặc có điều kiện một cách lặp lại và tự động, theo một khoảng thời gian xác định, mà không cần đầu vào hay kiểm soát từ bên ngoài.
Thông tin bắt buộc từ nhà cung cấp	
VE10.55.01	Nhà cung cấp phải cung cấp tài liệu quy định cách thức các quá trình tự kiểm thử thuật toán mật mã trước khi vận hành hoặc có điều kiện được thực hiện lặp lại theo một khoảng thời gian xác định, một cách tự động, mà không cần đầu vào hay kiểm soát từ bên ngoài.
VE10.55.02	Tài liệu do nhà cung cấp cung cấp phải bao gồm đặc tả về chỉ báo trạng thái được sử dụng nhằm biểu thị rằng các hoạt động của mô-đun mật mã đang bị gián đoạn do quá trình tự kiểm thử thuật toán mật mã trước khi vận hành hoặc có điều kiện.
VE10.55.03	Chính sách an toàn phi độc quyền do nhà cung cấp cung cấp phải cung cấp thông tin về khoảng thời gian được xác định và bất kỳ điều kiện nào dẫn đến sự gián đoạn hoạt động của mô-đun trong khoảng thời gian nhằm lặp lại quá trình tự kiểm thử thuật toán mật mã trước khi vận hành hoặc có điều kiện.
Quy trình kiểm thử bắt buộc	
TE10.55.01	Kiểm thử viên phải xác minh, bằng cách kiểm tra mô-đun mật mã, rằng quá trình tự kiểm thử thuật toán mật mã trước khi vận hành hoặc có điều kiện được thực hiện lặp lại như được quy định trong VE10.55.01, VE10.55.02 và VE10.55.03.

Bảng 343 - VE và TE của AS10.56

Tự kiểm thử có điều kiện - mức 3 và 4	
AS10.56 ISO/IEC 19790:2025, 7.10.4.8.2	Khoảng thời gian và mọi điều kiện có thể dẫn đến sự gián đoạn các hoạt động của mô-đun trong thời gian nhằm lặp lại quá trình tự kiểm thử thuật toán mật mã trước khi vận hành hoặc có điều kiện phải được quy định trong chính sách an toàn.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS10.55.	

Bảng 344 - VE và TE của AS10.57

Tự kiểm thử có điều kiện - mức 3 và 4
--

TCVN 12211:2026

AS10.57 ISO/IEC 19790:2025, 7.10.4.8.2	Nếu khoảng thời gian vận hành của một mô-đun giữa việc thiết lập lại, khởi động lại, hoặc chu kỳ nguồn là đủ ngắn, các yêu cầu tự kiểm thử định kỳ có thể được bỏ qua; trong trường hợp này, chính sách an toàn phải lập tài liệu về khoảng thời gian vận hành dự kiến của mô-đun, và do đó các bài tự kiểm thử định kỳ là không bắt buộc.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	

6.11 Đảm bảo vòng đời

6.11.1 Yêu cầu chung về đảm bảo vòng đời

Bảng 345 - VE và TE của AS11.01

Yêu cầu chung về đảm bảo vòng đời - mức 1, 2, 3 và 4	
AS11.01 ISO/IEC 19790:2025, 7.11.1	Tài liệu về đảm bảo vòng đời được quy định tại ISO/IEC 19790:2025, A.2.10 phải được cung cấp.
Thông tin bắt buộc từ nhà cung cấp	
VE11.01.01	Nhà cung cấp phải cung cấp các yêu cầu về tài liệu như được quy định trong ISO/IEC 19790:2025, A.2.10.
Quy trình kiểm thử bắt buộc	
TE11.01.01	Kiểm thử viên phải xác minh rằng nhà cung cấp cung cấp tài liệu như quy định trong ISO/IEC 19790:2025, A.2.10.

6.11.2 Quản lý cấu hình

6.11.2.1 Mức an toàn 1 và 2

Bảng 346 - VE và TE của AS11.02

Quản lý cấu hình - mức 1, 2, 3 và 4	
AS11.02 ISO/IEC 19790:2025, 7.11.2.2	Các yêu cầu sau đây phải được áp dụng đối với mức an toàn 1 và 2.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS11.03, AS11.04, AS11.05 và AS11.06.	

Bảng 347 - VE và TE của AS11.03

Quản lý cấu hình - mức 1 và 2	
AS11.03 ISO/IEC 19790:2025, 7.11.2.2	Một hệ thống quản lý cấu hình phải được sử dụng cho việc phát triển một mô-đun mật mã và các thành phần của mô-đun nằm trong biên mật mã, cùng các tài liệu mô-đun liên quan.
Thông tin bắt buộc từ nhà cung cấp	
VE11.03.01	Tài liệu do nhà cung cấp cung cấp phải mô tả hệ thống quản lý cấu hình dành cho mô-đun mật mã, các thành phần của mô-đun, và các tài liệu mô-đun liên quan.
Quy trình kiểm thử bắt buộc	

TE11.03.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có tuyên bố việc một hệ thống quản lý cấu hình đã được triển khai.
------------	---

Bảng 348 - VE và TE của AS11.04

Quản lý cấu hình - mức 1, 2, 3 và 4	
AS11.04 ISO/IEC 19790:2025, 7.11.2.2	Từng phiên bản của mỗi hạng mục cấu hình (ví dụ: thành phần phần cứng, phần mềm, và phần sụn, HDL của mô-đun, hướng dẫn sử dụng, chính sách an toàn) cấu thành nên mô-đun và tài liệu liên quan phải được gán và dán nhãn bằng một định danh duy nhất.
Thông tin bắt buộc từ nhà cung cấp	
VE11.04.01	Tài liệu về mô-đun mật mã của nhà cung cấp phải bao gồm một danh sách cấu hình của tất cả các hạng mục cấu hình. Tài liệu do nhà cung cấp cung cấp phải mô tả phương pháp được sử dụng để nhận diện duy nhất các hạng mục cấu hình.
VE11.04.02	Tài liệu do nhà cung cấp cung cấp phải mô tả phương pháp được sử dụng để nhận diện duy nhất phiên bản của từng hạng mục cấu hình đang được thẩm định.
Quy trình kiểm thử bắt buộc	
TE11.04.01	Kiểm thử viên phải xác minh rằng danh sách cấu hình do nhà cung cấp cung cấp có bao gồm các hạng mục cấu hình.
TE11.04.02	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định phương pháp được sử dụng để nhận diện duy nhất tất cả các hạng mục cấu hình.
TE11.04.03	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mô tả phương pháp được sử dụng để nhận diện duy nhất từng phiên bản của một hạng mục cấu hình đang được thẩm định.
TE11.04.04	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp nhận diện một cách duy nhất phiên bản của từng hạng mục cấu hình đang được thẩm định.

Bảng 349 - VE và TE của AS11.05

Quản lý cấu hình - mức 1, 2, 3 và 4	
AS11.05 ISO/IEC 19790:2025, 7.11.2.2	Hệ thống quản lý cấu hình phải theo dõi và duy trì các thay đổi đối với định danh và phiên bản hoặc bản sửa đổi của từng hạng mục cấu hình trong suốt vòng đời của mô-đun mật mã đã được thẩm định.
Thông tin bắt buộc từ nhà cung cấp	
VE11.05.01	Tài liệu do nhà cung cấp cung cấp phải mô tả cách hệ thống quản lý cấu hình theo dõi và duy trì các thay đổi đối với định danh và phiên bản hoặc bản sửa đổi của từng hạng mục cấu hình trong suốt vòng đời của mô-đun mật mã đã được thẩm định.
Quy trình kiểm thử bắt buộc	
TE11.05.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định các phương pháp được sử dụng để theo dõi và duy trì các thay đổi đối với định danh và phiên bản hoặc bản sửa đổi của từng hạng mục cấu hình trong suốt vòng đời của mô-đun mật mã đã được thẩm định.
TE11.05.02	Kiểm thử viên phải kiểm tra hệ thống quản lý cấu hình để xác minh rằng nó có theo dõi và duy trì các thay đổi đối với định danh và phiên bản hoặc bản sửa đổi của từng hạng mục cấu hình trong suốt vòng đời của mô-đun mật mã đã được

	thẩm định.
--	------------

Bảng 350 - VE và TE của AS11.06

Quản lý cấu hình - mức 1, 2, 3 và 4	
AS11.06 ISO/IEC 19790:2025, 7.11.2.2	Nhà cung cấp phải bảo vệ các tài liệu mô-đun bí mật khỏi sự truy cập trái phép.
Thông tin bắt buộc từ nhà cung cấp	
VE11.06.01	Tài liệu do nhà cung cấp cung cấp phải quy định cơ chế và thủ tục được sử dụng nhằm đảm bảo rằng các tài liệu mô-đun bí mật được bảo vệ khỏi sự truy cập trái phép.
Quy trình kiểm thử bắt buộc	
TE11.06.01	Kiểm thử viên phải xác minh tài liệu do nhà cung cấp cung cấp có quy định cơ chế và thủ tục, sao cho các tài liệu mô-đun bí mật được bảo vệ khỏi sự truy cập trái phép.

6.11.2.2 Mức an toàn 3 và 4

Bảng 351 - VE và TE của AS11.07

Quản lý cấu hình - mức 3 và 4	
AS11.07 ISO/IEC 19790:2025, 7.11.2.3	Ngoài các yêu cầu đối với mức an toàn 1 và 2, các hạng mục cấu hình phải được quản lý bằng một hệ thống quản lý cấu hình tự động.
Thông tin bắt buộc từ nhà cung cấp	
VE11.07.01	Tài liệu do nhà cung cấp cung cấp phải quy định cách hệ thống quản lý cấu hình cung cấp một phương tiện tự động để hỗ trợ cho việc tạo ra một mô-đun mật mã.
Quy trình kiểm thử bắt buộc	
TE11.07.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp quy định cách hệ thống quản lý cấu hình cung cấp một phương tiện tự động để hỗ trợ cho việc tạo ra một mô-đun mật mã.

6.11.3 Thiết kế

Bảng 352 - VE và TE của AS11.08

Thiết kế - mức 1, 2, 3 và 4	
AS11.08 ISO/IEC 19790:2025, 7.11.3	Các mô-đun mật mã phải được thiết kế để cho phép thử nghiệm tất cả các dịch vụ liên quan đến an toàn được cung cấp.
Quy trình kiểm thử bắt buộc	
Khẳng định này không được kiểm thử riêng.	
CHÚ THÍCH: Khẳng định này được kiểm thử trong 6.4.3.	

6.11.4 Mô hình trạng thái hữu hạn

Bảng 353 - VE và TE của AS11.09

Mô hình trạng thái hữu hạn - mức 1, 2, 3 và 4	
AS11.09 ISO/IEC 19790:2025, 7.11.4	Sự hoạt động của một mô-đun mật mã phải được quy định bằng việc sử dụng một mô hình trạng thái hữu hạn (FSM), hoặc tương đương, được biểu diễn bằng một biểu đồ chuyển đổi trạng thái cùng với một bảng chuyển đổi trạng thái và các mô tả trạng thái.
Thông tin bắt buộc từ nhà cung cấp	
VE11.09.01	Nhà cung cấp phải cung cấp một bản mô tả về mô hình trạng thái hữu hạn. Bản mô tả này phải chứa việc nhận diện và mô tả về tất cả các trạng thái của mô-đun cùng một mô tả về tất cả các sự chuyển đổi trạng thái tương ứng. Các mô tả về những chuyển đổi trạng thái phải bao gồm các điều kiện nội bộ của mô-đun, các đầu vào dữ liệu và các đầu vào điều khiển gây ra sự chuyển đổi từ trạng thái này sang trạng thái khác, các đầu ra dữ liệu và các đầu ra trạng thái là kết quả từ việc chuyển đổi từ trạng thái này sang trạng thái khác.
VE11.09.02	Tài liệu của nhà cung cấp phải thiết lập một mô tả hoàn chỉnh về những vấn đề sau: a) hoạt động bình thường; b) hoạt động suy giảm; c) giao diện đầu vào dữ liệu; d) giao diện đầu ra dữ liệu; e) giao diện đầu vào điều khiển; f) giao diện đầu ra điều khiển; g) giao diện đầu ra trạng thái; h) đường dẫn tin cậy dạng rõ; i) vai trò người dùng và chuyên viên mật mã ; j) các vai trò khác (nếu có); k) các dịch vụ an toàn; l) các dịch vụ nhập SSP (nếu có); m) dịch vụ hiển thị trạng thái; n) xác thực người vận hành; o) quá trình tự kiểm thử; p) các dịch vụ, hoạt động, và chức năng được ủy quyền khác (nếu có); q) các trạng thái lỗi; r) dịch vụ bỏ qua (nếu có); s) giao diện truy cập bảo trì (nếu có); t) vai trò bảo trì (nếu giao diện truy cập bảo trì được cung cấp); u) các dịch vụ thiết lập và tạo SSP (nếu có); v) các dịch vụ xuất SSP (nếu có); w) các trạng thái nhàn rỗi (nếu có);

	x) các trạng thái chưa khởi tạo (nếu có).
Quy trình kiểm thử bắt buộc	
TE11.09.01	Kiểm thử viên phải xác minh rằng nhà cung cấp đã cung cấp một mô tả về mô hình trạng thái hữu hạn. Bản mô tả này phải bao gồm việc nhận diện và mô tả tất cả các trạng thái của mô-đun và mô tả mọi quá trình chuyển đổi trạng thái tương ứng. Kiểm thử viên phải xác minh rằng các mô tả về sự chuyển đổi trạng thái có bao gồm các điều kiện nội bộ của mô-đun, các đầu vào dữ liệu và đầu vào điều khiển gây ra các quá trình chuyển đổi từ trạng thái này sang trạng thái khác, các đầu ra dữ liệu, đầu ra điều khiển và các đầu ra trạng thái là kết quả của việc chuyển đổi từ trạng thái này sang trạng thái khác.
TE11.09.02	Kiểm thử viên phải xác minh rằng mô hình trạng thái hữu hạn (ví dụ: biểu đồ chuyển đổi trạng thái, bảng chuyển đổi trạng thái và mô tả trạng thái) nhất quán với tài liệu do nhà cung cấp cung cấp, trong đó phải mô tả: a) hoạt động bình thường; b) hoạt động suy giảm; c) giao diện đầu vào dữ liệu; d) giao diện đầu ra dữ liệu; e) giao diện đầu vào điều khiển; f) giao diện đầu ra điều khiển; g) giao diện đầu ra trạng thái; h) đường dẫn tin cậy dạng rõ; i) vai trò người dùng và chuyên viên mật mã ; j) các vai trò khác (nếu có); k) các dịch vụ an toàn; l) các dịch vụ nhập SSP (nếu có); m) dịch vụ hiển thị trạng thái; n) xác thực người vận hành; o) quá trình tự kiểm thử; p) các dịch vụ, hoạt động, và chức năng được ủy quyền khác (nếu có); q) các trạng thái lỗi; r) dịch vụ bỏ qua (nếu có); s) giao diện truy cập bảo trì (nếu có); t) vai trò bảo trì (nếu giao diện truy cập bảo trì được cung cấp); u) các dịch vụ thiết lập và tạo SSP (nếu có); v) các dịch vụ xuất SSP (nếu có); w) các trạng thái nhàn rỗi (nếu có); x) các trạng thái chưa khởi tạo (nếu có).

TE11.09.03	Kiểm thử viên phải xác minh rằng mỗi dịch vụ của mô-đun mật mã riêng biệt, việc sử dụng chức năng an toàn, trạng thái lỗi, quá trình tự kiểm thử, hoặc xác thực người vận hành đều được mô tả như một trạng thái riêng biệt.
TE11.09.04	Kiểm thử viên phải xác minh rằng mọi trạng thái được nhận diện trong biểu đồ chuyển đổi trạng thái và bảng chuyển đổi trạng thái cũng đều được nhận diện và mô tả trong phần mô tả trạng thái.
TE11.09.05	Kiểm thử viên phải xác minh rằng mọi trạng thái được nhận diện và mô tả trong phần mô tả trạng thái cũng đều được nhận diện trong các biểu đồ chuyển đổi trạng thái và bảng chuyển đổi trạng thái.
TE11.09.06	Kiểm thử viên phải xác minh rằng sự hoạt động của mô-đun là nhất quán với biểu đồ chuyển đổi trạng thái, bảng chuyển đổi trạng thái, và các mô tả trạng thái.
TE11.09.07	Nếu mô-đun bao gồm một giao diện truy cập bảo trì, kiểm thử viên phải xác minh rằng mô hình trạng thái hữu hạn có định nghĩa ít nhất một trạng thái bảo trì. Tất cả các trạng thái bảo trì phải được chứa trong các biểu đồ chuyển đổi trạng thái và bảng chuyển đổi trạng thái, đồng thời được mô tả trong phần mô tả trạng thái.
TE11.09.08	Kiểm thử viên phải xác minh các mô tả về những trạng thái của mô-đun mật mã xem liệu các mô tả đó có định nghĩa rõ ràng các trạng thái tách biệt hay không. Kiểm thử viên phải xác minh rằng tất cả các tập hợp kết hợp có thể có giữa đầu vào dữ liệu và đầu vào điều khiển đều có thể được phân vùng thành các tập hợp tách biệt.
TE11.09.09	Kiểm thử viên phải thử sử dụng mô-đun mật mã, khiến nó bước vào từng trạng thái chính của nó. Đối với mỗi trạng thái có một chỉ báo riêng biệt, kiểm thử viên phải thử xác minh chỉ báo đó trong khi mô-đun đang ở trong trạng thái đó. Nếu không quan sát thấy chỉ báo dự kiến, hoặc có hai hoặc nhiều chỉ báo như vậy được quan sát thấy cùng một lúc (cho thấy rằng mô-đun đang ở nhiều hơn một trạng thái cùng một lúc), bài kiểm thử này đã thất bại.
TE11.09.10	Kiểm thử viên phải xác minh rằng tồn tại một chuỗi các bước chuyển đổi từ trạng thái bật nguồn ban đầu tới mọi trạng thái khác trong mô hình mà không phải là trạng thái bật nguồn ban đầu.
TE11.09.11	Kiểm thử viên phải xác minh rằng tồn tại một chuỗi các bước chuyển đổi từ mọi trạng thái không tắt nguồn đến một trạng thái tắt nguồn của mô hình.
TE11.09.12	Kiểm thử viên phải xác minh rằng các hành động của mô hình trạng thái hữu hạn, được xem là kết quả của tất cả các đầu vào dữ liệu và kiểm soát có thể có, đều được định nghĩa. Ví dụ: Một tuyên bố bao trùm có thể chấp nhận được là: "Hành động của mô hình trạng thái hữu hạn do tất cả các tập hợp kết hợp đầu vào dữ liệu và kiểm soát khác là đưa mô hình trạng thái hữu hạn vào trạng thái ERROR-3."

Bảng 354 - VE và TE của AS11.10

Mô hình trạng thái hữu hạn - mức 1, 2, 3 và 4	
AS11.10 ISO/IEC 19790:2025, 7.11.4	FSM phải đủ chi tiết để chứng minh rằng mô-đun mật mã tuân thủ các yêu cầu liên quan của ISO/IEC 19790:2025.
Quy trình kiểm thử bắt buộc	

Khẳng định này được kiểm thử như một phần của AS11.09.

Bảng 355 - VE và TE của AS11.11

Mô hình trạng thái hữu hạn - mức 1, 2, 3 và 4	
AS11.11 ISO/IEC 19790:2025, 7.11.4	FSM của một mô-đun mật mã, tối thiểu, phải bao gồm các trạng thái hoạt động và trạng thái lỗi riêng biệt sau đây: a) Trạng thái tắt nguồn: Một trạng thái trong đó mô-đun bị tắt nguồn. Toàn bộ nguồn điện chính, phụ, hoặc dự phòng không còn được cấp cho mô-đun nữa. Đối với một mô-đun phần mềm hoặc phần sụn và các thành phần phần mềm hoặc phần sụn của một mô-đun lai, việc tắt nguồn là hành động chấm dứt các tập tin ảnh thực thi của mô-đun phần mềm/phần sụn hoặc các thành phần phần mềm/phần sụn của một mô-đun lai. b) Trạng thái bật nguồn: Một trạng thái trong đó mô-đun được bật nguồn (sau khi đã bị tắt nguồn, thiết lập lại, khởi động lại, khởi động lạnh, bị gián đoạn nguồn điện) và nguồn điện chính, phụ, hoặc dự phòng được cấp cho mô-đun. Đối với một mô-đun phần mềm hoặc phần sụn và các thành phần phần mềm/phần sụn của một mô-đun lai, việc bật nguồn là hành động sinh ra một tập tin ảnh thực thi của mô-đun phần mềm/phần sụn hoặc các thành phần phần mềm/phần sụn của mô-đun lai. c) Trạng thái khởi tạo chung: Một trạng thái trong đó mô-đun mật mã đang trải qua quá trình khởi tạo trước khi mô-đun chuyển sang trạng thái đã phê duyệt. d) Trạng thái chuyên viên mật mã: Một trạng thái trong đó các dịch vụ của chuyên viên mật mã được thực hiện (ví dụ: khởi tạo mật mã, quản trị an toàn, và quản lý khóa) và trong đó những người dùng được ủy quyền có thể nhận được các dịch vụ an toàn, thực hiện các hoạt động mật mã, hoặc thực hiện các chức năng đã phê duyệt khác. e) Trạng thái nhập CSP (nếu việc nhập CSP được triển khai): Một trạng thái dành cho việc nhập các CSP vào mô-đun mật mã. f) Trạng thái tự kiểm thử: Một trạng thái trong đó mô-đun mật mã đang thực hiện các quá trình tự kiểm thử. g) Trạng thái lỗi: Một trạng thái khi mô-đun mật mã gặp phải một điều kiện lỗi (ví dụ: thất bại trong một quá trình tự kiểm thử). Có thể có một hoặc nhiều điều kiện lỗi dẫn đến một trạng thái lỗi duy nhất của mô-đun. Các trạng thái lỗi có thể bao gồm lỗi "cứng" biểu thị cho một sự cố thiết bị và có thể yêu cầu bảo trì, bảo dưỡng hoặc sửa chữa mô-đun mật mã, hoặc lỗi "mềm" có khả năng phục hồi được có thể yêu cầu khởi tạo hoặc thiết lập lại mô-đun.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS11.09.	

Bảng 356 - VE và TE của AS11.12

Mô hình trạng thái hữu hạn - mức 1, 2, 3 và 4
--

AS11.12 ISO/IEC 19790:2025, 7.11.4	Phải có khả năng phục hồi từ các trạng thái lỗi, trừ các trạng thái lỗi do lỗi cứng gây ra, đòi hỏi bảo trì, bảo dưỡng hoặc sửa chữa mô-đun mật mã.
Thông tin bắt buộc từ nhà cung cấp	
VE11.12.01	Tài liệu do nhà cung cấp cung cấp phải mô tả biện pháp phục hồi có thể áp dụng đối với từng trạng thái lỗi vốn không yêu cầu bảo trì, bảo dưỡng, hoặc sửa chữa mô-đun mật mã.
VE11.12.02	Tài liệu do nhà cung cấp cung cấp phải mô tả các trạng thái lỗi mà từ đó mô-đun không thể phục hồi nếu không bảo trì, bảo dưỡng, hoặc sửa chữa mô-đun mật mã.
Quy trình kiểm thử bắt buộc	
TE11.12.01	Từ mỗi trạng thái lỗi không yêu cầu bảo trì, bảo dưỡng, hoặc sửa chữa, kiểm thử viên phải xác minh rằng mô-đun mật mã có thể được đưa về một trạng thái hoạt động hoặc trạng thái khởi tạo chấp nhận được. Việc này bao gồm hai phần: thứ nhất, kiểm thử viên phải xác minh rằng mô-đun mật mã có chỉ báo khi nó ở trong trạng thái lỗi, và thứ hai, rằng mô-đun hoạt động chính xác trong trạng thái mục tiêu này. Kiểm thử viên phải báo cáo cách thức yêu cầu này được xác minh (tức là thông qua việc kiểm tra mã lệnh hay thông qua việc dùng thử mô-đun).
TE11.12.02	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có mô tả các trạng thái lỗi mà từ đó mô-đun không thể phục hồi nếu không bảo trì, bảo dưỡng, hoặc sửa chữa mô-đun mật mã.

6.11.5 Phát triển

6.11.5.1 Mức an toàn 1

Bảng 357 - VE và TE của AS11.13

Phát triển - mức 1	
AS11.13 ISO/IEC 19790:2025, 7.11.5.2	Các yêu cầu sau đây phải được áp dụng đối với các mô-đun mật mã ở mức an toàn 1:
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS11.14, AS11.15, AS11.16, AS11.17, AS11.18, AS11.19 và AS11.20.	

Bảng 358 - VE và TE của AS11.14

Phát triển - mức 1, 2, 3 và 4	
AS11.14 ISO/IEC 19790:2025, 7.11.5.2	Nếu một mô-đun mật mã có chứa phần mềm hoặc phần sụn, các thành phần sau đây phải được theo dõi bằng hệ thống quản lý cấu hình: mã nguồn, tài liệu tham khảo ngôn ngữ lập trình, các trình biên dịch, các phiên bản trình biên dịch và các tùy chọn trình biên dịch, trình liên kết và các tùy chọn trình liên kết, các thư viện thực thi và các cài đặt thư viện thực thi, các thiết lập cấu hình, các quá trình và phương pháp xây dựng, các tùy chọn xây dựng, các biến môi trường và mọi tài nguyên khác được sử dụng để biên dịch và liên kết mã nguồn thành định dạng thực thi.
Thông tin bắt buộc từ nhà cung cấp	

VE11.14.01	Đối với các mô-đun mật mã có chứa phần mềm hoặc phần sụn, nhà cung cấp phải cung cấp tài liệu về mã nguồn, tài liệu tham khảo ngôn ngữ lập trình, các trình biên dịch, các phiên bản trình biên dịch và các tùy chọn trình biên dịch, trình liên kết và các tùy chọn trình liên kết, các thư viện thực thi và cài đặt thư viện thực thi, các thiết lập cấu hình, các quá trình và phương pháp xây dựng, các tùy chọn xây dựng, các biến môi trường, và mọi tài nguyên khác được sử dụng để biên dịch và liên kết mã nguồn thành định dạng thực thi.
VE11.14.02	Đối với mỗi thành phần được lập tài liệu ở VE11.14.01, nhà cung cấp phải cung cấp tài liệu chứng minh rằng những thành phần này được theo dõi thông qua hệ thống quản lý cấu hình.
Quy trình kiểm thử bắt buộc	
TE11.14.01	Đối với các mô-đun mật mã có chứa phần mềm hoặc phần sụn, kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu về mã nguồn, tài liệu tham khảo ngôn ngữ lập trình, các trình biên dịch, phiên bản trình biên dịch và các tùy chọn trình biên dịch, trình liên kết và các tùy chọn trình liên kết, các thư viện thực thi và cài đặt thư viện thực thi, các thiết lập cấu hình, quá trình và phương pháp xây dựng, các tùy chọn xây dựng, các biến môi trường, và mọi tài nguyên khác được sử dụng để biên dịch và liên kết mã nguồn thành định dạng thực thi.
TE11.14.02	Đối với mỗi thành phần được lập tài liệu ở VE11.14.01, kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu chứng minh rằng các thành phần này được theo dõi thông qua hệ thống quản lý cấu hình.

Bảng 359 - VE và TE của AS11.15

Phát triển - mức 1, 2, 3 và 4	
AS11.15 ISO/IEC 19790:2025, 7.11.5.2	Nếu một mô-đun mật mã có chứa phần mềm hoặc phần sụn, mã nguồn phải được chú thích bằng các bình luận mô tả sự tương ứng giữa phần mềm hoặc phần sụn với thiết kế của mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE11.15.01	Nhà cung cấp phải cung cấp danh sách tên của tất cả các thành phần phần mềm và phần sụn nằm trong mô-đun mật mã.
VE11.15.02	Nhà cung cấp phải cung cấp một danh sách mã nguồn có chú thích đối với mỗi thành phần phần mềm và phần sụn nằm trong mô-đun mật mã.
Quy trình kiểm thử bắt buộc	
TE11.15.01	Kiểm thử viên phải sử dụng danh sách do nhà cung cấp cung cấp để xác minh rằng một danh sách mã nguồn dành cho mỗi thành phần phần mềm hoặc phần sụn đã được bao gồm trong mô-đun.

Bảng 360 - VE và TE của AS11.16

Phát triển - mức 1, 2, 3 và 4	
AS11.16 ISO/IEC 19790:2025, 7.11.5.2	Nếu một mô-đun mật mã có chứa phần cứng, tài liệu phải quy định các sơ đồ nguyên lý hoặc ngôn ngữ mô tả phần cứng (HDL), hoặc cả hai, nếu có thể áp dụng.
Thông tin bắt buộc từ nhà cung cấp	
VE11.16.01	Nhà cung cấp phải cung cấp danh sách các thành phần phần cứng nằm trong mô-đun mật mã.

Quy trình kiểm thử bắt buộc	
TE11.16.01	Kiểm thử viên phải sử dụng danh sách do nhà cung cấp cung cấp để xác minh rằng tài liệu có bao gồm các sơ đồ nguyên lý hoặc các danh sách Ngôn ngữ mô tả phần cứng (HDL), hoặc cả hai, đối với các thành phần phần cứng, nếu có thể áp dụng.

Bảng 361 - VE và TE của AS11.17

Phát triển - mức 1, 2, 3 và 4	
AS11.17 ISO/IEC 19790:2025, 7.11.5.2	Nếu một mô-đun mật mã có chứa phần cứng, và nếu HDL được sử dụng để quy định phần cứng đó, HDL phải được chú thích bằng các bình luận mô tả sự tương ứng giữa phần cứng với thiết kế của mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE11.17.01	Nhà cung cấp phải cung cấp một danh sách HDL có chú thích đối với mỗi thành phần phần cứng nằm trong mô-đun mật mã.
Quy trình kiểm thử bắt buộc	
TE11.17.01	Kiểm thử viên phải sử dụng danh sách do nhà cung cấp cung cấp để xác minh rằng một danh sách HDL dành cho mỗi thành phần phần cứng đã được bao gồm trong mô-đun.

Bảng 362 - VE và TE của AS11.18

Phát triển - mức 1, 2, 3 và 4	
AS11.18 ISO/IEC 19790:2025, 7.11.5.2	Đối với các mô-đun mật mã phần mềm và phần sụn và thành phần phần mềm hoặc phần sụn của một mô-đun lai: kết quả của các kỹ thuật xác thực dữ liệu và tính toàn vẹn đã phê duyệt được quy định trong ISO/IEC 19790:2025, 7.5 và 7.10 phải được nhà cung cấp tính toán và tích hợp vào phần mềm, phần sụn hoặc mô-đun lai trong suốt quá trình phát triển mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE11.18.01	Đối với các mô-đun mật mã phần mềm và phần sụn và thành phần phần mềm hoặc phần sụn của một mô-đun lai, nhà cung cấp phải cung cấp tài liệu chứng minh rằng kết quả của các cơ chế kỹ thuật xác thực và tính toàn vẹn đã phê duyệt được quy định trong ISO/IEC 19790:2025, 7.5 và 7.10 phải được nhà cung cấp tính toán và tích hợp vào phần mềm, phần sụn hoặc mô-đun lai trong suốt quá trình phát triển mô-đun.
Quy trình kiểm thử bắt buộc	
TE11.18.01	Đối với các mô-đun mật mã phần mềm và phần sụn và thành phần phần mềm hoặc phần sụn của một mô-đun lai, kiểm thử viên phải xác minh rằng nhà cung cấp cung cấp tài liệu chứng minh rằng kết quả của các cơ chế kỹ thuật xác thực và tính toàn vẹn đã phê duyệt được quy định trong ISO/IEC 19790:2025, 7.5 và 7.10 phải được nhà cung cấp tính toán và tích hợp vào phần mềm, phần sụn hoặc mô-đun lai trong suốt quá trình phát triển mô-đun.

Bảng 363 - VE và TE của AS11.19

Phát triển - mức 1, 2, 3 và 4	
AS11.19 ISO/IEC 19790:2025,	Đối với các mô-đun mật mã phần mềm và phần sụn và thành phần phần mềm hoặc phần sụn của một mô-đun lai: tài liệu mô-đun mật mã phải quy định trình biên dịch, các thiết lập cấu hình và các phương pháp để biên dịch mã nguồn thành định

7.11.5.2	dạng thực thi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS11.14.	

Bảng 364 - VE và TE của AS11.20

Phát triển - mức 1, 2, 3 và 4	
AS11.20 ISO/IEC 19790:2025, 7.11.5.2	Đối với các mô-đun mật mã phần mềm và phần sụn và thành phần phần mềm hoặc phần sụn của một mô-đun lai: mô-đun mật mã phải được phát triển bằng cách sử dụng các công cụ phát triển cấp độ sản xuất (ví dụ: trình biên dịch).
Thông tin bắt buộc từ nhà cung cấp	
VE11.20.01	Nhà cung cấp phải cung cấp tài liệu chứng minh rằng mô-đun mật mã được phát triển bằng cách sử dụng các công cụ phát triển cấp độ sản xuất (ví dụ: trình biên dịch).
Quy trình kiểm thử bắt buộc	
TE11.20.01	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp về mô-đun chứng minh mô-đun mật mã đã được phát triển bằng cách sử dụng các công cụ phát triển cấp độ sản xuất (ví dụ: trình biên dịch).

6.11.5.2 Mức an toàn 2 và 3**Bảng 365 - VE và TE của AS11.21**

Phát triển - mức 2, 3 và 4	
AS11.21 ISO/IEC 19790:2025, 7.11.5.3	Ngoài các yêu cầu đối với mức an toàn 1, các yêu cầu sau đây phải được áp dụng cho các mô-đun mật mã đối với mức an toàn 2 và 3: {AS11.24 đến AS11.27}.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS11.22, AS11.23, AS11.24, AS11.25 và AS11.26.	

Bảng 366 - VE và TE của AS11.22

Phát triển - mức 2, 3 và 4	
AS11.22 ISO/IEC 19790:2025, 7.11.5.3	Toàn bộ phần mềm hoặc phần sụn phải được triển khai bằng ngôn ngữ lập trình bậc cao, phi độc quyền hoặc {cơ sở hợp lý phải được cung cấp để chứng minh cho việc sử dụng một ngôn ngữ lập trình bậc thấp (ví dụ: hợp ngữ hoặc vi mã) nếu nó thiết yếu đối với hiệu suất của mô-đun hoặc khi ngôn ngữ lập trình bậc cao không có sẵn;}.
Thông tin bắt buộc từ nhà cung cấp	
VE11.22.01	Nhà cung cấp phải cung cấp tài liệu chứng minh rằng toàn bộ phần mềm hoặc phần sụn nằm trong một mô-đun mật mã được triển khai bằng ngôn ngữ lập trình bậc cao, phi độc quyền.
Quy trình kiểm thử bắt buộc	
TE11.22.01	Kiểm thử viên phải xác minh rằng nhà cung cấp cung cấp tài liệu chứng minh toàn bộ phần mềm hoặc phần sụn nằm trong mô-đun mật mã được triển khai bằng ngôn ngữ lập trình bậc cao, phi độc quyền.

Bảng 367 - VE và TE của AS11.23

Phát triển - mức 2, 3 và 4	
AS11.23 ISO/IEC 19790:2025, 7.11.5.3	{Toàn bộ phần mềm hoặc phần sụn phải được triển khai bằng ngôn ngữ lập trình bậc cao, phi độc quyền} hoặc cơ sở hợp lý phải được cung cấp để chứng minh cho việc sử dụng ngôn ngữ lập trình bậc thấp (ví dụ: hợp ngữ hoặc vi mã) nếu nó thiết yếu đối với hiệu suất của mô-đun hoặc khi ngôn ngữ lập trình bậc cao không có sẵn.
Thông tin bắt buộc từ nhà cung cấp	
VE11.23.01	Nhà cung cấp phải nhận diện mỗi thành phần phần mềm và phần sụn không được viết bằng ngôn ngữ lập trình bậc cao và cung cấp một cơ sở hợp lý hoặc lời giải thích tại sao thành phần đó lại được viết bằng ngôn ngữ bậc thấp. Cơ sở hợp lý phải trích dẫn sự không có sẵn của ngôn ngữ lập trình bậc cao hoặc sự cần thiết phải tăng cường hiệu suất đối với phần mềm hoặc phần sụn đó.
Quy trình kiểm thử bắt buộc	
TE11.23.01	Kiểm thử viên phải xem xét mã nguồn của từng thành phần phần mềm hoặc phần sụn để xác minh xem thành phần nào được viết bằng ngôn ngữ bậc thấp. Kiểm thử viên phải xác minh rằng không có thành phần phần mềm hoặc phần sụn nào được viết bằng ngôn ngữ bậc thấp mà lại không được nhà cung cấp nhận diện trong VE11.23.01.

Bảng 368 - VE và TE của AS11.24

Phát triển - mức 2, 3 và 4	
AS11.24 ISO/IEC 19790:2025, 7.11.5.3	Các mạch tích hợp tùy chỉnh nằm trong mô-đun mật mã phải được tạo ra bằng cách sử dụng các phương pháp hỗ trợ sự thấu hiểu hoặc khả năng phân tích, ví dụ: sử dụng ngôn ngữ mô tả phần cứng bậc cao (HDL) hoặc sơ đồ nguyên lý đối với các linh kiện tương tự.
Thông tin bắt buộc từ nhà cung cấp	
VE11.24.01	Nhà cung cấp phải cung cấp tài liệu về các thành phần phần cứng được triển khai bằng ngôn ngữ đặc tả bậc cao.
Quy trình kiểm thử bắt buộc	
TE11.24.01	Kiểm thử viên phải xác minh rằng tài liệu của nhà cung cấp có chứa thông tin quy định tại VE11.24.01.

Bảng 369 - VE và TE của AS11.25

Phát triển - mức 2, 3 và 4	
AS11.25 ISO/IEC 19790:2025, 7.11.5.3	Toàn bộ phần mềm hoặc phần sụn phải được thiết kế và triển khai theo cách thức tránh sử dụng mã lệnh, tham số hoặc ký hiệu không cần thiết cho chức năng và quá trình thực thi của mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE11.25.01	Đối với toàn bộ phần mềm hoặc phần sụn, nhà cung cấp phải cung cấp tài liệu chứng minh phần mềm hoặc phần sụn được thiết kế và triển khai theo cách thức tránh sử dụng mã lệnh, tham số, hoặc ký hiệu không cần thiết cho chức năng và quá trình thực thi của mô-đun.
Quy trình kiểm thử bắt buộc	

TE11.25.01	Đối với toàn bộ phần mềm hoặc phần sụn, kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu chứng minh phần mềm hoặc phần sụn được thiết kế và triển khai theo cách thức tránh sử dụng mã lệnh, tham số, hoặc ký hiệu không cần thiết cho chức năng và quá trình thực thi của mô-đun.
------------	--

Bảng 370 - VE và TE của AS11.26

Phát triển - mức 2, 3 và 4	
AS11.26 ISO/IEC 19790:2025, 7.11.5.3	Mô-đun phải được thiết kế và triển khai theo cách thức sử dụng các yêu cầu như được định nghĩa tại ISO/IEC 19790:2025, Phụ lục G.
Thông tin bắt buộc từ nhà cung cấp	
VE11.26.01	Đối với toàn bộ phần mềm hoặc phần sụn, nhà cung cấp phải cung cấp tài liệu chứng minh phần mềm hoặc phần sụn được thiết kế và triển khai theo cách thức sử dụng các yêu cầu như được định nghĩa tại ISO/IEC 19790:2025, Phụ lục G.
Quy trình kiểm thử bắt buộc	
TE11.26.01	Đối với toàn bộ phần mềm hoặc phần sụn, kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu chứng minh phần mềm hoặc phần sụn được thiết kế và triển khai theo cách thức sử dụng các yêu cầu như được định nghĩa tại ISO/IEC 19790:2025, Phụ lục G.

6.11.5.3 Mức an toàn 4**Bảng 371 - VE và TE của AS11.27**

Phát triển - mức 1, 2, 3 và 4	
AS11.27 ISO/IEC 19790:2025, 7.11.5.4	Ngoài các yêu cầu đối với mức an toàn 1, 2 và 3, yêu cầu sau đây phải được áp dụng đối với các mô-đun mật mã ở mức an toàn 4.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS11.28.	

Bảng 372 - VE và TE của AS11.28

Phát triển – Mức 4	
AS11.28 ISO/IEC 19790:2025, 7.11.5.4	Đối với từng thành phần phần cứng, phần mềm và phần sụn của mô-đun mật mã, tài liệu phải được chú thích bằng các bình luận quy định rõ: a) các tiền điều kiện được yêu cầu ngay khi bắt đầu truy cập vào mỗi thành phần, chức năng và thủ tục của mô-đun nhằm đảm bảo việc thực thi diễn ra chính xác; và b) các hậu điều kiện được kỳ vọng là đúng khi quá trình thực thi của mỗi thành phần, chức năng, hoặc thủ tục của mô-đun hoàn tất.
Thông tin bắt buộc từ nhà cung cấp	
VE11.28.01	Các danh sách mã nguồn đối với tất cả các thành phần phần cứng, phần mềm, và phần sụn phải bao gồm các bình luận trình bày các tiền điều kiện và hậu điều kiện như được yêu cầu trong AS11.28.
VE11.28.02	Tài liệu do nhà cung cấp cung cấp phải cung cấp một cơ sở hợp lý hoặc lời giải thích chứng minh lý do tại sao mỗi tiền điều kiện lại được đáp ứng, cùng với các

	trường hợp sử dụng cho phép đối với mô-đun mật mã. CHÚ THÍCH 1: Các trường hợp sử dụng sẽ bao gồm việc cung cấp dịch vụ cho nhiều người vận hành đồng thời mang các vai trò khác nhau và phát hiện sự can thiệp vật lý.
VE11.28.03	Nếu có bất kỳ tiền điều kiện nào không được đáp ứng hoàn toàn bởi thiết kế của mô-đun mật mã, thì tài liệu do nhà cung cấp cung cấp cũng phải đề cập đến thực tế đó và xác định xem những thực thể nào sẽ chịu trách nhiệm cho mỗi tiền điều kiện. Các thực thể này có thể là các mô-đun đã được thẩm định bổ sung được nhúng bên trong mô-đun mật mã, hoặc là các thành phần phần cứng được lắp ráp trong mô-đun. Nếu các thực thể nằm ngoài biên mật mã chịu trách nhiệm cho một tiền điều kiện, thì tài liệu hướng dẫn quản trị viên phải cung cấp tiền điều kiện đó dưới dạng một quy tắc bắt buộc áp dụng đối với việc sử dụng mô-đun mật mã.
VE11.28.04	Tài liệu do nhà cung cấp cung cấp phải cung cấp một cơ sở hợp lý hoặc lời giải thích chứng minh lý do tại sao mỗi hậu điều kiện lại được đáp ứng.
Quy trình kiểm thử bắt buộc	
TE11.28.01	Kiểm thử viên phải xác minh các danh sách mã nguồn để đảm bảo rằng thông tin được quy định trong VE11.28.01 đã được đưa vào.
TE11.28.02	Kiểm thử viên phải kiểm tra mô-đun và xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng mỗi tiền điều kiện thực sự đã được đáp ứng, trong khi xem xét các trường hợp sử dụng cho phép. Trách nhiệm chứng minh thuộc về nhà cung cấp; nếu có bất kỳ sự không chắc chắn hoặc mơ hồ nào, kiểm thử viên phải yêu cầu nhà cung cấp cung cấp thêm thông tin khi cần thiết. CHÚ THÍCH 2: Việc kiểm tra này sẽ được thực hiện thông qua việc xem xét tính nhất quán với các hậu điều kiện khác đã được xác minh hoặc bằng cách kiểm tra mã nguồn, hoặc cả hai.
TE11.28.03	Kiểm thử viên phải kiểm tra mô-đun và xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng mỗi hậu điều kiện thực sự đã được đáp ứng, trong khi xem xét các tiền điều kiện và hậu điều kiện khác đã được xác minh. Trách nhiệm chứng minh thuộc về nhà cung cấp; nếu có bất kỳ sự không chắc chắn hoặc mơ hồ nào, kiểm thử viên phải yêu cầu nhà cung cấp cung cấp thêm thông tin khi cần thiết.
TE11.28.04	Nếu có một mô-đun đã được thẩm định khác được nhúng bên trong mô-đun mật mã, kiểm thử viên phải xác minh rằng các quy tắc áp đặt lên việc sử dụng mô-đun đã được thẩm định khác đó thực sự đã được đáp ứng.
CHÚ THÍCH 3: Các tiền điều kiện và hậu điều kiện có thể được xác định bằng cách sử dụng bất kỳ ký hiệu nào đủ chi tiết để giải thích một cách trọn vẹn và rõ ràng hành vi của thành phần, chức năng, thủ tục của mô-đun mật mã.	

6.11.6 Kiểm thử từ phía nhà cung cấp

6.11.6.1 Mức an toàn 1 và 2

Bảng 373 - VE và TE của AS11.29

Kiểm thử từ phía nhà cung cấp - mức 1, 2, 3 và 4	
AS11.29 ISO/IEC 19790:2025, 7.11.6.2	Đối với mức an toàn 1 và 2, tài liệu phải quy định quá trình kiểm thử chức năng được thực hiện trên mô-đun mật mã.
Thông tin bắt buộc từ nhà cung cấp	

VE11.29.01	Nhà cung cấp phải cung cấp tài liệu quy định quá trình kiểm thử chức năng được thực hiện trên mô-đun mật mã, cung cấp sự đảm bảo rằng mô-đun mật mã hoạt động tuân thủ theo chính sách an toàn của mô-đun và các đặc tả chức năng.
Quy trình kiểm thử bắt buộc	
TE11.29.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu quy định quá trình kiểm thử chức năng được thực hiện trên mô-đun mật mã.
TE11.29.02	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp mang lại sự đảm bảo rằng mô-đun mật mã hoạt động tuân thủ theo chính sách an toàn của mô-đun và các đặc tả chức năng.

Bảng 374 - VE và TE của AS11.30

Kiểm thử từ phía nhà cung cấp - mức 1, 2, 3 và 4	
AS11.30 ISO/IEC 19790:2025, 7.11.6.2	Nhà cung cấp phải sử dụng các công cụ chẩn đoán an toàn tự động (ví dụ: phát hiện tràn bộ đệm) đối với các mô-đun mật mã phần mềm hoặc phần sụn và thành phần phần mềm hoặc phần sụn của một mô-đun lai, hoặc thành phần phần sụn của một mô-đun phần cứng.
Thông tin bắt buộc từ nhà cung cấp	
VE11.30.01	Nhà cung cấp phải cung cấp tài liệu chứng minh rằng các công cụ chẩn đoán an toàn tự động hiện tại (ví dụ: phát hiện tràn bộ đệm) đã được sử dụng để kiểm thử các mô-đun mật mã phần mềm hoặc phần sụn, thành phần phần mềm hoặc phần sụn của một mô-đun lai, hoặc thành phần phần sụn của một mô-đun phần cứng.
VE11.30.02	Tài liệu do nhà cung cấp cung cấp phải xác định các loại sự cố, mối quan ngại hoặc khiếm khuyết trong triển khai an toàn nào có thể được phát hiện thông qua việc sử dụng các công cụ chẩn đoán an toàn tự động. Nhà cung cấp có thể phân loại các loại sự cố này bằng cách sử dụng danh sách Danh mục điểm yếu phổ biến.
VE11.30.03	Tài liệu do nhà cung cấp cung cấp phải cung cấp bằng chứng cho thấy các công cụ chẩn đoán an toàn tự động đã thực sự được áp dụng nhằm phát hiện ra các sự cố, mối quan ngại hoặc khiếm khuyết trong triển khai an toàn. VÍ DỤ 1: Cấu hình của các công cụ chẩn đoán an toàn tự động, các kịch bản kiểm thử phục vụ cho việc phân tích động, và các bản ghi chẩn đoán.
VE11.30.04	Tài liệu do nhà cung cấp cung cấp phải cung cấp một lý do chứng minh sự phù hợp cho phạm vi bao phủ của quá trình chẩn đoán. VÍ DỤ 2: Tài liệu do nhà cung cấp cung cấp đưa ra lý do chứng minh cho phạm vi bao phủ của quá trình chẩn đoán theo từng dịch vụ hoặc theo từng thành phần.
Quy trình kiểm thử bắt buộc	
TE11.30.01	Kiểm thử viên phải xác minh rằng nhà cung cấp cung cấp tài liệu chứng minh rằng các công cụ chẩn đoán an toàn tự động hiện tại (ví dụ: phát hiện tràn bộ đệm, v.v.) đã được sử dụng để kiểm thử các mô-đun mật mã phần mềm hoặc phần sụn, thành phần phần mềm hoặc phần sụn của một mô-đun lai, hoặc thành phần phần sụn của một mô-đun phần cứng.
TE11.30.02	Kiểm thử viên phải xác minh rằng tài liệu do nhà cung cấp cung cấp có xác định rõ những loại sự cố, mối quan ngại và khiếm khuyết trong triển khai an toàn nào có thể được phát hiện thông qua việc sử dụng các công cụ chẩn đoán an toàn tự động.
TE11.30.03	Kiểm thử viên phải xem xét tài liệu do nhà cung cấp cung cấp để đảm bảo rằng thông tin được quy định trong VE11.30.04 đã được bao gồm. Kiểm thử viên phải xác định mức độ chính xác của mọi lý do giải thích do nhà cung cấp đưa ra. Trách

	nhiệm chứng minh thuộc về nhà cung cấp; nếu có bất kỳ sự không chắc chắn hoặc mơ hồ nào, kiểm thử viên phải yêu cầu nhà cung cấp cung cấp thêm thông tin khi cần thiết.
TE11.30.04	Đối với các mô-đun mật mã phần mềm hoặc phần sụn, thành phần phần mềm hoặc phần sụn của một mô-đun lai, hoặc thành phần phần sụn của một mô-đun phần cứng, kiểm thử viên phải kiểm tra mô-đun và xem xét tài liệu do nhà cung cấp cung cấp để xác minh rằng các sự cố, mối quan ngại hoặc khiếm khuyết trong triển khai an toàn đã được xác định thực sự đã bị loại bỏ hoặc đã được giảm thiểu khỏi phần mềm. Kiểm thử viên có thể lặp lại quá trình chẩn đoán có hoặc không có việc thay đổi cấu hình chẩn đoán hoặc các kịch bản kiểm thử, hoặc cả hai.

6.11.6.2 Mức an toàn 3 và 4

Bảng 375 - VE và TE của AS11.31

Kiểm thử từ phía nhà cung cấp - mức 3 và 4	
AS11.31 ISO/IEC 19790:2025, 7.11.6.3	Ngoài các yêu cầu đối với mức an toàn 1 và 2, tài liệu phải quy định các thủ tục và kết quả của quá trình kiểm thử mức thấp được thực hiện trên mô-đun mật mã.
Thông tin bắt buộc từ nhà cung cấp	
VE11.31.01	Nhà cung cấp phải cung cấp tài liệu quy định các thủ tục và kết quả của quá trình kiểm thử mức thấp được thực hiện trên mô-đun mật mã.
Quy trình kiểm thử bắt buộc	
TE11.31.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu quy định các thủ tục và kết quả của quá trình kiểm thử mức thấp được thực hiện trên mô-đun mật mã.

6.11.7 Phân phối và hoạt động

6.11.7.1 Mức an toàn 1

Bảng 376 - VE và TE của AS11.32

Phân phối và hoạt động - mức 1, 2, 3 và 4	
AS11.32 ISO/IEC 19790:2025, 7.11.7.2	Đối với mức an toàn 1, tài liệu phải quy định các thủ tục nhằm lắp đặt, khởi tạo, và khởi động an toàn cho mô-đun mật mã.
Thông tin bắt buộc từ nhà cung cấp	
VE11.32.01	Tài liệu do nhà cung cấp cung cấp phải mô tả các bước cần thiết nhằm lắp đặt, khởi tạo, và khởi động an toàn cho mô-đun mật mã.
Quy trình kiểm thử bắt buộc	
TE11.32.01	Kiểm thử viên phải xác minh tài liệu do nhà cung cấp cung cấp rằng nó có bao gồm các thủ tục lắp đặt, khởi tạo, và khởi động mang lại một cấu hình an toàn.
TE11.32.02	Kiểm thử viên phải thực hiện các thủ tục lắp đặt, khởi tạo, và khởi động an toàn cho mô-đun mật mã và xác minh tính chính xác của chúng.

6.11.7.2 Mức an toàn 2 và 3

Bảng 377 - VE và TE của AS11.33

Phân phối và hoạt động - mức 2, 3 và 4	
AS11.33 ISO/IEC 19790:2025, 7.11.7.3	Ngoài yêu cầu đối với mức an toàn 1, tài liệu phải quy định các thủ tục bắt buộc nhằm duy trì an toàn trong quá trình phân phối, lắp đặt và khởi tạo các phiên bản của một mô-đun mật mã cho những người vận hành được ủy quyền.
Thông tin bắt buộc từ nhà cung cấp	
VE11.33.01	Tài liệu phân phối phải mô tả các thủ tục cần thiết nhằm duy trì an toàn khi phân phối mô-đun mật mã cho những người vận hành được ủy quyền.
Quy trình kiểm thử bắt buộc	
TE11.33.01	Kiểm thử viên phải xác minh tài liệu do nhà cung cấp cung cấp nhằm đảm bảo rằng các thủ tục bắt buộc để duy trì an toàn trong quá trình phân phối và giao các phiên bản của mô-đun mật mã cho những người vận hành được ủy quyền là chính xác.

Bảng 378 - VE và TE của AS11.34

Phân phối và hoạt động - mức 2, 3 và 4	
AS11.34 ISO/IEC 19790:2025, 7.11.7.3	Các thủ tục phải quy định cách thức phát hiện sự can thiệp trong quá trình phân phối, lắp đặt và khởi tạo mô-đun cho những người vận hành được ủy quyền.
Thông tin bắt buộc từ nhà cung cấp	
VE11.34.01	Nhà cung cấp phải cung cấp tài liệu quy định các thủ tục về cách thức phát hiện sự can thiệp trong quá trình phân phối, lắp đặt và khởi tạo mô-đun cho những người vận hành được ủy quyền.
Quy trình kiểm thử bắt buộc	
TE11.34.01	Kiểm thử viên phải xác minh rằng nhà cung cấp cung cấp tài liệu quy định các thủ tục về cách thức phát hiện sự can thiệp trong quá trình phân phối, lắp đặt và khởi tạo mô-đun cho những người vận hành được ủy quyền.

6.11.7.3 Mức an toàn 4**Bảng 379 - VE và TE của AS11.35**

Phân phối và hoạt động - mức 4	
AS11.35 ISO/IEC 19790:2025, 7.11.7.4	Ngoài các yêu cầu của mức an toàn 1, 2 và 3, các thủ tục phải yêu cầu mô-đun xác thực người vận hành được ủy quyền bằng dữ liệu xác thực riêng cho từng người vận hành, do nhà cung cấp cung cấp.
Thông tin bắt buộc từ nhà cung cấp	
VE11.35.01	Nhà cung cấp phải cung cấp tài liệu cho các thủ tục bắt buộc người vận hành được ủy quyền phải được mô-đun xác thực bằng cách sử dụng dữ liệu xác thực do nhà cung cấp cung cấp.
VE11.35.02	Tài liệu do nhà cung cấp cung cấp phải quy định các thủ tục nhằm tạo ra dữ liệu xác thực sao cho nó trở thành thông tin riêng biệt cho từng người vận hành.
VE11.35.03	Tài liệu do nhà cung cấp cung cấp phải quy định cách thức dữ liệu xác thực được nhà cung cấp tạo ra một cách an toàn đối với mỗi người vận hành.
VE11.35.04	Tài liệu do nhà cung cấp cung cấp phải quy định cách thức gửi an toàn dữ liệu xác thực riêng biệt của người vận hành đến mỗi người vận hành.
Quy trình kiểm thử bắt buộc	

TE11.35.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu cho các thủ tục bắt buộc người vận hành được ủy quyền phải được mô-đun xác thực bằng cách sử dụng dữ liệu xác thực do nhà cung cấp cung cấp.
TE11.35.02	Kiểm thử viên phải xác định xem dữ liệu xác thực được thiết lập tại nhà máy hoặc mặc định có được tạo ra sao cho nó trở thành thông tin riêng biệt cho từng người vận hành hay không.
TE11.35.03	Kiểm thử viên phải xác định xem dữ liệu xác thực được thiết lập tại nhà máy hoặc mặc định có được tạo ra một cách an toàn hay không.
TE11.35.04	Kiểm thử viên phải xác định xem dữ liệu xác thực được thiết lập tại nhà máy hoặc mặc định có được gửi một cách an toàn đến người vận hành được ủy quyền hay không.

6.11.7.4 Chứng thực

Bảng 380 - VE và TE của AS11.36

Phân phối và hoạt động - mức 1, 2, 3 và 4	
AS11.36 ISO/IEC 19790:2025, 7.11.7.5	Dịch vụ chứng thực phải được thiết kế và triển khai theo cách tuân thủ các tiêu chuẩn và yêu cầu áp dụng, như được định nghĩa trong ISO/IEC 19790:2025, Phụ lục G;
Thông tin bắt buộc từ nhà cung cấp	
VE11.36.01	Nhà cung cấp phải cung cấp tài liệu quy định cách thức mô-đun đã được thiết kế và triển khai theo cách thức tuân thủ các tiêu chuẩn và yêu cầu áp dụng cho dịch vụ chứng thực như được định nghĩa trong ISO/IEC 19790:2025, Phụ lục G.
Quy trình kiểm thử bắt buộc	
TE11.36.01	Kiểm thử viên phải xác minh rằng nhà cung cấp cung cấp tài liệu quy định cách thức mô-đun đã được thiết kế và triển khai theo cách thức tuân thủ các tiêu chuẩn và yêu cầu áp dụng cho dịch vụ chứng thực như được định nghĩa trong ISO/IEC 19790:2025, Phụ lục G.
TE11.36.02	Kiểm thử viên phải kiểm tra mô-đun để xác minh rằng mô-đun triển khai các tính năng có khả năng đáp ứng các mục tiêu chứng thực của các tiêu chuẩn áp dụng.
TE11.36.03	Kiểm thử viên phải xác nhận thông qua kiểm tra thực tế rằng bất kỳ thay đổi nào đối với mô-đun cũng được phản ánh vào các giá trị đo hỗ trợ cho dịch vụ chứng thực đã được thực hiện.

Bảng 381 - VE và TE của AS11.37

Phân phối và hoạt động - mức 1, 2, 3 và 4	
AS11.37 ISO/IEC 19790:2025, 7.11.7.5	Chính sách an toàn của mô-đun phải cung cấp hướng dẫn cho người dùng về việc sử dụng dịch vụ chứng thực của mô-đun bao gồm cách lấy bất kỳ danh tính mật mã nào của mô-đun được yêu cầu và lấy các bản ghi chứng thực; cách xác minh các bản ghi; và loại giá trị đo được bao gồm trong các bản ghi do mô-đun trả về.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	
Thông tin bắt buộc từ nhà cung cấp	
VE11.37.01	Chính sách an toàn của mô-đun do nhà cung cấp cung cấp phải cung cấp hướng dẫn cho người dùng về cách lấy bất kỳ danh tính mật mã nào của mô-đun được yêu cầu, cách lấy và xác minh các bản ghi chứng thực, và loại giá trị đo nào được

	bao gồm trong các bản ghi đó.
TE11.37.01	Kiểm thử viên phải xác minh xem chính sách an toàn có cung cấp hướng dẫn cho người dùng về cách lấy bất kỳ danh tính mật mã nào của mô-đun được yêu cầu, cách lấy và xác minh các bản ghi chứng thực, và loại giá trị đo nào được bao gồm trong các bản ghi đó hay không.
TE11.37.02	Kiểm thử viên phải sử dụng các thủ tục được lập tài liệu trong chính sách an toàn để lấy một danh tính từ mô-đun để được sử dụng với dịch vụ chứng thực. Nếu kiểm thử viên không thể lấy được danh tính của mô-đun, bài kiểm thử sẽ thất bại.
TE11.37.03	Kiểm thử viên phải sử dụng các thủ tục được lập tài liệu trong chính sách an toàn để lấy một bản ghi chứng thực được sinh ra bởi dịch vụ chứng thực của mô-đun. Nếu kiểm thử viên không thể lấy được bản ghi chứng thực, bài kiểm thử sẽ thất bại.

6.11.7.5 Kết thúc vòng đời

6.11.7.5.1 Yêu cầu chung về kết thúc vòng đời

Bảng 382 - VE và TE của AS11.38

Phân phối và hoạt động - mức 1, 2, 3 và 4	
AS11.38 ISO/IEC 19790:2025, 7.11.7.6.1	Chính sách an toàn phải lập tài liệu về các thủ tục kết thúc vòng đời, cung cấp một bản tóm tắt về các thủ tục kết thúc vòng đời, hoặc một tham chiếu bên ngoài có sẵn công khai chỉ ra nơi có thể tìm thấy các thủ tục kết thúc vòng đời của mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE11.38.01	Nhà cung cấp phải cung cấp tài liệu quy định các thủ tục cho việc kết thúc vòng đời của mô-đun mật mã.
Quy trình kiểm thử bắt buộc	
TE11.38.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu quy định các thủ tục cho việc kết thúc vòng đời của mô-đun mật mã.

6.11.7.5.2 Mức an toàn 1 và 2

Bảng 383 - VE và TE của AS11.39

Phân phối và hoạt động - mức 1 và 2	
AS11.39 ISO/IEC 19790:2025, 7.11.7.6.2	Đối với mức an toàn 1 và 2, tài liệu phải quy định các thủ tục để xóa an toàn mô-đun mật mã.
Thông tin bắt buộc từ nhà cung cấp	
VE11.39.01	Nhà cung cấp phải cung cấp tài liệu quy định các thủ tục để xóa an toàn mô-đun mật mã.
Quy trình kiểm thử bắt buộc	
TE11.39.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu quy định các thủ tục để xóa an toàn mô-đun mật mã.

6.11.7.5.3 Mức an toàn 3 và 4

Bảng 384 - VE và TE của AS11.40

Phân phối và hoạt động - mức 3 và 4	
AS11.40 ISO/IEC 19790:2025, 7.11.7.6.3	Ngoài các yêu cầu đối với mức an toàn 1 và 2, tài liệu phải quy định các thủ tục cần thiết cho việc phá hủy an toàn (ví dụ: khiến cho mô-đun không thể vận hành và không thể sửa chữa được) đối với mô-đun.
Thông tin bắt buộc từ nhà cung cấp	
VE11.40.01	Nhà cung cấp phải cung cấp tài liệu quy định các thủ tục cần thiết cho việc phá hủy an toàn mô-đun.
Quy trình kiểm thử bắt buộc	
TE11.40.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu quy định các thủ tục cần thiết cho việc phá hủy an toàn mô-đun.

6.11.8 Tài liệu hướng dẫn

Bảng 385 - VE và TE của AS11.41

Tài liệu hướng dẫn - mức 1, 2, 3 và 4	
AS11.41 ISO/IEC 19790:2025, 7.11.8	Hướng dẫn dành cho quản trị viên phải quy định: a) các chức năng quản trị, các sự kiện an toàn, các tham số an toàn (và các giá trị tham số, nếu phù hợp), các cổng vật lý, và các giao diện logic của mô-đun mật mã có sẵn cho chuyên viên mật mã hoặc các vai trò quản trị, hoặc cả hai; b) thông tin và các thủ tục bắt buộc đối với dữ liệu xác thực và các cơ chế, chẳng hạn như cho lần xác thực đầu tiên và việc quản lý các vai trò, cũng như mọi hướng dẫn khác bắt buộc đối với việc xác thực; c) các thủ tục về cách thức quản trị mô-đun mật mã; và d) các giả định liên quan đến hành vi của người dùng vốn có liên quan đến việc vận hành an toàn của mô-đun mật mã.
Thông tin bắt buộc từ nhà cung cấp	
VE11.41.01	Nhà cung cấp phải cung cấp tài liệu bao gồm các thông tin được liệt kê trong AS11.41.
VE11.41.02	Hướng dẫn phi độc quyền phải có sẵn cho các quản trị viên phù hợp của mô-đun.
Quy trình kiểm thử bắt buộc	
TE11.41.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu bao gồm các thông tin được liệt kê trong AS11.41.

Bảng 386 - VE và TE của AS11.42

Tài liệu hướng dẫn - mức 1, 2, 3 và 4	
AS11.42 ISO/IEC 19790:2025, 7.11.8	Hướng dẫn không dành cho quản trị viên phải quy định: a) các chức năng an toàn đã phê duyệt và không được phê duyệt, các cổng vật lý, và các giao diện logic có sẵn cho người dùng của một mô-đun mật mã; và b) tất cả các trách nhiệm của người dùng cần thiết đối với sự hoạt động của một mô-đun mật mã.
Thông tin bắt buộc từ nhà cung cấp	

TCVN 12211:2026

VE11.42.01	Nhà cung cấp phải cung cấp tài liệu bao gồm danh sách thông tin trong AS11.42.
VE11.42.02	Hướng dẫn phi độc quyền phải có sẵn cho những đối tượng không phải là quản trị viên phù hợp của mô-đun.
Quy trình kiểm thử bắt buộc	
TE11.42.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu bao gồm danh sách thông tin trong AS11.42.

6.12 Giảm thiểu các tấn công khác**6.12.1 Yêu cầu chung về giảm thiểu các tấn công khác**

CHÚ THÍCH 1 Sự tồn tại và hoạt động thích hợp của các cơ chế an toàn sẽ được thẩm định khi các yêu cầu và các bài kiểm thử liên quan được phát triển.

CHÚ THÍCH 2 Chính sách an toàn phi độc quyền bao gồm thông tin được yêu cầu trong ISO/IEC 19790:2025, B.2.12.

Bảng 387 - VE và TE của AS12.01

Yêu cầu chung về giảm thiểu các tấn công khác - mức 1, 2, 3 và 4	
AS12.01 ISO/IEC 19790:2025, 7.1.2.1	Tài liệu về giảm thiểu các tấn công khác được quy định trong ISO/IEC 19790:2025, A.2.11 phải được cung cấp.
Thông tin bắt buộc từ nhà cung cấp	
VE12.01.01	Nhà cung cấp phải cung cấp các yêu cầu về tài liệu như được quy định trong ISO/IEC 19790:2025, A.2.11.
Quy trình kiểm thử bắt buộc	
TE12.01.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu như quy định trong ISO/IEC 19790:2025, A.2.11.

6.12.2 Mức an toàn 1, 2 và 3**Bảng 388 - VE và TE của AS12.02**

Mức an toàn 1, 2 và 3 - mức 1, 2, 3 và 4	
AS12.02 ISO/IEC 19790:2025, 7.1.2.2	Nếu một mô-đun mật mã được thiết kế để giảm thiểu một hoặc nhiều tấn công cụ thể không được định nghĩa trong tiêu chuẩn này và được nhà cung cấp mô-đun tuyên bố, thì các tài liệu hỗ trợ của mô-đun phải liệt kê các tấn công mà mô-đun được thiết kế để giảm thiểu.
Thông tin bắt buộc từ nhà cung cấp	
VE12.02.01	Nhà cung cấp phải cung cấp tài liệu hỗ trợ liệt kê các tấn công mà mô-đun được thiết kế để giảm thiểu.
Quy trình kiểm thử bắt buộc	
TE12.02.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu hỗ trợ liệt kê các tấn công mà mô-đun được thiết kế để giảm thiểu.

6.12.3 Mức an toàn 4**Bảng 389 - VE và TE của AS12.03**

Mức an toàn 4 - mức 4

AS12.03 ISO/IEC 19790:2025, 7.1.2.3	Ngoài các yêu cầu đối với mức an toàn 1, 2 và 3, yêu cầu sau đây phải được áp dụng cho các mô-đun mật mã ở mức an toàn 4:
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của AS12.04.	

Bảng 390 - VE và TE của AS12.04

Mức an toàn 4 - mức 4	
AS12.04 ISO/IEC 19790:2025, 7.1.2.3	Nếu việc giảm thiểu các tấn công cụ thể không được định nghĩa trong tiêu chuẩn này được tuyên bố, tài liệu phải quy định các phương pháp được sử dụng để giảm thiểu các tấn công và các phương pháp để kiểm thử tính hiệu quả của các kỹ thuật giảm thiểu này.
Thông tin bắt buộc từ nhà cung cấp	
VE12.04.01	Nhà cung cấp phải quy định trong tài liệu các phương pháp được sử dụng để giảm thiểu các tấn công.
VE12.04.02	Nhà cung cấp phải quy định trong tài liệu các phương pháp kiểm thử được sử dụng để kiểm thử tính hiệu quả của các kỹ thuật giảm thiểu.
VE12.04.03	Nhà cung cấp phải quy định trong tài liệu tính hiệu quả của các kỹ thuật giảm thiểu.
Quy trình kiểm thử bắt buộc	
TE12.04.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu quy định các phương pháp được sử dụng để giảm thiểu các tấn công.
TE12.04.02	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu quy định các phương pháp kiểm thử được sử dụng để kiểm thử tính hiệu quả của các kỹ thuật giảm thiểu.
TE12.04.03	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu quy định tính hiệu quả của các kỹ thuật giảm thiểu.

7 Các yêu cầu về tài liệu

7.1 Mục đích

Bảng 391 - VE và TE của ASA.01

Mục đích - mức 1, 2, 3 và 4	
ASA.01 ISO/IEC 19790:2025, A.1	ISO/IEC 19790:2025, Phụ lục A quy định các tài liệu tối thiểu bắt buộc phải có đối với một mô-đun mật mã trải qua quá trình kiểm thử độc lập.
Thông tin bắt buộc từ nhà cung cấp	
VEA.01.01	Nhà cung cấp phải cung cấp tài liệu cho mô-đun mật mã đáp ứng nhưng không giới hạn ở các yêu cầu về tài liệu tối thiểu như được quy định trong ISO/IEC 19790:2025, từ A.2.1 đến A.2.11.
Quy trình kiểm thử bắt buộc	
TEA.01.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp tài liệu cho mô-đun mật mã đáp ứng nhưng không giới hạn ở các yêu cầu về tài liệu tối thiểu như được quy định trong ISO/IEC 19790:2025, từ A.2.1 đến A.2.11.

7.2 Các hạng mục

7.2.1 Đặc tả mô-đun mật mã

Bảng 392 - VE và TE của ASA.02

Đặc tả mô-đun mật mã - mức 1, 2, 3 và 4	
ASA.02 ISO/IEC 19790:2025, A.2.1	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 1, 2, 3 và 4: a) đặc tả về loại mô-đun (phần cứng, phần mềm, phần sụn, mô-đun phần mềm lai ghép hoặc mô-đun phần sụn lai ghép); b) đặc tả về biên mật mã của mô-đun; c) đặc tả về các thành phần phần cứng, phần mềm và phần sụn của mô-đun mật mã, và mô tả về cấu hình vật lý của mô-đun; d) đặc tả về các thành phần phần cứng, phần mềm hoặc phần sụn của mô-đun mật mã được loại trừ khỏi các yêu cầu an toàn của ISO/IEC 19790:2025, Điều 7 và lời giải thích về lý do của việc loại trừ đó; e) đặc tả về các cổng vật lý và giao diện logic của một mô-đun mật mã; f) đặc tả về các kiểm soát thủ công hoặc logic của một mô-đun mật mã, các chỉ báo trạng thái vật lý hoặc logic, và các đặc tính vật lý, logic, và điện có thể áp dụng; g) đặc tả về tất cả các chức năng an toàn, cả đã phê duyệt và không được phê duyệt, được sử dụng bởi một mô-đun mật mã và đặc tả về tất cả các chế độ hoạt động, cả đã phê duyệt và không được phê duyệt; h) sơ đồ khối mô tả tất cả các thành phần phần cứng chính của một mô-đun mật mã và các kết nối giữa các thành phần, bao gồm bất kỳ bộ vi xử lý nào, bộ đệm đầu vào/đầu ra, bộ đệm bản rõ/bản mã, bộ đệm kiểm soát, bộ lưu trữ khóa, bộ nhớ làm việc, và bộ nhớ chương trình; i) đặc tả về thiết kế của phần cứng, phần mềm và phần sụn của một mô-đun mật mã; j) đặc tả về tất cả các thông tin liên quan đến bảo mật, bao gồm các khóa mật mã bí mật và riêng tư (cả dạng rõ và dạng mã hóa), dữ liệu xác thực (ví dụ: mật khẩu, mã PIN), dữ liệu kiểm chứng, các CSP, các PSP, và các thông tin được bảo vệ khác (ví dụ: các sự kiện được kiểm toán, dữ liệu kiểm toán) mà việc tiết lộ hoặc sửa đổi chúng có thể làm tổn hại đến tính an toàn của mô-đun mật mã; k) đặc tả về cách mô-đun hỗ trợ hoạt động suy giảm; và l) đặc tả về một chính sách an toàn của mô-đun mật mã bao gồm các hướng dẫn bắt nguồn từ các yêu cầu của ISO/IEC 19790:2025, Điều 7 và các hướng dẫn bắt nguồn từ bất kỳ yêu cầu bổ sung nào do nhà cung cấp áp đặt.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

7.2.2 Giao diện mô-đun mật mã

Bảng 393 - VE và TE của ASA.03

Giao diện mô-đun mật mã - mức 1, 2, 3 và 4	
ASA.03 ISO/IEC 19790:2025, A.2.2	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 1, 2, 3 và 4: a) đặc tả về giao diện đầu vào dữ liệu, đầu ra dữ liệu, đầu vào điều khiển, đầu ra điều khiển, đầu ra trạng thái và các giao diện nguồn điện, cả vật lý và logic; và b) đặc tả về các ngoại lệ và cơ sở hợp lý nếu giao diện đầu ra điều khiển không bị chặn trong trạng thái lỗi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

Bảng 394 - VE và TE của ASA.04

Giao diện mô-đun mật mã - mức 1, 2, 3 và 4	
ASA.04 ISO/IEC 19790:2025, A.2.2	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 3 và 4: a) đặc tả về giao diện đường dẫn tin cậy dạng rõ.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

7.2.3 Vai trò, dịch vụ và xác thực**Bảng 395 - VE và TE của ASA.05**

Vai trò, dịch vụ và xác thực - mức 1, 2, 3 và 4	
ASA.05 ISO/IEC 19790:2025, A.2.3	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 1, 2, 3 và 4: a) đặc tả về tất cả các vai trò được ủy quyền do một mô-đun mật mã hỗ trợ; b) đặc tả về các dịch vụ, hoạt động, hoặc chức năng do một mô-đun mật mã cung cấp, cả đã phê duyệt và không được phê duyệt. Đối với mỗi dịch vụ, phải có đặc tả về đầu vào dịch vụ, đầu ra dịch vụ tương ứng, và các vai trò được ủy quyền mà theo đó dịch vụ có thể được thực hiện; c) đặc tả về bất kỳ dịch vụ nào do một mô-đun mật mã cung cấp mà người vận hành không bắt buộc phải đảm nhận một vai trò được ủy quyền, và cách các dịch vụ này không sửa đổi, tiết lộ, hoặc thay thế các khóa mật mã và các CSP khác, hoặc tổn hại đến tính an toàn của mô-đun; d) đặc tả về các dịch vụ của mô-đun thực hiện hiển thị thông tin phiên bản của mô-đun, hiển thị trạng thái, thực hiện tự kiểm thử, thực hiện các chức năng an toàn đã phê duyệt và thực hiện việc xóa trắng; e) đặc tả về các cơ chế bỏ qua mật mã; f) đặc tả về các cơ chế nạp phần mềm hoặc phần sụn; và g) đặc tả về các kiểm soát và giao diện bỏ qua xác thực lại.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

Bảng 396 - VE và TE của ASA.06

Vai trò, dịch vụ và xác thực - mức 1, 2, 3 và 4
--

ASA.06 ISO/IEC 19790:2025, A.2.3	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 2, 3 và 4: a) đặc tả về các cơ chế xác thực do một mô-đun mật mã hỗ trợ, các loại dữ liệu kiểm chứng bắt buộc để triển khai các cơ chế xác thực được hỗ trợ, các phương pháp được ủy quyền sử dụng để kiểm soát truy cập vào mô-đun lần đầu tiên và khởi tạo cơ chế xác thực, và các phương pháp giới hạn tốc độ của các cơ chế xác thực do mô-đun hỗ trợ, bao gồm cơ sở hợp lý hỗ trợ cho việc sử dụng nhiều cơ chế xác thực.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

7.2.4 An toàn phần mềm/phần sụn

Bảng 397 - VE và TE của ASA.07

An toàn phần mềm/phần sụn - mức 1, 2, 3 và 4	
ASA.07 ISO/IEC 19790:2025, A.2.4	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 1, 2, 3 và 4: a) đặc tả về các kỹ thuật toàn vẹn đã phê duyệt hoặc mã phát hiện sai (EDC) được sử dụng; b) đặc tả về phương pháp để người vận hành thực hiện bài kiểm thử tính toàn vẹn theo yêu cầu.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

Bảng 398 - VE và TE của ASA.08

An toàn phần mềm/phần sụn - mức 1, 2, 3 và 4	
ASA.08 ISO/IEC 19790:2025, A.2.4	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 2, 3 và 4: a) đặc tả về định dạng của mã thực thi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

7.2.5 Môi trường hoạt động

Bảng 399 - VE và TE của ASA.09

Môi trường hoạt động - mức 1, 2, 3 và 4	
ASA.09 ISO/IEC 19790:2025, A.2.5	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 1 và 2: a) đặc tả về môi trường hoạt động và quản lý phiên bản bao gồm, nếu có thể áp dụng, hệ điều hành do mô-đun sử dụng; b) đặc tả về các chính sách an toàn, cài đặt hoặc các hạn chế đối với cấu hình của hệ điều hành.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

Bảng 400 - VE và TE của ASA.10

Môi trường hoạt động - mức 1, 2, 3 và 4
--

ASA.10 ISO/IEC 19790:2025, A.2.5	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 2: a) tài liệu hướng dẫn quản trị viên để cấu hình hệ điều hành theo các yêu cầu đặc tả và các phương pháp xác thực.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

7.2.6 An toàn vật lý

Bảng 401 - VE và TE của ASA.11

An toàn vật lý - mức 1, 2, 3 và 4	
ASA.11 ISO/IEC 19790:2025, A.2.6	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 1, 2, 3 và 4: a) đặc tả về hình thái vật lý và mức an toàn mà các cơ chế an toàn vật lý của một mô-đun mật mã được triển khai. Đặc tả về các cơ chế an toàn vật lý được sử dụng bởi một mô-đun; và b) nếu một mô-đun mật mã bao gồm một vai trò bảo trì yêu cầu quyền truy cập vật lý vào các nội dung của mô-đun hoặc nếu mô-đun được thiết kế để cho phép truy cập vật lý, phải có đặc tả về giao diện bảo trì và cách thức cũng như việc các SSP nào sẽ bị xóa trắng khi giao diện bảo trì được truy cập.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

Bảng 402 - VE và TE của ASA.12

An toàn vật lý - mức 1, 2, 3 và 4	
ASA.12 ISO/IEC 19790:2025, A.2.6	Các đặc tả mô-đun mật mã bổ sung sau đây phải được lập tài liệu đối với mức an toàn 2, 3 và 4: a) đặc tả về tất cả các đường dẫn tin cậy được bảo vệ, nếu có, trong các mô-đun đa chip, và chức năng mật mã đã phê duyệt được sử dụng.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

Bảng 403 - VE và TE của ASA.13

An toàn vật lý - mức 1, 2, 3 và 4	
ASA.13 ISO/IEC 19790:2025, A.2.6	Các đặc tả mô-đun mật mã bổ sung sau đây phải được lập tài liệu đối với mức an toàn 3: a) đặc tả về các dải hoạt động bình thường của một mô-đun mật mã. Đặc tả về các tính năng bảo vệ chống sự cố môi trường được sử dụng bởi một mô-đun mật mã hoặc đặc tả về các bài kiểm thử sự cố môi trường được thực hiện.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

Bảng 404 - VE và TE của ASA.14

An toàn vật lý - mức 1, 2, 3 và 4
--

ASA.14 ISO/IEC 19790:2025, A.2.6	Các đặc tả mô-đun mật mã bổ sung sau đây phải được lập tài liệu đối với mức an toàn 4: a) đặc tả về các tính năng bảo vệ chống sự cố môi trường được sử dụng bởi một mô-đun mật mã; và b) đặc tả về các kỹ thuật giảm thiểu việc tiêm lỗi được sử dụng.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

7.2.7 An toàn không xâm lấn

Bảng 405 - VE và TE của ASA.15

An toàn không xâm lấn - mức 1, 2, 3 và 4	
ASA.15 ISO/IEC 19790:2025, A.2.7	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 1, 2, 3 và 4: a) đặc tả về các kỹ thuật giảm thiểu được sử dụng để chống lại các tấn công không xâm lấn bao gồm cả những kỹ thuật được quy định trong ISO/IEC 19790:2025, Phụ lục F; và b) bằng chứng về tính hiệu quả của mỗi kỹ thuật giảm thiểu tấn công được sử dụng.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

7.2.8 Quản lý tham số an toàn nhạy cảm

Bảng 406 - VE và TE của ASA.16

Quản lý tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
ASA.16 ISO/IEC 19790:2025, A.2.8	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 1, 2, 3 và 4: a) đặc tả về tất cả các SSP được sử dụng bởi một mô-đun mật mã; b) đặc tả về tất cả các RBG và việc sử dụng chúng; c) đặc tả về entropy tối thiểu được yêu cầu bởi mô-đun đối với mỗi tham số đầu vào entropy được nhập vào; d) đặc tả về mỗi RBG (đã phê duyệt và không được phê duyệt cùng với các nguồn entropy) được sử dụng bởi một mô-đun mật mã; e) đặc tả về đầu vào entropy tối thiểu và phương pháp tạo ra lượng entropy tối thiểu như được tuyên bố nếu đầu vào entropy được thu thập từ bên trong biên mật mã của mô-đun mật mã; f) đặc tả về mỗi phương pháp tạo SSP có sử dụng RBG; g) đặc tả về mỗi phương pháp tạo SSP được sử dụng bởi một mô-đun; h) đặc tả về mỗi phương pháp tạo khóa (đã phê duyệt và không được phê duyệt) được sử dụng bởi một mô-đun mật mã; i) đặc tả về các phương pháp thiết lập SSP được sử dụng bởi một mô-đun mật mã;

	j) đặc tả về các phương pháp nhập và xuất SSP được sử dụng bởi một mô-đun; k) đặc tả về các SSP được lưu trữ trong các mô-đun; l) đặc tả về cách các CSP được bảo vệ nhằm chống lại việc truy cập, sử dụng, tiết lộ, sửa đổi, và thay thế trái phép khi chúng được lưu trữ trong mô-đun; m) đặc tả về cách các PSP được bảo vệ nhằm chống lại sự sửa đổi và thay thế trái phép khi được lưu trữ bên trong mô-đun; n) đặc tả về cách mô-đun liên kết một PSP được lưu trữ trong mô-đun với thực thể (người vận hành, vai trò, hoặc quá trình) mà tham số đó được gán cho; o) đặc tả về các phương pháp xóa trắng được sử dụng bởi một mô-đun, bao gồm cả về mặt thủ tục, và cơ sở hợp lý về cách các phương pháp đó ngăn chặn việc truy xuất và tái sử dụng các giá trị đã bị xóa trắng; và p) danh sách các SSP được tuyên bố miễn trừ khỏi các yêu cầu xóa trắng, bao gồm: các yêu cầu xóa trắng cụ thể không được thực thi đối với từng SSP; lý giải đối với từng SSP về việc sự tồn tại của SSP đó không trực tiếp gây tổn hại đến dữ liệu người dùng, quyền riêng tư hoặc các SSP khác bảo vệ dữ liệu người dùng hoặc quyền riêng tư; và cách thức các SSP được miễn trừ đóng góp vào tính an toàn của mô-đun
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

Bảng 407 - VE và TE của ASA.17

Quản lý tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
ASA.17 ISO/IEC 19790:2025, A.2.8	Các đặc tả mô-đun mật mã bổ sung sau đây phải được lập tài liệu đối với mức an toàn 3 và 4: a) nếu các thủ tục phân chia thông tin được sử dụng, tài liệu được cung cấp nhằm chứng minh rằng nếu yêu cầu phải biết về n thành phần để tái tạo lại CSP ban đầu, thì việc biết bất kỳ số lượng $n-1$ thành phần nào cũng không cung cấp thông tin nào về CSP ban đầu ngoài độ dài của nó; và b) đặc tả về các thủ tục phân chia thông tin được sử dụng bởi một mô-đun.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

7.2.9 Tự kiểm thử**Bảng 408 - VE và TE của ASA.18**

Tự kiểm thử - mức 1, 2, 3 và 4	
ASA.18 ISO/IEC 19790:2025, A.2.9	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 1, 2, 3 và 4: a) đặc tả về các quá trình tự kiểm thử được thực hiện bởi một mô-đun mật mã, bao gồm các bài kiểm thử trước khi vận hành và có điều kiện;

	b) đặc tả về việc liệu một bài tự kiểm thử đang được thực hiện trên dữ liệu nội bộ của mô-đun, hay dữ liệu được cung cấp từ một nguồn bên ngoài; c) đặc tả về chỉ báo trạng thái thất bại của bài tự kiểm thử; d) đặc tả về các trạng thái lỗi mà một mô-đun mật mã có thể bước vào khi một bài tự kiểm thử thất bại, và các điều kiện cũng như hành động cần thiết để thoát khỏi trạng thái lỗi đó và tiếp tục sự vận hành bình thường của mô-đun mật mã (ví dụ: có thể bao gồm việc bảo trì mô-đun, khởi động lại nguồn mô-đun, sự phục hồi tự động của mô-đun, đi vào trạng thái vận hành suy giảm hoặc trả mô-đun về nhà cung cấp để bảo dưỡng). Việc này bao gồm cả những điều kiện nào sẽ kích hoạt trạng thái lỗi khi bài kiểm thử chức năng trọng yếu có điều kiện thất bại; e) đặc tả về tất cả các chức năng an toàn mang tính trọng yếu đối với sự hoạt động an toàn của một mô-đun mật mã, đồng thời xác định các quá trình tự kiểm thử trước khi vận hành và tự kiểm thử có điều kiện có thể áp dụng được thực hiện bởi mô-đun; và f) nếu một mô-đun mật mã triển khai khả năng bỏ qua, phải có đặc tả về cơ chế hoặc logic chi phối thủ tục chuyển đổi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

7.2.10 Đảm bảo vòng đời

Bảng 409 - VE và TE của ASA.19

Đảm bảo vòng đời - mức 1, 2, 3 và 4	
ASA.19 ISO/IEC 19790:2025, A.2.10	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 1, 2, 3 và 4: a) đặc tả về hệ thống quản lý cấu hình được sử dụng cho mô-đun mật mã; b) đặc tả về các tài liệu hỗ trợ cho việc phát triển mô-đun mật mã và các tài liệu liên quan do hệ thống quản lý cấu hình cung cấp; c) đặc tả về các thủ tục để lắp đặt, khởi tạo, và khởi động an toàn cho một mô-đun mật mã; d) đặc tả về sự tương ứng giữa thiết kế của các thành phần phần cứng và phần mềm hoặc phần sụn của một mô-đun mật mã, với chính sách an toàn của mô-đun mật mã và mô hình trạng thái hữu hạn (FSM); e) nếu một mô-đun mật mã có chứa phần mềm, phải có đặc tả về mã nguồn cho phần mềm đó, được chú thích bằng các bình luận mô tả một cách rõ ràng sự tương ứng của phần mềm với thiết kế của mô-đun; f) nếu một mô-đun mật mã có chứa phần cứng, phải có đặc tả về các sơ đồ nguyên lý, hoặc danh sách HDL, hoặc cả hai cho phần cứng đó nếu có thể áp dụng; g) đặc tả về FSM (hoặc tương đương) bằng cách sử dụng một biểu đồ chuyển đổi trạng thái và bảng chuyển đổi trạng thái, trong đó bao

	gồm: 1) các trạng thái hoạt động và trạng thái lỗi của một mô-đun mật mã; 2) các quá trình chuyển đổi tương ứng từ trạng thái này sang trạng thái khác; 3) các sự kiện đầu vào, bao gồm các đầu vào dữ liệu và đầu vào điều khiển, vốn gây ra sự chuyển đổi từ trạng thái này sang trạng thái khác; và 4) các sự kiện đầu ra, bao gồm các điều kiện nội bộ của mô-đun, các đầu ra dữ liệu, và đầu ra trạng thái, vốn là kết quả từ việc chuyển đổi từ trạng thái này sang trạng thái khác; h) đặc tả về mã nguồn của phần mềm hoặc phần sụn; i) đặc tả về các tiêu chuẩn chứng thực được mô-đun đáp ứng; j) đối với hướng dẫn dành cho quản trị viên, đặc tả về: 1) các chức năng quản trị, sự kiện an toàn, tham số an toàn (và các giá trị tham số, nếu phù hợp), cổng vật lý, và giao diện logic của mô-đun mật mã có sẵn cho chuyên viên mật mã ; 2) các thủ tục về cách thức quản trị mô-đun mật mã một cách an toàn; và 3) các giả định liên quan đến hành vi người dùng vốn liên quan đến sự vận hành an toàn của mô-đun mật mã; k) đối với hướng dẫn không dành cho quản trị viên, đặc tả về: 1) các chức năng an toàn đã phê duyệt, cổng vật lý, và giao diện logic có sẵn cho những người dùng của mô-đun mật mã; và 2) tất cả các trách nhiệm của người dùng cần thiết đối với sự hoạt động an toàn của mô-đun.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

Bảng 410 - VE và TE của ASA.20

Đảm bảo vòng đời - mức 1, 2, 3 và 4	
ASA.20 ISO/IEC 19790:2025, A.2.10	Các đặc tả mô-đun mật mã bổ sung sau đây phải được lập tài liệu đối với mức an toàn 2, 3 và 4: a) đặc tả về một đặc tả chức năng mô tả không chính thức mô-đun mật mã, chức năng của mô-đun mật mã, các cổng vật lý bên ngoài và giao diện logic của mô-đun mật mã, cũng như mục đích của các cổng vật lý và giao diện logic đó; và b) đặc tả về các thủ tục nhằm duy trì an toàn trong quá trình phân phối và giao các phiên bản của một mô-đun mật mã cho những người vận hành được ủy quyền.

Quy trình kiểm thử bắt buộc

Khẳng định này được kiểm thử như một phần của ASA.01.

Bảng 411 - VE và TE của ASA.21

Đảm bảo vòng đời - mức 1, 2, 3 và 4	
ASA.21 ISO/IEC 19790:2025, A.2.10	Các đặc tả mô-đun mật mã bổ sung sau đây phải được lập tài liệu đối với mức an toàn 3 và 4: a) đặc tả về thiết kế chi tiết mô tả chức năng bên trong của các thành phần chính yếu thuộc mô-đun mật mã, các giao diện nội bộ giữa các thành phần, mục đích của các giao diện đó, và luồng thông tin nội bộ (bên trong toàn bộ biên mật mã cũng như bên trong từng thành phần chính yếu).
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

Bảng 412 - VE và TE của ASA.22

Đảm bảo vòng đời - mức 1, 2, 3 và 4	
ASA.22 ISO/IEC 19790:2025, A.2.10	Các đặc tả mô-đun mật mã bổ sung sau đây phải được lập tài liệu đối với mức an toàn 4: a) đặc tả về (bao gồm các tiền điều kiện và hậu điều kiện) sự tương ứng giữa thiết kế của mô-đun mật mã và đặc tả chức năng; và b) đối với mỗi thành phần phần cứng và phần mềm, việc chú thích mã nguồn bằng các bình luận phải quy định rõ (1) các tiền điều kiện được yêu cầu ngay khi bắt đầu truy cập vào thành phần, chức năng hoặc thủ tục của mô-đun nhằm đảm bảo việc thực thi diễn ra chính xác và (2) các hậu điều kiện được kỳ vọng là đúng khi quá trình thực thi của thành phần, chức năng, hoặc thủ tục của mô-đun hoàn tất.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

7.2.11 Giảm thiểu các tấn công khác**Bảng 413 - VE và TE của ASA.23**

Giảm thiểu các tấn công khác - mức 1, 2, 3 và 4	
ASA.23 ISO/IEC 19790:2025, A.2.11	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 1, 2 và 3: a) nếu một mô-đun mật mã được thiết kế để giảm thiểu một hoặc nhiều cuộc tấn công cụ thể không được định nghĩa trong ISO/IEC 19790:2025, Điều 7, tài liệu của mô-đun phải liệt kê các cơ chế an toàn được sử dụng bởi mô-đun mật mã nhằm giảm thiểu các cuộc tấn công đó.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

Bảng 414 - VE và TE của ASA.24

Giảm thiểu các tấn công khác - mức 1, 2, 3 và 4	
ASA.24 ISO/IEC 19790:2025, A.2.10	Các đặc tả mô-đun mật mã sau đây phải được lập tài liệu đối với mức an toàn 4: a) nếu một mô-đun mật mã được thiết kế để giảm thiểu một hoặc nhiều

	cuộc tấn công cụ thể không được định nghĩa trong ISO/IEC 19790:2025, Điều 7, tài liệu của mô-đun phải liệt kê các cơ chế an toàn được sử dụng bởi mô-đun mật mã nhằm giảm thiểu các cuộc tấn công đó; và b) nếu một mô-đun mật mã được thiết kế để giảm thiểu một hoặc nhiều cuộc tấn công cụ thể không được định nghĩa trong ISO/IEC 19790:2025, Điều 7, tài liệu phải ghi lại các phương pháp được sử dụng để giảm thiểu các cuộc tấn công cùng các phương pháp để kiểm thử tính hiệu quả của các kỹ thuật giảm thiểu đó.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASA.01.	

8 Chính sách an toàn cho mô-đun mật mã

8.1 Quy định chung

CHÚ THÍCH: ISO/IEC 19790:2025, Phụ lục B quy định các yêu cầu tối thiểu của một chính sách an toàn cho mô-đun mật mã.

Bảng 415 - VE và TE của ASB.01

Quy định chung - mức 1, 2, 3 và 4	
ASB.01 ISO/IEC 19790:2025, B.1	ISO/IEC 19790:2025, Phụ lục B tóm tắt các yêu cầu bắt buộc phải được đáp ứng trong chính sách an toàn phi độc quyền.
Thông tin bắt buộc từ nhà cung cấp	
VEB.01.01	Nhà cung cấp phải cung cấp một chính sách an toàn cho mô-đun mật mã phi độc quyền đáp ứng nhưng không giới hạn ở các yêu cầu tối thiểu về chính sách an toàn như được quy định trong ISO/IEC 19790:2025, từ B.2.1 đến B.2.12.
Quy trình kiểm thử bắt buộc	
TEB.01.01	Kiểm thử viên phải xác minh rằng nhà cung cấp có cung cấp một chính sách an toàn cho mô-đun mật mã phi độc quyền đáp ứng nhưng không giới hạn ở các yêu cầu tối thiểu về chính sách an toàn như được quy định trong ISO/IEC 19790:2025, từ B.2.1 đến B.2.12.

Bảng 416 - VE và TE của ASB.02

Quy định chung - mức 1, 2, 3 và 4	
ASB.02 ISO/IEC 19790:2025, B.1	Định dạng của chính sách an toàn phải được trình bày theo trình tự được chỉ định trong phụ lục này hoặc theo quy định của một tổ chức chứng nhận.
Thông tin bắt buộc từ nhà cung cấp	
VEB.02.01	Nhà cung cấp phải cung cấp một chính sách an toàn cho mô-đun mật mã phi độc quyền được trình bày theo trình tự được quy định trong ISO/IEC 19790:2025, từ B.2.1 đến B.2.12 hoặc theo quy định của một tổ chức chứng nhận.
Quy trình kiểm thử bắt buộc	
TEB.02.01	Kiểm thử viên phải xác minh rằng nhà cung cấp cung cấp một chính sách an toàn cho mô-đun mật mã phi độc quyền được trình bày theo trình tự quy định trong ISO/IEC 19790:2025, từ B.2.1 đến B.2.12 hoặc theo quy định của một tổ chức chứng nhận.

Bảng 417 - VE và TE của ASB.03

Quy định chung - mức 1, 2, 3 và 4	
ASB.03 ISO/IEC 19790:2025, B.1	Chính sách an toàn không được đánh dấu là độc quyền hoặc có bản quyền mà không kèm theo tuyên bố cho phép sao chép hoặc phân phối.
Thông tin bắt buộc từ nhà cung cấp	
VEB.03.01	Nhà cung cấp phải cung cấp một chính sách an toàn không được đánh dấu là độc quyền hoặc có bản quyền.
VEB.03.02	Nếu chính sách an toàn do nhà cung cấp cung cấp được đánh dấu là có bản quyền, thì nó phải bao gồm một tuyên bố cho phép sao chép hoặc phân phối.
Quy trình kiểm thử bắt buộc	
TEB.03.01	Kiểm thử viên phải xác minh rằng chính sách an toàn do nhà cung cấp cung cấp không được đánh dấu là độc quyền hoặc có bản quyền.
TEB.03.02	Nếu chính sách an toàn do nhà cung cấp cung cấp được đánh dấu là có bản quyền, thì kiểm thử viên phải xác minh rằng nó có bao gồm một tuyên bố cho phép sao chép hoặc phân phối.

8.2 Các hạng mục

8.2.1 Quy định chung

Bảng 418 - VE và TE của ASB.04

Quy định chung - mức 1, 2, 3 và 4	
ASB.04 ISO/IEC 19790:2025, B.2.1	Nội dung sau đây phải được bao gồm trong chính sách an toàn: a) một bảng chỉ ra các mức an toàn của các lĩnh vực riêng lẻ và, nếu có thể áp dụng, mức xếp hạng an toàn tổng thể của mô-đun.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	

8.2.2 Đặc tả mô-đun mật mã

Bảng 419 - VE và TE của ASB.05

Đặc tả mô-đun mật mã - mức 1, 2, 3 và 4	
ASB.05 ISO/IEC19790:2025, B.2.2	Nội dung sau đây phải được bao gồm trong chính sách an toàn: a) mục đích hoặc mục tiêu sử dụng của mô-đun bao gồm cả môi trường sử dụng dự kiến; b) sơ đồ minh họa, sơ đồ mạch điện hoặc hình ảnh của mô-đun. Một hình ảnh được bao gồm đối với các mô-đun phần cứng. Nếu chính sách an toàn bao gồm nhiều phiên bản của mô-đun, mỗi phiên bản được biểu diễn riêng biệt hoặc được chú thích sao cho phần hình ảnh minh họa cho tất cả các phiên bản. Đối với một mô-đun mật mã phần mềm hoặc phần sụn, chính sách an toàn bao gồm một sơ đồ khối minh họa: 1) vị trí đối tượng logic của mô-đun phần mềm hoặc phần sụn so với hệ điều hành, các ứng dụng hỗ trợ khác và biên mật mã sao cho tất cả các lớp logic và vật lý giữa đối tượng logic và biên mật mã

	đều được định nghĩa rõ ràng; và 2) các tương tác của đối tượng logic của mô-đun phần mềm hoặc phần sụn với hệ điều hành và các ứng dụng hỗ trợ khác nằm bên trong biên mật mã. c) mô tả về các mô-đun: 1) phiên bản hoặc định danh của các mô-đun và tất cả các thành phần (phần cứng, phần mềm hoặc phần sụn). d) sự chỉ định phần cứng, phần mềm, phần sụn, hoặc lai: 1) đối với các mô-đun mật mã phần mềm, phần sụn và lai, các hệ điều hành trên đó mô-đun đã được kiểm thử và các hệ điều hành mà nhà cung cấp khẳng định rằng có thể được mô-đun sử dụng. e) định nghĩa chính xác về các biên mật mã của mô-đun: 1) phần cứng, phần mềm hoặc phần sụn nằm trong các biên mật mã vốn được loại trừ khỏi các yêu cầu của tiêu chuẩn này và được quy định trong chính sách an toàn. f) các chế độ hoạt động và cách thức chuyển vào/ra từng chế độ. Chính sách an toàn mô tả mỗi chế độ hoạt động được triển khai trong mô-đun mật mã và cách thức mỗi chế độ được cấu hình; g) mô tả về hoạt động suy giảm; h) bảng liệt kê tất cả các chức năng an toàn, kèm theo các mức độ mạnh của khóa cụ thể được sử dụng cho các dịch vụ đã phê duyệt, cũng như các chế độ hoạt động được triển khai (ví dụ: CBC, CCM), nếu phù hợp; i) sơ đồ khối, nếu có thể áp dụng; j) thiết kế an toàn tổng thể và các quy tắc hoạt động; và k) các yêu cầu khởi tạo, nếu có thể áp dụng.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	

8.2.3 Giao diện mô-đun mật mã

Bảng 420 - VE và TE của ASB.06

Giao diện mô-đun mật mã - mức 1, 2, 3 và 4	
ASB.06 ISO/IEC 19790:2025, B.2.3	Nội dung sau đây phải được bao gồm trong chính sách an toàn: a) bảng liệt kê tất cả các cổng và giao diện (vật lý và logic); b) đặc tả về thông tin truyền qua năm giao diện logic; c) đặc tả về các cổng vật lý và dữ liệu truyền qua chúng; d) đặc tả về đường dẫn tin cậy dạng rõ; và e) đặc tả về các ngoại lệ và cơ sở hợp lý nếu giao diện đầu ra điều khiển

	không bị chặn trong trạng thái lỗi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	

8.2.4 Vai trò, dịch vụ và xác thực

Bảng 421 - VE và TE của ASB.07

Vai trò, dịch vụ và xác thực - mức 1, 2, 3 và 4	
ASB.07 ISO/IEC 19790:2025, B.2.4	Nội dung sau đây phải được bao gồm trong chính sách an toàn a) đặc tả về tất cả các vai trò; b) bảng các vai trò, cùng các lệnh dịch vụ tương ứng có đầu vào và đầu ra; c) đặc tả về từng phương pháp xác thực và liệu phương pháp đó dựa trên danh tính hay dựa trên vai trò; d) mô tả về cách thức đáp ứng yêu cầu về độ mạnh của việc xác thực (ví dụ: mô tả các phương pháp giới hạn tốc độ được sử dụng); e) nếu mô-đun bị khóa sau một số lần thử xác thực, mô tả về cách thức nó được mở khóa; f) nếu có khả năng bỏ qua mật mã, mô tả về hai hành động độc lập và cách thức trạng thái được kiểm tra; g) nếu có khả năng bỏ qua xác thực lại, mô tả về hai hành động độc lập và cách thức trạng thái được thể hiện. Đặc tả về những hoạt động mật mã nào và các chức năng an toàn đã phê duyệt khác hoặc các kỹ thuật quản lý SSP nào có thể được truy cập mà không cần tái xác thực khi tính năng bỏ qua đang được sử dụng; h) nếu có phần mềm hoặc phần sụn bên ngoài được nạp vào, đặc tả về các kiểm soát đối với việc nạp và sự cô lập mã lệnh nhằm ngăn chặn truy cập và sử dụng mô-đun trái phép; i) các danh sách riêng biệt đối với các dịch vụ an toàn và phi an toàn, cả đã phê duyệt và không được phê duyệt; j) đối với mỗi dịch vụ: 1) tên dịch vụ, 2) một mô tả ngắn gọn về mục đích hoặc ứng dụng của dịch vụ (trong một số trường hợp, chỉ riêng tên dịch vụ cũng có thể cung cấp thông tin này), 3) danh sách các chức năng an toàn đã phê duyệt được sử dụng bởi, hoặc được triển khai thông qua, việc gọi dịch vụ, 4) danh sách các SSP liên kết với dịch vụ hoặc với các chức năng an toàn đã phê duyệt mà nó sử dụng và chỉ báo đầu ra mà nó sử dụng để chỉ ra liệu một dịch vụ có thực thi một quá trình hay chức năng dịch vụ đã phê duyệt hay không. 5) Đối với mỗi vai trò người vận hành được ủy quyền sử dụng dịch

	vụ: 6) thông tin mô tả quyền truy cập riêng lẻ đối với tất cả các SSP; 7) thông tin mô tả phương pháp được sử dụng để xác thực từng vai trò k) nếu mô-đun mật mã có khả năng nạp các thành phần phần mềm hoặc phần sụn của nó từ một nguồn bên ngoài, phải có văn bản quy định rằng chỉ có phần mềm hoặc phần sụn đã được thẩm định bởi tổ chức chứng nhận mới được người vận hành nạp vào, nhằm duy trì tính hợp lệ của quá trình thẩm định.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	

8.2.5 An toàn phần mềm/phần sụn

Bảng 422 - VE và TE của ASB.08

An toàn phần mềm/phần sụn - mức 1, 2, 3 và 4	
ASB.08 ISO/IEC 19790:2025, B.2.5	Nội dung sau đây phải được bao gồm trong chính sách an toàn: a) đặc tả về các kỹ thuật toàn vẹn đã phê duyệt hoặc mã EDC được sử dụng; b) đặc tả về cách người vận hành có thể kích hoạt quá trình kiểm tra tính toàn vẹn theo yêu cầu; c) đặc tả về hình thức và từng thành phần của mã thực thi được cung cấp; và d) nếu mô-đun là mã nguồn mở, đặc tả về các trình biên dịch và các tham số kiểm soát bắt buộc nhằm biên dịch mã nguồn thành định dạng thực thi.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	

8.2.6 Môi trường hoạt động

Bảng 423 - VE và TE của ASB.09

Môi trường hoạt động - mức 1, 2, 3 và 4	
ASB.09 ISO/IEC 19790:2025, B.2.6	Nội dung sau đây phải được bao gồm trong chính sách an toàn: a) đặc điểm nhận diện của môi trường hoạt động (ví dụ: không thể sửa đổi, bị giới hạn, hoặc có thể sửa đổi); b) đặc điểm nhận diện của các hệ điều hành và các nền tảng được kiểm thử; c) đối với từng mức có thể áp dụng được, giải thích về cách thức đáp ứng các yêu cầu; d) những tuyên bố của nhà cung cấp liên quan đến việc chuyển đổi mô-đun sang các hệ điều hành khác (OS) chưa được kiểm thử cụ thể, nhưng

	nhà cung cấp vẫn khẳng định rằng mô-đun sẽ hoạt động chính xác; e) đặc tả về các quy tắc an toàn, các cài đặt hoặc các giới hạn đối với cấu hình của hệ điều hành; và f) đặc tả về bất kỳ giới hạn nào đối với cấu hình của hệ điều hành.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	

8.2.7 An toàn vật lý

Bảng 424 - VE và TE của ASB.10

An toàn vật lý - mức 1, 2, 3 và 4	
ASB.10 ISO/IEC 19790:2025, B.2.7	Nội dung sau đây phải được bao gồm trong chính sách an toàn: a) đặc tả về hình thái vật lý (đơn chip hoặc đa chip); b) đặc tả về các cơ chế an toàn vật lý được triển khai trong mô-đun (ví dụ: niêm phong chống can thiệp, khóa bảo vệ, công tắc xóa trắng và phản hồi can thiệp, và báo động); c) đặc tả về các hành động bắt buộc đối với các người vận hành để đảm bảo rằng an toàn vật lý được duy trì (ví dụ: kiểm tra định kỳ các niêm phong chống can thiệp hoặc thử nghiệm các công tắc xóa trắng và phản hồi can thiệp): 1) Quy định rõ liệu mô-đun có yêu cầu người vận hành dán/lắp niêm phong chống can thiệp hoặc thiết bị an toàn hay không, và nếu có, những niêm phong/thiết bị này sẽ được người vận hành áp dụng hoặc thay đổi như thế nào trong suốt vòng đời của mô-đun. Hình ảnh hoặc hình minh họa tham khảo được yêu cầu trong ISO/IEC 19790:2025, B.2.2 sẽ phản ánh mô-đun được cấu hình hoặc cấu tạo theo quy định. Các hình ảnh/hình minh họa bổ sung có thể được cung cấp để phản ánh các cấu hình khác; 2) nếu các tấm che là bắt buộc để che đậy các khe cắm hoặc lỗ hồng chưa được sử dụng nhằm đáp ứng các yêu cầu về độ mờ, cần thể hiện các tấm che đó trong hình ảnh hoặc hình minh họa, kèm theo niêm phong chống can thiệp đã được dán lên các tấm che. Các tấm che này sẽ được liệt kê trong danh sách các bộ phận; 3) hình ảnh hoặc hình minh họa chỉ ra vị trí chính xác của bất kỳ niêm phong chống can thiệp hoặc thiết bị an toàn nào bắt buộc để đáp ứng các yêu cầu về an toàn vật lý; 4) quy định tổng số lượng niêm phong chống can thiệp hoặc thiết bị an toàn bắt buộc (ví dụ: năm niêm phong chống can thiệp và hai màn hình đục). Hình ảnh hoặc hình minh họa dùng để hướng dẫn về vị trí chính xác phải đánh số từng hạng mục trong ảnh hoặc hình minh họa, và số lượng hạng mục được đánh số phải khớp với tổng số lượng đã quy định (bản thân niêm phong chống can thiệp thực tế hoặc thiết bị an toàn thì không bắt buộc phải đánh

	số); 5) nếu niêm phong chống can thiệp hoặc thiết bị an toàn là các bộ phận có thể đặt hàng lại từ nhà cung cấp mô-đun, cần chỉ ra số hiệu linh kiện của nhà cung cấp mô-đun đối với niêm phong, thiết bị an toàn hoặc bộ công cụ an toàn tương ứng. Sau khi cấu hình lại, người vận hành mô-đun có thể được yêu cầu phải gỡ bỏ và đưa vào các niêm phong chống can thiệp hoặc thiết bị an toàn mới; 6) đặc tả về vai trò người vận hành chịu trách nhiệm về việc bảo vệ và kiểm soát tại mọi thời điểm mọi niêm phong chưa được sử dụng, cũng như trực tiếp kiểm soát và quan sát bất kỳ thay đổi nào đối với mô-đun chẳng hạn như việc cấu hình lại nơi mà niêm phong chống can thiệp hoặc thiết bị an toàn bị gỡ bỏ hoặc lắp đặt, nhằm đảm bảo rằng tính an toàn của mô-đun được duy trì trong suốt những thay đổi đó và mô-đun được đưa trở lại hoạt động; và 7) nếu niêm phong chống can thiệp hoặc thiết bị an toàn có thể được gỡ bỏ hoặc lắp đặt, phải có các hướng dẫn rõ ràng liên quan đến cách thức chuẩn bị bề mặt hoặc thiết bị để dán/lắp đặt niêm phong chống can thiệp hoặc thiết bị an toàn mới. d) đặc tả về dải nhiệt độ hoạt động của mô-đun; e) đặc tả về dải điện áp hoạt động của mô-đun, nếu có; và f) đặc tả về các phương pháp giảm thiểu việc tiêm lỗi được triển khai
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	

8.2.8 An toàn không xâm lấn

Bảng 425 - VE và TE của ASB.11

An toàn không xâm lấn - mức 1, 2, 3 và 4	
ASB.11 ISO/IEC 19790:2025, B.2.8	Nội dung sau đây phải được bao gồm trong chính sách an toàn: a) đặc tả về tất cả các kỹ thuật giảm thiểu tấn công không xâm lấn được tham chiếu trong ISO/IEC 19790:2025, Phụ lục F, vốn được sử dụng bởi mô-đun để bảo vệ các CSP của mô-đun khỏi các cuộc tấn công không xâm lấn; và b) mô tả về tính hiệu quả của các kỹ thuật giảm thiểu tấn công không xâm lấn nằm trong ISO/IEC 19790:2025, Phụ lục F, vốn được sử dụng bởi mô-đun để bảo vệ các CSP của mô-đun khỏi các cuộc tấn công không xâm lấn. Mức độ chi tiết trong bản mô tả này được kỳ vọng là tương tự như những gì được tìm thấy trong tài liệu tiếp thị bên ngoài.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	

8.2.9 Quản lý tham số an toàn nhạy cảm

Bảng 426 - VE và TE của ASB.12

Quản lý tham số an toàn nhạy cảm - mức 1, 2, 3 và 4	
ASB.12 ISO/IEC 19790:2025, B.2.9	Nội dung sau đây phải được bao gồm trong chính sách an toàn: a) bảng khóa quy định: các loại khóa; độ mạnh tính bằng bit; các chức năng an toàn; số chứng nhận chức năng an toàn; nơi và cách thức tạo khóa; việc khóa được nhập hay xuất; phương pháp tạo và thiết lập SSP được sử dụng; và các khóa liên quan (nếu có); b) bảng các SSP khác và cách thức chúng được tạo; c) đặc tả về các bộ tạo bit ngẫu nhiên (RBG) đã phê duyệt và không được phê duyệt; d) mô tả về mục đích sử dụng các đầu ra của RBG; e) đặc tả về các nguồn đầu vào entropy của RBG; f) đặc tả về các phương pháp I/O điện tử và thủ tục thủ công của SSP; g) đặc tả về các kỹ thuật lưu trữ SSP; h) đặc tả về các phương pháp xóa trắng SSP và cơ sở hợp lý, cùng khả năng khởi tạo của người vận hành; i) các hướng dẫn về quá trình xóa trắng theo quy trình thủ tục, nếu có; j) đặc tả về các SSP và bất kỳ dữ liệu nào khác sẽ bị xóa trắng khi thao tác xóa trắng được gọi; k) đặc tả về các khoảng thời gian chuyển đổi hoặc khung thời gian có thể áp dụng nơi mà một thuật toán hoặc độ dài khóa chuyển từ trạng thái đã phê duyệt sang không được phê duyệt; và l) đặc tả về việc các SSP nào được miễn trừ khỏi quá trình xóa trắng và đối với mỗi SSP, phải liệt kê những yêu cầu xóa trắng nào không bị bắt buộc thi hành
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	

8.2.10 Tự kiểm thử

Bảng 427 - VE và TE của ASB.13

Tự kiểm thử - mức 1, 2, 3 và 4	
ASB.13 ISO/IEC 19790:2025, B.2.10	Nội dung sau đây phải được bao gồm trong chính sách an toàn: a) danh sách các bài tự kiểm thử trước khi vận hành và các bài tự kiểm thử có điều kiện với các tham số được xác định cùng danh sách các điều kiện mà theo đó các bài kiểm thử được thực hiện; b) đặc tả về khoảng thời gian và chính sách liên quan đến mọi điều kiện có thể dẫn đến việc gián đoạn các hoạt động của mô-đun trong khoảng thời gian nhằm lập lại các bài tự kiểm thử định kỳ; c) Nếu các bài tự kiểm thử định kỳ không bắt buộc vì khoảng thời gian hoạt

	động của mô-đun giữa các lần thiết lập lại, khởi động lại hoặc chu kỳ nguồn đủ ngắn, thì cần nêu rõ: khoảng thời gian hoạt động dự kiến của mô-đun; và tuyên bố rằng các tự kiểm thử định kỳ là không bắt buộc; d) mô tả về tất cả các trạng thái lỗi và các chỉ báo trạng thái; e) đặc tả về các hành động được thực hiện đối với các bài kiểm thử chức năng trọng yếu sau khi phát hiện lỗi; và f) mô tả về quá trình khởi tạo hoạt động, nếu có.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	

8.2.11 Đảm bảo vòng đời

Bảng 428 - VE và TE của ASB.14

Đảm bảo vòng đời - mức 1, 2, 3 và 4	
ASB.14 ISO/IEC 19790:2025, B.2.11	Nội dung sau đây phải được bao gồm trong chính sách an toàn: a) đặc tả về các thủ tục để lắp đặt, khởi tạo, khởi động và vận hành an toàn mô-đun; b) đặc tả về bất kỳ yêu cầu bảo trì nào; c) hướng dẫn cho quản trị viên và người dùng không phải quản trị viên (có thể là một tài liệu riêng); d) Nếu mô-đun mật mã hỗ trợ chứng thực và tính năng này đã được xem xét là tuân thủ các yêu cầu đặt ra trong ISO/IEC 19790:2025, Phụ lục G, cần có các hướng dẫn về cách: 1) lấy bất kỳ danh tính mật mã nào của mô-đun được yêu cầu; 2) lấy các bản ghi chứng thực; và 3) xác minh các bản ghi. e) một đặc tả về các thủ tục kết thúc vòng đời kèm theo bản tóm tắt các thủ tục kết thúc vòng đời, hoặc một đặc tả về một tham chiếu bên ngoài có sẵn công khai chỉ ra nơi có thể tìm thấy các thủ tục kết thúc vòng đời của mô-đun.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	

8.2.12 Giảm thiểu các tấn công khác

Bảng 429 - VE và TE của ASB.15

Giảm thiểu các tấn công khác - mức 1, 2, 3 và 4	
ASB.15 ISO/IEC 19790:2025, B.2.12	Nội dung sau đây phải được bao gồm trong chính sách an toàn: a) đặc tả về những tấn công khác nào được giảm thiểu; b) mô tả về tính hiệu quả của các kỹ thuật giảm thiểu được liệt kê. Mức độ chi tiết trong mô tả này được kỳ vọng là tương tự như những gì được tìm thấy trong tài liệu tiếp thị bên ngoài; và

	c) danh sách các hướng dẫn và ràng buộc liên quan đến an toàn.
Quy trình kiểm thử bắt buộc	
Khẳng định này được kiểm thử như một phần của ASB.01.	

Thư mục tài liệu tham khảo

- [1] ISO/IEC/TS 20540, *Information technology - Security techniques - Testing cryptographic modules in their operational environment*
- [2] ISO/IEC/TS 23532-2, *Information security, cybersecurity và privacy protection - Requirements for the competence of IT security testing and evaluation laboratories - Part 2: Testing for ISO/IEC 19790*