TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 12821:2020

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – HỒ SƠ BẢO VỆ CHO THIẾT BỊ LƯU TRỮ DI ĐỘNG

Information technology - Security techniques – Protection profile for portable storage media

HÀ NỘI - 2020

Mục lục

Lời nói đầu

TCVN 12821:2020 được xây dựng dựa trên cơ sở tham khảo "Protection Profile for Portable Storage Media (PSMPP)" được phê chuẩn bởi Tổ chức thừa nhận lẫn nhau về tiêu chí chung CCRA, phiên bản 1.0, ngày 11/9/2012.

TCVN 12821:2020 do Cục An toàn thông tin biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Công nghệ thông tin - Các kỹ thuật an toàn - Hồ sơ bảo vệ cho thiết bị lưu trữ di động

Information Technology - Security techniques - Protection profile for Portable Storage Media

1 Phạm vi áp dụng

Tiêu chuẩn này quy định hồ sơ bảo vệ cho thiết bị lưu trữ di động, thể hiện các yêu cầu chức năng an toàn (SFR) và các yêu cầu đảm bảo an toàn (SAR) đối với thiết bị lưu trữ di động, phù hợp với bộ tiêu chuẩn quốc gia TCVN 8709-1:2011 (ISO/IEC 15408-1:2009), TCVN 8709-2:2011 (ISO/IEC 15408-2:2008) và TCVN 8709-3:2011 (ISO/IEC 15408-3:2008).

Các loại thiết bị lưu trữ di động thuộc phạm vi áp dụng của tiêu chuẩn này được gọi chung là Đích đánh giá (TOE) và được quy định cụ thể tại điều 4.1.

2 Tài liệu viện dẫn

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

TCVN 8709-1:2011 (ISO/IEC 15408-1:2009), "Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 1: Giới thiệu và mô hình tổng quát".

TCVN 8709-2:2011 (ISO/IEC 15408-2:2008), "Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 2: Các thành phần chức năng an toàn".

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

3 Thuật ngữ, định nghĩa, ký hiệu và chữ viết tắt

Tiêu chuẩn này sử dụng các thuật ngữ, định nghĩa, ký hiệu và chữ viết tắt quy định tại TCVN 8709-1:2011.

4 Giới thiệu Hồ sơ bảo vệ

4.1 Tổng quan TOE

4.1.1 Kiểu TOE

Đích đánh giá (TOE) là thiết bị lưu trữ di động có kết nối vật lý với máy chủ, dùng để lưu trữ dữ liệu và mã hóa kèm cơ chế xác thực quyền truy cập chặt chẽ.

4.1.2 Phạm vi TOE

Mục tiêu của tiêu chuẩn này là đưa ra các yêu cầu an toàn đối với thiết bị lưu trữ di động để đảm bảo rằng khi mất hoặc bị đánh cắp thì dữ liệu lưu trữ trong đó được an toàn.

Tiêu chuẩn này không đưa ra các yêu cầu kiểm soát truy cập đối với thiết bị lưu trữ, do đó việc sử dụng thiết bị lưu trữ trong các hệ thống cụ thể và việc kiểm soát truy cập không thuộc phạm vi của tiêu chuẩn này.

Chức năng chống ghi đè tuy không nằm trong yêu cầu của Hồ sơ bảo vệ, nhưng nó được xem như chức năng an toàn bổ sung cho thiết bị lưu trữ. Ví dụ: Chức năng chống ghi đè sẽ bảo đảm an toàn cho dữ liệu, tránh bị sửa, xóa khi kết nối vào môi trường tiềm ẩn các rủi ro an toàn thông tin hoặc có các phần mềm độc hại.

Chức năng bảo vệ ghi không nằm trong yêu cầu của Hồ sơ bảo vệ, nhưng tương tự như chức năng chống ghi đè, nó cũng được xem như chức năng an toàn bổ sung cho thiết bị lưu trữ. Ví dụ: chương trình nhập mật khẩu để cho phép được thay đổi dữ liệu hay không.

4.1.3 Cách sử dụng và đặc điểm an toàn chính của TOE

Tiêu chuẩn này sử dụng cho tất cả các thiết bị lưu trữ di động có kết nối vật lý với một hệ thống máy chủ lưu trữ. Ví dụ như thẻ nhớ kết nối qua cổng USB hoặc ổ đĩa kết nối qua cổng FireWire.

TOE này dành cho các loại thiết bị lưu trữ như USB, ổ cứng di động, áp dụng với các kết nối vật lý. Dữ liệu bên trong thiết bị lưu trữ được mã hóa và chống truy cập trong trường hợp bị mất, thất lạc hoặc bị đánh cắp.

Tóm lại, tiêu chuẩn này đưa ra tập hợp các yêu cầu an toàn cơ bản nhằm bảo vệ dữ liệu trước các hình thức tấn công cả logic lẫn vật lý.

Trạng thái kích hoạt mặc định chỉ cung cấp cơ chế xác thực quyền truy cập.

Một khía cạnh quan trọng khác trong an toàn thông tin trên thiết bị lưu trữ di động là các chức năng an toàn nằm hoàn toàn trên chính thiết bị đó. Điều này cho phép thiết bị có cơ chế an toàn phù hợp với PP có thể hoạt động với mọi hệ thống máy chủ vì nó không yêu cầu phần mềm hỗ trợ.

Chỉ cần một quy trình xác thực duy nhất để mở khóa quyền truy cập vào dữ liệu người dùng được mã hóa trên thiết bị lưu trữ và người dùng có thể truy cập. Sau khi xác thực thành công, phương tiện lưu trữ cung cấp dịch vụ an toàn một cách minh bạch mà không cần bất kỳ yêu cầu kiểm soát truy cập nào khác trên thiết bị.

Dữ liệu TSF (chứa thông tin xác thực và khóa mã hóa) cần được lưu trữ an toàn trong TOE.

Chú thích áp dụng: Dữ liệu TSF có thể được lưu trữ trong HSM (High Security Module – Mô đun an toàn cao) hoặc ở dạng được mã hóa trên thiết bị.

TOE phải đảm bảo tính an toàn của dữ liệu người dùng và TSF trong trường hợp TOE bị tách ra khỏi máy chủ do sự cố (Ví dụ: hệ thống ngừng hoạt động bất thường hoặc mất điện) hoặc các tác động vật lý khác, ngay cả khi xảy ra trong lúc đang truy cập để đọc hoặc ghi.

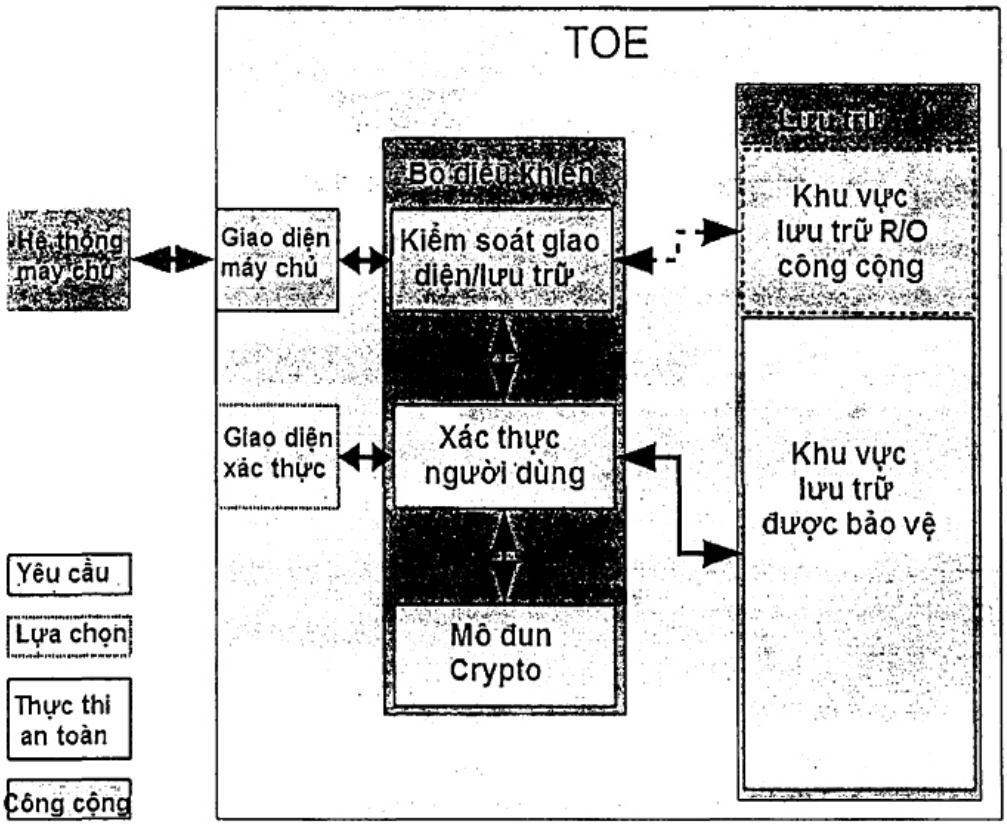
Các thay đổi khác như đặt máy chủ vào trạng thái ngủ hoặc ngủ đông có thể kích hoạt khóa, cũng như theo quyết định của tác giả ST.

Tiêu chuẩn này chỉ xác định các giả định nếu chúng cần thiết. Điều này tạo điều kiện thực hiện một loạt các giải pháp kỹ thuật khả thi.

Các nhà sản xuất có thể tăng khả năng an toàn trong các sản phẩm của họ bằng cách bổ sung các chức năng an toàn nếu các chức năng thêm vào này không trái với các mô tả trong hồ sơ bảo vệ theo tiêu chuẩn này. Tiêu chuẩn này có một số hướng dẫn về vấn đề này dưới dạng các chú thích áp dụng. Các chức năng bổ sung có thể được đưa vào ST, là tài liệu cơ bản để dựa vào đó chứng nhận sản phẩm.

Môi trường hoạt động của TOE khá đa dạng. Các thiết bị lưu trữ di động có khả năng dùng ở bất cứ đâu, bất cứ máy chủ nào thông qua cổng kết nối quen thuộc như USB, FireWire hoặc Thunderbolt.

Hình 1 là cấu trúc cơ bản của TOE.



Hình 1 - Cấu trúc TOE

TOE có ít nhất một giao diện bên ngoài kết nối hệ thống máy chủ lưu trữ. Ngoài ra, TOE có thể thực hiện một giao diện xác thực cục bộ tùy chọn hoặc dựa vào máy chủ để cung cấp giao diện người dùng để có được dữ liệu xác thực.

Các phần chính của TOE bao gồm bộ điều khiển (thực hiện gửi lệnh đến khu vực lưu trữ, xác thực người dùng và các chức năng mã hóa) và vùng bảo vệ lưu trữ.

TOE có thể triển khai vùng lưu trữ công khai tùy chọn chỉ đọc dành cho người dùng TOE.

Nhà sản xuất TOE sử dụng vật liệu kín niêm phong bên trong, ví dụ: với nhựa đúc, các thành phần an toàn liên quan. Vật liệu kín niêm phong này có thể cản trở các tấn công vật lý.

CHÚ THÍCH: Do cơ chế bảo vệ trên không đo lường được, nên không thể xác nhận cơ chế này theo CC.

Nhìn chung, TOE thực hiện các đặc điểm an toàn then chốt sau:

- Bảo vệ bí mật dữ liệu người dùng bằng mã hóa;

- Bảo vệ dữ liệu TSF.

4.1.4 Phần cứng/phần mềm/phần sụn phi - TOE

Tiêu chuẩn này không yêu cầu môi trường cụ thể hoặc phần mềm máy chủ chuyên dụng.

4.2 Giới hạn TOE

Giới hạn TOE vật lý được định nghĩa bởi giao diện máy chủ và giao diện xác thực tùy chọn. Về mặt vật lý, TOE bao gồm thiết bị lưu trữ hoàn chỉnh.

5 Khung Hồ sơ bảo vệ cho thiết bị lưu trữ di động (PSMPP)

PSMPP cho phép xác định các mở rộng chức năng có thể được yêu cầu bởi một ST ngoài PSMPP cơ sở. Như vậy, PSMPP định nghĩa các thành phần sau:

- PSMPP cơ sở xác định yêu cầu an toàn và yêu cầu này được áp dụng trên tất cả thiết bị lưu trữ di động. Đây là bắt buộc và xác định chung cho tất cả các thiết bị lưu trữ di động phù hợp với PSMPP.

- Gói mở rộng PSMPP nêu rõ định nghĩa về vấn đề an toàn, các mục tiêu và yêu cầu chức năng cho các cơ chế có thể được thực hiện ngoài PSMPP cơ sở. Thông thường, gói mở rộng PSMPP xác định tiện ích mong muốn hoặc được thực hiện bởi một số thiết bị lưu trữ di động. Tuy nhiên, chức năng được chỉ định trong một gói mở rộng PSMPP thường không được tìm thấy trong các thiết bị lưu trữ di động.

Các gói mở rộng PSMPP có thể được thêm vào chức năng cơ bản khi viết ST. Tác giả ST có thể chọn từ gói PSMPP khác. Để tránh phân mảnh chức năng an toàn vào các gói mở rộng PSMPP, gói PSMPP mở rộng sẽ xác định một tập hợp yêu cầu chức năng nhằm giải quyết một hoặc nhiều vấn đề về an toàn chung.

PSMPP được định nghĩa là một khung có thể mở rộng. Tập hợp các gói mở rộng PSMPP hiện tại có thể được tăng cường với các gói mở rộng phát triển mới hoặc cập nhật PSMPP. Sau đó, các gói mở

rộng này được đánh giá lại và tái xác nhận PSMPP cơ sở. Do đó, khung này cho phép bất kỳ ai quan tâm đến việc chỉ định một khía cạnh của thiết bị lưu trữ di động có thể tạo ra một gói mở rộng PSMPP và đề xuất với cơ quan quản lý PSMPP. Với cách tiếp cận này, sẽ có một bộ PSMPP cơ sở hợp lệ và các gói mở rộng phù hợp. Sự phụ thuộc vào các gói mở rộng khác của PSMPP có thể được chỉ định.

5.1 Thông tin bắt buộc do ST cung cấp

Các thông tin sau đây phải được cung cấp như một phần của ST lấy từ PSMPP.

5.1.1 Yêu cầu phù hợp

Khi chỉ định phù hợp với PSMPP, ST phải chỉ định bất kỳ gói mở rộng nào của PSMPP mà ST yêu cầu phù hợp.

5.1.2 Tham chiếu SFR với tài liệu tham khảo gói mở rộng PSMPP

Khi chỉ định các SFR như là một phần của ST, tham chiếu đến PSMPP cơ sở hoặc gói mở rộng PSMPP phải được đưa ra để tạo điều kiện ánh xạ trực tiếp tới SFR, đặc biệt xem xét các lần lặp.

Yêu cầu này sẽ hỗ trợ tác giả ST và các bên đánh giá để đảm bảo không có SFR từ PSMPP cơ sở hoặc một gói mở rộng PSMPP mà ST yêu cầu phù hợp bị bỏ qua.

5.2 Thông tin bắt buộc được cung cấp bởi các gói mở rộng PSMPP

Các thông tin sau phải được cung cấp cho mỗi gói mở rộng PSMPP.

5.2.1 Quy tắc thành phần gói mở rộng

Để gói mở rộng PSMPP sử dụng được cùng với các gói khác, cần có các thông tin sau:

- Danh sách các gói mở rộng PSMPP phụ thuộc với các phiên bản tối thiểu tương ứng.

- Danh sách các gói mở rộng không được cho phép PSMPP với các phiên bản tối thiểu tương ứng.

CHÚ THÍCH: Gói mở rộng không được loại trừ PSMPP cơ sở hoặc bất kỳ phần nào của PSMPP cơ sở; tuy nhiên, gói mở rộng có thể chỉ định phiên bản tối thiểu của PSMPP cơ sở được yêu cầu cho gói mở rộng tương ứng.

Trường hợp phải thay đổi gói mở rộng PSMPP để phù hợp với một gói mở rộng khác, tác giả của gói mở rộng PSMPP phải tiếp cận chủ sở hữu gói mở rộng khác để đạt được sự đồng ý về các sửa đổi cần thiết.

5.3 Thông số kỹ thuật bị hạn chế đối với PSMPP cơ sở

PSMPP cơ sở xác định riêng các thuộc tính sau:

- Yêu cầu phù hợp với các hồ sơ bảo vệ khác

- Loại phù hợp (nghiêm ngặt hoặc có thể diễn giải được)

- Yêu cầu phù hợp đối với EAL bao gồm các yêu cầu mở rộng

Một gói mở rộng PSMPP có thể quy định các tinh chỉnh cho các thành phần đảm bảo. Các tinh chỉnh cung cấp phương pháp để đáp ứng các yêu cầu đảm bảo cho các SFR trong gói mở rộng. Tuy nhiên, một trong những ý định cốt lõi của PSMPP là giữ hồ sơ bảo vệ và tất cả các mô-đun của nó theo thỏa thuận thừa nhận lẫn nhau. Vì vậy, không có gói mở rộng PSMPP nào sẽ thêm hoặc sửa đổi cấp độ một SAR.

6 Các tuyên bố tuân thủ

Các phần sau đây mô tả các tuyên bố tuân thủ của Hồ sơ bảo vệ đối với thiết bị lưu trữ di động.

6.1 Các yêu cầu phù hợp CC

PSMPP phù hợp TCVN 8709-2:2011 và TCVN 8709-3:2011.

6.2 Yêu cầu gói

Tiêu chuẩn này yêu cầu đảm bảo cấp EAL2.

6.3 Yêu cầu PP

Tiêu chuẩn này không yêu cầu phù hợp với các hồ sơ bảo vệ khác.

6.4 Báo cáo phù hợp

Tiêu chuẩn này đòi hỏi các ST hoặc PP tuyên bố tuân thủ có thể diễn giải được với PP của tiêu chuẩn này.

7 Mô tả các vấn đề an toàn

Phần này mô tả mục đích tại sao tài sản cần được bảo vệ và chống lại các mối đe dọa.

7.1 Tài sản

Tài sản được bảo vệ là:

- Dữ liệu người dùng: Dữ liệu lưu trữ trong thiết bị lưu trữ di động, được mã hóa và bảo vệ.

- Dữ liệu TSF: Dữ liệu xác thực dùng để xác thực người dùng được ủy quyền và dữ liệu khóa mã hóa dùng để mã hóa dữ liệu người dùng.

7.2 Vai trò

PSMPP chỉ xác định duy nhất một vai trò cho thiết bị, người dùng được ủy quyền, là người dùng được xác thực thành công đối với thiết bị. Những người dùng không được xác thực đang cố gắng truy cập tài sản (dữ liệu được bảo vệ) thì được coi là các tác nhân đe dọa.

Người dùng TOE được ủy quyền

- Đã xác thực thành công với TOE và được nắm giữ dữ liệu xác thực.

- Được phép truy cập vào vùng lưu trữ được bảo vệ của TOE, trong đó lưu trữ dữ liệu người dùng bí mật.

- Được phép sửa đổi dữ liệu xác thực sau khi xác thực lại thành công.

- Không có quyền truy cập đọc dữ liệu TSF.

Người dùng không được ủy quyền khi không nắm giữ vai trò trên, có nghĩa là:

- Không được xác thực bởi TOE.

- Không được truy cập vùng lưu trữ được bảo vệ của TOE.

- Không được truy cập dữ liệu xác thực hoặc mã hóa.

Chú thích áp dụng: Cả người có quyền và người sử dụng trái phép đều có thể là cùng một cá nhân, chỉ phân biệt được bằng việc đã xác thực hay không. Bất kỳ cá nhân nào cũng chỉ có thể giữ một trong hai vai trò này vào bất kỳ lúc nào.

7.3. Các mối đe dọa

Đây là các tác nhân đe dọa xuất hiện từ các nhóm thực thể bên ngoài, không được phép truy cập dữ liệu. Các tác nhân đe dọa thường được đặc trưng bởi một số yếu tố, ví dụ: chuyên môn, nguồn lực sẵn có, với động lực được liên kết trực tiếp với giá trị của tài sản bị đe dọa.

TOE bảo vệ và chống lại hành động cố ý hoặc không cố ý vi phạm an toàn TOE bởi những tin tặc.

Các tác nhân đe dọa đáp ứng một hoặc nhiều điều sau đây:

- Cố gắng truy cập tài sản bằng cách giả mạo là một người dùng được ủy quyền hoặc bằng cách cố gắng sử dụng các dịch vụ TSF mà không cần sự ủy quyền.

- Muốn truy cập dữ liệu người dùng, dữ liệu xác thực hoặc mã hóa trong thiết bị lưu trữ di động.

- Tin tặc thử tấn công logic và vật lý trên một thiết bị lưu trữ di động cùng loại, chuẩn bị cho việc tấn công TOE.

- Có thể sở hữu TOE tương đối dễ dàng vì TOE có hình thức nhỏ gọn.

- Không giữ dữ liệu xác thực.

7.3.1 Các mối đe dọa TOE

T.LogicalAccess	Dữ liệu người dùng, dữ liệu xác thực hoặc mã hóa trên TOE bị truy cập
T.PhysicalAccess	Bộ nhớ TOE bị truy cập bằng cách tấn công vật lý, không thông qua TOE để lấy dữ liệu người dùng, dữ liệu xác thực hoặc mã hóa.
T.AuthChange	Một tác nhân đe dọa thay đổi dữ liệu xác thực.
T.Disruption	Dữ liệu dự định được bảo vệ nhưng lại không được bảo vệ nữa do lỗi làm gián đoạn hoạt động chính xác của TOE.
Chú thích áp dụng:	Các mối đe dọa phát sinh từ hành vi trộm cắp lặp lại và phân tích mã hóa khác nhau của thiết bị không được xem xét.

7.3.2 Các mối đe dọa môi trường vận hành TOE

Không có mối đe dọa nào.

7.4 Các chính sách an toàn thông tin của tổ chức

Tiêu chuẩn này không chỉ định bất kỳ chính sách an toàn thông tin của tổ chức nào.

Tất cả các tác động đối với chức năng an toàn thông tin bắt nguồn từ những mối đe dọa.

7.5 Giả định

Phần này liệt kê các giả định liên quan đến an toàn cho môi trường, trong đó TOE sẽ được sử dụng. Nó có thể được coi là một bộ quy tắc cho nhà vận hành TOE.

A.TrustedWS Khi người dùng được mở khóa vùng bảo vệ, nghĩa là người dùng đã xác thực với TOE, sẽ không có bất kỳ truy cập trái phép vào TOE từ hệ thống máy chủ hoặc bất kỳ mạng kết nối nào nữa. Giả định này cũng bao gồm việc chuyển giao phần mềm độc hại lên TOE.

8 Các mục tiêu an toàn

8.1 Các mục tiêu an toàn cho TOE

O.ProtectTSF TOE phải cung cấp tính năng bảo vệ cho dữ liệu TSF để dữ liệu xác thực và mã hóa được bảo vệ khỏi sự truy cập.

O.AuthAccess TOE phải cung cấp cơ chế xác thực mạnh mẽ, chỉ cho phép những người dùng đã được xác thực truy cập vào vùng lưu trữ được bảo vệ.

O.Encrypt TOE mã hóa tất cả dữ liệu được lưu trữ, đặc biệt bảo vệ tính an toàn trong trường hợp các cuộc tấn công vật lý trên TOE.

O.AuthChange Chỉ người dùng được xác thực mới được phép thay đổi dữ liệu xác thực.

O.FailSafe TOE trở về trạng thái ổn định sau khi bị gián đoạn. Thiết bị sẽ về trạng thái khóa, không cho truy cập dữ liệu sau khi lỗi xảy ra. Việc xác thực thành công sẽ mở khóa thiết bị trở lại.

8.2 Các mục tiêu an toàn cho môi trường hoạt động

OE.TrustedWS Hệ thống máy chủ lưu trữ phải bảo vệ đúng cách tất cả các dữ liệu được truy xuất từ vùng lưu trữ được bảo vệ của TOE và phải bảo đảm không có phần mềm độc hại nào được chuyển sang TOE.

OE.AuthConf Người dùng TOE phải giữ bí mật dữ liệu xác thực của họ.

OE.AuthProt Nếu máy chủ cung cấp giao diện người dùng cho cơ chế xác thực, máy chủ sẽ bảo vệ dữ liệu xác thực khỏi việc sử dụng sai.

Chú thích áp dụng: Tác giả ST có thể loại bỏ OE.AuthProt nếu TOE cung cấp giao diện xác thực riêng và không dựa vào máy chủ để xác thực.

8.3 Phân tích các mục tiêu an toàn

8.3.1 Phạm vi mục tiêu an toàn

Bảng 1 - Mục tiêu theo dõi các mối đe dọa và giả định

Mục tiêu	Mối đe dọa	Giả định
O.ProtectTSF	T.LogicalAccess T.PhysicalAccess	
O.AuthAccess	T.LogicalAccess	
O.Encrypt	T.PhysicalAccess	
O.AuthChange	T.AuthChange	
O.FailSafe	T.Disruption	
OE.TrustedWS		A.TrustedWS
OE.AuthConf	T.LogicalAccess	
OE.AuthProt	T.LogicalAccess	

8.3.2 Nội dung chi tiết của các mục tiêu an toàn

Nội dung sau đây mô tả cách thức các mục tiêu chống lại các mối đe dọa và đáp ứng các giả định:

T.LogicalAccess

Mối đe dọa của truy cập logic không được xác thực vào khu vực lưu trữ được bảo vệ bị chặn bởi O.AuthAccess, đảm bảo chỉ các truy cập xác thực có khả năng thực hiện. Mối đe dọa của các truy cập logic hoặc vật lý không hợp lệ vào dữ liệu TSF bị chặn bởi O.ProtectTSF nhằm đảm bảo vệ TSF.

OE.AuthConf đảm bảo giữ bí mật dữ liệu xác thực của người dùng và OE.AuthProt bảo vệ máy chủ lưu giữ dữ liệu xác thực. Cả hai mục tiêu này rất cần thiết để đảm bảo an toàn cho cơ chế xác thực.

T.PhysicalAccess

Việc truy cập vật lý trái phép vào dữ liệu được bảo vệ sẽ bị chặn bởi O.Encrypt, đảm bảo rằng dữ liệu không thể truy cập nếu không có chìa khóa giải mã thích hợp. Tấn công vật lý trên TOE có thể dẫn đến việc tiết lộ dữ liệu được mã hóa trong vùng lưu trữ bảo vệ của TOE. Đối với O.Encrypt, các thuật toán mã hóa và độ dài khóa cần phải đủ mạnh, để chặn mọi sự truy cập vật lý vào dữ liệu TSF trái phép bởi O.ProtectTSF.

T.AuthChange

Mối đe dọa của việc sửa đổi trái phép thông tin xác thực bị chặn bởi O.AuthChange, đảm bảo rằng chỉ có người dùng đã được xác thực mới có thể thay đổi dữ liệu xác thực.

T.Disruption

Sự đe dọa của sự gián đoạn dịch vụ do truy cập trái phép vào các dữ liệu được bảo vệ bị chặn bởi O.FailSafe, đảm bảo rằng: không có dữ liệu được bảo vệ nào có thể truy cập được bằng bản rõ sau khi lỗi và việc xác thực lại sau khi bị gián đoạn là cần thiết.

A.TrustedWS

Giả định về một máy trạm đáng tin cậy được hỗ trợ bởi mục tiêu OE.TrustedWS cho rằng hệ thống máy chủ đảm bảo việc bảo vệ tất cả các dữ liệu thu được từ vùng lưu trữ bảo vệ của TOE và bảo vệ chống lại việc lưu trữ phần mềm độc hại trên TOE.

9 Định nghĩa các thành phần mở rộng

9.1 FPT_SDC Lưu trữ dữ liệu TSF đáng tin cậy

FPT_SDC.1 Lưu trữ dữ liệu TSF đáng tin cậy, gồm dữ liệu xác thực và mã hóa, phải được lưu trữ an toàn để tránh tiết lộ dữ liệu TSF.

9.1.1 Hành vi theo họ FPT_SDC

Họ này xác định các yêu cầu về bảo vệ đối với dữ liệu xác thực và mã hóa được lưu trữ dùng để kích hoạt tính năng an toàn của thiết bị.

9.1.2 Phân cấp thành phần FPT_SDC.1

FPT_SDC.1 không phân cấp đối với bất kỳ thành phần nào khác trong họ FPT_SDC.

9.1.3 Quản lý FPT_SDC.1

Các hành động sau đây có thể được xem xét cho các chức năng quản lý trong FMT:

9.1.4 Kiểm soát FPT_SDC.1

Các hành động sau phải được kiểm tra nếu FAU_GEN tạo dữ liệu kiểm soát an toàn bao gồm trong PP/ST:

Không có hành động được xác định là có thể kiểm tra được.

9.1.5 FPT_SDC.1 Lưu trữ dữ liệu TSF đáng tin cậy

Phân cấp:	Không có thành phần khác.
Phụ thuộc:	Không có phụ thuộc.
FPT_SDC.1.1	TSF phải cung cấp không gian lưu trữ an toàn cho dữ liệu xác thực và mã hóa.

Chú thích áp dụng: Phụ thuộc vào nhà phát triển xem những cơ chế nào được sử dụng để đảm bảo bảo vệ an toàn cho dữ liệu xác thực và mã hóa. Có thể là một HSM, một thẻ thông minh, lưu trữ mã hóa hoặc các hình thức bảo vệ khác sẽ đảm bảo rằng không có bất kỳ khóa và dữ liệu xác thực nào có thể truy cập được.

9.1.6 Phân tích

SFR mở rộng này đòi hỏi phải có một yêu cầu rõ ràng đối với việc bảo vệ dữ liệu TSF, nếu không sẽ không xác định được các yêu cầu vì loại hình bảo vệ này thường được đảm bảo bằng kết cấu của TOE và không được mô phỏng bằng các SFR được quy định tại TCVN 8709.

10. Các yêu cầu an toàn

10.1. Các yêu cầu chức năng an toàn

Các quy ước định dạng sau đây được sử dụng để xác định các thao tác (tinh chỉnh, lựa chọn và chỉ định) đã được thực hiện trong tiêu chuẩn này:

Thao tác **tinh chỉnh** được sử dụng để bổ sung thông tin chi tiết cho một yêu cầu và do đó giới hạn thêm một yêu cầu. Tinh chỉnh các yêu cầu về an toàn được biểu thị theo cách là các từ thêm vào sẽ được in **chữ đậm** còn các từ đã gỡ bỏ sẽ được ~~gạch ngang~~. Nếu một lần tinh chỉnh được thêm vào như một đoạn riêng biệt cho một SFR thay vì sửa đổi từ ngữ của nó, thì đoạn này bắt đầu bằng từ **Tinh chỉnh**: bằng chữ đậm.

Thao tác **lựa chọn** được sử dụng để chọn một hoặc nhiều tùy chọn quy định tại TCVN 8709 khi làm rõ yêu cầu. Lựa chọn của tác giả PP được biểu thị dưới dạng văn bản được gạch chân; ngoài ra, một chú thích ở cuối trang sẽ hiển thị nội dung ban đầu theo TCVN 8709-2. Các lựa chọn sẽ do tác giả ST điền vào, xuất hiện trong dấu ngoặc vuông với dấu hiệu chỉ ra rằng một lựa chọn sẽ được thực hiện [lựa chọn:] và được *in nghiêng*.

Thao tác **chỉ định** được sử dụng để chỉ định một giá trị cụ thể cho một tham số không xác định như độ dài của mật khẩu. Những phép chỉ định của tác giả PP đều được biểu thị dưới dạng <u>văn bản được gạch chân;</u> ngoài ra, một chú thích ở cuối trang sẽ hiển thị nội dung ban đầu theo TCVN 8709-2. Các phép chỉ định sẽ do tác giả ST điền vào, xuất hiện trong dấu ngoặc vuông với dấu hiệu chỉ ra rằng một phép chỉ định sẽ được thực hiện [chỉ định:] và được *in nghiêng*. Trong một số trường hợp, thao tác chỉ định do tác giả PP thực hiện sẽ xác định một sự lựa chọn hoặc chỉ định do tác giả ST thực hiện. Vì vậy, đoạn văn bản này sẽ được gạch chân và *in nghiêng <u>như thế này</u>*.

10.1.1 Định danh và xác thực (FIA)

TOE phải cung cấp ít nhất một cơ chế xác thực cơ bản đủ mạnh để đáp ứng các yêu cầu của FIA_SOS.1.

Quyền truy cập dữ liệu chỉ được cấp sau khi xác thực thành công. Quyền này sẽ bị hủy nếu TOE bị ngắt kết nối tới máy chủ lưu trữ hoặc lỗi thiết bị.

FIA_UAU.2 Xác thực người dùng trước mọi hành động

Phân cấp:	FIA_UAU.1 Thời gian xác thực
Phụ thuộc:	FIA_UID.1 Thời gian định danh
FIA_UAU.2.1	TSF yêu cầu từng người dùng phải xác thực thành công trước khi cho phép bất kỳ hành động nào khác đại diện cho người dùng đó.

FIA_UAU.6 Xác thực lại

Phân cấp:	Không có thành phần khác.
Phụ thuộc:	Không có phụ thuộc.
FIA_UAU.6.1	TSF sẽ xác thực lại người dùng theo các điều kiện thay đổi dữ liệu xác thực[1].
Chú thích áp dụng:	Việc xác thực lại phải sử dụng cùng một cơ chế xác thực như xác thực ban đầu.

FIA_SOS.1 Xác minh các bí mật

Phân cấp:	Không có thành phần khác.
Phụ thuộc:	Không có phụ thuộc.
FIA_SOS.1.1	TSF sẽ cung cấp một cơ chế để xác minh các bí mật đáp ứng a) Với mỗi lần thử sử dụng cơ chế xác thực, xác suất có một lần thử ngẫu nhiên sẽ thành công thường nhỏ hơn 1/1.000.000; b) Bất kỳ phản hồi nào được đưa ra trong khi thử sử dụng cơ chế xác thực sẽ không làm giảm xác suất xuống dưới chỉ số trên[2].

FIA_AFL.1 Xử lý lỗi xác thực

Phân cấp:	Không có thành phần khác.
Phụ thuộc:	FIA_UAU.1 Thời gian xác thực
FIA_AFL.1.1	TSF sẽ phát hiện khi *[lựa chọn: [chỉ định: số nguyên dương], một số nguyên dương có thể cấu hình bởi quản trị viên trong phạm vi [chỉ định:*

[1] [chỉ định: danh sách các điều kiện yêu cầu xác thực lại]

[2] [chỉ định: chỉ số chất lượng đã được xác định]

khoảng các giá trị có thể chấp nhận được]] những lần thử xác thực không thành công xảy ra liên quan đến việc xác thực của người dùng[3].

FIA_AFL.1.2 Khi số lần thử xác thực không thành công vượt ngưỡng[4], TSF sẽ vô hiệu hóa quyền truy cập vào vùng lưu trữ được bảo vệ[5].

Chú thích áp dụng: Các ngưỡng cần phải được xác định là hợp lý cho môi trường hoạt động dự kiến và hình thức chặn được thực hiện. Nếu việc chặn được thực hiện bằng cách hủy khóa, do đó hiển thị dữ liệu được lưu trữ sẽ hoàn toàn không thể truy cập, thì các ngưỡng cao hơn sẽ thích hợp hơn cho môi trường mà quản trị viên có khả năng bỏ chặn thiết bị.

Chú thích áp dụng: Yêu cầu này có thể làm thiết bị không sử dụng được. Việc này tùy thuộc tác giả ST. Nếu một cơ chế được thực hiện cho phép đặt lại bộ đếm xác thực không thành công, thì các vấn đề an toàn liên quan cần phải được giải quyết và mô phỏng trong ST.

10.1.2 Hoạt động mã hóa (FCS)

TOE bảo vệ dữ liệu thông qua các công cụ mã hóa. Việc thực hiện chính xác tuân thủ các quy định quốc gia về mã hóa và phải được nêu trong ST.

FCS_CKM.1 Tạo khóa bằng mã hóa

Phân cấp: Không có thành phần khác.

Phụ thuộc: [FCS_CKM.2 Phân phối khóa mã hóa, hoặc

FCS_COP.1 Thao tác mã hóa]

FCS_CKM.4 Hủy khóa mã hóa

FCS_CKM.1.1 TSF sẽ tạo các khóa bằng mã hóa theo một thuật toán tạo khóa mã hóa được quy định cụ thể [*chỉ định: thuật toán tạo khoá bằng mã hóa*][6] và các kích thước khóa mã hóa quy định [*chỉ định: kích thước khóa mã hóa*][7] đáp ứng như sau: [*chỉ định: danh sách các tiêu chuẩn được **chấp nhận***][8].

---

[3] [chỉ định: danh sách các trường hợp xác thực] XEM LAI: Gán => chỉ định ?

[4] [lựa chọn: đáp ứng, thông qua]

[5] [chỉ định: danh sách cách hành động]

[6] [chỉ định: thuật toán tạo khoá bằng mật mã]

[7] [chỉ định: kích thước khóa mật mã]

[8] [chỉ định: danh sách các tiêu chuẩn]

Chú thích áp dụng 1: Liên hệ với tổ chức chứng nhận để biết danh sách các tiêu chuẩn được chấp nhận. Danh sách các tiêu chuẩn được chấp nhận sẽ cung cấp các thuật toán mã hóa thích hợp, các chế độ thao tác và độ dài khóa, các thuật toán tạo khóa phù hợp và bộ tạo số ngẫu nhiên.

Chú thích áp dụng 2: TOE sẽ tạo một khóa mã hóa mới khi được khởi động hoặc khi có yêu cầu rõ ràng để tạo một khóa mới.

FCS_CKM.4 Hủy khoá mã hóa

Phân cấp: Không có thành phần khác.

Phụ thuộc: [FDP_ITC.1 Nhập dữ liệu người dùng không có thuộc tính an toàn, hoặc FDP_ITC.2 Nhập dữ liệu người dùng có các thuộc tính an toàn, hoặc FCS_CKM.1 Tạo khóa mã hóa]

FCS_CKM.4.1 TSF sẽ hủy các khóa mã hóa theo phương pháp hủy khóa mã hóa quy định [*chỉ định: phương pháp hủy khóa mã hóa*][9] đáp ứng như sau: [*chỉ định: danh sách các tiêu chuẩn được* ***chấp nhận***][10].

Chú thích áp dụng 1: Nếu các tiêu chuẩn được chấp nhận được tham chiếu trong các phương pháp hủy khóa ủy nhiệm FCS_CKM.1, thì những tiêu chuẩn này sẽ được áp dụng tại đây. Liên hệ với tổ chức chứng nhận để biết danh sách các tiêu chuẩn được chấp nhận.

Chú thích áp dụng 2: Một kịch bản điển hình để hủy khóa là khởi động lại thiết bị. Nếu thao tác xóa dữ liệu được bao gồm trong chức năng an toàn của TOE, thì việc này có thể được thực hiện bằng cách xóa khóa.

Chú thích áp dụng 3: Nếu người dùng TOE nghi ngờ TOE bị xâm nhập, thì người dùng nên xóa bỏ hoàn toàn, không cần lập lại bằng cách xóa khóa.

FCS_COP.1 Thao tác mã hóa

Phân cấp: Không có thành phần khác.

Phụ thuộc: [FDP_ITC.1 Nhập dữ liệu người dùng không có thuộc tính an toàn hoặc FDP_ITC.2 Nhập dữ liệu người dùng có các thuộc tính an toàn hoặc FCS_CKM.1 Tạo khóa bằng mã hóa]

FCS_CKM.4 Hủy khóa mã hóa

FCS_COP.1.1 TSF sẽ thực hiện *mã hóa và giải mã dữ liệu khi ghi/đọc từ vùng lưu trữ được bảo vệ của thiết bị lưu trữ*[11] theo một thuật toán mã hóa được quy

[9] [chỉ định: phương pháp hủy khóa mật mã]

[10] [chỉ định: danh sách các tiêu chuẩn]

định cụ thể [*chỉ định: thuật toán mã hóa*][12] và các kích thước khóa mã hóa [*chỉ định: kích thước khóa mã hóa*][13] đáp ứng như sau: [*chỉ định: danh sách các tiêu chuẩn được chấp nhận*][14].

Chú thích áp dụng: Liên hệ với tổ chức chứng nhận để biết danh sách các tiêu chuẩn được chấp nhận.

10.1.3 Chức năng quản lý (FMT)

TOE hỗ trợ các chức năng quản lý cho vai trò của người dùng được xác thực để thay đổi dữ liệu xác thực hoặc khởi động thiết bị.

FMT_SMF.1 Đặc điểm kỹ thuật của các chức năng quản lý

Phân cấp: Không có thành phần khác.

Phụ thuộc: Không có phụ thuộc

FCS_SMF.1.1 TSF sẽ có khả năng thực hiện các chức năng quản lý sau đây:

a) sửa đổi dữ liệu xác thực

b) khởi tạo thiết bị bằng cách tạo mới khóa mã hóa và xóa các khóa trước đó [15].

Chú thích áp dụng 1: Tác giả ST có thể quy định các chức năng quản lý khác.

Chú thích áp dụng 2: Xóa các khóa trước đó sẽ làm vô hiệu hóa dữ liệu cũ được mã hóa trên thiết bị. Để tăng tính an toàn, một thiết bị cũng có thể chọn xóa bộ nhớ dữ liệu.

10.1.4 Bảo vệ dữ liệu người dùng (FDP)

Dữ liệu người dùng và dữ liệu TSF chỉ có thể truy cập được trong trạng thái TOE mở khóa. TOE phải đảm bảo rằng không có thông tin còn sót lại nào có thể truy cập được trong trạng thái khóa.

FDP_RIP.1 Bảo vệ thông tin dư thừa

Phân cấp: Không có thành phần khác.

Phụ thuộc: Không có phụ thuộc

---

[11] [chỉ định: danh sách các thao tác mật mã]

[12] [chỉ định: thuật toán mật mã]

[13] [chỉ định: kích thước khóa mật mã]

[14] [chỉ định : danh sách các tiêu chuẩn]

[15] [chỉ định: danh sách các chức năng quản lý do TSF cung cấp]

FCS_RIP.1.1	TSF đảm bảo rằng bất kỳ nội dung thông tin nào trước đây của một tài nguyên sẽ không có sẵn sau khi giải phóng tài nguyên vật lý hay theo logic từ[16] các đối tượng sau đây: người dùng bản rõ và dữ liệu TSF[17].
Chú thích áp dụng:	Giải phóng trong bối cảnh của tiêu chuẩn này được định nghĩa là kết thúc theo logic hoặc vật lý của kết nối máy chủ.

10.1.5 Bảo vệ dữ liệu TSF (FPT)

TOE sẽ bảo vệ các dữ liệu TSF và xử lý các gián đoạn trong một hệ thống an toàn, loại bỏ bất kỳ truy cập nào trong những trường hợp xảy ra sự cố.

FPT_FLS.1 Sự cố duy trì trạng thái an toàn

Phân cấp:	Không có thành phần khác.
Phụ thuộc:	Không có phụ thuộc
FCS_FLS.1.1	TSF sẽ duy trì trạng thái an toàn khi xảy ra các kiểu sự cố sau: hủy bỏ bất thường của TSF[18].
Chú thích áp dụng 1:	Các thông tin chi tiết của trạng thái an toàn được định nghĩa trong O.FailSafe.
Chú thích áp dụng 2:	Tính toàn vẹn của dữ liệu lưu trữ trên thiết bị không thuộc phạm vi của Hồ sơ bảo vệ.
Chú thích áp dụng 3:	Các sự cố theo nghĩa của SFR này nằm trong môi trường của TOE, ví dụ: sự cố hệ thống trong máy chủ, sự cố nguồn điện hoặc ngắt kết nối vật lý không cố ý hay các sự cố khác gây ra lỗi trong TSF, nghĩa là hủy bỏ bất thường của TSF, ví dụ: hủy bỏ một thao tác đọc hoặc ghi.

FPT_SDC.1 Lưu trữ dữ liệu TSF đáng tin cậy

Phân cấp:	Không có thành phần khác.
Phụ thuộc:	Không có phụ thuộc
FCS_SDC.1.1	TSF phải cung cấp không gian lưu trữ an toàn cho dữ liệu xác thực và mã hóa.
Chú thích áp dụng:	Phụ thuộc vào nhà phát triển xem những cơ chế nào được sử dụng để đảm bảo bảo vệ an toàn dữ liệu xác thực và mã hóa. Có thể là một HSM, một thẻ thông minh hoặc các hình thức bảo vệ khác để đảm bảo không thể truy cập khóa và dữ liệu xác thực.

[16] [lựa chọn: phân bổ tài nguyên đến, giải phóng tài nguyên từ]

[17] [chỉ định: danh sách các đối tượng

[18] [chỉ định: danh sách các kiểu sự cố trong TSF]

10.2 Phân tích các yêu cầu chức năng an toàn

10.2.1 Tính nhất quán nội bộ của các yêu cầu

Sự hỗ trợ lẫn nhau và tính nhất quán nội bộ của các thành phần được chọn cho tiêu chuẩn này sẽ được mô tả trong phần này.

Phân tích sau đây cho thấy tính nhất quán nội bộ của các yêu cầu chức năng.

10.2.1.1 Xác thực

Người dùng muốn truy cập vào vùng lưu trữ được bảo vệ phải được xác thực trước. TOE sẽ khóa truy cập sau nhiều lần xác thực không thành công.

Điều này được thi hành thông qua yêu cầu xác thực trước khi sử dụng (FIA_UAU.2), yêu cầu về chất lượng của yếu tố xác thực (FIA_SOS.1) và bảo vệ cơ chế xác thực thông qua FIA_AFL1. Yêu cầu quay trở lại trạng thái an toàn (FPT_FLS.1) sẽ hỗ trợ thao tác này. Yêu cầu bảo vệ thông tin còn sót lại (FDP_RIP.1) sẽ đảm bảo không có sẵn dữ liệu người dùng thuần và dữ liệu TSF.

10.2.1.2 Hỗ trợ mã hóa

TOE sẽ cung cấp không gian lưu trữ được bảo vệ theo mã hóa dựa trên các thuật toán mã hóa, các phương thức thao tác hoạt động và độ dài khóa được chấp nhận bởi quy định quốc gia.

Điều này được thi hành bởi yêu cầu mã hóa dữ liệu TSF (FCS_COP.1), được hỗ trợ bởi FCS_CKM.1 và FCS_CKM.4

10.2.1.3 Chức năng quản lý

TOE sẽ cho phép những người dùng đã xác thực sửa đổi các thuộc tính an toàn dùng để xác thực và khởi động thiết bị.

Quản lý dữ liệu xác thực được quy định thông qua FMT_SMF.1 và được hỗ trợ bởi FIA_UAU.6.

10.2.1.4 Bảo vệ dữ liệu TSF

TOE sẽ quay trở lại trạng thái an toàn trong trường hợp có sự cố về thông tin liên lạc. Thao tác này được thực hiện thông qua FPT_FLS.1

TOE sẽ bảo vệ dữ liệu TSF. Thao tác này được thực hiện thông qua FPT_SDC.1 và FDP_RIP.1.

10.2.2 Phạm vi yêu cầu an toàn

Bảng 2 - Theo dõi mục tiêu SFR

SFR	O.ProtectTSF	O.AuthAccess	O.Encrypt	O.AuthChange	O.FailSafe
FIA_UAU.2		X			
FIA_UAU.6				X	
FIA_SOS.1		X			
FIA_AFL.1		X			
FCS_CKM.1			X		
FCS_CKM.4			X		
FCS_COP.1			X		
FDP_RIP.1	X	X			X
FMT_SMF.1				X	
FPT_FLS.1					X
FPT_SDC.1	X				

Các mục tiêu sẽ được SFR đáp ứng theo cách như sau:

O.ProtectTSF Việc truy cập trái phép vào dữ liệu TSF sẽ được ngăn chặn bởi FPT_SDC.1 (yêu cầu lưu trữ an toàn cho dữ liệu xác thực và mã hóa) và FDP_RIP.1 để đảm bảo không có dữ liệu còn sót lại. Để truy cập dữ liệu xác thực, xem phần O.AuthChange bên dưới.

O.AuthAccess Quyền truy cập vào vùng lưu trữ được bảo vệ chỉ được cấp sau khi xác thực được mô phỏng qua FIA_UAU.2 và FIA_SOS.1. FIA_AFL.1 sẽ đảm bảo những lần thử xác thực không thể tiếp tục vô thời hạn, do đó có thể ngăn chặn tấn công Brute Force. FDP_RIP.1 sẽ đảm bảo dữ liệu người dùng còn sót lại không có sẵn ở trạng thái khóa.

O.Encrypt Mã hóa dữ liệu trong vùng lưu trữ được bảo vệ được thực hiện thông qua việc bảo vệ bằng mã hóa được mô phỏng trong FCS_CKM.1, FCS_CKM.4, FCS_COP.1.

O.AuthChange Quản lý dữ liệu xác thực được mô phỏng bởi FMT_SMF.1 và được hỗ trợ bởi FIA_UAU.6.

O.FailSafe Yêu cầu an toàn được mô phỏng bởi FDP_RIP.1 để bảo vệ dữ liệu còn sót lại và FPT_FLS.1 yêu cầu TOE không chuyển sang trạng thái an toàn.

10.2.3 Phân tích các yêu cầu an toàn phụ thuộc

Bảng dưới đây hiển thị cách thức các phụ thuộc của SFR được đáp ứng.

Bảng 3 - Giải quyết phụ thuộc SFR

SFR	Phụ thuộc được định nghĩa theo TCVN 8709	Giải quyết trong Hồ sơ bảo vệ / Phân tích các phụ thuộc chưa được giải quyết
FIA_UAU.2	FIA_UID.1	Chưa được giải quyết vì TOE không cần ID người dùng. Chỉ yêu cầu xác thực.
FIA_UAU.6	Không	N/A
FIA_SOS.1	Không	N/A
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FCS_CKM.1	[FCS_CKM.2 hoặc FCS_COP.1], FCS_CKM.4	FCS_COP.1, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 hoặc FDP_ITC.2 hoặc FCS_CKM.1]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 hoặc FDP_ITC.2 hoặc FCS_CKM.1], FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FDP_RIP.1	Không	N/A
FMT_SMF.1	Không	N/A
FPT_FLS.1	Không	N/A
FPT_SDC.1	Không	N/A

10.3 Yêu cầu đảm bảo an toàn

Các yêu cầu đảm bảo an toàn cho TOE là các thành phần cấp đảm bảo đánh giá 2, như quy định cụ thể trong TCVN 8709-3:2011. Không có thao tác nào được áp dụng cho các thành phần đảm bảo.

10.4 Phân tích các yêu cầu đảm bảo an toàn

Cấp độ đảm bảo đánh giá được lựa chọn tương xứng với độ an toàn môi trường TOE.

11 Gói mở rộng - Xác thực mở rộng PSMPP-EA

Gói mở rộng PSMPP này quy định các cơ chế và giao diện cho các cơ chế xác thực mở rộng áp dụng cho các thiết bị lưu trữ di động, ví dụ như xác thực dựa trên thẻ thông minh.

11.1 Tổng quan về gói mở rộng

Hồ sơ bảo vệ cơ sở được định nghĩa trong các phần trước chỉ yêu cầu xác thực người dùng. Gói mở rộng này làm tăng thêm Hồ sơ bảo vệ cơ sở để bao gồm cơ chế xác thực hai lớp ví dụ như thẻ thông minh, tin nhắn OTP, email.

11.2 Các tuyên bố tuân thủ

11.2.1 Các yêu cầu phù hợp với TCVN 8709-2:2011 và TCVN 8709-3:2011

Gói mở rộng này không làm tăng thêm yêu cầu tương thích của hồ sơ bảo vệ cơ sở như đã xác định trong Điều 6.

11.2.2 Quy tắc cấu tạo gói mở rộng

Gói mở rộng này không phụ thuộc vào các gói mở rộng khác.

Gói này chỉ có thể được yêu cầu cùng với gói cơ sở được định nghĩa trong tiêu chuẩn này.

11.3 Mô tả các vấn đề an toàn

Mô tả các vấn đề an toàn của gói mở rộng này phù hợp với mô tả các vấn đề an toàn của gói cơ sở. Gói mở rộng này không xác định bất kỳ mối đe dọa, hoặc chính sách an toàn nào khác.

11.4 Các mục tiêu an toàn

11.4.1 Các mục tiêu an toàn cho TOE

Mục tiêu O.AuthAccess từ Hồ sơ bảo vệ cơ sở sẽ được tăng cường để xác định xác thực hai yếu tố thay vì chỉ xác thực mạnh. Nó được thay thế như sau:

O.AuthAccess-EA — TOE sẽ cung cấp cơ chế xác thực hai yếu tố để chỉ cho phép những người dùng đã được xác thực mới có quyền truy cập vào vùng lưu trữ được bảo vệ.

Chú thích áp dụng: Khi sử dụng gói mở rộng này, O.AuthAccess-EA sẽ thay thế O.AuthAccess từ Hồ sơ bảo vệ cơ sở.

11.4.2 Các mục tiêu an toàn cho môi trường hoạt động

Gói mở rộng này không xác định bất kỳ mục tiêu bổ sung nào cho môi trường hoạt động.

11.4.3 Phân tích các mục tiêu an toàn

11.4.3.1 Phạm vi mục tiêu an toàn

Bảng 4 - Theo dõi mục tiêu đối với các đe dọa và giả định

Mục tiêu	Mối Đe dọa
O.AuthAccess-EA	T.LogicalAccess (từ Hồ sơ bảo vệ cơ sở)

11.4.3.2 Nội dung chi tiết của các mục tiêu an toàn

Phân tích sau đây mô tả cách thức các mục tiêu chống lại các mối đe dọa và đáp ứng các giả định:

T.LogicalAccess — Mối đe dọa về truy cập logic chưa được xác thực vào khu vực lưu trữ được bảo về sẽ bị chặn bởi O.AuthAccess-EA để đảm bảo chỉ cho phép truy cập đã được xác thực.

Chú thích áp dụng: Phần còn lại của phân tích này được lấy từ Hồ sơ bảo vệ cơ sở.

11.5 Các yêu cầu chức năng an toàn

11.5.1 Định danh và xác thực (FIA)

TOE phải cung cấp sự xác thực mạnh thông qua cơ chế xác thực dựa trên token hoặc cơ chế xác thực hai yếu tố.

FIA_UAU.5-EA Cơ chế xác thực nhiều lần

Phân cấp:	Không có thành phần khác.
Phụ thuộc:	Không có phụ thuộc
FIA_UAU.5.1	TSF sẽ cung cấp một trong các cơ chế xác thực sau đây: m1: *[lựa chọn: thẻ thông minh, [chỉ định: token mã hóa khác]]* và m2: *[lựa chọn: mật khẩu, PIN, xác thực sinh trắc học, [chỉ định: cơ chế xác thực khác]]*[19] để hỗ trợ xác thực người dùng.
Chú thích áp dụng 1:	Các phương pháp xác thực được sử dụng phải bao gồm ít nhất một token mã hóa và một phương pháp thứ hai.
Chú thích áp dụng 2:	Phần yếu hơn của hai phương pháp phải đáp ứng FIA_SOS.1 từ Hồ sơ bảo vệ cơ sở.
FIA_UAU.5.2	TSF sẽ xác thực định danh đã đưa bởi người dùng bất kỳ sau khi thành công cả hai cơ chế xác thực[20].

11.5.2 Phân tích các yêu cầu chức năng an toàn

Phần này cung cấp phân tích cho tính nhất quán nội bộ và đầy đủ của các yêu cầu chức năng an toàn được xác định trong gói mở rộng này.

11.5.2.1 Tính nhất quán nội bộ của các yêu cầu

Phần này mô tả sự hỗ trợ lẫn nhau và tính nhất quán bên trong của các thành phần được chọn cho gói mở rộng.

Phân tích sau đây cho thấy tính nhất quán bên trong của các yêu cầu chức năng.

11.5.2.1.1 Xác thực

Người dùng muốn truy cập vào vùng lưu trữ được bảo vệ sẽ được xác thực hai lớp trước khi được phép truy cập vùng lưu trữ được bảo vệ đó.

11.5.2.2 Phạm vi yêu cầu an toàn

Điều 10.2.2 được mở rộng như sau:

Bảng 5 - Gói mở rộng - theo dõi mục tiêu SFR

SFR	O.AuthAccess-EA
FIA_UAU.5-EA	X

[19] [chỉ định: danh sách các cơ chế xác thực nhiều lần]

[20] [chỉ định: các quy tắc mô tả cách thức cung cấp xác thực của các cơ chế xác thực nhiều lần]

Các mục tiêu sẽ được SFR đáp ứng theo cách như sau:

O.AuthAccess-EA Quyền truy cập vào khu vực lưu trữ được bảo vệ chỉ được cấp sau khi xác thực thông qua FIA_UAU.2 và FIA_UAU.5-EA, FIA_AFL.1 và FIA_SOS.1. FDP_RIP.1 sẽ đảm bảo dữ liệu người dùng còn sót lại không có sẵn ở trạng thái bị khóa.

11.5.2.3. Phân tích sự phụ thuộc các yêu cầu an toàn

Điều 10.2.3 được mở rộng như sau:

Bảng 6 - Gói mở rộng - giải quyết phụ thuộc SFR

SFR	Phụ thuộc được định nghĩa theo TCVN 8709	Giải quyết trong Hồ sơ bảo vệ / Phân tích các phụ thuộc chưa được giải quyết
FIA_UAU.5-EA	Không.	N/A

Thư mục tài liệu tham khảo

[1] Protection Profile for Portable Storage Media (PSMPP) (Hồ sơ bảo vệ cho thiết bị lưu trữ di động) Version 1.0, ngày 11/9/2012 của CCRA.