TCVN TIÊU CHUẨN QUỐC GIA

TCVN 8709-2 : 2011
ISO/IEC 15408-2:2008

Xuất bản lần 1

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

Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 2: Security functional components

HÀ NỘI - 2011

Mục lục

Lời nói đầu

TCVN 7809-2:2011 hoàn toàn tương đương ISO/IEC 15408-2:2008

TCVN 7809-2:2011 do Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam 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.

Lời giới thiệu

Các thành phần chức năng an toàn định nghĩa trong tiêu chuẩn này (TCVN 7809–2) là cơ sở cho các yêu cầu chức năng an toàn biểu thị trong một Hồ sơ bảo vệ (PP) hoặc một Đích An toàn (ST). Các yêu cầu này mô tả các hành vi an toàn mong muốn dự kiến đối với một Đích đánh giá (TOE) và nhằm đáp ứng các mục tiêu an toàn đã tuyên bố trong một PP hoặc một ST. Các yêu cầu này mô tả các đặc tính an toàn mà người dùng có thể phát hiện ra thông qua tương tác trực tiếp (nghĩa là qua đầu vào, đầu ra) với công nghệ thông tin (CNTT) hoặc qua phản ứng của CNTT với các tương tác.

Các thành phần chức năng an toàn biểu thị các yêu cầu an toàn nhằm mục đích chống lại các mối đe dọa trong môi trường hoạt động chỉ định của TOE với các chính sách an toàn của tổ chức xác định và các giả thiết.

Đối tượng của phần 2 tiêu chuẩn TCVN 7809 bao gồm người tiêu thụ, nhà phát triển và các đánh giá viên cho các sản phẩm CNTT an toàn. Điều 5 của TCVN 7809–1 cung cấp thông tin bổ sung về các đối tượng mục tiêu của TCVN 7809, và về các nhóm đối tượng sử dụng TCVN 7809. Các nhóm đối tượng có thể sử dụng TCVN 7809-2 gồm:

a) Người tiêu thụ là người sử dụng TCVN 7809–2 khi chọn lựa các thành phần để biểu thị các yêu cầu chức năng nhằm thỏa mãn các mục tiêu an toàn đã thể hiện trong một PP hoặc ST. TCVN 7809–1 cung cấp thông tin chi tiết hơn về mối quan hệ giữa các mục tiêu an toàn và các yêu cầu an toàn.

b) Nhà phát triển là người phản ánh thực tế hoặc nhận thức các yêu cầu an toàn của người tiêu thụ trong việc kiến thiết ra TOE. Họ cũng có thể sử dụng nội dung trong TCVN 7809-2 làm cơ sở để xác định rõ hơn các chức năng an toàn của TOE và các cơ chế tuân thủ các yêu cầu đó.

c) Đánh giá viên là người sử dụng các yêu cầu chức năng nêu trong TCVN 7809-2 để thẩm tra các yêu cầu chức năng TOE đã thể hiện trong PP hoặc ST có thỏa mãn các mục tiêu an toàn CNTT không; và thẩm tra mọi mối liên thuộc đã được xem xét đến và được thỏa mãn. Các đánh giá viên cũng cần sử dụng TCVN 7809-2 để giúp xác định xem một TOE đã cho có thỏa mãn các yêu cầu đã được công bố hay không.

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

Information Technology – Security Techniques – Evaluation Criteria for IT –

Part 2: Security functional components

1 Phạm vi áp dụng

Tiêu chuẩn này sẽ định nghĩa cấu trúc và nội dung cần thiết của các thành phần chức năng an toàn cho mục đích đánh giá an toàn. Tiêu chuẩn bao gồm danh mục các thành phần chức năng đáp ứng các yêu cầu chức năng an toàn chung cho nhiều sản phẩm CNTT.

2 Tài liệu viện dẫn

Các tài liệu sau đây không thể thiếu được đối với việc áp dụng tài liệu này:

TCVN 7809-1, *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.*

3 Thuật ngữ, định nghĩa, ký hiệu và các từ viết tắt

Các thuật ngữ, định nghĩa, Ký hiệu và các từ viết tắt được sử dụng như trong TCVN 7809-1.

4 Tổng quan

TCVN 7809 và các yêu cầu chức năng an toàn liên quan được mô tả ở đây không phải là câu trả lời rõ ràng về mọi vấn đề an toàn CNTT. Đúng hơn, TCVN 7809 cung cấp một tập các yêu cầu chức năng an toàn dễ hiểu, có thể được sử dụng để tạo ra các hệ thống và sản phẩm tin cậy phản ánh sự cần thiết của thị trường. Các yêu cầu chức năng an toàn này biểu diễn trình độ hiện tại về đánh giá và đặc tả các yêu cầu này.

Phần này của TCVN 7809 không phải bao gồm tất cả các yêu cầu chức năng an toàn thông tin có thể có mà nó chỉ gồm các phần được biết đến và được chấp nhận bởi các tác giả biên soạn tiêu chuẩn tại thời điểm phát hành.

Bởi vì hiểu biết và nhu cầu của người tiêu dùng có thể thay đổi, các yêu cầu chức năng trong phần này của TCVN 7809 cần phải được cập nhật thường xuyên. Điều này có thể hiểu là một số tác giả PP/ST có thể thấy các thành phần yêu cầu chức năng trong phần này của TCVN 7809 (hiện tại) không bao hàm hết nhu cầu về an toàn. Trong trường hợp này, tác giả PP/ST có thể xem xét lựa chọn các yêu cầu chức năng không có trong TCVN 7809 (được xem như phần mở rộng), như được giải thích trong Phụ lục A và B của TCVN 7809-1.

4.1 Bố cục của tiêu chuẩn

Điều 5 mô tả mô hình sử dụng trong các yêu cầu chức năng an toàn trong phần này của TCVN 7809.

Điều 6 giới thiệu danh mục các thành phần chức năng trong phần này của TCVN 7809, còn điều 7 đến điều 17 mô tả các lớp chức năng.

Phụ lục A cung cấp thông tin giải thích cho người dùng tiềm năng của các thành phần chức năng bao gồm bảng tham chiếu chéo tổng hợp về sự phụ thuộc của các thành phần chức năng.

Phụ lục B đến Phụ lục M cung cấp thông tin giải thích về các lớp chức năng. Tài liệu này được xem như là các hướng dẫn bắt buộc về việc áp dụng các hoạt động phù hợp và lựa chọn quy trình kiểm toán hoặc thông tin tài liệu phù hợp. Việc sử dụng các trợ động từ nên hiểu là các chỉ dẫn được ưa chuộng nhất, các chỉ dẫn khác có thể được điều chỉnh phù hợp. Nếu có các tùy chọn khác, việc lựa chọn được dành cho tác giả PP/ST.

Tác giả của PP hoặc ST nên tham khảo điều 2 của TCVN 7809-1 để có các cấu trúc, quy tắc và hướng dẫn liên quan.

a) TCVN 7809-1, điều 3 định nghĩa các thuật ngữ sử dụng trong TCVN 7809.

b) TCVN 7809-1, Phụ lục A định nghĩa cấu trúc của ST.

c) TCVN 7809-1, Phụ lục B định nghĩa cấu trúc của PP.

5 Mô hình các yêu cầu chức năng

Điều này mô tả mô hình sử dụng trong các yêu cầu chức năng an toàn trong TCVN 7809-2. Các khái niệm chủ yếu được in đậm hoặc nghiêng. Phần này sẽ không thay thế hoặc hủy bỏ các thuật ngữ có trong điều 3 của TCVN 7809-1.

Phần này của TCVN 7809 là danh mục các yêu cầu chức năng an toàn có thể được chỉ rõ cho một **Đích đánh giá (TOE)**. Một TOE là một tập gồm phần mềm/phần sụn và/hoặc phần cứng có thể kèm theo tài liệu hướng dẫn người dùng và quản trị viên. Một TOE có thể chứa các tài nguyên như các phương tiện lưu trữ điện tử (ví dụ đĩa), các thiết bị ngoại vi (ví dụ máy in), và năng lực tính toán (ví dụ thời gian CPU) được sử dụng cho xử lý và lưu trữ thông tin, và là chủ thể cho đánh giá.

Đánh giá TOE chủ yếu liên quan tới việc đảm bảo rằng một tập **các yêu cầu chức năng an toàn (SFR)** xác định được thực thi trên các tài nguyên TOE. Các SFR định nghĩa các quy tắc mà TOE kiểm soát truy cập tài nguyên của nó cũng như các thông tin và dịch vụ được điều khiển bởi TOE.

Các SFR có thể định nghĩa nhiều **Chính sách Chức năng An toàn** (SFP) biểu thị các quy tắc mà TOE phải thực thi. Mỗi SFP phải xác định **phạm vi kiểm soát** của nó, bằng cách định nghĩa các chủ thể, đối tượng, tài nguyên hay thông tin và các hoạt động được kiểm soát với SFP. Tất cả các SFP được thực thi bởi TSF (xem bên dưới); các cơ chế của TSF thực thi các quy tắc định nghĩa trong các SFR và cung cấp các khả năng cần thiết.

Các phần đã nêu trên của TOE cần phải được tin cậy cho thực thi chính xác của các SFR, được tham chiếu đến như **Chức năng An toàn của TOE (TSF)**. TSF bao gồm tất cả các phần cứng, phần mềm, phần sụn của TOE, trực tiếp và gián tiếp liên quan đến việc thực thi an toàn.

TOE có thể là một sản phẩm đơn nhất chứa cả phần cứng, phần sụn và phần mềm.

Mặt khác, TOE có thể là một sản phẩm phân bổ bao gồm nhiều thành phần khác nhau bên trong. Mỗi phần này của TOE cung cấp một dịch vụ riêng cho TOE và được kết nối với phần khác của TOE thông qua **Kênh truyền thông nội bộ**. Kênh này có thể là một phần nhỏ như bus xử lý hoặc bao bọc trong mạng nội bộ tới TOE.

Khi TOE bao gồm nhiều phần, mỗi phần của TOE có TSF riêng thực hiện trao đổi dữ liệu người dùng và dữ liệu TSF trên các kênh truyền thông nội bộ với các phần khác của TSF. Quá trình tương tác này được gọi là **Vận chuyển TOE nội bộ**. Trong trường hợp này các phần tách biệt của TSF được tạo thành TSF hỗn hợp để thực thi các SFR.

Các giao diện TOE có thể được đặt tại TOE riêng, hoặc chúng có thể tương tác với các sản phẩm CNTT qua **các kênh truyền thông bên ngoài**. Các tương tác ra bên ngoài này với các sản phẩm CNTT khác có thể thực hiện dưới hai dạng :

a) Các SFR của "Sản phẩm CNTT được tin cậy" khác và các SFR của TOE đã được kết hợp quản trị và các sản phẩm CNTT tin cậy khác được giả thiết là thực thi các SFR của chúng một cách chính xác (ví dụ được đánh giá riêng biệt). Việc trao đổi thông tin trong tình huống này được gọi là **Vận chuyển xuyên TSF**, vì chúng là giữa các TSF của các sản phẩm tin cậy khác biệt.

b) Sản phẩm CNTT khác có thể không được tin cậy, nó có thể được gọi là "sản phẩm CNTT không tin cậy". Do đó, các SFR của chúng hoặc là không được biết hoặc việc triển khai nó được không xem là đáng tin cậy. Các trao đổi trung gian qua TSF trong trường hợp này được gọi là **vận chuyển bên ngoài TOE**, vì không có TSF (hoặc các đặc điểm chính sách không biết trước) trong sản phẩm CNTT khác.

Tập các giao diện, hoặc qua tương tác (giao diện người-máy) hoặc qua chương trình (giao diện lập trình ứng dụng), qua đó các tài nguyên này được truy cập trung gian bởi TSF, hoặc các thông tin thu được từ TSF, được coi là **Giao diện TSF (TSFI)**. TSFI định nghĩa biên giới của chức năng TOE được cung cấp cho việc thực thi các SFR.

Người dùng ở bên ngoài TOE. Mặc dù vậy, để yêu cầu rằng các dịch vụ được thực hiện bởi TOE là chủ thể cho các quy tắc định nghĩa trong các SFR, thì người dùng sẽ tương tác với TOE thông qua các TSFI. Có hai kiểu người dùng được quan tâm trong TCVN 7809-2: **người dùng cụ thể và các thực thể CNTT bên ngoài**. Người dùng cụ thể còn có thể được phân thành, **người dùng nội bộ**, nghĩa là người dùng tương tác trực tiếp với TOE qua các thiết bị TOE (ví dụ, các trạm làm việc) hoặc **người dùng từ xa**, nghĩa là thực hiện tương tác gián tiếp với TOE qua sản phẩm CNTT khác.

Một giai đoạn tương tác giữa các người dùng và TSF là được xem như là một **phiên** người dùng. Thiết lập các phiên người dùng có thể được kiểm soát dựa trên các suy xét, ví dụ, xác thực người dùng, thời gian trong ngày, phương pháp truy nhập TOE và số lượng các phiên tương tranh cho phép (trên một người dùng hoặc toàn bộ).

Tiêu chuẩn này sử dụng thuật ngữ **"có thẩm quyền"** để biểu thị người dùng có quyền và/hoặc đặc quyền cần thiết để thực hiện một hoạt động. Thuật ngữ **người dùng có thẩm quyền**, chỉ ra rằng có thể cho phép người dùng thực hiện một hoạt động cụ thể hoặc một số hoạt động được định nghĩa bởi các SFR.

Để biểu diễn các yêu cầu có đòi hỏi việc phân chia trách nhiệm của người quản trị, các thành phần chức năng an toàn liên quan (trong họ FMT_SMR) tuyên bố rõ ràng về **các vai trò** của người quản trị là cần thiết. Vai trò là một tập được định nghĩa trước của các quy tắc thiết lập các tương tác được phép giữa một người dùng hoạt động trong vai trò này và TOE. Một TOE có thể hỗ trợ định nghĩa bất kỳ số lượng phân vai nào. Ví dụ, các vai trò liên quan đến hoạt động an toàn của một TOE có thể bao gồm "Quản trị viên Kiểm toán " và "Quản trị viên tài khoản người dùng".

TOE chứa **các tài nguyên** có thể được sử dụng cho xử lý và lưu trữ thông tin. Mục tiêu đầu tiên của TSF là hoàn tất và chỉnh sửa các các thực thi của các SFR trên các tài nguyên, và thông tin mà TOE kiểm soát.

Các tài nguyên TOE có thể được cấu trúc và thực hiện theo nhiều cách khác nhau. Mặc dù vậy, phần này của TCVN 7809 thực hiện các phân chia đặc biệt mà cho phép chỉ ra các thuộc tính an toàn mong muốn. Tất cả các thực thể có thể được tạo từ các tài nguyên mà có thể được biểu diễn theo một hoặc hai cách. Các thực thể có thể là chủ động, nghĩa là chúng là nguyên nhân của các hành động xuất hiện bên trong TOE và là nguyên nhân của các hoạt động được thực hiện với thông tin. Mặt khác, các thực thể có thể là bị động, nghĩa là chúng hoặc được đặt trong các thông tin nguyên bản hoặc các thông tin được lưu trữ trong đó.

Các thực thể chủ động trong TOE thực hiện các hoạt động trên các đối tượng được xem như là các **chủ thể**. Một vài kiểu chủ thể có thể tồn tại bên trong một TOE:

a) Các chủ thể hành động thay mặt cho một người dùng có thẩm quyền (ví dụ các tiến trình UNIX);

b) Các chủ thể hành động như các tiến trình chức năng cụ thể, và như vậy hoạt động thay mặt cho nhiều người dùng (ví dụ các chức năng có thể thấy trong các kiến trúc client/server); hoặc

c) Các chủ thể hành động như là một phần của chính TOE (ví dụ các tiến trình không hành động thay mặt cho một người dùng).

Phần này của TCVN 7809 đề cập đến việc thực thi các SFR với các kiểu chủ thể được liệt kê ở trên.

Các thực thể bị động trong TOE chứa hoặc nhận thông tin và dựa vào đó các chủ thể thực hiện các hoạt động, được gọi là các **đối tượng**. Trong trường hợp chủ thể (thực thể chủ động) là đích của một hoạt động (ví dụ truyền thông liên tiến trình), một chủ thể có thể bị tác động như một đối tượng.

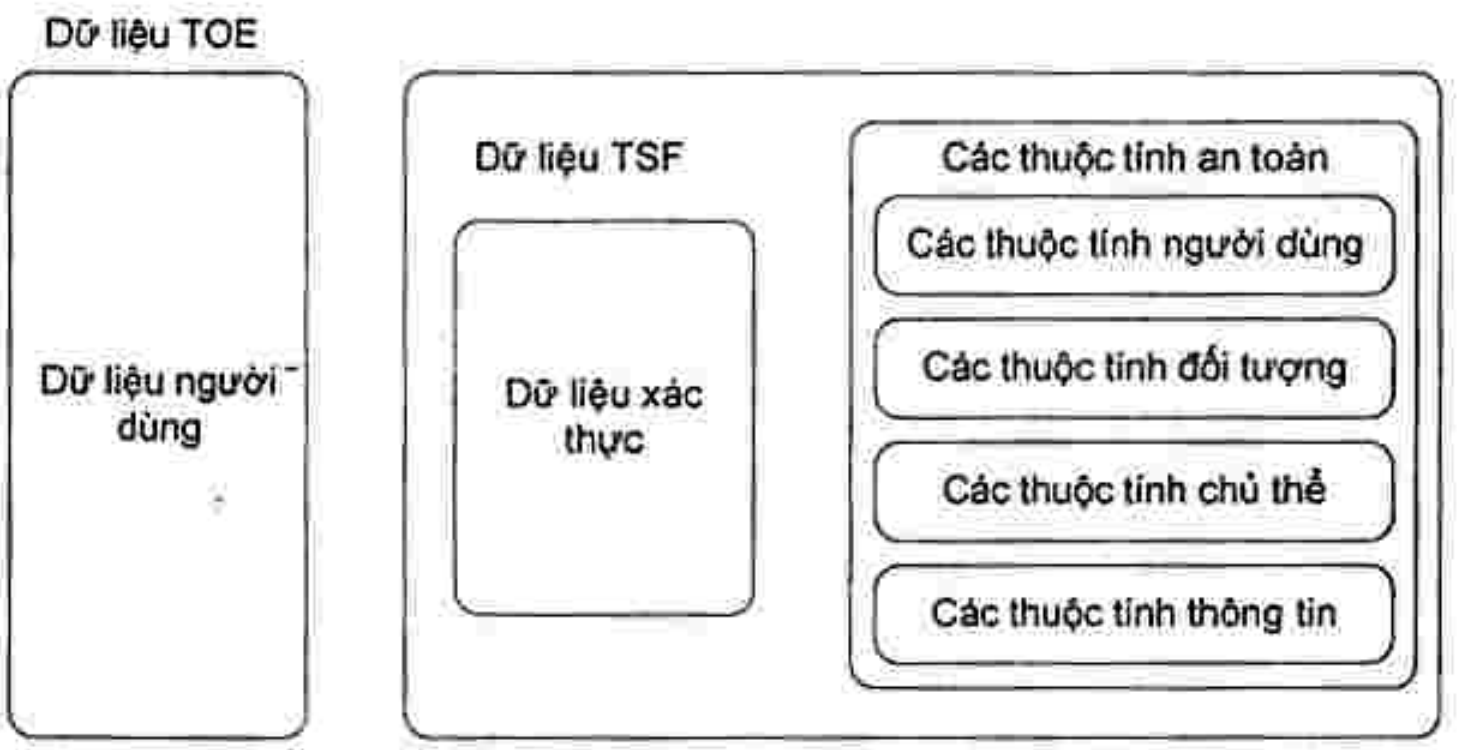
Các đối tượng có thể chứa **thông tin**. Khái niệm này cần thiết để xác định các chính sách kiểm soát luồng thông tin như được đề cập đến trong lớp FDP.

Các người dùng, chủ thể, thông tin, đối tượng, phiên và tài nguyên được kiểm soát bởi các quy tắc trong các SFR có thể có **các thuộc tính** trong đó chứa thông tin dùng cho TOE để thực hiện hoạt động chính xác của nó. Một vài thuộc tính, như tên tệp, có thể dùng cho cung cấp thông tin hoặc có thể dùng để định danh các tài nguyên riêng, trong khi đó, các thuộc tính khác, ví dụ như thông tin kiểm soát truy nhập, có thể tồn tại đặc biệt cho thực thi các SFR. Các thuộc tính vừa kể đến sau cùng này được gọi chung là " **các thuộc tính an toàn**". Từ thuộc tính sẽ được sử dụng ngắn gọn thay cho "thuộc tính an toàn" ở một số chỗ trong phần này của TCVN 7809. Tuy nhiên, không quan trọng là mục đích của thông tin thuộc tính là gì, vì đều cần thiết kiểm soát các thuộc tính được chỉ ra bởi các SFR.

Dữ liệu trong TOE được phân nhóm thành dữ liệu người dùng và dữ liệu TSF. Hình 1 cho thấy mối quan hệ này. **Dữ liệu người dùng** là thông tin lưu trữ trong các tài nguyên của TOE, được vận hành bởi người dùng tuân theo các SFR và trên đó TSF không đề ra ý nghĩa đặc biệt nào. Ví dụ, nội dung của một thông điệp thư điện tử là dữ liệu người dùng. Dữ liệu TSF là thông tin được sử dụng bởi TSF trong việc tạo ra các quyết định theo yêu cầu bởi các SFR. **Dữ liệu TSF** có thể bị ảnh hưởng bởi người dùng nếu được cho phép bởi các SFR. Các thuộc tính an toàn, dữ liệu xác thực, các biến trạng thái bên trong TSF được dùng bởi các quy tắc định nghĩa trong các SFR hoặc được dùng cho việc bảo vệ TSF, và các đầu vào của danh sách kiểm soát truy nhập là các ví dụ về dữ liệu TSF.

Có một số SFPs áp dụng cho bảo vệ dữ liệu, ví dụ như các **SFP kiểm soát truy nhập** và các **SFP kiểm soát luồng thông tin**. Các cơ chế thực thi các SFP kiểm soát truy nhập dựa trên chính sách quyết định về các thuộc tính của người dùng, tài nguyên, chủ thể, đối tượng và các phiên, dữ liệu trạng thái TSF và các hoạt động của TSF trong phạm vi kiểm soát. Các thuộc tính này thường được sử dụng trong tập các quy tắc để quản lý các hoạt động mà các chủ thể có thể thực hiện trên các đối tượng.

Các cơ chế thực thi các SFP kiểm soát luồng thông tin dựa trên chính sách quyết định về các thuộc tính của chủ thể và thông tin trong phạm vi kiểm soát và tập các quy tắc để quản lý các hoạt động thông tin bởi các chủ thể. Các thuộc tính của thông tin có thể được kết hợp với thuộc tính của côn-ten-nơ hoặc có thể rút ra từ dữ liệu trong côn-ten-nơ, sẽ được giữ lại với thông tin vì chúng được xử lý bởi TSF.



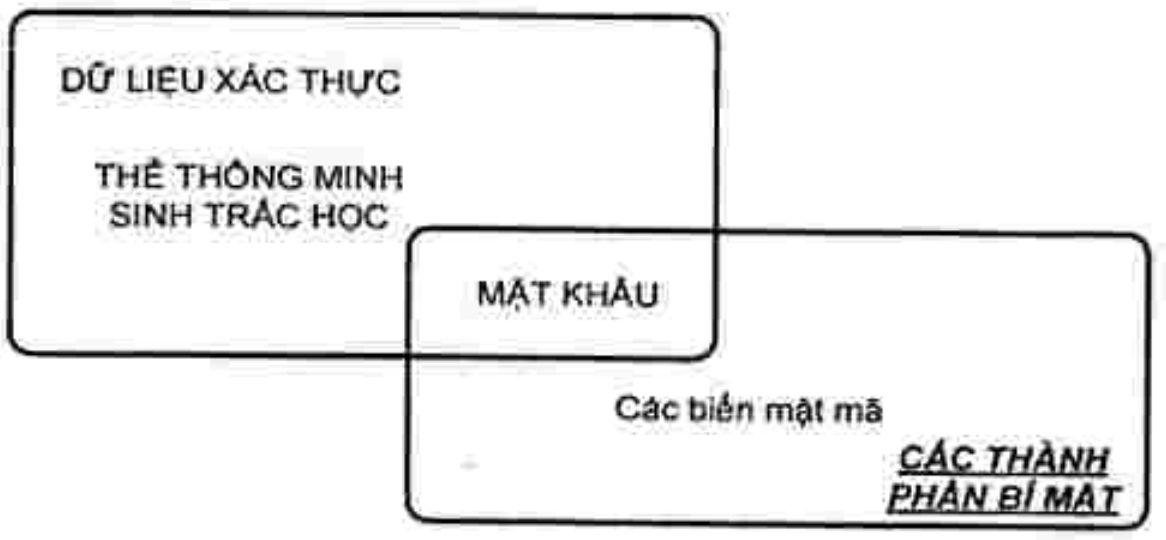
Hình 1 - Quan hệ giữa dữ liệu người dùng và dữ liệu TSF

Hai kiểu dữ liệu TSF đặc trưng có thể được đề cập đến trong phần này của TCVN 7809, song không nhất thiết giống nhau. Chúng là **dữ liệu xác thực** và **các bí mật**.

Dữ liệu xác thực được sử dụng để thẩm tra danh tính đòi hỏi của một người dùng đang yêu cầu các dịch vụ từ một TOE. Dạng phổ biến của dữ liệu xác thực là mật khẩu, phụ thuộc vào việc giữ bí mật để tạo thành một cơ chế an toàn hiệu quả. Mặc dù vậy, không phải tất cả các dạng của dữ liệu xác thực cần phải giữ bí mật. Thiết bị xác thực sinh học (ví dụ đọc vân tay hoặc quét võng mạc) không dựa vào việc giữ bí mật dữ liệu, mà dựa vào việc dữ liệu chỉ do một người dùng sở hữu và không thể bị giả mạo.

Thuật ngữ bí mật như được dùng trong phần này của TCVN 7809 vào việc áp dụng cho dữ liệu xác thực, song cũng dùng được cho các kiểu dữ liệu khác với yêu cầu phải giữ bí mật để thực thi một SFP cụ thể. Ví dụ, một cơ chế kênh tin cậy dựa vào mã hóa để bảo vệ tính bí mật của thông tin truyền trên kênh chỉ có thể mạnh như phương pháp sử dụng để giữ bí mật các khóa mã chống các khai thác không được phép.

Do đó, một số song không phải tất cả dữ liệu xác thực cần được giữ bí mật, và một số song không phải tất cả các bí mật được dùng như dữ liệu xác thực. Hình 2 chỉ ra mối quan hệ giữa bí mật và dữ liệu xác thực. Trong hình này, các kiểu thường gặp của dữ liệu xác thực và các điều khoản bí mật được chỉ ra.



Hình 2 – Mối quan hệ giữa "dữ liệu xác thực" và "các bí mật"

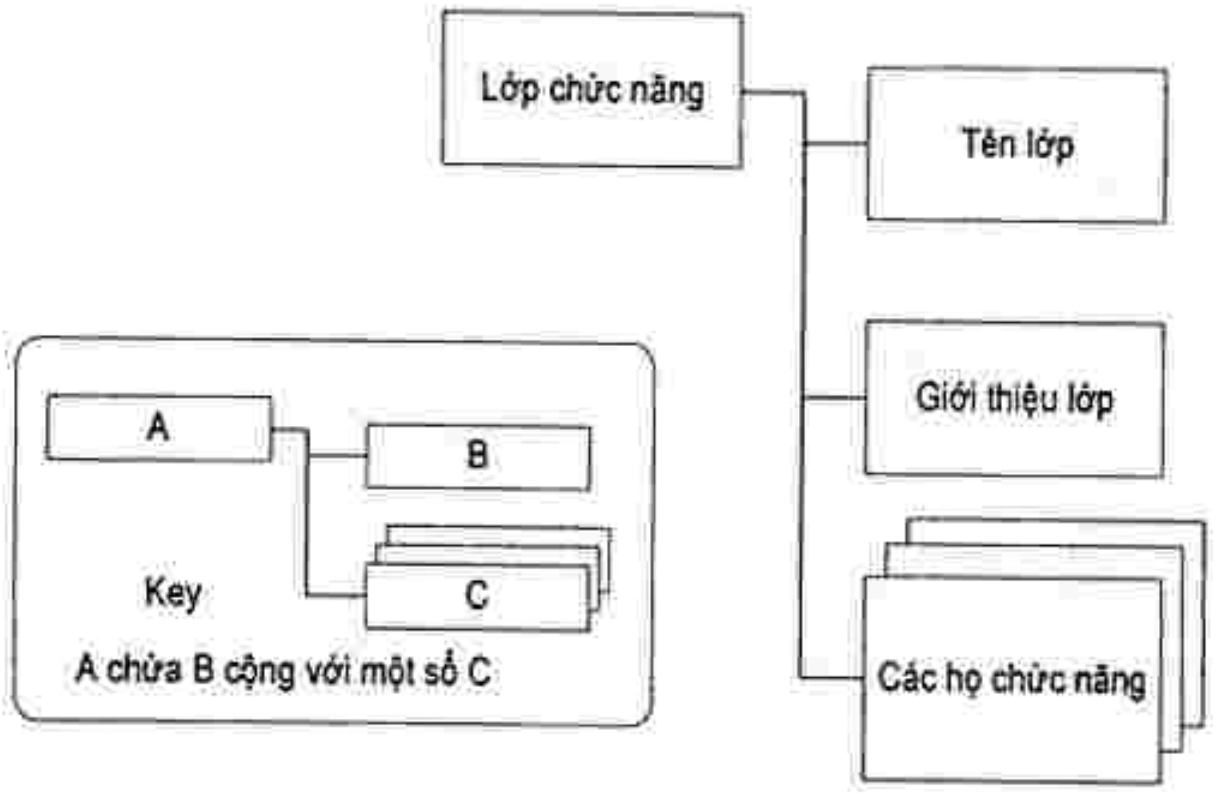
6 Các thành phần chức năng an toàn

6.1 Tổng quan

Điều này này định nghĩa nội dung và trình bày của các yêu cầu chức năng của ISO 15408, và cung cấp các hướng dẫn về tổ chức của các yêu cầu cho các thành phần mới được đặt trong ST. Các yêu cầu chức năng được biểu diễn theo các lớp, họ và thành phần.

6.1.1 Cấu trúc lớp

Hình 3 biểu diễn các cấu trúc lớp chức năng dưới dạng biểu đồ. Mỗi lớp chức năng bao gồm tên lớp, giới thiệu về lớp và một hoặc nhiều họ chức năng.



Hình 3 - Cấu trúc lớp chức năng

6.1.1.1 Tên lớp

Mục tên lớp cung cấp thông tin cần thiết để chỉ ra và phân nhóm một lớp chức năng. Mỗi lớp chức năng có một tên duy nhất. Thông tin phân nhóm bao gồm một tên viết tắt ba ký tự. Tên viết tắt của lớp thường sử dụng để xác định tên viết tắt của các họ của lớp đó.

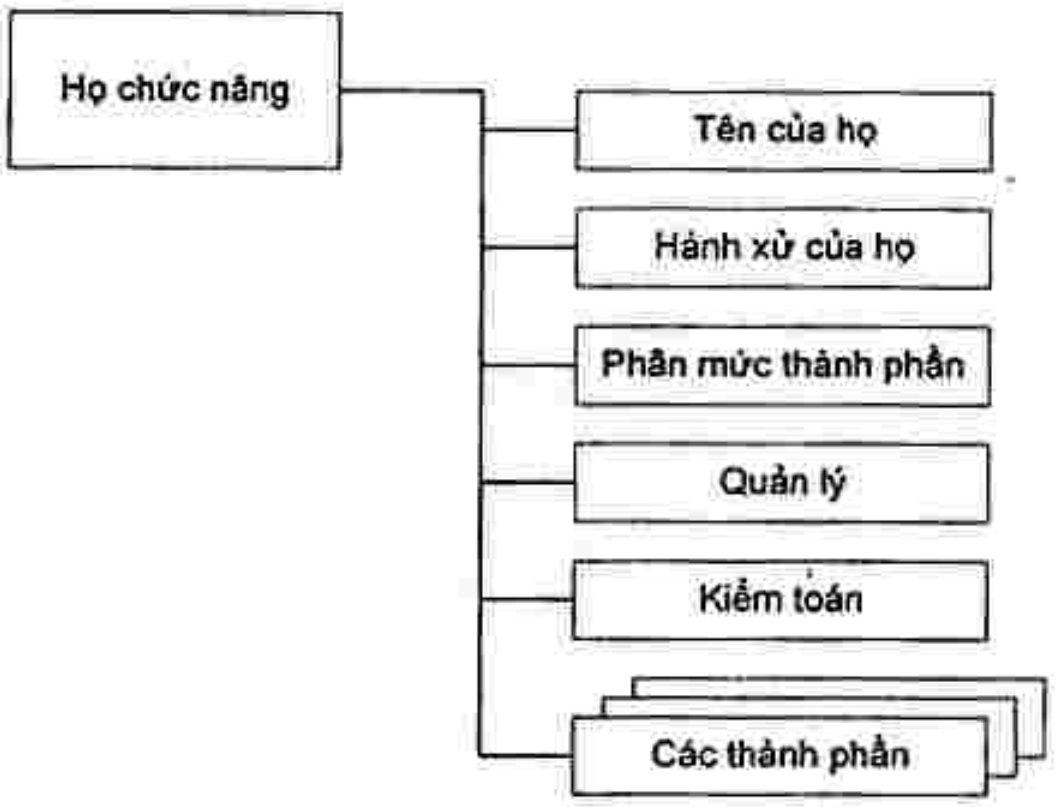
6.1.1.2 Giới thiệu lớp

Giới thiệu lớp biểu diễn ý định chung hoặc cách tiếp cận của các họ của chúng để thỏa mãn các mục tiêu an toàn. Định nghĩa các lớp chức năng không phản ánh bất kỳ một sự phân loại chính thức nào về đặc tả của các yêu cầu.

Giới thiệu lớp cung cấp một bức tranh mô tả các họ trong lớp này và phân cấp của các thành phần trong mỗi họ, như được trình bày trong 6.2

6.1.2 Cấu trúc họ

Hình 4 mô tả các cấu trúc họ chức năng dưới dạng biểu đồ.



Hình 4 - Cấu trúc họ chức năng

6.1.2.1 Tên của họ

Mục tên của họ quy định sự phân loại và thông tin mô tả cần thiết để chỉ ra và phân nhóm một họ chức năng. Mỗi họ chức năng có một tên duy nhất. Thông tin phân nhóm gồm một tên viết tắt 7 ký tự với 3 ký tự đầu tiên là tên viết tắt của lớp, tiếp theo là dấu gạch chân và tên viết tắt của họ dưới dạng XXX_YYY. Dạng viết tắt duy nhất của tên họ cung cấp tên tham chiếu cho các thành phần

6.1.2.2 Hành xử của họ

Cách hành xử của họ là mô tả chi tiết các họ chức năng phản ánh mục tiêu an toàn của nó và mô tả chung về các yêu cầu chức năng. Chúng được mô tả chi tiết hơn dưới đây

a) Các *mục tiêu an toàn* của họ đề cập đến một vấn đề an toàn có thể được giải quyết với sự trợ giúp của TOE kết hợp với một thành phần của họ này

b) Mô tả của các *yêu cầu chức năng* tóm tắt tất cả các yêu cầu được chứa trong các thành phần. Việc mô tả được thực hiện bởi các tác giả của PP, ST và các gói chức năng; đó là những người sẽ thực hiện *đánh giá* xem họ này có phù hợp với các yêu cầu cụ thể đặt ra hay không

6.1.2.3 Phân mức các thành phần

Các họ chức năng chứa một hoặc nhiều thành phần, mà bất kỳ thành phần nào cũng có thể được lựa chọn để đưa vào các PP, ST và các gói chức năng. Đích của điều khoản này là cung cấp thông tin cho người dùng để lựa chọn ra một thành phần chức năng phù hợp sau khi đã được xác định được họ là phần cần thiết và hữu ích của các yêu cầu an toàn.

Mục mô tả họ chức năng này sẽ mô tả các thành phần sẵn sàng và sở cứ hợp lý của chúng. Chi tiết chính xác về mỗi thành phần được đặt bên trong mỗi thành phần.

Mối quan hệ giữa các thành phần bên trong một họ chức năng có thể được hoặc không được phân cấp. Một thành phần được phân cấp với thành phần khác nếu nó cung cấp mức độ an toàn cao hơn.

Như được giải thích trong 6.2, việc mô tả các họ cung cấp một bức tranh chung dạng đồ thị về sự phân cấp của các thành phần trong một họ

6.1.2.4 Quản lý

Điều khoản *quản lý* chứa thông tin cho các tác giả PP/ST để xem xét các hoạt động quản lý cho các thành phần được đưa ra. Các điều khoản tham chiếu đến các thành phần của lớp quản lý (FMT) và cung cấp hướng dẫn liên quan đến các hoạt động quản lý tiềm năng có thể áp dụng qua các hoạt động tới các thành phần đó.

Tác giả PP/ST có thể lựa chọn các thành phần quản lý định trước hoặc đưa vào các yêu cầu quản lý khác chưa được liệt kê cho các hoạt động quản lý chi tiết. Vì vậy, thông tin nên xem xét là tham khảo.

6.1.2.5 Kiểm toán

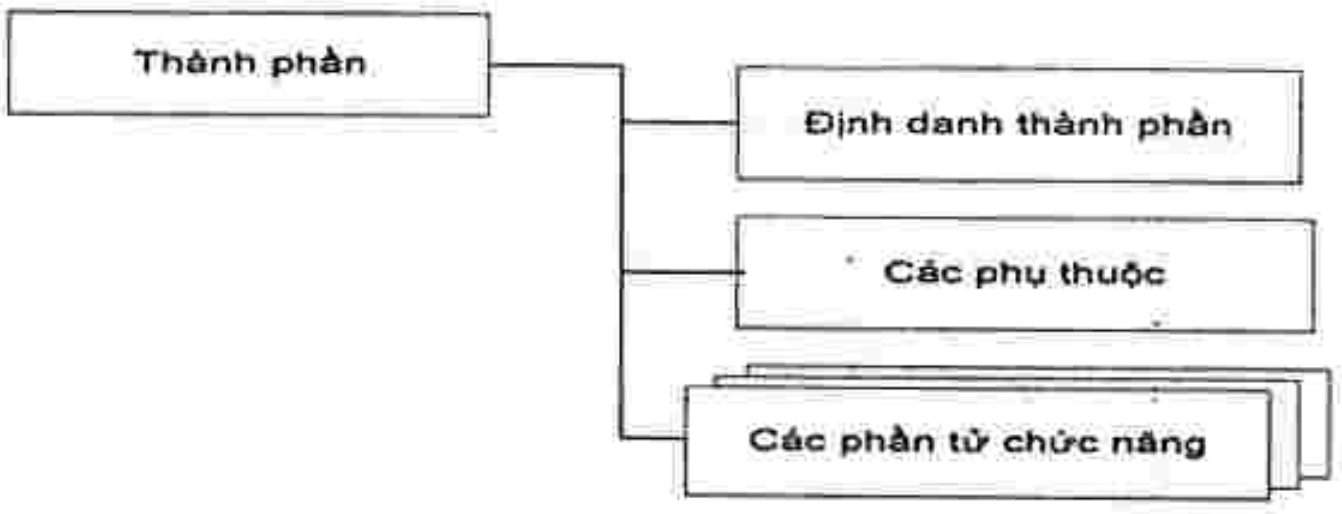
Các yêu cầu *kiểm toán* chứa các sự kiện kiểm toán cho các tác giả PP/ST lựa chọn, nếu các yêu cầu từ lớp FAU:Kiểm toán an toàn được đưa vào trong PP/ST. Các yêu cầu này bao gồm các sự kiện an toàn phù hợp ở các mức chi tiết khác nhau được hỗ trợ bởi các thành phần của họ Tạo dữ liệu kiểm toán an toàn (FAU_GEN). Ví dụ, một ghi chú kiểm toán có thể bao gồm các hoạt động dưới dạng: Tối thiểu - Sử dụng thành công các cơ chế an toàn; Cơ bản - sử dụng bất kỳ cơ chế an toàn cũng như thông tin phù hợp đối với các thuộc tính an toàn liên quan; Chi tiết - bất kỳ sự thay đổi cấu hình nào thực hiện với cơ chế bao gồm các giá trị cấu hình thực tế trước và sau khi thay đổi.

Nên thấy việc phân nhóm các sự kiện có thể kiểm toán là có phân cấp. Ví dụ, khi muốn Tạo kiểm toán cơ bản, nên đưa tất cả các sự kiện có thể kiểm toán, được xác định dưới cả hai dạng cơ bản và tối thiểu, vào trong PP/ST, thông qua sử dụng các hoạt động chỉ định phù hợp, ngoại trừ các sự kiện mức cao hơn cung cấp nhiều chi tiết hơn các sự kiện mức thấp hơn. Khi muốn Tạo kiểm toán chi tiết, nên đưa tất cả các sự kiện có thể kiểm toán (tối thiểu, cơ sở và chi tiết) vào trong PP/ST.

Trong lớp FAU:Kiểm toán an toàn, các quy tắc quản lý kiểm toán sẽ được giải thích chi tiết hơn.

6.1.3 Cấu trúc thành phần

Hình 5 biểu diễn cấu trúc thành phần chức năng.



Hình 5 - Cấu trúc thành phần chức năng

6.1.3.1 Định danh thành phần

Điều khoản định danh thành phần này cung cấp thông tin mô tả cần thiết để định danh, phân nhóm, đăng ký và tham chiếu chéo cho một thành phần. Sau đây là các phần được cung cấp cho mỗi thành phần chức năng.

Tên duy nhất: Tên phản ánh mục đích của các thành phần

Tên viết tắt: Dạng viết tắt duy nhất của tên thành phần chức năng. Tên viết tắt này sử dụng như là tên tham chiếu chính cho việc phân nhóm, đăng ký và thực hiện tham chiếu chéo của thành phần. Tên viết tắt này biểu thị lớp và họ mà thành phần này trực thuộc và số thành phần bên trong họ.

Danh sách phân cấp: Một danh sách của các thành phần khác mà thành phần này phân cấp và dựa vào đó thành phần này có thể được sử dụng để đáp ứng sự phụ thuộc với các thành phần đã được liệt kê.

6.1.3.2 Các phần tử chức năng

Tập các phần tử được cung cấp cho mỗi thành phần. Mỗi phần tử này được định nghĩa riêng và chứa chính nó.

Một phần tử chức năng là một yêu cầu chức năng an toàn mà nếu phân chia nhỏ hơn thì kết quả đánh giá sẽ không còn ý nghĩa. Nó là yêu cầu chức năng an toàn nhỏ nhất được xác định và chấp nhận trong TCVN 7809.

Khi xây dựng các gói, các PP và ST, không được phép lựa chọn chỉ một hoặc nhiều phần tử từ một thành phần. Tập đầy đủ các phần tử của một thành phần cần phải được lựa chọn từ một PP, ST hoặc gói.

Một dạng viết tắt duy nhất của tên phần tử chức năng được cung cấp. Ví dụ tên yêu cầu FDP_IFF.4.2 đọc như sau: F - yêu cầu chức năng; DP - lớp "Bảo vệ dữ liệu người dùng"; IFF - Họ "Các chức năng kiểm soát luồng thông tin"; 4 - tên của thành phần thứ tư "Loại trừ từng phần các luồng thông tin không hợp pháp"; 2 - phần tử thứ 2 của thành phần.

6.1.3.3 Mối phụ thuộc

Mối phụ thuộc giữa các thành phần chức năng tăng lên khi một thành phần tự nó không đủ khả năng và độ tin cậy về chức năng, hoặc tương tác, với thành phần khác về các chức năng phù hợp của nó.

Mỗi thành phần chức năng cung cấp một danh sách đầy đủ các mối phụ thuộc với các thành phần chức năng và đảm bảo khác. Một vài thành phần có thể liệt kê "Không phụ thuộc". Các thành phần phụ thuộc trên có thể có sự phụ thuộc trong các thành phần khác. Danh sách được cung cấp trong các thành phần sẽ là các mối phụ thuộc trực tiếp. Đó chỉ là sự tham chiếu đến các yêu cầu chức năng đòi hỏi đối với các yêu cầu này để thực hiện công việc của nó chính xác. Các mối phụ thuộc gián tiếp, nghĩa là các phụ thuộc là kết quả từ sự phụ thuộc vào các thành phần, thì có thể xem trong Phụ lục A của TCVN 7809-2. Chý ý rằng trong một vài trường hợp, sự phụ thuộc là tùy chọn, trong đó số các yêu cầu chức năng được cung cấp, tại đó mỗi thành phần của chúng có thể đáp ứng đầy đủ sự phụ thuộc (xem ví dụ FDP_UIT.1 Toàn vẹn trao đổi dữ liệu)

Danh sách phụ thuộc xác định các thành phần đảm bảo hoặc thành phần chức năng tối thiểu cần thiết để thỏa mãn các yêu cầu an toàn liên quan đến một thành phần xác định. Các thành phần được phân cấp theo thành phần đã định danh có thể được sử dụng để thỏa mãn mối phụ thuộc.

Các mối phụ thuộc chỉ ra trong phần này của TCVN 7809 là bắt buộc. Chúng phải được thỏa mãn trong PP hoặc ST. Trong các tình huống cụ thể, các mối phụ thuộc xác định có thể không được áp dụng. Tác giả PP/ST thông qua việc cung cấp sở cứ vì sao nó không được áp dụng, có thể bỏ đi các mối phụ thuộc với các thành phần ra ngoài gói, PP hoặc ST.

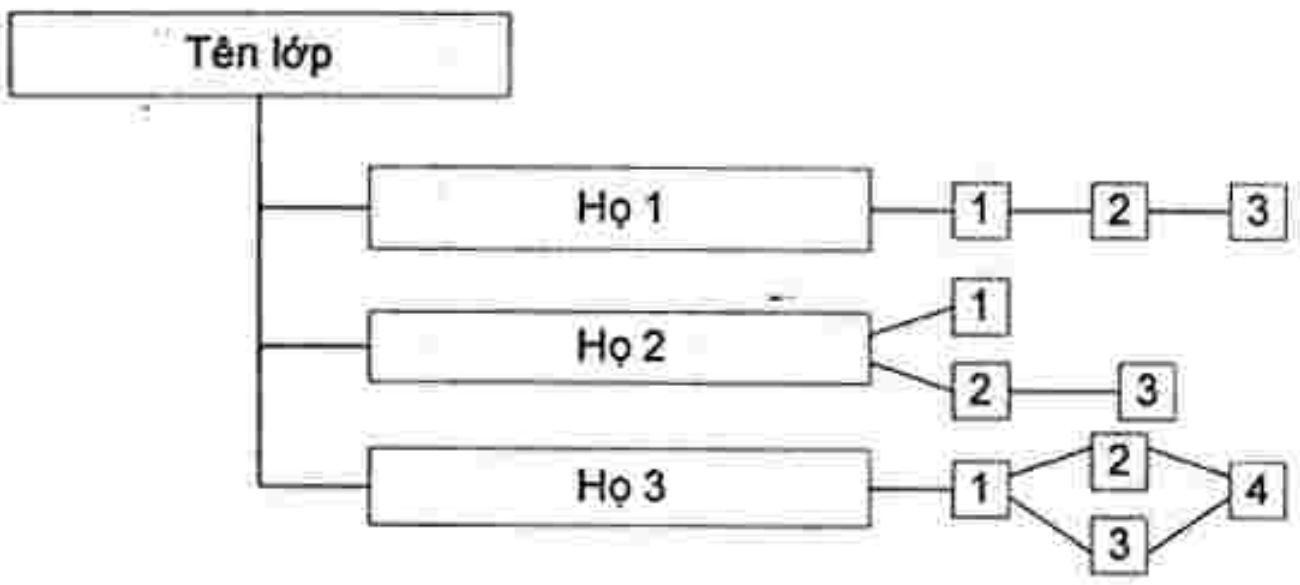
6.2 Danh mục thành phần

Nhóm của các thành phần trong phần này của TCVN 7809 không phản ánh bất kỳ sự phân loại chính thức nào.

Phần này của TCVN 7809 chứa các lớp của các họ và các thành phần, chúng được phân nhóm dựa trên cơ sở của các chức năng hoặc mục đích liên quan, được biểu diễn theo thứ tự chữ cái. Bắt đầu của mỗi lớp là một biểu đồ thông tin chỉ ra phân loại của mỗi lớp, chỉ ra các họ trong mỗi lớp và các tp trong mỗi họ. Biểu đồ là một chỉ dẫn hữu ích cho quan hệ phân cấp có thể tồn tại giữa các thành phần.

Trong việc mô tả các thành phần chức năng, có một điều khoản nhỏ xác định các mối phụ thuộc giữa thành phần và bất kỳ thành phần nào khác.

Trong mỗi lớp, một hình vẽ mô tả phân cấp lớp tương tự như Hình 6 được cung cấp. Trong Hình 6, họ đầu tiên, Họ 1, chứa ba thành phần phân cấp, tại đó cả hai thành phần 2 và thành phần 3 có thể sử dụng để thỏa mãn các mối phụ thuộc vào thành phần 1. Thành phần 3 được phân cấp theo thành phần 2 và có thể được sử dụng để thỏa mãn sự phụ thuộc vào thành phần 2.



Hình 6 - Biểu đồ phân cấp lớp đơn giản

Trong họ 2 có ba thành phần, trong đó không phải tất cả được phân cấp. Các thành phần 1 và 2 không phân cấp theo các thành phần khác. Thành phần 3 được phân cấp theo thành phần 2, có thể dùng để thỏa mãn mối phụ thuộc vào thành phần 2, nhưng không thỏa mãn sự phụ thuộc vào thành phần 1.

Trong họ 3, các thành phần 2, 3 và 4 được phân cấp theo thành phần 1. Các thành phần 2 và 3 được phân cấp theo thành phần 1, nhưng không so sánh chúng được. Thành phần 4 phân cấp theo cả thành phần 2 và 3.

Những biểu đồ này bổ sung cho văn bản của các họ và tạo ra định danh cho các mối quan hệ dễ dàng hơn. Chúng không thay thế cho ghi chú "Phân cấp cho :" trong mỗi thành phần, đó là đòi hỏi bắt buộc về phân cấp cho mỗi thành phần.

6.2.1 Nhấn mạnh các thay đổi thành phần

Mối quan hệ giữa các thành phần trong một họ được nhấn mạnh qua việc sử dụng **in đậm**. Cách in đậm này dùng cho in đậm các yêu cầu mới. Với các thành phần phân cấp, các yêu cầu được in đậm khi chúng được cải tiến hoặc sửa đổi từ các yêu cầu của thành phần trước đó. Ngoài ra, bất kỳ hoạt động được phép nào mới hoặc được cải tiến từ thành phần trước đó đều được nhấn mạnh qua sử dụng kiểu **in đậm**.

7 Lớp FAU: Kiểm toán an toàn

Kiểm toán an toàn liên quan đến việc nhận biết, ghi lại, lưu trữ và phân tích thông tin liên quan đến các hoạt động an toàn liên quan (ví dụ các hoạt động được kiểm soát bởi TSF). Các kết quả kiểm toán được ghi lại có thể được kiểm tra để quyết định các hoạt động an toàn liên quan nào cần được thực hiện và ai (người dùng nào) có trách nhiệm với nó.

Hình 7 - Phân cấp lớp FAU: Kiểm toán an toàn

7.1 Phản hồi tự động kiểm toán an toàn (FAU_ARP)

7.1.1 Hành xử của họ

Họ này định nghĩa phản hồi cần được thực hiện trong trường hợp phát hiện các sự kiện chỉ ra các khả năng phá hoại an toàn.

7.1.2 Phân mức thành phần

Tại các cảnh báo an toàn FAU_ARP.1, TSF cần thực hiện các hành động trong trường hợp có phá hoại an toàn được phát hiện.

7.1.3 Quản lý của FAU_ARP.1

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

a) Quản lý (thêm, bớt hoặc điều chỉnh) các hành động.

7.1.4 Kiểm toán FAU_ARP.1

Các hành động sau nên có khả năng kiểm toán, nếu FAU_GEN Tạo các dữ liệu kiểm toán an toàn được đặt trong PP/ST.

a) Tối thiểu: thực hiện các hành động do có các vi phạm an toàn sắp xảy ra.

7.1.5 Cảnh báo an toàn FAU_ARP.1

Phân cấp từ: không có các thành phần nào.

Các mối phụ thuộc: FAU_SAA.1 Phân tích khả năng vi phạm.

7.1.5.1 FAU_ARP.1.1

TSF cần thực hiện [chỉ định: *danh sách các hành động]* khi phát hiện một khả năng vi phạm an toàn.

7.2 Tạo các dữ liệu kiểm toán an toàn (FAU_GEN)

7.2.1 Hành xử của họ

Họ này định nghĩa các yêu cầu cho việc ghi lại sự xuất hiện của các sự kiện an toàn liên quan được thực hiện dưới kiểm soát của TSF. Họ này xác định các mức kiểm toán, liệt kê các kiểu sự kiện mà có thể kiểm toán được bởi TSF, và xác định tập nhỏ nhất của các thông tin liên quan đến kiểm toán được cung cấp bên trong nhiều kiểu hồ sơ kiểm toán.

7.2.2 Phân mức thành phần

FAU_GEN.1 Tạo dữ liệu kiểm toán, định nghĩa mức của các sự kiện có thể kiểm toán và chỉ ra danh sách dữ liệu cần được ghi lại trong mỗi bản ghi.

Tại FAU_GEN.2 Kết hợp định danh người dùng, TSF cần kết hợp các sự kiện có thể kiểm toán theo từng định danh người dùng riêng biệt.

7.2.3 Quản lý của FAU_GEN.1, FAU_GEN.2

Không có các hoạt động quản lý nào.

7.2.4 Kiểm toán của FAU_GEN1, FAU_GEN2

Không có sự kiện có thể kiểm toán nào.

7.2.5 Tạo dữ liệu kiểm toán FAU_GEN.1

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FPT_STM.1 Các nhãn thời gian tin cậy.

7.2.5.1 FAU_GEN.1.1

TSF cần có khả năng tạo ra một bản ghi kiểm toán cho các sự kiện có thể kiểm toán được sau:

a) Khởi động và tắt các chức năng kiểm toán;

b) Tất cả các sự kiện có thể kiểm toán được cho [lựa chọn, chọn một trong số: *tối thiểu, cơ bản, chi tiết, không xác định*] và

c) [chỉ định: *Các sự kiện có thể kiểm toán được định nghĩa cụ thể khác*].

7.2.5.2 FAU_GEN.1.2

TSF cần ghi lại trong mỗi bản ghi kiểm toán ít nhất các thông tin sau đây:

a) Ngày và giờ của sự kiện, kiểu sự kiện, định danh chủ thể (nếu có), và đầu ra (thành công hoặc lỗi) của sự kiện; và

b) Với mỗi kiểu sự kiện kiểm toán, dựa trên định nghĩa các sự kiện có thể kiểm toán của các thành phần chức năng có trong PP/ST, [chỉ định: *thông tin liên quan kiểm toán khác*]

7.2.6 FAU_GEN.2 Kết hợp định danh người dùng

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FAU_GEN.1 Tạo dữ liệu kiểm toán

FIA_UID.1 Định thời cho định danh

7.2.6.1 FAU_GEN.2.1

Đối với các sự kiện kiểm toán có được từ các hành động của người dùng đã định danh, TSF cần có khả năng kết hợp mỗi sự kiện có thể kiểm toán với định danh của người dùng đã gây ra sự kiện.

7.3 Phân tích kiểm toán an toàn (FAU_SAA)

7.3.1 Hành xử của họ

Họ này định nghĩa các yêu cầu cho tự động hóa, nghĩa là phân tích các hoạt động hệ thống và dữ liệu kiểm toán để tìm kiếm các phá hoại an toàn thực tế và có thể xảy ra. Phân tích này có thể thực hiện với sự hỗ trợ của phát hiện xâm nhập hoặc phản ứng tự động với một vi phạm an toàn sẽ xảy ra.

Các hành động này cần được thực hiện dựa trên phát hiện, có thể được xác định qua Họ phản ứng tự động kiểm toán an toàn (FAU_ARP).

7.3.2 Phân mức thành phần

Trong FAU_SAA.1 Phân tích khả năng vi phạm, phát hiện ngưỡng cơ sở dựa trên cơ sở của tập quy tắc được yêu cầu.

Trong FAU_SAA.2 Phát hiện bất thường dựa trên mô tả tóm tắt, TSF duy trì các mô tả riêng về sử dụng hệ thống, tại đó các mô tả biểu diễn các mẫu liên quan đến quá khứ thường được thực hiện bởi các thành viên của nhóm mô tả đích. Một nhóm mô tả đích tham chiếu đến một nhóm của một hoặc nhiều cá nhân (ví dụ một người dùng đơn, nhiều người dùng chia sẻ một nhóm ID hoặc tài khoản nhóm, nhiều người dùng vận hành dưới các vai trò được chỉ định trước, người dùng của toàn bộ hệ thống hoặc một nút mạng); đó là người tương tác với TSF. Mỗi thành viên của nhóm hồ sơ đích được chỉ định một loại nghi ngờ riêng, nó đại diện cho việc làm thế nào mà các hoạt động tương ứng hiện thời của các thành viên thực hiện thiết lập mẫu để biểu diễn trong các mô tả.

Trong FAU_SAA.3 Thử nghiệm tấn công đơn giản, TSF cần có thể phát hiện sự xuất hiện của các sự kiện với các dấu hiệu mà đại diện cho một dấu hiệu nguy cơ đến thực thi TSP. Tìm kiếm các sự kiện với các dấu hiệu này có thể xuất hiện trong thời gian thực hoặc trong thời gian phân tích chế độ xử lý mẻ (batch mode) với các thông tin được thu thập hậu kỳ (post-collection).

Trong FAU_SAA.4 Thử nghiệm tấn công phức tạp, TSF cần đại diện và phát hiện các kịch bản xâm nhập nhiều bước. TSF có thể so sánh các sự kiện hệ thống (có thể thực hiện bởi nhiều cá nhân) với các sự kiện liên tiếp được biết để đại diện cho toàn bộ các kịch bản xâm nhập. TSF cần có thể chỉ ra khi một sự kiện có dấu hiệu hoặc các sự kiện liên tiếp được tìm thấy chỉ ra khả năng vi phạm từ các SFR.

7.3.3 Quản lý của FAU_SAA.1

Các hành động sau có thể được cân nhắc cho các chức năng quản lý trong FMT :

a) Duy trì các quy tắc bởi (thêm, thay đổi, xóa) các quy tắc từ tập các quy tắc.

7.3.4 Quản lý của FAU_SAA.2

Các hành động sau có thể được cân nhắc cho các chức năng quản lý trong FMT :

a) Duy trì (Xóa, thay đổi, thêm) nhóm người dùng trong nhóm mô tả đích.

7.3.5 Quản lý của FAU_SAA.3

Các hành động sau có thể được cân nhắc cho các chức năng quản lý trong FMT :

a) Duy trì (Xóa, thay đổi, thêm) tập con của các sự kiện hệ thống.

7.3.6 Quản lý của FAU_SAA.4

Các hành động sau có thể được cân nhắc cho các chức năng quản lý trong FMT :

a) Duy trì (Xóa, thay đổi, thêm) tập con của các sự kiện hệ thống ;

b) Duy trì (Xóa, thay đổi, thêm) tập liên tiếp của các sự kiện hệ thống.

7.3.7 Kiểm toán của FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Bật hoặc tắt bất kỳ một cơ chế phân tích nào ;

b) Tối thiểu: Các phản hồi tự động được thực hiện bởi công cụ.

7.3.8 FAU_SAA.1 Phân tích khả năng phá hoại

Phân cấp từ: Không có thành phần nào.

Các mối phụ thuộc: FAU_GEN.1 Tạo dữ liệu kiểm toán.

7.3.8.1 FAU_SAA.1.1

TSF cần cung cấp một tập các quy tắc để giám sát các sự kiện đã kiểm toán và dựa trên những quy tắc này chỉ ra các khả năng phá hoại việc thực thi các SFR.

7.3.8.2 FAU_SAA.1.2

TSF cần thực thi các quy tắc sau cho việc giám sát các sự kiện đã kiểm toán:

a) **Tích lũy hoặc kết hợp của [chỉ định: tập con các sự kiện đã kiểm toán xác định trước] được biết để chỉ ra khả năng phá hoại an toàn;**

b) **[Chỉ định: bất kỳ quy tắc nào khác].**

7.3.9 FAU_SAA.2 Phát hiện bất thường dựa trên mô tả tóm tắt

Phân cấp từ: Không có thành phần nào.

Các mối phụ thuộc: FIA_UID.1 Định thời cho định danh.

7.3.9.1 FAU_SAA.2.1

TSF cần có khả năng duy trì mô tả sử dụng hệ thống, tại đó một mô tả riêng đại diện cho các mẫu quá khứ về việc sử dụng được thực hiện bởi các thành viên của [chỉ định: *Nhóm mô tả mục tiêu*].

7.3.9.2 FAU_SAA.2.2

TSF cần có khả năng duy trì một xếp hạng nghi ngờ với mỗi người dùng với các hoạt động được ghi lại trong mô tả tóm tắt, khi đó xếp hạng nghi ngờ đại điện cho mức độ mà hoạt động của người dùng hiện thời được tìm thấy không mâu thuẫn với các mẫu được thiết lập được biểu diễn trong mô tả tóm tắt.

7.3.9.3 FAU_SAA.2.3

TSF cần có khả năng chỉ ra phá hoại thực thi các SFR sẽ xảy ra khi xếp hạng nghi ngờ người dùng vượt quá các điều kiện ngưỡng cho phép [chỉ định: *các điều kiện theo đó các hoạt động bất thường được báo cáo bởi TSF*].

7.3.10 FAU_SAA.3 Thử nghiệm tấn công đơn giản

Phân cấp từ: Không có thành phần nào.

Các mối phụ thuộc: Không có phụ thuộc nào.

7.3.10.1 FAU_SAA.3.1

TSF cần có khả năng duy trì một biểu diễn nội bộ cho các sự kiện có dấu hiệu [chỉ định: *một tập con của các sự kiện hệ thống*] có thể chỉ ra sự phá hoại việc thực thi các SFR.

7.3.10.2 FAU_SAA.3.2

TSF cần có khả năng so sánh các sự kiện có dấu hiệu với các bản ghi về hoạt động của hệ thống nhận được từ việc kiểm tra của [chỉ định: *thông tin được dùng để xác định hoạt động của hệ thống*].

7.3.10.3 FAU_SAA.3.3

TSF cần có khả năng biểu thị một phá hoại tiềm năng việc thực thi các SFR khi sự kiện hệ thống trùng với một sự kiện có dấu hiệu biểu thị khả năng phá hoại tiềm năng việc thực thi các SFR.

7.3.11 AU_SAA.4 Thử nghiệm tấn công phức tạp

Phân cấp từ: FAU_SAA.3 Thử nghiệm tấn công đơn giản.

Các mối phụ thuộc: Không có phụ thuộc nào.

7.3.11.1 FAU_SAA.4.1

TSF cần có khả năng duy trì một biểu diễn nội bộ cho các **sự kiện liên tiếp của các kịch bản xâm nhập [chỉ định: *danh sách liên tiếp của các sự kiện hệ thống mà sự hiện diện của chúng là đại diện cho các kịch bản xâm nhập được biết*]** và các sự kiện có dấu hiệu **tiếp theo** [chỉ định: *một tập con của các sự kiện hệ thống*] có thể chỉ ra sự phá hoại việc thực thi các SFR.

7.3.11.2 FAU_SAA.4.2

TSF cần có khả năng so sánh các sự kiện có dấu hiệu **và chuỗi các sự kiện** với các bản ghi về hoạt động của hệ thống nhận được từ việc kiểm tra của [chỉ định: *thông tin được dùng để xác định hoạt động của hệ thống*].

7.3.11.3 FAU_SAA.4.3

TSF cần có khả năng biểu thị một phá hoại tiềm năng việc thực thi các SFR khi sự kiện hệ thống trùng với một sự kiện có dấu hiệu **hoặc chuỗi các sự kiện** biểu thị khả năng phá hoại tiềm năng việc thực thi các SFR.

7.4 Soát xét kiểm toán an toàn (FAU_SAR)

7.4.1 Hành xử của họ

Họ này định nghĩa các yêu cầu cho các công cụ kiểm toán cần phải sẵn sàng cho người dùng có thẩm quyền để hỗ trợ xem lại dữ liệu kiểm toán.

7.4.2 Phân mức thành phần

FAU_SAR.1 Soát xét kiểm toán, cung cấp khả năng đọc thông tin từ các bản ghi kiểm toán.

FAU_SAR.2 Soát xét kiểm toán có hạn chế, yêu cầu không có người dùng khác, ngoại trừ những ai đã được định danh trong soát xét kiểm toán FAU.SAR.1 có thể đọc được thông tin.

FAU_SAR.3 Soát xét kiểm toán có chọn lựa, yêu cầu các công cụ soát xét kiểm toán để lựa chọn dữ liệu kiểm toán cần được xem lại dựa trên các tiêu chí.

7.4.3 Quản lý của FAU_SAR.1

Các hành động sau có thể được cân nhắc cho các chức năng quản lý trong FMT :

a) Duy trì (Xóa, thay đổi, thêm) của nhóm các người dùng với việc đọc quyền truy nhập đến các hồ sơ kiểm toán.

7.4.4 Quản lý của FAU_SAR.2, FAU_SAR.3

Không có các hoạt động quản lý nào.

7.4.5 Kiểm toán của FAU_SAR.1

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn chứa trong PP/ST :

a) Cơ sở: đọc thông tin từ các hồ sơ kiểm toán.

7.4.6 Kiểm toán của FAU_SAR.2

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn chứa trong PP/ST:

a) Cơ sở: Số lần thử đọc tin không thành công từ các bản ghi kiểm toán.

7.4.7 Kiểm toán của FAU_SAR.3

Các hành động sau đây có thể kiểm toán được nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Chi tiết: Các tham số được sử dụng để xem lại.

7.4.8 FAU_SAR.1 Soát xét kiểm toán

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FAU_GEN.1 Tạo dữ liệu kiểm toán.

7.4.8.1 FAU_SAR.1.1

TSF cần cung cấp [chỉ định: *người dùng có thẩm quyền*] khả năng đọc [chỉ định: *danh sách của các thông tin kiểm toán*] từ các hồ sơ kiểm toán.

7.4.8.2 FAU_SAR.1.2

TSF cần cung cấp các hồ sơ kiểm toán theo cách thức phù hợp cho người dùng để giải thích thông tin.

7.4.9 FAU_SAR.2 Soát xét kiểm toán có hạn chế

Phân cấp từ: Không có thành phần nào.

Các mối phụ thuộc: FAU_SAR.1 Soát xét kiểm toán.

7.4.9.1 FAU_SAR.2.1

TSF cần ngăn cản tất cả người dùng truy cập đọc các hồ sơ kiểm toán, ngoại trừ những người dùng được cấp phép truy cập đọc rõ ràng.

7.4.10 FAU_SAR.3 Soát xét kiểm toán có chọn lựa

Phân cấp từ: Không có thành phần nào.

Các mối phụ thuộc: FAU_SAR.1 Soát xét kiểm toán.

7.4.10.1 FAU_SAR.3.1

TSF cần cung cấp khả năng áp dụng [Chỉ định: *các phương pháp chọn lựa và/hoặc sắp xếp*] các dữ liệu kiểm toán dựa trên [chỉ định: *tiêu chí với các quan hệ logic*].

7.5 Lựa chọn sự kiện kiểm toán an toàn (FAU_SEL)

7.5.1 Hành xử của họ

Họ này định nghĩa các yêu cầu để lựa chọn các sự kiện cần được kiểm toán trong thời gian hoạt động của TOE từ tập tất cả các sự kiện có thể kiểm toán.

7.5.2 Phân mức thành phần

FAU_SEL.1 Kiểm toán lựa chọn, đòi hỏi khả năng chọn ra tập các sự kiện cần được kiểm toán từ tập tất cả các sự kiện có thể kiểm toán, xác định trong FAU_GEN.1 Tạo dữ liệu kiểm toán, dựa trên các thuộc tính được chỉ ra bởi tác giả PP/ST.

7.5.3 Quản lý của FAU_SEL.1

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

a) Duy trì các quyền để xem/thay đổi các sự kiện kiểm toán

7.5.4 Kiểm toán của FAU_SEL.1

Các hành động sau có khả năng kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được chứa trong PP/ST:

a) Tối thiểu: tất cả các thay đổi đến cấu hình kiểm tra mà xuất hiện khi các chức năng thu thập kiểm toán được vận hành.

7.5.5 FAU_SEL.1 Kiểm toán lựa chọn

Phân cấp từ: không có thành phần nào.

Các mối phụ thuộc: FAU_GEN.1 Tạo dữ liệu kiểm toán
FMT_MTD.1 Quản lý dữ liệu TSF

7.5.5.1 FAU_SEL.1.1

TSF cần có khả nằn chọn ra tập các sự kiện đã kiểm toán từ tập tất cả các sự kiện có thể kiểm toán, dựa trên các thuộc tính sau đây:

a) **[lựa chọn: *định danh đối tượng, định danh người dùng, định danh chủ thể, định danh máy chủ, kiểu sự kiện*]**

b) **[chỉ định: *danh sách các thuộc tính bổ sung mà việc lựa chọn kiểm toán dựa theo*]**

7.6 Lưu trữ sự kiện kiểm toán an toàn (FAU_STG)

7.6.1 Hành xử của họ

Họ này định nghĩa các yêu cầu cho TSF để có thể tạo ra và duy trì một dấu vết kiểm toán an toàn. Các bản ghi kiểm toán đã lưu tham chiếu đến các bản ghi có trong dấu vết kiểm toán, và không phải là các bản ghi kiểm toán đã gọi ra (vào bộ nhớ tạm thời) thông qua lựa chọn.

7.6.2 Phân mức thành phần

Tại FAU_STG.1 Lưu trữ các vết kiểm toán có bảo vệ, các yêu cầu được đặt trong vết kiểm toán. Nó sẽ được bảo vệ chống lại việc xóa hay thay đổi trái phép.

FAU_STG.2 Đảm bảo sự sẵn sàng của dữ liệu kiểm toán, xác định các đảm bảo mà TSF duy trì trên dữ liệu kiểm toán được đưa ra trong sự xuất hiện một điều kiện không mong muốn.

FAU_STG.3 Hành động trong trường hợp có thể mất mát dữ liệu kiểm toán, xác định các hành động cần thực hiện nếu ngưỡng trong vết an toàn bị vượt quá.

FAU_STG.4 Ngăn chặn mất mát dữ liệu kiểm toán, xác định các hành động cần thực hiện trong trường hợp vết kiểm toán bị đầy.

7.6.3 Quản lý của FAU_STG.1

Không có các hoạt động quản lý nào.

7.6.4 Quản lý của FAU_STG.2

Các hành động sau có thể được cân nhắc cho các chức năng quản lý trong FMT :

a) Duy trì các tham số kiểm soát khả năng lưu trữ kiểm toán.

7.6.5 Quản lý của FAU_STG.3

Các hành động sau cần xem xét cho các chức năng quản lý trong FMT:

a) Duy trì ngưỡng ;

b) Duy trì (xóa, thay đổi, thêm) các hành động cần được thực hiện trong trường hợp lỗi lưu trữ kiểm toán sẽ xảy ra.

7.6.6 Quản lý của FAU_STG.4

Các hành động sau có thể được cân nhắc cho các chức năng quản lý trong FMT :

a) Duy trì (xóa, thay đổi, thêm) các hành động cần được thực hiện trong trường hợp có lỗi lưu trữ kiểm toán.

7.6.7 Kiểm toán của FAU_STG.1, FAU_STG.2

Không có các sự kiện có thể kiểm toán nào.

7.6.8 Kiểm toán của FAU_STG.3

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Cơ sở: Các hành động thực hiện do bị vượt quá ngưỡng.

7.6.9 Kiểm toán của FAU_STG.4

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Cơ sở: Các hành động thực hiện do lỗi lưu trữ kiểm toán.

7.6.10 FAU_STG.1 Lưu trữ vết kiểm toán có bảo vệ

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FAU_GEN.1 Tạo dữ liệu kiểm toán.

7.6.10.1 FAU_STG.1.1

TSF cần bảo vệ các hồ sơ kiểm toán đã lưu trong vết kiểm toán chống lại việc xóa trái phép.

7.6.10.2 FAU_STG.1.2

TSF cần có khả năng [lựa chọn, chọn một trong số: *ngăn chặn, phát hiện*] các thay đổi trái phép vào các bản ghi kiểm toán đã lưu trữ trong vết kiểm toán.

7.6.11 FAU_STG.2 Đảm bảo sự sẵn sàng của dữ liệu kiểm toán

Phân cấp từ: FAU_STG.1 Lưu trữ vết an toàn có bảo vệ

Các mối phụ thuộc: FAU_GEN.1 Tạo dữ liệu kiểm toán

7.6.11.1 FAU_STG.2.1

TSF cần bảo vệ các hồ sơ kiểm toán đã lưu trong vết kiểm toán chống lại việc xóa trái phép.

7.6.11.2 FAU_STG.2.2

TSF cần có khả năng [lựa chọn, chọn một trong số: *ngăn chặn, phát hiện*] các thay đổi trái phép vào các bản ghi kiểm toán đã lưu trữ trong vết kiểm toán.

7.6.11.3 FAU_STG.2.3

TSF cần đảm bảo rằng [chỉ định: đơn vị đo việc lưu trữ hồ sơ kiểm toán] các hồ sơ kiểm tra sẽ được duy trì khi các hành động sau xuất hiện: [lựa chọn: tràn bộ nhớ lưu kiểm toán, lỗi, tấn công].

7.6.12 FAU_STG.3 Hành động trong trường hợp dữ liệu kiểm toán có thể bị mất

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FAU_STG.1 Lưu trữ vết an toàn có bảo vệ

7.6.12.1 FAU_STG.3.1

TSF cần [chỉ định: *các hành động cần được thực hiện trong trường hợp lỗi lưu trữ an toàn có thể xảy ra*] nếu vết kiểm toán vượt quá [chỉ định: *giới hạn được định nghĩa trước*]

7.6.13 FAU_STG.4 Ngăn chặn mất dữ liệu kiểm toán

Phân cấp từ: FAU_STG.3 Hành động trong trường hợp dữ liệu kiểm toán có thể bị mất.

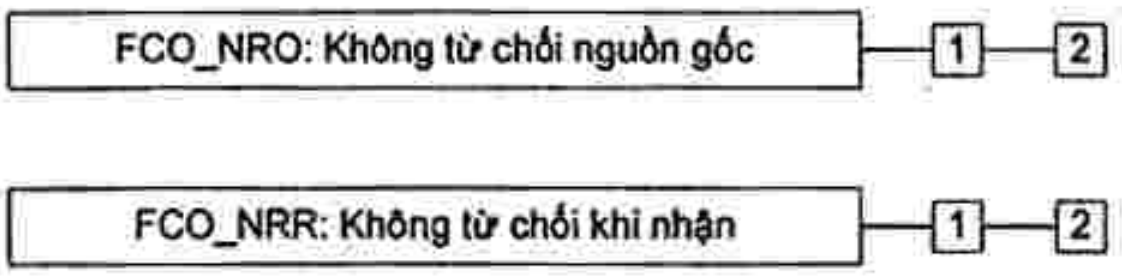
Các mối phụ thuộc: FAU_STG.1 Lưu trữ vết an toàn có bảo vệ

7.6.13.1 FAU_STG.4.1

TSF cần **[lựa chọn, chọn một trong số: *"Lờ đi các sự kiện đã kiểm toán", "ngăn chặn các sự kiện đã kiểm toán, ngoại trừ các sự kiện này được lấy ra bởi người dùng có thẩm quyền với các quyền đặc biệt", "Viết đè lên hồ sơ kiểm toán lưu trữ lâu nhất"*]** và [chỉ định: ***các hành động khác*** *trong trường hợp lỗi lưu trữ kiểm toán*] nếu vết kiểm toán đầy.

8 Lớp FCO: Truyền thông

Lớp này quy định hai họ liên quan đặc biệt đến việc đảm bảo danh tính của phần tử tham gia trong trao đổi dữ liệu. Các họ này liên quan đến việc đảm bảo danh tính người tạo ra thông tin đã truyền đi (kiểm chứng thông tin) và đảm bảo danh tính người nhận các thông tin đã truyền đi (kiểm chứng người nhận). Các họ này đảm bảo rằng người tạo ra thông tin không thể từ chối việc gửi đi các thông điệp hoặc người nhận từ chối việc đã nhận nó.



Hình 8 - phân cấp lớp FCO: Truyền thông

8.1 Không chối bỏ nguồn gốc (FCO_NRO)

8.1.1 Hành xử của họ

Không chối bỏ nguồn gốc đảm bảo rằng nguồn gốc của thông tin không thể từ chối việc đã gửi tin đi. Họ này yêu cầu TSF quy định một phương pháp để đảm bảo rằng chủ thể đã nhận thông tin qua quá trình trao đổi dữ liệu được cung cấp một bằng chứng về nguồn gốc thông tin. Bằng chứng này có thể được thẩm định hoặc qua chủ thể này hoặc các chủ thể khác.

8.1.2 Phân mức thành phần

FCO_NRO.1 Lựa chọn kiểm chứng nguồn gốc, đòi hỏi TSF quy định các chủ thể với khả năng yêu cầu chứng cứ về nguồn gốc của thông tin.

FCO_NRO.2 Thực thi kiểm chứng nguồn gốc thông tin, đòi hỏi TSF luôn tạo ra chứng cứ về nguồn gốc của thông tin được truyền

8.1.3 Quản lý của FCO_NRO.1, FCO_NRO.2

Các hành động sau được xem xét cho các chức năng quản lý FMT

a) Quản lý các thay đổi kiểu thông tin, lĩnh vực, các thuộc tính của người tạo ra thông tin và người nhận chứng cứ

8.1.4 Kiểm toán của FCO_NRO.1

Các hành động sau đây cần được kiểm tra nếu FAU_GEN Tạo dữ liệu kiểm tra được đặt trong PP/ST

a) Tối thiểu: Xác định người dùng mà yêu cầu chứng chứ về nguồn gốc được tạo ra

b) Tối thiểu: Viện chứng đến dịch vụ không thể từ chối

c) Cơ sở: Định danh thông tin, đích và một bản sao của chứng cứ được quy định

d) Chi tiết: Xác định người dùng mà đòi hỏi thẩm tra chứng cứ

8.1.5 Kiểm toán của FCO_NRO.2

Các hành động sau đây cần được kiểm tra nếu FAU_GEN Tạo dữ liệu kiểm tra được đặt trong PP/ST

d) Tối thiểu: Viện chứng đến dịch vụ không thể từ chối

e) Cơ sở: Định danh thông tin, đích và một bản sao của chứng cứ được quy định

f) Chi tiết: Xác định người dùng mà đòi hỏi thẩm tra chứng cứ

8.1.6 FCO_NRO.1 Lựa chọn kiểm chứng nguồn gốc

Phân cấp từ: Không có thành phần nào.

Các mối phụ thuộc: FIA_UID.1 Định thời cho định danh

8.1.6.1 FCO_NRO.1.1

TSF cần có khả năng tạo ra chứng cứ về nguồn gốc thông tin được truyền [chỉ định: *danh sách kiểu thông tin*] tại yêu cầu của [chỉ định: *bên gửi, bên nhận, [chỉ định: danh sách các đối tác thứ 3]*].

8.1.6.2 FCO_NRO.1.2

TSF cần có khả năng liên quan đến [chỉ định: *danh sách các thuộc tính*] người tạo ra thông tin và [chỉ định: *danh sách các trường thông tin*] của thông tin được cung cấp chứng cứ.

8.1.6.3 FCO_NRO.1.3

TSF cần cung cấp khả năng thẩm tra chứng cứ về nguồn gốc của thông tin [lựa chọn: *bên gửi,, người nhận, [chỉ định: danh sách của đối tác thứ 3]*] được cho [chỉ định: *các giới hạn về chứng cứ của nguồn gốc*].

8.1.7 FCO_NRO.2 Thực thi kiểm chứng nguồn gốc

Phân cấp từ: FCO_NRO.1 Lựa chọn kiểm chứng nguồn gốc

Các mối phụ thuộc: FIA_UID.1 Định thời cho định danh

8.1.7.1 FCO_NRO.2.1

TSF cần **thực thi để tạo ra các chứng cứ** về nguồn gốc thông tin được truyền [chỉ định: *danh sách của các kiểu thông tin*] tại tất cả các thời gian.

8.1.7.2 FCO_NRO.2.2

TSF cần có khả năng liên quan đến [chỉ định: *danh sách các thuộc tính*] người tạo ra thông tin và [chỉ định: *danh sách các trường thông tin*] của thông tin được cung cấp chứng cứ.

8.1.7.3 FCO_NRO.2.3

TSF cần cung cấp khả năng thẩm tra chứng cứ về nguồn gốc của thông tin [lựa chọn: *bên gửi,, người nhận, [chỉ định: danh sách của đối tác thứ 3]*] được cho [chỉ định: *các giới hạn về chứng cứ của nguồn gốc*].

8.2 Không thể từ chối của bên nhận (FCO_NRR)

8.2.1 Hành xử của họ

Không thể từ chối của bên nhận đảm bảo rằng người nhận thông tin không thể từ chối việc nhận thành công thông tin. Họ này đòi hỏi, TSF cung cấp một phương pháp để đảm bảo rằng một chủ thể truyền thông tin trong thời gian trao đổi dữ liệu được cung cấp một chứng cứ về việc nhận thông tin. Chứng cứ này có thể được thẩm tra bởi chủ thể này hoặc các chủ thể khác.

8.2.2 Phân mức thành phần

FCO_NRR.1 Lựa chọn kiểm chứng bên nhận, yêu cầu TSF để cung cấp cho chủ thể khả năng đòi hỏi chứng cứ của việc nhận thông tin.

FCO_NRR.2 Thực thi kiểm chứng bên nhận, đòi hỏi TSF luôn tạo ra chứng cứ nhận cho các thông tin đã nhận.

8.2.3 Quản lý của FCO_NRR.1, FCO_NRR.2

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

a) Quản lý các thay đổi về kiểu thông tin, trường tin, các thuộc tính của người gửi và người nhận là đối tác thứ 3 về chứng cứ.

8.2.4 Kiểm toán của FCO_NRR.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: Xác định người dùng mà đòi hỏi chứng cứ của việc nhận sẽ được tạo ra.

b) Tối thiểu: Viện chứng dịch vụ không thể từ chối.

c) Cơ sở: Định danh thông tin, đích đến và một bản sao của thông tin được quy định.

d) Chi tiết: Xác định người dùng mà đòi hỏi việc thẩm tra chứng cứ.

8.2.5 Kiểm toán của FCO_NRR.2

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán được đặt trong PP/ST:

a) Tối thiểu: Viện chứng dịch vụ không thể từ chối.

b) Cơ sở: Định danh thông tin, đích đến và một bản sao của thông tin được quy định.

c) Chi tiết: Xác định người dùng mà đòi hỏi việc thẩm tra chứng cứ.

8.2.6 FCO_NRR.1 Lựa chọn kiểm chứng bên nhận

Phân cấp từ: Không có thành phần nào.

Các mối phụ thuộc: FIA_UID.1 Định thời cho định danh.

8.2.6.1 FCO_NRR.1.1

TSF cần có khả năng tạo ra chứng cứ nhận tin cho [chỉ định: *danh sách của các kiểu thông tin*] đã nhận theo các đòi hỏi của [lựa chọn: *người gửi, người nhận, [chỉ định: danh sách các đối tác thứ ba]*].

8.2.6.2 FCO_NRR.1.2

TSF cần có khả năng kết nối các [chỉ định: *danh sách các thuộc tính*] của người nhận thông tin, và [chỉ định: *danh sách của các trường thông tin*] của thông tin cho áp dụng các chứng cứ.

8.2.6.3 FCO_NRR.1.3

TSF cần cung cấp khả năng thẩm tra chứng cứ nhận thông tin tới [lựa chọn: *người gửi, người nhận, [chỉ định: danh sách của đối tác thứ ba]*] dựa trên [chỉ định: *các giới hạn trong chứng cứ của việc nhận*].

8.2.7 FCO_NRR.2 Thực thi kiểm chứng bên nhận

Phân cấp từ: FCO_NRR.1 lựa chọn kiểm chứng bên nhận.

Các mối phụ thuộc: FIA_UID.1 Định thời cho định danh.

8.2.7.1 FCO_NRR.2.1

TSF cần **thực thi việc tạo chứng cứ** nhận thông tin cho [chỉ định: *danh sách các kiểu thông tin*] đã nhận **tại mọi thời điểm**.

8.2.7.2 FCO_NRR.2.2

TSF cần có khả năng kết nối các [chỉ định: *danh sách các thuộc tính*] của người nhận thông tin, và [chỉ định: *danh sách của các trường thông tin*] của thông tin cho áp dụng các chứng cứ.

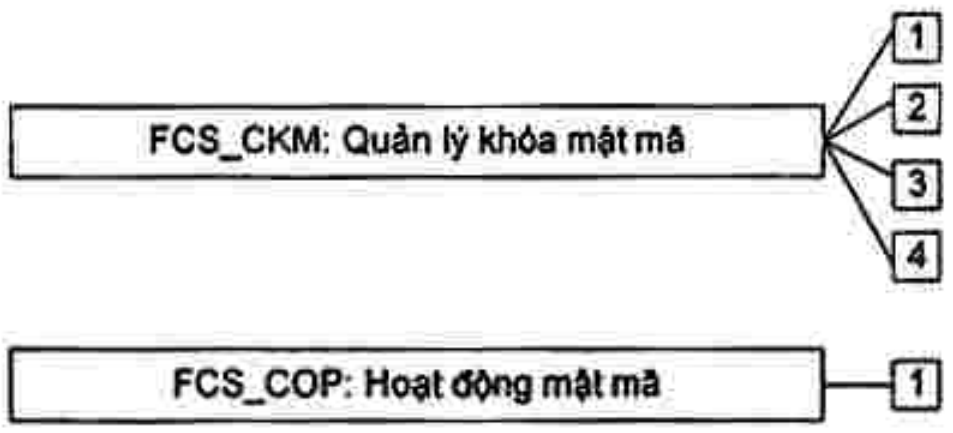
8.2.7.3 FCO_NRR.2.3

TSF cần cung cấp khả năng thẩm tra chứng cứ nhận thông tin tới [lựa chọn: *người gửi, người nhận, [chỉ định: danh sách của đối tác thứ ba]*] dựa trên [chỉ định: *các giới hạn trong chứng cứ của việc nhận*].

9 Class FCS: Hỗ trợ mật mã

TSF có thể triển khai các chức năng mã hóa để giúp thỏa mãn một số mục tiêu an toàn mức cao. Chúng bao gồm (nhưng không giới hạn): định danh và xác thực, không thể từ chối, đường dẫn tin cậy, kênh tin cậy và phân tách dữ liệu. Lớp này được sử dụng khi TOE thực hiện các chức năng mã hóa, việc thực hiện này có thể dưới dạng phần cứng, phần sụn hoặc phần mềm.

FCS: Lớp hỗ trợ mật mã được tạo dưới hai họ: Quản lý khóa mật mã (FCS_CKM) và vận hành mật mã (FCS_COP). Hộ Quản lý khóa mật mã (FCS_CKM) đề cập đến các khía cạnh quản lý của các khóa mật mã, trong khi họ vận hành mật mã (FCS_COP) lại quan tâm đến việc sử dụng vận hành của các khóa mã này.



Hình 9 – Phân cấp lớp FCS: Hỗ trợ mật mã

9.1 Quản lý khóa mật mã (FCS_CKM)

9.1.1 Hành xử của họ

Các khóa mật mã phải được quản lý trong suốt chu trình tồn tại chúng. Họ này dùng để hỗ trợ chu trình này và định nghĩa các yêu cầu đối với các hoạt động sau : Tạo khóa mật mã, phân bố khóa mật mã, truy nhập khóa mật mã và hủy bỏ khóa mật mã. Họ này nên được đưa vào mỗi khi có các yêu cầu chức năng quản lý mã khóa mật mã.

9.1.2 Phân mức thành phần

FCS_CKM.1 Tạo khóa mật mã, đòi hỏi khóa mật mã được tạo ra phù hợp với một thuật toán riêng với kích thước khóa có thể dựa trên một tiêu chuẩn được ấn định

FCS_CKM.2 Phân phối khóa mật mã, đòi hỏi các khóa mật mã được phân phối phù hợp với một phương pháp phân phối riêng mà có thể dựa trên một tiêu chuẩn được ấn định

FCS_CKM.3 Truy nhập khóa mật mã, đòi hỏi truy nhập đến các khóa mã phải được thực hiện phù hợp với một phương pháp truy nhập riêng mà có thể dựa trên tiêu chuẩn được ấn định.

FCS_CKM.4 Hủy bỏ khóa mật mã, đòi hỏi các khóa hóa bị hủy bỏ phù hợp với phương pháp hủy bỏ riêng mà có thể dựa trên tiêu chuẩn được ấn định

9.1.3 Quản lý của FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4

Không có các hoạt động quản lý nào.

9.1.4 Kiểm toán của FCS_CKM FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4

Các hành động sau có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm tra an toàn được đặt trong PP/ST :

a) Tối thiểu: thành công và lỗi của các hoạt động.

b) Cơ sở: Các thuộc tính của đối tượng, và giá trị của đối tượng ngoại trừ bất kỳ thông tin nhạy cảm nào (ví dụ khóa bí mật hoặc khóa riêng).

9.1.5 FCS_CKM.1 Tạo khóa mật mã

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: [FCS_CKM.2 Phân phối khóa mật mã hoặc

FCS_COP.1 Hoạt động mật mã]

FCS_CKM.4 Hủy bỏ khóa mật mã

9.1.5.1 FCS_CKM.1.1

TSF cần tạo ra các khóa mật mã phù hợp với các thuật toán tạo khóa mật mã được chỉ ra [chỉ định: *thuật toán tạo khóa mật mã*] và chỉ ra các kích thước khóa được mật mã [chỉ định: *kích thước khóa mật mã*] mà đáp ứng theo [chỉ định: *danh sách các tiêu chuẩn*].

9.1.6 FCS_CKM.2 Phân phối khóa mật mã

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: [FDP_ITC.1 Nhập vào dữ liệu người dùng không có các thuộc tính an toàn, hoặc

FDP_ITC.2 Nhập vào dữ liệu người dùng có các thuộc tính an toàn, hoặc

FCS_CKM..1 Tạo khóa mật mã]

FCS_CKM.4 Hủy bỏ khóa mật mã

9.1.6.1 FCS_CKM.2.1

TSF cần phân phối các khóa mật mã phù hợp với phương pháp phân phối khóa mật mã được chỉ ra [chỉ định: *phương pháp phân phối khóa mật mã*] mà đáp ứng theo [chỉ định: *danh sách các tiêu chuẩn*].

9.1.7 FCS_CKM.3 Truy nhập khóa mật mã

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: [FDP_ITC.1 Nhập vào dữ liệu người dùng không có các thuộc tính an toàn, hoặc

FDP_ITC.2 Nhập vào dữ liệu người dùng có các thuộc tính an toàn, hoặc

FCS_CKM.1 Tạo khóa mật mã]

FCS_CKM.4 Hủy bỏ khóa mật mã

9.1.7.1 FCS_CKM.3.1

TSF cần thực hiện [chỉ định: *kiểu truy nhập khóa mật mã*] phù hợp với phương pháp truy nhập khóa mật mã được chỉ ra [chỉ định: *phương pháp truy cập khóa mật mã*] đáp ứng theo [chỉ định: *danh sách các tiêu chuẩn*].

9.1.8 FCS_CKM.4 Hủy bỏ khóa mật mã

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: [FDP_ITC.1 Nhập vào dữ liệu người dùng không có các thuộc tính an toàn, hoặc

FDP_ITC.2 Nhập vào dữ liệu người dùng có các thuộc tính an toàn, hoặc

FCS_CKM.1 Tạo khóa mật mã]

9.1.8.1 FCS_CMK.4.1

TSF cần hủy bỏ các khóa mật mã phù hợp với phương pháp hủy khóa mật mã được chỉ ra [chỉ định: *phương pháp hủy bỏ khóa mật mã*] đáp ứng theo: [chỉ định: *danh sách các tiêu chuẩn*].

9.2 Hoạt động mật mã (FCS_COP)

9.2.1 Hành xử của họ

Theo yêu cầu cho hoạt động mật mã vận hành chính xác, hoạt động này cần phải được thực hiện phù hợp với một thuật toán được chỉ ra và với một khóa mật mã có kích thước được chỉ ra. Họ này chứa các yêu cầu cho các hoạt động mật mã được thực hiện.

Kiểu các hoạt động mật mã gồm mã hóa và giải mã dữ liệu, tạo chữ ký điện tử và thẩm tra, tạo kiểm tra chẵn lẻ mật mã để đảm bảo toàn vẹn và thẩm tra kiểm tra chẵn lẻ, băm an toàn (liệt kê thông điệp), mã hóa và giải mã khóa mật mã, thỏa thuận khóa mật mã.

9.2.2 Phân mức thành phần

FCS_COP.1 hoạt động mật mã, đòi hỏi một hoạt động mật mã được thực hiện phù hợp với một thuật toán được chỉ ra và với một khóa mật mã có kích thước được chỉ ra. Thuật toán được chỉ ra và các kích thước khóa mật mã có thể dựa trên một tiêu chuẩn được ấn định.

9.2.3 Quản lý của FCS_COP.1

Không có các hoạt động quản lý nào.

9.2.4 Kiểm toán của FCS_COP.1

Các hành động sau có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: thành công và lỗi, và kiểu của các hoạt động mật mã.

b) Cơ sở: Bất kỳ một chế độ mật mã được ứng dụng nào của hoạt động, các thuộc tính của chủ thể và các thuộc tính đối tượng.

9.2.5 FCS_COP.1 Hoạt động mật mã

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: [FDP_ITC.1 Nhập vào dữ liệu người dùng không có các thuộc tính an toàn, hoặc

FDP_ITC.2 Nhập vào dữ liệu người dùng có các thuộc tính an toàn, hoặc

FCS_CKM.1 Tạo khóa mật mã]

FCS_CKM.4 Hủy bỏ khóa mật mã

9.2.5.1 FCS_COP.1.1

TSF cần thực hiện [chỉ định: *danh sách các hoạt động mật mã*] phù hợp với thuật toán mật mã được chỉ ra [chỉ định: *thuật toán mật mã*] và kích thước khóa mật mã [chỉ định: *kích thước khóa mật mã*] mà đáp ứng theo [chỉ định: *danh sách các tiêu chuẩn*].

10 Lớp FDP: Bảo vệ dữ liệu người dùng

Lớp này chứa các họ chỉ ra các yêu cầu cho các chức năng an toàn TOE và các chính sách chức năng an toàn TOE liên quan đến bảo vệ dữ liệu người dùng. FDP: bảo vệ dữ liệu người dùng được chia thành bốn nhóm thuộc của các họ (được liệt kê bên dưới) mà đề cập đến dữ liệu người dùng bên trong một TOE, trong thời gian nhập, xuất và lưu trữ cũng như các thuộc tính an toàn trực tiếp liên quan đến dữ liệu người dùng.

Các họ trong lớp này được tổ chức thành bốn nhóm sau:

a) Các chính sách chức năng an toàn bảo vệ dữ liệu người dùng:

- Chính sách kiểm soát truy nhập (FDP_ACC); và
- Chính sách kiểm soát luồng thông tin (FDP_IFC)

Các thành phần trong những họ này cho phép tác giả PP/ST đặt tên cho các chính sách chức năng an toàn bảo vệ dữ liệu người dùng và định nghĩa phạm vi kiểm soát của chính sách, sự cần thiết để đề cập đến các mục tiêu an toàn. Tên của các chính sách này có nghĩa được sử dụng liên tục phần còn lại của các thành phần chức năng mà có một hoạt động gọi phép ấn định hoặc lựa chọn "kiểm soát truy nhập SFP" hoặc "kiểm soát luồng thông tin SFPs". Các quy tắc định nghĩa chức năng kiểm soát truy nhập và kiểm soát luồng thông tin SFP sẽ được định nghĩa trong các họ (một cách lần lượt) các hàm kiểm soát truy nhập (FDP_ACF) và các hàm kiểm soát luồng thông tin (FDP_IF) (tương ứng).

b) Các dạng bảo vệ dữ liệu người dùng:

- Các chức năng kiểm soát truy nhập (FDP_ACF)
- Các chức kiểm soát luồng thông tin (FDP_IFF);
- Vận chuyển nội bộ TOE (FDP_ITT);
- Bảo vệ thông tin còn dư thừa (FDP_RIP)
- Khôi phục lại (FDP_ROL) và
- Toàn vẹn dữ liệu đã lưu trữ (FDP_SDI)

c) Lưu trữ ngoại tuyến, nhập và xuất

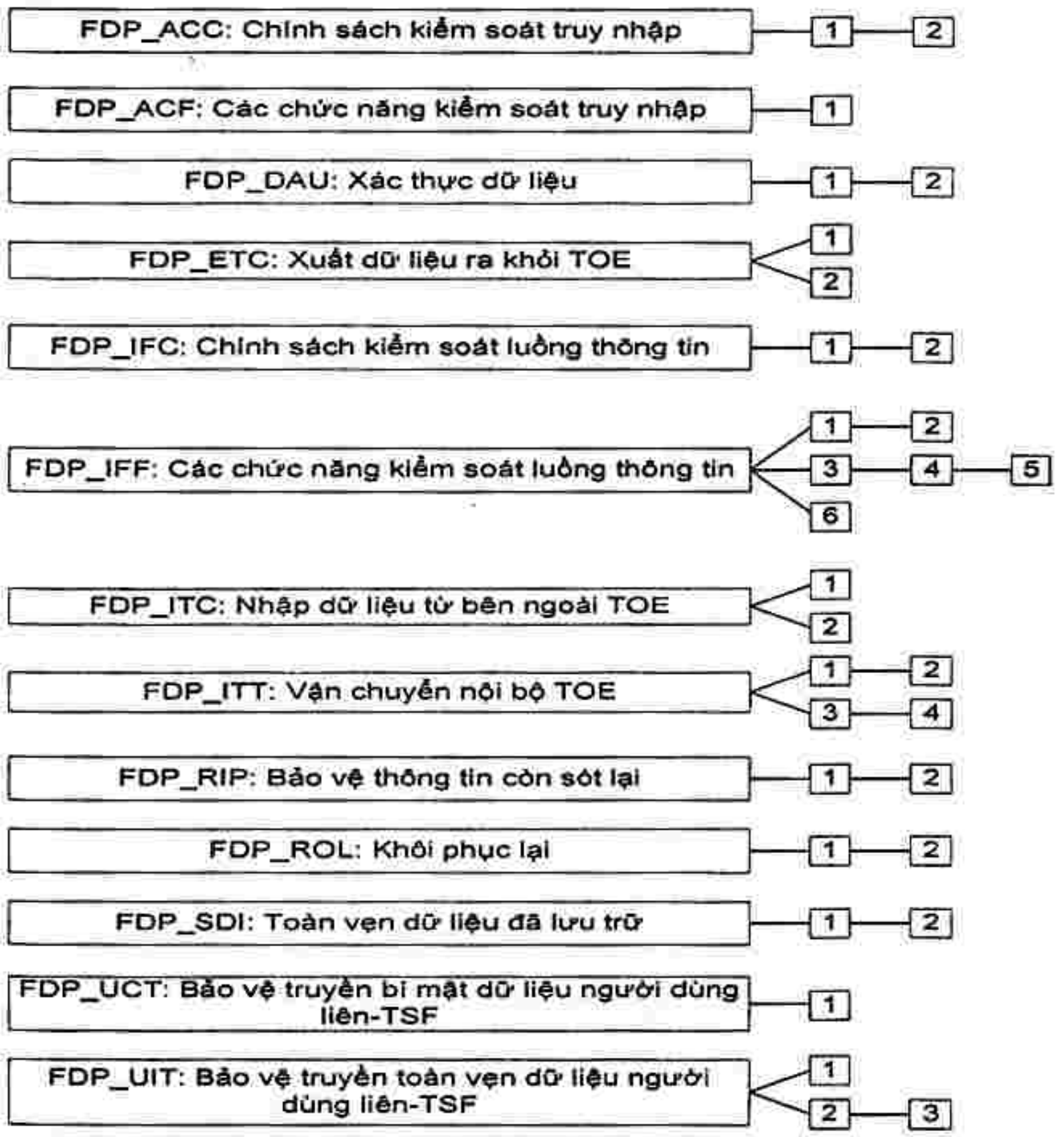
- Xác thực dữ liệu (FDP_DAU)
- Xuất dữ liệu ra khỏi TOE (FDP_ETC)
- Nhập dữ liệu từ ngoài TOE (FDP_ITC)

Các thành phần trong các họ này đề cập chuyển đổi các giá trị đáng tin cậy vào trong hoặc ra ngoài của TOE.

d) Truyền thông Liên-TSF

- Bảo vệ truyền bí mật dữ liệu người dùng liên-TSF (FDP_UCT); và
- Bảo vệ truyền toàn vẹn dữ liệu người dùng liên-TSF (FDP_UIT)

Các thành phần trong các họ này đề cập đến sự truyền thông giữa TSF của TOE và các sản phẩm IT được tin cậy khác.



Hình 10 - Phân cấp lớp FDP: Bảo vệ dữ liệu người dùng

10.1 Chính sách kiểm soát truy nhập (FDP_ACC)

10.1.1 Hành xử của họ

Họ này xác định các SFP kiểm soát truy nhập (Theo tên) và định nghĩa phạm vi kiểm soát của các chính sách mà định dạng việc xác định phần kiểm soát truy nhập của TSP. Phạm vi kiểm soát này được mô tả bởi 3 tập: Các chủ thể dưới kiểm soát của chính sách, các đối tượng dưới kiểm soát của chính sách và các hoạt động giữa các chủ thể được kiểm soát và đối tượng được kiểm soát mà được bao trùm bởi chính sách. Tiêu chí này cho phép tồn tại nhiều chính sách, mỗi cái có một tên duy nhất.

Điều này đạt được bởi các thành phần khởi tạo từ họ này một lần cho mỗi chính sách kiểm soát truy nhập được đặt tên. Quy tắc này định nghĩa chức năng của kiểm soát truy nhập SFP mà sẽ được định nghĩa bởi các họ khác như các chức năng kiểm soát truy nhập (FDP_ACF) và toàn vẹn dữ liệu lưu trữ (FDP_SDI). Các tên của các kiểm soát truy nhập được xác định ở đây trong chính sách kiểm soát truy nhập (FDP_ACC) có nghĩa là được sử dụng liên tục phần còn lại của các thành phần chức năng mà có một hoạt động gọi phép ấn định hoặc phép chọn của "kiểm soát truy nhập SFP".

10.1.2 Phân mức thành phần

FDP_ACC.1 kiểm soát truy nhập tập con, đòi hỏi mỗi cái chỉ ra kiểm soát truy nhập SFP được đặt trong một tập con của các hoạt động có thể trong một tập con của các đối tượng trong TOE.

FDP_ACC.2 Kiểm soát truy nhập toàn bộ, đòi hỏi mỗi cái chỉ ra kiểm soát truy nhập SFP bao trùm tất cả các hoạt động của chủ thể và đối tượng được bao trùm bởi SFP. Nếu các yêu cầu thêm mà tất cả các đối tượng và hoạt động với TSC được bao trùm bởi ít nhất một kiểm soát truy nhập SFP được chỉ ra

10.1.3 Quản lý của FDP_ACC.1, FDP_ACC.2

Không có các hoạt động quản lý nào.

10.1.4 Kiểm toán của FDP_ACC.1, FDP_ACC.2

Không có sự kiện có thể kiểm toán nào.

10.1.5 FDP_ACC.1 Kiểm soát truy nhập tập con

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FDP_ACF.1 Kiểm soát truy nhập dựa trên các thuộc tính an toàn.

10.1.5.1 FDP_ACC.1.1

TSF cần thực thi [chỉ định: *Kiểm soát truy nhập SFP*] trong [chỉ định: *danh sách các chủ thể, đối tượng, và các hoạt động giữa các chủ thể và đối tượng bao trùm bởi SFP*]

10.1.6 FDP_ACC.2 Kiểm soát truy nhập toàn bộ

Phân cấp từ: FDP_ACC.1 Kiểm soát truy nhập tập con.

Các mối phụ thuộc: FDP_ACF.1 Kiểm soát truy nhập dựa trên các thuộc tính an toàn.

10.1.6.1 FDP_ACC.2.1

TSF cần thực thi [chỉ định: *Kiểm soát truy nhập SFP*] trong [chỉ định: *danh sách các chủ thể, đối tượng, và tất cả các hoạt động giữa các chủ thể và đối tượng bao trùm bởi SFP*]

10.1.6.2 FDP_ACC.2.2

TSF cần đảm bảo rằng tất cả các hoạt động giữa bất kỳ chủ thể nào trong TSC và bất kỳ đối tượng nào bên trong TSC được bao trùm bởi một kiểm soát truy nhập SFP.

10.2 Các chức năng kiểm soát truy nhập (FDP_ACF)

10.2.1 Hành xử của họ

Họ này mô tả các quy tắc cho các chức năng riêng mà có thể thực hiện chính sách kiểm soát truy nhập được đặt tên là chính sách kiểm soát truy nhập (FDP_ACC). Chính sách kiểm soát truy nhập (FDP_ACC) chỉ ra phạm vi kiểm soát của chính sách

10.2.2 Phân mức thành phần

Họ này đề cập đến các thuộc tính an toàn thông thường và đặc điểm của các chính sách. Thành phần trong họ này có nghĩa là cần được sử dụng để mô tả các quy tắc cho chức năng mà thực hiện SFP như được chỉ ra trong chính sách kiểm soát truy nhập (FDP_ACC). Tác giả PP/ST có thể lặp lại thành phần này để đề cập đến nhiều chính sách trong TOE.

FDP_ACF.1 Thuộc tính an toàn dựa trên kiểm soát truy nhập, thuộc tính an toàn dựa trên kiểm soát truy nhập cho phép TSF thực thi truy nhập dựa trên các thuộc tính an toàn và nhóm các thuộc tính được đặt tên. Thêm vào đó, TSF có thể có khả năng cấp phép hoặc từ chối truy nhập với đối tượng dựa trên các thuộc tính an toàn.

10.2.3 Quản lý của FDP_ACF.1

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

a) Quản lý các thuộc tính sử dụng để đưa ra quyết định cho phép hoặc từ chối truy nhập.

10.2.4 Kiểm toán của FDP_ACF.1

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm tra được đặt trong PP/ST :

a) Tối thiểu: Các yêu cầu thực hiện thành công trong vận hành một đối tượng được bao bọc bởi SFP.

b) Cơ sở: Tất cả các yêu cầu thực hiện vận hành một đối tượng được bao bọc bởi SFP.

c) Chi tiết: Các thuộc tính an toàn đặc biệt được sử dụng trong thực hiện kiểm tra truy nhập.

10.2.5 FDP_ACF.1 Kiểm soát truy nhập dựa trên thuộc tính an toàn

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FDP_ACC.1 Kiểm soát truy nhập tập con

FDP_MSA.3 Khởi tạo thuộc tính tĩnh.

10.2.5.1 FDP_ACF.1.1

TSF cần thực thi [chỉ định: *Kiểm soát truy nhập SFP*] đến các đối tượng dựa trên [chỉ định: *Danh sách các chủ thể và đối tượng được kiểm soát dưới SFP đã chỉ định, và với danh sách, các thuộc tính an toàn tương ứng SFP, hoặc các nhóm đã gắn tên của các thuộc tính an toàn tương ứng SFP*].

10.2.5.2 FDP_ACF.1.2

TSF cần thực thi các quy tắc sau để quyết định nếu một hoạt động giữa các chủ thể được kiểm soát và các đối tượng được kiểm soát cho phép: [chỉ định: *các quy tắc quản lý truy nhập giữa các chủ thể được kiểm soát và các đối tượng được kiểm soát sử dụng các hoạt động có kiểm soát với các đối tượng được kiểm soát*]

10.2.5.3 FDP_ACF.1.3

TSF cần cấp phép truy nhập rõ ràng cho các chù thể đến các đối tượng dựa trên các quy tắc sau: [chỉ định: *các quy tắc, dựa trên các thuộc tính an toàn, để cấp phép truy nhập rõ ràng cho các chủ thể đến các đối tượng*].

10.2.5.4 FDP_ACF.1.4

TSF cần từ chối rõ ràng truy nhập của các chủ thể đến các đối tượng dựa trên [chỉ định: *các quy tắc, dựa trên các thuộc tính an toàn, để từ chối rõ ràng truy nhập của các chủ thể đến các đối tượng*] .

10.3 Xác thực dữ liệu (FDP_DAU)

10.3.1 Hành xử của họ

Xác thực dữ liệu cho phép một thực thể chấp nhận trách nhiệp xác thực thông tin (ví dụ, các chữ ký số). Họ này cung cấp một phương pháp quy định sự đảm bảo tính hợp lệ của một đơn vị đặc biệt của dữ liệu mà có thể được sử dụng để thẩm tra nội dung thông tin giả mạo hoặc thay đổi lừa dối. Trái lại với FAU: Kiểm tra an toàn, họ này được dự định cung cấp các dữ liệu tĩnh hơn là các dữ liệu mà đang được truyền đi.

10.3.2 Phân mức thấnh phần

FDP_DAU.1 Xác thực dữ liệu cơ sở, đòi hỏi TSF có khả năng tạo một sự đảm bảo của xác thực với các nội dung thông tin của các đối tượng (ví dụ tài liệu).

FDP_DAU.2 Xác thực dữ liệu với chỉ ra người đảm bảo thêm vào các yêu cầu mà TSF có khả năng thiết lập định danh của đối tượng mà cung cấp đảm bảo xác thực.

10.3.3 Quản lý của FDP_DAU.1, FDP_DAU.2

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

a) Chỉ định hoặc thay đổi đối tượng, để có thể được cấu hình được xác thực dữ liệu đã áp dụng.

10.3.4 Kiểm toán của FDP_DAU.1

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán được đặt trong PP/ST :

a) Tối thiểu: Tạo thành công các chứng cứ có giá trị.

b) Cơ sở: Tạo không thành công các chứng cứ có giá trị.

c) Chi tiết: Định danh của chủ thể mà yêu cầu chứng cứ.

10.3.5 Kiểm toán của FDP_DAU.2

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán được đặt trong PP/ST :

a) Tối thiểu: Tạo thành công các chứng cứ có giá trị.

b) Cơ sở: Tạo không thành công các chứng cứ có giá trị.

c) Chi tiết: Định danh của chủ thể mà yêu cầu chứng cứ.

d) Chi tiết: Định danh của chủ thể tạo ra chứng cứ.

10.3.6 FDP_DAU.1 Xác thực dữ liệu cơ sở

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có phụ thuộc nào.

10.3.6.1 FDP_DAI.1.1

TSF cần cung cấp khả năng tạo chứng cứ mà có thể được sử dụng như sự đảm bảo của xác định tính hợp lệ của [chỉ định: *danh sách của các đối tượng hoặc các kiểu thông tin*].

10.3.6.2 FDP_DAU.1.2

TSF cần cung cấp [chỉ định: *danh sách của các chủ thể*] với khả năng thẩm tra chứng cứ có tính hợp lệ của các thông tin đã xác định.

10.3.7 FDP_DAU.2 Xác thực dữ liệu với định danh người đảm bảo

Phân cấp từ: FDP_DAU.1 Xác thực dữ liệu cơ sở.

Các mối phụ thuộc: FIA_UID.1 Định thời cho định danh

10.3.7.1 FDP_DAU.2.1

TSF cần cung cấp khả năng tạo chứng cứ mà có thể được sử dụng như sự đảm bảo của xác định tính hợp lệ của [chỉ định: *danh sách của các đối tượng hoặc các kiểu thông tin*].

10.3.7.2 FDP_DAU.2.2

TSF cần cung cấp [chỉ định: *danh sách của các chủ thể*] với khả năng thẩm tra chứng cứ có tính hợp lệ của các thông tin đã xác định **và định danh của người dùng đã tạo ra chứng cứ.**

10.4 Xuất dữ liệu từ TOE (FDP_ETC)

10.4.1 Hành xử của họ

Họ này định nghĩa các chức năng để xuất dữ liệu người dùng ra ngoài TOE như các thuộc tính an toàn của nó và sự bảo vệ không chỉ được bảo toàn mà còn được bỏ qua khi nó được xuất ra. Nó được quan tâm với các giới hạn trong xuất và với sự phối hợp của các các thuộc tính an toàn với dữ liệu người dùng được xuất ra.

10.4.2 Phân mức thành phần

FPD_ETC.1 xuất dữ liệu người dùng không có các thuộc tính an toàn, đòi hỏi TSF thực thi các SFP phù hợp khi xuất ra ngoài dữ liệu người dùng TSF. Dữ liệu người dùng, được xuất bởi chức năng này được xuất ra mà không có các thuộc tính an toàn kết hợp với nó.

FDP_ETC.2 Xuất dữ liệu người dùng với các thuộc tính an toàn, đòi hỏi TSF thực thi các SFP phù hợp sử dụng một chức năng chính xác và đơn nghĩa kết hợp với các thuộc tính an toàn với dữ liệu người dùng được xuất ra

10.4.3 Quản lý của FDP_ETC.1

Không có các hoạt động quản lý nào.

10.4.4 Quản lý của FDP_ETC.2

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

a) Các quy tắc kiểm soát xuất bổ sung có thể được cấu hình bởi người dùng trong một vai trò định nghĩa trước.

10.4.5 Kiểm toán của FDP_ETC.1, FDP_ETC.2

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán được đặt trong PP/ST

a) Tối thiểu: Xuất thành công thông tin.

b) Cơ sở: Tất cả các nỗ lực để xuất thông tin.

10.4.6 FDP_ETC.1 Xuất dữ liệu người dùng không có các thuộc tính an toàn

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: [FDP_ACC.1 Kiểm soát truy nhập tập con, hoặc
FDP_IFC.1 Kiểm soát luồng thông tin tập con]

10.4.6.1 FDP_ETC.1.1

TSF cần thực thi [chỉ định: *kiểm soát truy nhập SFP và/hoặc kiểm soát luồng thông tin SFP*] khi xuất dữ liệu người dùng, được kiểm soát dưới SFP, bên ngoài của TOE.

10.4.6.2 10.4.6.2 FDP_ETC.1.2

TSF cần xuất dữ liệu người dùng không có có các thuộc tính an toàn kết hợp với dữ liệu người dùng.

10.4.7 FDP_ETC.2 xuất dữ liệu người dùng với các thuộc tính an toàn

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: [FDP_ACC.1 Kiểm soát truy nhập tập con, hoặc
FDP_IFC.1 Kiểm soát luồng thông tin tập con]

10.4.7.1 FDP_ETC.2.1

TSF cần thực thi [chỉ định: *kiểm soát truy nhập SFP và/hoặc kiểm soát luồng thông tin SFP*] khi xuất dữ liệu người dùng, được kiểm soát dưới SFP, bên ngoài của TOE.

10.4.7.2 FDP_ETC.2.2

TSF cần xuất dữ liệu người dùng với các thuộc tính an toàn kết hợp với dữ liệu người dùng.

10.4.7.3 FDP_ETC.2.3

TSF cần đảm bảo rằng các thuộc tính an toàn, khi xuất ra ngoài TOE là duy nhất được kết hợp với dữ liệu người dùng được xuất ra.

10.4.7.4 FDP_ETC.2.4

TSF thực thi các quy tắc sau khi dữ liệu người dùng được xuất ra từ TOE: [Chỉ định: *các quy tắc kiểm soát dữ liệu xuất ra bổ sung*].

10.5 Chính sách kiểm soát luồng thông tin (FDP_IFC)

10.5.1 Hành xử của họ

Họ này chỉ ra kiểm soát luồng thông tin SFPs (theo tên) và định nghĩa phạm vi kiểm soát của mỗi chính sách kiểm soát luồng thông tin SFP. Phạm vi kiểm soát được biểu diễn với ba tập: Các chủ thể chịu sự kiểm soát của chính sách, thông tin dưới sự kiểm soát của chính sách và các hoạt động gây ra chuyển luồng tin có kiểm soát ra và vào chủ thể kiểm soát bao trùm bởi chính sách. Các tiêu chí cho phép nhiều chính sách tồn tại, mỗi cái có một tên duy nhất. Điều này thực hiện bằng việc lặp lại các thành phần từ họ này với mỗi chính sách kiểm soát luồng thông tin đã đặt tên. Các quy tắc định nghĩa các chức năng của kiểm soát luồng thông tin SFP sẽ được định nghĩa bởi các họ khác như các chức năng

kiểm soát luồng thông tin (FDP_IFF) và Xuất dữ liệu ra ngoài TOE (FDP_ETC). Tên của kiểm soát luồng thông tin SFP xác định chính sách kiểm soát luồng thông tin (FDP_IFC) có nghĩa là được sử dụng liên tục phần còn lại của các thành phần chức năng mà có một hoạt động gọi phép ấn định hoặc phép chọn của "kiểm soát luồng thông tin SFP"

Cơ chế TSF kiểm soát luồng tin phù hợp với chính sách kiểm soát luồng thông tin SFP. Các hoạt động mà có thể thay đổi các thuộc tính an toàn của thông tin là không được phép nói chung, do điều đó sẽ phá hoại việc kiểm soát luồng thông tin SFP. Mặc dù các hoạt động như thế sẽ được giới hạn như các trường hợp ngoại lệ để kiểm soát luồng thông tin nếu được chỉ ra rõ ràng.

10.5.2 Phân mức thành phần

FDP_IFC.1 Kiểm soát luồng thông tin tập con, đòi hỏi mỗi kiểm soát luồng thông tin được chỉ ra SFP được đặt tại vị trí cho tập con của các hoạt động có thể trong tập con của các luồng thông tin trong TOE.

FDP_ICF.2 Kiểm soát luồng thông tin đầy đủ, đòi hỏi mỗi kiểm soát luồng thông tin được xác định SFP bao trùm tất cả các hoạt động trên các chủ thể và thông tin được bao trùm bởi SFP. Nếu các yêu cầu thêm với tất cả thông tin chuyển tới và hoạt động với TSC được bao trùm bởi ít nhất bởi mọt kiểm soát luồng thông tin được xác định SFP. Trong sự kết nối với thành phần FPT_RVM.1, điều này mang lại khía cạnh "luôn viện dẫn" của giám sát tham chiếu.

10.5.3 Quản lý của FDP_IFC.1, FDP_IFC.2

Không có các hoạt động quản lý được dự báo

10.5.4 Kiểm tra của FDP_IFC.1, FDP_IFC.2

Không có các hoạt động quản lý nào.

10.5.5 FDP_IFC.1 Kiểm soát luồng thông tin tập con

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FDP_IFF.1.1 Các thuộc tính an toàn đơn giản

10.5.5.1 FDP_IFC.1.1

TSF cần thực thi [chỉ định: *kiểm soát luồng thông tin SFP*] trong [chỉ định: *danh sách của các chủ thể, thông tin, và các hoạt động mà là nguyên nhân thông tin được kiểm soát chuyển tới và từ các chủ thể được kiểm soát bao trùm bởi SFP*]

10.5.6 FDP_IFC Kiểm soát luồng thông tin đầy đủ

Phân cấp từ: FDP_IFC.1 kiểm soát luồng thông tin tập con

Các mối phụ thuộc: FDP_IFF Các thuộc tính an toàn đơn giản

10.5.6.1 FDP_IFC.2.1

TSF cần thực thi [chỉ định: *kiểm soát luồng thông SFP*] trong [chỉ định: *danh sách của các chủ thể và thông tin*] *và tất cả các hoạt động mà là nguyên nhân thông tin chuyển tới và từ các chủ thể được bao trùm bởi SFP*].

10.5.6.2 FDP_IFC.2.2

TSF cần đảm bảo rằng tất cả các hoạt động mà là nguyên nhân bất kỳ thông tin trong TSC được chuyển tới và từ chủ thể trong TSC được bao trùm bởi kiểm soát luồng thông tin SFP.

10.6 Các chức năng kiểm soát luồng thông tin (FDP_IFF)

10.6.1 Hành xử của họ

Họ này mô tả các quy tắc cho các chức năng riêng mà thực hiện kiểm soát luồng thông tin SFP được đặt tên trong chính sách kiểm soát luồng thông tin (FDP_IFC), mà cũng chỉ ra phạm vi kiểm soát của chính sách. Nó bao gồm hai kiểu yêu cầu: kiểu thứ nhất đề cập đến chức năng kiểm soát luồng thông tin và kiểu thứ hai để cập các luồng thông tin không được phép (ví dụ các kênh che dậy). Sự phân chia này tăng lên bởi vì các vấn đề liên quan đến các luồng thông tin không được phép, trong một số trường hợp nhậy cảm, nó trực giao với phần còn lại của kiểm soát luồng thông tin SFP. Theo tính tự nhiên chúng phá vỡ kiểm soát luồng thông tin dẫn đến phá hoại chính sách. Do đó, chúng đòi hỏi các chức năng đặc biệt trong cả việc giới hạn và ngăn chặn sự xuất hiện của chúng.

10.6.2 Phân mức thành phần

FDP_IFF.1 Các thuộc tính an toàn đơn giản, đòi hỏi các thuộc tính an toàn trên thông tin, và trong các chủ thể là nguyên nhân thông tin chuyển tới và trong các chủ thể mà hành động như là bên nhận thông tin đó. Nó chỉ ra các quy tắc này cần được thực thi bởi chức năng và mô tả các thuộc tính an toàn được lấy từ chức năng như thế nào

FDP_IFF.2 Các thuộc tính an toàn phân cấp mở rộng các yêu cầu của FDP_IFF.1 Các thuộc tính an toàn đơn giản, bằng cách đòi hỏi tất cả SFP kiểm soát luồng thông tin trong tập các SFR sử dụng các thuộc tính an toàn phân cấp tạo thành một lưới mắt cáo (như định nghĩa trong toán học). FDP_IF.2.6 được dẫn xuất từ các đặc tính của lưới mắt cáo về mặt toán học. Một lưới mắt cáo bao gồm một tập các phần tử với một mối quan hệ đặt hàng với thuộc tính đã định nnghĩa ở dòng đầu tiên ; một giới hạn dưới lớn nhất mà tại đó phần tử duy nhất trong tập lớn hơn hay bằng (trong mối quan hệ đặt hàng) với mọi phần tử khác của lưới mắt cáo ; và một giới hạn trên bé nhất mà tại đó phần tử duy nhất trong tập nhỏ hơn hoặc bằng với mọi phần tử khác của lưới mắt cáo.

FDP_IFF.3 Giới hạn các luồng thông tin bất hợp pháp, đòi hỏi SFP bao trùm các luồng thông tin bất hợp pháp, song không cần thiết phải loại trừ chúng.

FDP_IFF.4 Loại trừ từng phần các luồng thông tin bất hợp pháp, đòi hỏi SFP bao trùm một số (nhưng không cần thiết là tất cả) các luồng thông tin bất hợp pháp.

FDP_IFF.5 Không chứa các luồng thông tin bất hợp pháp, đòi hỏi SFP bao trùm phần loại trừ của tất cả các luồng thông tin bất hợp pháp.

FDP_IFF.6 Giám sát các luồng thông tin bất hợp pháp, đòi hỏi SFP giám sát các luồng thông tin bất hợp pháp về khả năng tối đa và danh nghĩa.

10.6.3 Quản lý của FDP_IFF.1, FDP_IFF.2

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

a) Quản lý các thuộc tính sử dụng để thực hiện các quyết định dựa trên truy nhập.

10.6.4 Quản lý của FDP_IFF.3, FDP_IFF.4, FDP_IFF.5

Không có các hoạt động quản lý nào.

10.6.5 Quản lý của FDP_IFF.6

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

a) Bật hoặc tắt chức năng giám sát

b) Thay đổi khả năng tối đa khi có sự giám sát xuất hiện.

10.6.6 Kiểm toán của FDP_IFF.1, FDP_IFF.2, FDP_IFF.5

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán được đặt trong PP/ST :

a) Tối thiểu: Các quyết định cho phép các luồng thông tin được yêu cầu

b) Cơ sở: Tất cả các quyết định dựa trên các đòi hỏi về luồng thông tin

c) Chi tiết: Các thuộc tính an toàn đặc biệt sử dụng để ra quyết định về thực thi luồng thông tin

d) Chi tiết: Một vài tập con đặc biệt của thông tin được đưa đến dựa trên các đích chính sách (ví dụ Kiểm tra về vật liệu đánh giá thấp)

10.6.7 Kiểm toán của FDP_IFF.3, FDP_IFF.4, FDP_IFF.6

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán được đặt trong PP/ST :

a) Tối thiểu: Các quyết định cho phép các luồng thông tin được yêu cầu

b) Cơ sở: Tất cả các quyết định dựa trên các đòi hỏi về luông thông tin

c) Cơ sở: Sử dụng các kênh luồng thông tin không hợp pháp được xác định

d) Chi tiết: Các thuộc tính an toàn đặc biệt sử dụng để ra quyết định về thực thi luồng thông tin

e) Chi tiết: Một vài tập con đặc biệt của thông tin được đưa đến dựa trên các đích chính sách (ví dụ Kiểm tra về vật liệu đánh giá thấp).

f) Chi tiết: Sử dụng các kênh luồng thông tin không hợp pháp được xác định với khả năng loại trừ tối đa vượt quá một giá trị danh nghĩa.

10.6.8 FDP_IFF.1 Các thuộc tính an toàn đơn giản

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FDP_IFC.1 Kiểm soát luồng thông tin tập con

FMT_MSA.3 Khởi tạo thuộc tính tĩnh.

10.6.8.1 FDP_IFF.1.1

TSF cần thực thi [chỉ định: *kiểm soát luông thông tin SFP*] dựa trên các kiểu chủ thể và các thuộc tính an toàn thông tin sau: [chỉ định: *danh sách các chủ thể và thông tin được kiểm soát dưới SFP được chỉ ra và với mỗi cái có các thuộc tính an toàn*].

10.6.8.2 FDP_IFF.1.2

TSF cần cho phép thông tin đến từ giữa các chỉ thể được kiểm soát và thông tin được kiểm soát qua hoạt động kiểm soát nếu các quy tắc sau được thực hiện: [chỉ định: *với mỗi hoạt động, mối quan hệ dựa trên các thuộc tính an toàn cần phải áp dụng giữa chủ thể và các thuộc tính an toàn thông tin*].

10.6.8.3 FDP_IFF.1.3

TSF cần thực thi [chỉ định: *các quy tắc kiểm soát luồng thông tin SFP bổ sung*]

10.6.8.4 FDP_IFF.1.4

TSF cần cấp phép rõ ràng một luồng thông tin dựa trên những quy tắc sau đây: [chỉ định: *các quy tắc, dựa theo các thuộc tính an toàn, cấp phép rõ ràng cho các luồng thông tin*].

10.6.8.5 FDP_IFF.1.5

TSF cần từ chối rõ ràng một luồng thông tin dựa trên những quy tắc sau đây: [chỉ định: *các quy tắc, dựa theo các thuộc tính an toàn, từ chối rõ ràng các luồng thông tin*].

10.6.9 FDP_IFF.2 Các thuộc tính an toàn phân cấp

Phân cấp từ: FDP_IFF.1 Các thuộc tính an toàn đơn giản.

Các mối phụ thuộc: FDP_IFC.1 Kiểm soát luồng thông tin tập con.

FMT_MSA.3 khởi tạo thuộc tính tĩnh

10.6.9.1 FDP_IFF.2.1

TSF cần thực thi [chỉ định: *kiểm soát luông thông tin SFP*] dựa trên các kiểu chủ thể và các thuộc tính an toàn thông tin sau: [chỉ định: *danh sách các chủ thể và thông tin được kiểm soát dưới SFP được chỉ ra và với mỗi cái có các thuộc tính an toàn*].

10.6.9.2 FDP_IFF.2.2

TSF cần cho phép thông tin đến từ giữa các chủ thể được kiểm soát và thông tin được kiểm soát qua hoạt động kiểm soát nếu các quy tắc sau, **dựa theo mối quan hệ đặt hàng giữa các thuộc tính an toàn**, được thực hiện: [chỉ định: *với mỗi hoạt động, mối quan hệ dựa trên các thuộc tính an toàn cần phải áp dụng giữa chủ thể và các thuộc tính an toàn thông tin*].

10.6.9.3 FDP_IFF.2.3

TSF cần thực thi [chỉ định: *các quy tắc kiểm soát luồng thông tin SFP bổ sung*]

10.6.9.4 FDP_IFF.2.4

TSF cần cấp phép rõ ràng một luồng thông tin dựa trên những quy tắc sau đây: [chỉ định: *các quy tắc, dựa theo các thuộc tính an toàn, cấp phép rõ ràng cho các luồng thông tin*].

10.6.9.5 FDP_IFF.2.5

TSF cần từ chối rõ ràng một luồng thông tin dựa trên những quy tắc sau đây: [chỉ định: *các quy tắc, dựa theo các thuộc tính an toàn, từ chối rõ ràng các luồng thông tin*].

10.6.9.6 FDP_IFF.2.6

TSF cần thực thi các mối quan hệ sau cho bất kỳ hai thuộc tính an toàn cho kiểm soát luồng thông tin:

a) **Tồn tại một chức năng yêu cầu sao cho với hai thuộc tính an toàn hợp lệ, thì chức năng này sẽ quyết định các thuộc tính an toàn giống nhau, hoặc một thuộc tính an toàn lớn hơn cái còn lại, hoặc các thuộc tính an toàn không thể so sánh được.**

b) **Tồn tại "biên trên nhỏ nhất" trong tập các thuộc tính an toàn, sao cho, với bất kỳ hai thuộc tính an toàn hợp lệ nào, sẽ có một thuộc tính an toàn hợp lệ lớn hơn hoặc bằng hai thuộc tính an toàn hợp lệ kia, và**

c) **Tồn tại một "biên dưới lớn nhất" trong tập các thuộc tính an toàn, sao cho, với bất kỳ hai thuộc tính an toàn hợp lệ nào, sẽ có một thuộc tính an toàn hợp lệ không lớn hơn hai thuộc tính an toàn hợp lệ kia.**

10.6.10 FDP_IFF.3 Giới hạn các luồng thông tin bất hợp pháp

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FDP_IFC.1 Kiểm soát luồng thông tin tập con

10.6.10.1 FDP_IFF.3.1

TSF cần thực thi [chỉ định: *kiểm soát luồng thông tin SFP*] để giới hạn khả năng của [chỉ định: *các kiểu luồng thông tin bất hợp pháp*] đến một [chỉ định: *khả năng tối đa*].

10.6.11 FDP_IFF.4 Loại trừ từng phần các luồng thông tin bất hợp pháp

Phân cấp từ: FDP_IFF.2 Giới hạn các luồng thông tin bất hợp pháp

Các mối phụ thuộc: FDP_IFC.1 Kiểm soát luồng thông tin tập con

10.6.11.1 FDP_IFF.4.1

TSF cần thực thi [chỉ định: *kiểm soát luồng thông tin SFP*] để giới hạn khả năng của [chỉ định: *các kiểu luồng thông tin bất hợp pháp*] đến một [chỉ định: *khả năng tối đa*].

10.6.11.2 FDP_IFF.4.2

TSF cần ngăn chặn [chỉ định: *các kiểu luồng thông tin bất hợp pháp*]

10.6.12 FDP_IFF.5 Không có các luồng thông tin bất hợp pháp

Phân cấp từ: FDP_IFF.4 Loại trừ từng phần các luồng thông tin bất hợp pháp.

Các mối phụ thuộc: FDP_IFC.1 Kiểm soát luồng thông tin tập con.

10.6.12.1 FDP_IFF.5.1

TSF cần đảm bảo rằng không có các luồng thông tin bất hợp pháp tồn tại để phá hỏng [chỉ định: *tên của kiểm soát luồng thông tin SFP*]

10.6.13 FDP_IFF.6 Giám sát luồng thông tin bất hợp pháp

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FDP_IFC.1 Kiểm soát luồng thông tin tập con.

10.6.13.1 FDP_IFF.6.1

TSF cần thực thi [chỉ định: *kiểm soát luồng thông tin SFP*] để giám sát [chỉ định: *các kiểu luồng thông tin không hợp pháp*] khi nó vượt quá [chỉ định: *khả năng tối đa*]

10.7 Nhập dữ liệu từ bên ngoài TOE (FDP_ITC)

10.7.1 Hành xử của họ

Họ này định nghĩa các cơ chế để đưa dữ liệu người dùng vào trong TOE như vậy nó có các thuộc tính an toàn tương ứng và được bảo vệ phù hợp. Nó được quan tâm với các giới hạn trong nhập, quyết định các thuộc tính an toàn mong muốn và trình bày các thuộc tính an toàn kết hợp với dữ liệu người dùng.

10.7.2 Phân mức thành phần

FDP_ITC.1 nhập dữ liệu người dùng không có các thuộc tính an toàn, đòi hỏi các thuộc tính an toàn biểu diễn chính xác dữ liệu người dùng và được hỗ trợ phân tách từ đối tượng này

FDP_ITC.2 Nhập dữ liệu người dùng với các thuộc tính an toàn, đòi hỏi các thuộc tính an toàn biểu diễn chính xác dữ liệu người dùng và kết hợp chính xác và rõ ràng với dữ liệu người dùng từ bên ngoài TSC.

10.7.3 Quản lý của FDP_ITC.1, FDP_ITC.2

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

a) Thay đổi các quy tắc kiểm soát bổ sung sử dụng cho nhập dữ liệu.

10.7.4 Kiểm toán của FDP_ITC.1, FDP_ITC.2

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn chứa trong PP/ST :

a) Tối thiểu: nhập vào thành công dữ liệu người dùng, bao gồm bất kỳ các thuộc tính an toàn nào

b) Cơ sở: Tất cả các nỗ lực để nhập vào dữ liệu người dùng, bao gồm bất kỳ các thuộc tính an toàn nào

c) Chi tiết: Các đặc tả của các thuộc tính an toàn cho dữ liệu an toàn được nhập vào được quy định bởi người dùng có ủy quyền

10.7.5 FDP_ITC.1 Nhập dữ liệu người dùng không có các thuộc tính an toàn

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: [FDP_ACC.1 Kiểm soát truy cập tập con, hoặc

FDP_IFC.1 Kiểm soát luồng thông tin tập con

FMT_MSA.3 Khởi tạo các thuộc tính tĩnh

10.7.5.1 FDP_ITC.1.1

TSF cần thực thi [chỉ định: *kiểm soát truy nhập SFP và/hoặc kiểm soát luồng thông tin SFP*] khi nhập dữ liệu người dùng, kiểm soát dưới SFP, từ bên ngoài TOE.

10.7.5.2 FDP_ITC.1.2

TSF cần bỏ qua bất kỳ các thuộc tính an toàn nào kết hợp với dữ liệu người dùng khi nhập dữ liệu người dùng từ bên ngoài TOE.

10.7.5.3 FDP_ITC.1.3

TSF cần thực thi các quy tắc sau đây khi nhập dữ liệu người dùng được kiểm soát dưới SFP từ bên ngoài của TSC: [chỉ định: *các quy tắc kiểm soát bổ sung*]

10.7.6 FDP_ITC.2 Nhập dữ liệu người dùng với các thuộc tính an toàn

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: [FDP_ACC.1 Kiểm soát truy nhập tập con, hoặc

FDP_IFC.1 Kiểm soát luồng thông tin tập con]

[FTP_ITC.1 Kênh tin cậy liên-TSF, hoặc

FTP_TRP.1 đường dẫn tin cậy]

FPT_TDC.1 Nhất quán dữ liệu TSF cơ bản liên-TSF

10.7.6.1 FDP_ITC.2.1

TSF cần thực thi [chỉ định: *kiểm soát truy nhập SFP và/ hoặc kiểm soát luồng thông tin SFP*] khi nhập dữ liệu người dùng, được kiểm soát dưới SFP, từ bên ngoài của TOE.

10.7.6.2 FDP_ITC.2.2

TSF cần sử dụng các thuộc tính an toàn kết hợp với dữ liệu người dùng được nhập vào.

10.7.6.3 FDP_ITC.2.3

TSF cần đảm bảo rằng giao thức sử dụng để cung cấp với sự kết hợp rõ ràng giữa các thuộc tính an toàn và dữ liệu người dùng nhận được.

10.7.6.4 FDP_ITC.2.4

TSF cần đảm bảo rằng việc biểu diễn các thuộc tính an toàn của dữ liệu người dùng được nhập vào như là nguồn dữ liệu người dùng dự định.

10.7.6.5 FDP_ITC.2.5

TSF cần thực thi các quy tắc sau đây khi nhập dữ liệu người dùng được kiểm soát dưới SFP từ bên ngoài TSC: [chỉ định: *các quy tắc kiểm soát nhập bổ sung*].

10.8 Vận chuyển nội bộ TOE (FDP_ITT)

10.8.1 Hành xử của họ

Họ này quy định các yêu cầu để cập đến bảo vệ dữ liệu người dùng khi nó được chuyển giao giữa các phần của TOE qua một kênh bên trong. Điều này có thể trái ngược với các họ Bảo vệ vận chuyển bí mật dữ liệu người dùng liên-TSF (FDP_UCT) và Bảo vệ vận chuyển toàn vẹn dữ liệu người dùng liên – TSF (FDP_UIT), cung cấp tính năng bảo vệ dữ liệu người dùng khi vận chuyển chúng giữa các TSF khác nhau qua các kênh bên ngoài, và Xuất dữ liệu từ TOE (FDP_ETC), Nhập dữ liệu từ bên ngoài TOE (FDP_ITC) đề cập đến việc vận chuyển trung gian TSF cho dữ liệu ra khỏi TOE và từ bên ngoài vào TOE.

10.8.2 Phân mức thành phần

FDP_ITT.1 Bảo vệ vận chuyển nội bộ cơ sở, đòi hỏi dữ liệu người dùng được bảo vệ khi truyền giữa các phần của TOE.

FDP_ITT.2 Phân chia việc truyền tải theo thuộc tính, đòi hỏi phân chia dữ liệu dựa trên giá trị của các thuộc tính liên quan-SFP trong thành phần đầu tiên được bổ sung.

FDP_ITT.3 Giám sát toàn vẹn, đòi hỏi TSF giám sát dữ liệu người dùng được truyền giữa các phần của TOE với các lỗi toàn vẹn dữ liệu được chỉ ra.

FDP_ITT.4 Giám sát toàn vẹn dựa trên các thuộc tính, mở rộng đến thành phần thứ ba với việc cho phép định dạng giám sát toàn vẹn về khác biệt của các thuộc tính SFP liên quan.

10.8.3 Quản lý của FDP_ITT.1, FDP_ITT.2

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

a) Nếu TSF quy định nhiều phương pháp để bảo vệ dữ liệu người dùng trong thời gian truyền giữa các phần vật lý được phân tách bởi TOE, TSF có thể đưa ra các tập phân vai được định nghĩa trước với khả năng lựa chọn phương pháp sẽ được sử dụng.

10.8.4 Quản lý của FDP_ITT.3, FDP_ITT.4

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

a) Đặc tả của các hoạt động được thực hiện dựa trên phát hiện lỗi toàn vẹn có thể được cấu hình

10.8.5 Kiểm toán của FDP_ITT.1, FDP_ITT.2

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn chứa trong PP/ST :

a) Tối thiểu: các chuyển giao thành công dữ liệu người dùng, bao gồm xác định phương pháp bảo vệ được sử dụng.

b) Cơ sở: Tất cả các nỗ lực để chuyển giao dữ liệu người dùng, bao gồm phương pháp bảo vệ được sử dụng và bất kỳ lỗi nào xuất hiện.

10.8.6 Kiểm toán của FDP_ITT.3, FDP_ITT.4

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn chứa trong PP/ST :

a) Tối thiểu: các chuyển giao thành công dữ liệu người dùng, bao gồm xác định phương pháp bảo vệ toàn vẹn được sử dụng.

b) Cơ sở: Tất cả các nỗ lực để chuyển giao dữ liệu người dùng, bao gồm phương pháp bảo vệ toàn vẹn được sử dụng và bất kỳ lỗi nào xuất hiện.

c) Cơ sở: Các nỗ lực không được ủy quyền để thay đổi phương pháp bảo vệ toàn vẹn

d) Chi tiết: Hành động được thực hiện dựa trên phát hiện về lỗi toàn vẹn

10.8.7 FDP_ITT.1 Bảo vệ vận chuyển nội bộ cơ sở

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: [FDP_ACC.1 kiểm soát truy nhập tập con, hoặc
FDP_IFC.1 Kiểm soát luồng thông tin tập con]

10.8.7.1 FDP_ITT.1.1

TSF cần thực thi [chỉ định: *kiểm soát truy nhập SFP và/hoặc kiểm soát luồng thông tin SFP*] để ngăn chặn [lựa chọn: *phơi bày, thay đổi, không sử dụng được*] với dữ liệu người dùng khi nó được truyền giữa các phần vật lý phân tách của TOE.

10.8.8 FDP_ITT.2 Phân tách truyền tải bởi các thuộc tính

Phân cấp từ: FDP_ITT.1 Bảo vệ vận chuyển nội bộ cơ sở

Các mối phụ thuộc: [FDP_ACC.1 Kiểm soát truy nhập tập con, hoặc
FDP_IFC.1 Kiểm soát luồng thông tin tập con]

10.8.8.1 FDP_ITT.2.1

TSF cần thực thi [chỉ định: *kiểm soát truy nhập SFP và/hoặc kiểm soát luồng thông tin SFP*] để ngăn chặn [lựa chọn: *phơi bày, thay đổi, không sử dụng được*] với dữ liệu người dùng khi nó được truyền giữa các phần vật lý phân tách của TOE.

10.8.8.2 FDP_ITT.2.2

TSF cần phân tách dữ liệu kiểm soát bởi SFP khi truyền tải các thành phần của TOE, dựa trên các giá trị sau: [chỉ định: *các thuộc tính an toàn đòi hỏi phân tách*].

10.8.9 FDP_ITT.3 Giám sát toàn vẹn

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: [FDP_ACC.1 Kiểm soát truy nhập tập con, hoặc

FDP_IFC.1 Kiểm soát luồng thông tin tập con]

FDP_ITT.1 Bảo vệ vận chuyển nội bộ cơ sở

10.8.9.1 FDP_ITT.3.1

TSF cần thực thi [chỉ định: *Kiểm soát truy nhập SFP và/hoặc kiểm soát luồng thông tin SFP*] thông qua giám sát dữ liệu người dùng được truyền giữa ác phần vật lý phân tách của TOE theo các lỗi sau: [chỉ định: *các lỗi toàn vẹn*].

10.8.9.2 FDP_ITT.3.2

Dựa trên các phát hiện về toàn vẹn dữ liệu, TSF cần [chỉ định: *chỉ ra các hành động được thực hiện dựa trên lỗi toàn vẹn dữ liệu*].

10.8.10 FDP_ITT.4 Giám sát toàn vẹn dựa trên thuộc tính

Phân cấp từ: FDP_ITT.3 giám sát toàn vẹn

Các mối phụ thuộc: [FDP_ACC.1 Kiểm soát truy nhập tập con, hoặc

FDP_IFC.1 Kiểm soát luồng thông tin tập con]

FDP_ITT.2 Phân tách truyền theo thuộc tính

10.8.10.1 FDP_ITT.4.1

TSF cần thực thi [chỉ định: *Kiểm soát truy nhập SFP và/hoặc kiểm soát luồng thông tin SFP*] thông qua giám sát dữ liệu người dùng được truyền giữa các phần vật lý phân tách của TOE theo các lỗi sau: [chỉ định: *các lỗi toàn vẹn*], **dựa theo các thuộc tính sau : [chỉ định: *các thuộc tính an toàn đòi hỏi phân tách kênh truyền*].**

10.8.10.2 FDP_ITT.4.2

Dựa trên các phát hiện về toàn vẹn dữ liệu, TSF cần [chỉ định: *chỉ ra các hành động được thực hiện dựa trên lỗi toàn vẹn dữ liệu*].

10.9 Bảo vệ thông tin dư thừa (FDP_RIP)

10.9.1 Hành xử của họ

Họ này đề cập đến sự cần thiết đảm bảo rằng các thông tin bị xóa sẽ không thể truy nhập sau đó, và các đối tượng được tạo gần nhất không chứa các thông tin mà không thể truy nhập. Họ này đòi hỏi bảo

vệ thông tin được xóa hoặc giải phóng lô-gic, nhưng vẫn có thể được biểu diễn bên trong tài nguyên có kiểm soát của TSF và do vậy có thể được cấp phát lại cho đối tượng khác.

10.9.2 Phân mức thành phần

FDP_RIP.1 Bảo vệ thông tin dư thừa tập con, yêu cầu TSF đảm bảo rằng bất kỳ nội dung thông tin dư thừa nào của bất kỳ nguồn nào là không sẵn sàng với một tập con được định nghĩa của các đối tượng trong TSC dựa trên cấp phát hoặc hủy cấp phát tài nguyên.

FDP_RIP.2 Bảo vệ thông tin dư thừa đầy đủ, yêu cầu TSF đảm bảo rằng bất kỳ nội dung thông tin dư thừa của bất kỳ nguồn nào là không sẵn sàng với tất cả các đối tượng dựa trên cấp phát hoặc hủy cấp phát tài nguyên.

10.9.3 Quản lý của FDP_RIP.1, FDP_RIP.2

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

a) Lựa chọn khi thực hiện bảo vệ thông tin dư thừa (vi dụ dựa trên cấp phát hoặc hủy cấp phát) có thể được cấu hình bên trong TOE

10.9.4 Kiểm tra của FDP_RIP.1, FDP_RIP.2

Không có sự kiện có thể kiểm toán nào.

10.9.5 FDP_RIP.1 Bảo vệ thông tin dư thừa tập con

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có phụ thuộc nào.

10.9.5.1 FDP_RIP.1.1

TSF cần đảm bảo rằng bất kỳ nội dung thông tin trước đó của một tài nguyên được thực hiện không sẵn sàng [chỉ định: *cấp phát của tài nguyên cho, hủy cấp phát của tài nguyên từ*] theo các đối tượng: [chỉ định: *danh sách của các đối tượng*]

10.9.6 FDP_RIP.2 Bảo vệ thông tin dư thừa đầy đủ

Phân cấp từ: FDP_RIP.1 Bảo vệ thông tin dư thừa tập con

Các mối phụ thuộc: không phụ thuộc

10.9.6.1 FDP_RIP.2.1

TSF cần đảm bảo bất kỳ nội dung thông tin trước đó của tài nguyên được thực hiện không sẵn có dựa trên [lựa chọn: *cấp phát tài nguyên cho, hủy cấp phát của các tài nguyên từ*] tất cả các đối tượng.

10.10 Khôi phục (FDP_ROL)

10.10.1 Hành xử của họ

Hoạt động khôi phục (rollback) liên quan đến việc hoàn lại thao tác hoặc chuỗi các thao tác, được giới hạn bởi một hạn định ví dụ như chu kỳ thời gian, quay trở lại trạng thái biết trước đó. Rollback cho khả năng hoàn lại các hiệu ứng của một thao tác hoặc một chuỗi thao tác nhằm bảo toàn tính toàn vẹn của dữ liệu người dùng.

10.10.2 Phân mức thành phần

FDP_ROL.1 Trở lại trạng thái trước cơ bản đề cập đến sự cần thiết hoặc dưới một số giới hạn các hoạt động bên trong các ranh giới được định nghĩa

FDP_ROL.2 Trở lại trạng thái trước nâng cao đề cập đến sự cần thiết quay lại trạng thái trước đó hoặc không thực hiện tất cả các hoạt động bên trong ranh giới được định nghĩa

10.10.3 Quản lý của FDP_ROL.1, FDP_ROL.2

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

a) Giới hạn biên theo đó việc trở lại trạng thái trước có thể được thực hiện và các mẫu được cấu hình bên trong TOE

b) Cho phép thực hiện hoạt động quay lại trạng thái trước có thể bị ngăn cản với tập phân vai được định nghĩa tốt

10.10.4 Kiểm toán của FDP_ROL.1, FDP_ROL.2

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn chứa trong PP/ST :

a) Tối thiểu: tất cả các hoạt động thực hiện thành công để quay trở lại trạng thái trước đó

b) Cơ sở: Tất cả các nỗ lực để thực hiện quay trở lại trạng thái trước đó

c) Chi tiết: Tất cả các nỗ lực để thực hiện quay trở lại trạng thái trước đó, bao gồm việc định danh các kiểu thực hiện quay trở lại trạng thái trước

10.10.5 FDP_ROL.1 Khôi phục cơ bản

Phân cấp từ: Không có các thành phần nào,

Các mối phụ thuộc: [FDP_ACC.1 Kiểm soát truy nhập tập con, hoặc
FDP_IFC.1 Kiểm soát luồng thông tin tập con]

10.10.5.1 FDP_ROL.1.1

TSF cần thực thi [chỉ định: *kiểm soát truy nhập SFP và/hoặc kiểm soát luồng thông tin SFP*] để cho phép khôi phục lại trạng thái trước đó của [chỉ định: *danh sách các hoạt động*] dựa trên [chỉ định: *thông tin và/hoặc danh sách của các đối tượng*]

10.10.5.2 FDP_ROL.1.2

TSF cần cho phép các hoạt động để quay lại trạng thái trước đó bên trong [chỉ định: *giới hạn biên cho việc khôi phục lại trạng thái trước đó*].

10.10.6 FDP_ROL.2 Khôi phục cải tiến

Phân cấp từ: FDP_ROL.1 Khôi phục cơ bản

Các mối phụ thuộc: [FDP_ACC.1 Kiểm soát truy nhập tập con, hoặc
FDP_IFC.1 Kiểm soát luồng thông tin tập con]

10.10.6.1 FDP_ROL.2.1

TSF cần thực thi [chỉ định: *kiểm soát truy nhập SFP và/hoặc kiểm soát luồng thông tin SFP*] để cho phép khôi phục lại **toàn bộ hoạt động trên [chỉ định: danh sách các đối tượng]**

10.10.6.2 FDP_ROL.2.2

TSF cần cho phép các hoạt động có thể khôi phục lại trong khoảng [chỉ định: *giới hạn biên cho việc khôi phục có thể thực hiện*]

10.11 Toàn vẹn dữ liệu lưu trữ (FDP_SDI)

10.11.1 Hành xử của họ

Họ này quy định các yêu cầu đề cập đến việc bảo vệ dữ liệu người dùng khi nó được lưu trữ trong TSC. Các lỗi toàn vẹn có thể ảnh hưởng đến việc lưu trữ dữ liệu người dùng trong bộ nhớ hoặc trong thiết bị lưu trữ. Họ này khác với Chuyển giao TOE nội bộ (FDP_ITT) mà bảo vệ dữ liệu người dùng khỏi các lỗi toàn vẹn khi đang được truyền bên trong TOE.

10.11.2 Phân mức thành phần

FDP_SDI.1 Giám sát toàn vẹn dữ liệu lưu trữ, đòi hỏi bộ giám sát dữ liệu người dùng SF được lưu trữ trong TSC cho các lỗi toàn vẹn được chỉ ra

FDP_SDI.2 Giám sát toàn vẹn dữ liệu lưu trữ và các hành động thêm vào để bổ xung cho khả năng đến thành phần đầu tiên bởi việc cho phép các hoạt động được thực hiện như kết quả của phát hiện lỗi.

10.11.3 Quản lý của FDP_SDI.1

Không có các hoạt động quản lý nào.

10.11.4 Quản lý của FDP_SDI.2

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

a) Các hành động cần được thực hiện dựa trên phát hiện lỗi toàn vẹn có thể cấu hình được

10.11.5 Kiểm toán của FDP_SDI.1

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn chứa trong PP/ST :

a) Tối thiểu: Các nỗ lực thành công để soát xét sự toàn vẹn của dữ liệu người dùng, bao gồm biểu thị của các kết quả soát xét

b) Cơ sở: Tất cả các nỗ lực để soát xét sự toàn vẹn của dữ liệu, bao gồm biểu thị của các kết quả soát xét nếu được thực hiện.

c) Chi tiết: Kiểu lỗi toàn vẹn mà đã xuất hiện

d) Chi tiết: Các hành động được thực hiện dựa trên phát hiện về các lỗi toàn diện

10.11.6 Kiểm toán của FDP_SDI.2

Các hành động sau đây có thể được kiểm tra nếu FAU_GEN Tạo dữ liệu kiểm tra được đặt trong PP/ST

e) Tối thiểu: Các nỗ lực thành công để soát xét sự toàn vẹn của dữ liệu người dùng, bao gồm biểu thị của các kết quả soát xét

f) Cơ sở: Tất cả các nỗ lực để soát xét sự toàn vẹn của dữ liệu, bao gồm biểu thị của các kết quả soát xét nếu được thực hiện.

g) Chi tiết: Kiểu lỗi toàn vẹn mà đã xuất hiện

h) Chi tiết: Các hành động được thực hiện dựa trên phát hiện về các lỗi toàn diện

10.11.7 FDP_SDI.1 Giám sát toàn vẹn dữ liệu lưu trữ

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: không phụ thuộc

10.11.7.1 FDP_SDI.1.1

TSF cần giám sát dữ liệu người dùng *được* lưu trữ trong TSF cho [chỉ thị: các lỗi toàn vẹn] trong tất cả các đối tượng, dựa trên các thuộc tính sau: [chỉ thị: *các thuộc tính dữ liệu người dùng*].

10.11.8 FDP_SDI.2 Giám sát toàn vẹn dữ liệu lưu trữ và hành động

Phân cấp từ: FDP_SDI.1 Giám sát toàn vẹn lưu trữ dữ liệu

Các mối phụ thuộc: Không phụ thuộc

10.11.8.1 FDP_SDI.2.1

TSF cần giám sát dữ liệu người dùng được lưu trữ trong TSC cho [chỉ thị: các lỗi toàn vẹn] trên tất cả các đối tượng, dựa trên các thuộc tính sau: [chỉ thị: các thuộc tính dữ liệu người dùng]

10.11.8.2 FDP_SDI.2.2

Dựa trên phát hiện về lỗi toàn vẹn dữ liệu, TSF cần [chỉ thị: hành động được thực hiện]

10.12 Bảo vệ vận chuyển bí mật dữ liệu người dùng liên-TSF (FDP_UCT)

10.12.1 Hành xử của họ

Họ này định nghĩa các yêu cầu để đảm bảo sự tin cậy của dữ liệu người dùng khi nó được chuyển giao sử dụng kênh ngoài giữa các TOE khác nhau hoặc người dùng trong các TOE khác nhau.

10.12.2 Phân mức thành phần

Trong FDP_UCT.1 Trao đổi dữ liệu tin cậy cơ bản, mục đích đặt ra là bảo vệ chống lại sự khai thác dữ liệu người dùng khi truyền.

10.12.3 Quản lý của FDP_UCT.1

Không có các hoạt động quản lý nào.

10.12.4 Kiểm toán của FDP_UCT.1

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn chứa trong PP/ST :

a) Tối thiểu: Định danh của bất kỳ người dùng hoặc thực thể nào sử dụng các cơ chế trao đổi dữ liệu.

b) Cơ sở: Định danh của bất kỳ người dùng hoặc thực thể không được ủy quyền nào cố gắng sử dụng các cơ chế trao đổi dữ liệu.

c) Cơ sở: Một tham chiếu đến tên hoặc thông tin đánh chỉ mục hữu ích khác trong việc xác định dữ liệu người dùng được truyền hay nhận. Nó bao gồm các thuộc tính an toàn kết hợp với thông tin.

10.12.5 FDP_UCT.1 Bí mật trao đổi dữ liệu cơ bản

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: [FTP_ICT.1 Kênh tin cậy liên TSF, hoặc
FTP_TRP.1 Đường dẫn tin cậy]

[FDP_ACC.1 Kiểm soát truy nhập tập con, hoặc

FDP_IFC.1 Kiểm soát luồng thông tin tập con]

10.12.5.1 FDP_UCT.1.1

TSF cần thực thi [chỉ thị: *kiểm soát truy nhập SFP và/hoặc kiểm soát luồng thông tin SFP*] có thể [lựa chọn: *truyền, nhận*] đến các đối tượng theo cách thức được bảo vệ từ việc khai thác không được cấp phép.

10.13 Bảo vệ vận chuyển toàn vẹn dữ liệu người dùng liên-TSF (FDP_UIT)

10.13.1 Hành xử của họ

Họ này định nghĩa các yêu cầu cho quy định sự toàn vẹn của dữ liệu người dùng trong việc truyền giữa TSF và các sản phẩm IT được tin cậy khác và khôi phục từ các lỗi có thể được phát hiện. Tại mức tối thiểu, họ này giám sát sự toàn vẹn của dữ liệu người dùng với các thay đổi. Thêm vào đó, họ này hỗ trợ các cách khác nhau của việc chỉnh sửa các lỗi toàn vẹn được xác định.

10.13.2 Phân mức thành phần

FDP_UIT.1 Toàn vẹn trao đổi dữ liệu đề cập đến sự phát hiện các thay đổi, xóa, thêm, lặp lại lỗi trong dữ liệu người dùng được truyền

FDP_UIT.2 Khôi phục trao đổi dữ liệu nguồn đề cập đến việc khôi phục dữ liệu người dùng gốc với việc nhận TSF với sự giúp đỡ từ sản phẩm CNTT có nguồn gốc đáng tin cậy

FDP_UIT.3 Khôi phục trao đổi dữ liệu đích đề cập đến việc khôi phục dữ liệu người dùng với việc nhận TSF của nó mà không có bất kỳ sự trợ giúp nào từ các sản phẩm IT có nguồn gốc tin cậy.

10.13.3 Quản lý của FDP_UIT.1, FDP_UIT.2, FDP_UIT.3

Không có các hoạt động quản lý nào.

10.13.4 Kiểm toán của FDP_UIT.1

Các hành động sau đây có thể được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn chứa trong PP/ST :

a) Tối thiểu: Định danh của bất kỳ người dùng hoặc thực thể nào sử dụng các cơ chế trao đổi dữ liệu.

b) Cơ sở: Định danh của bất kỳ người dùng hoặc cố gắng sử dụng các cơ chế trao đổi dữ liệu, nhưng lại không được ủy quyền để làm điều đó

c) Cơ sở: Một tham chiếu đến tên hoặc thông tin đánh chỉ mục hữu ích khác trong việc xác định dữ liệu người dùng được truyền hay nhận. Nó bao gồm các thuộc tính an toàn kết hợp với thông tin.

d) Cơ sở: bất kỳ nỗ lực xác định nào để ngăn chặn việc truyền dữ liệu người dùng

e) Chi tiết: các kiểu và/hoặc các ảnh hưởng của bất kỳ sự thay đổi được phát hiện trong truyền dữ liệu người dùng.

10.13.5 Kiểm toán của FDP_UIT.2, FDP_UIT.3

Các hành động sau đây có thể được kiểm tra nếu FAU_GEN Tạo dữ liệu kiểm tra được đặt trong PP/ST

a) Tối thiểu: Định danh của bất kỳ người dùng hoặc thực thể nào sử dụng các cơ chế trao đổi dữ liệu.

b) Tối thiểu: Khôi phục thành công các lỗi bao gồm kiểu của lỗi đã được phát hiện

c) Cơ sở: Định danh của bất kỳ người dùng hoặc cố gắng sử dụng các cơ chế trao đổi dữ liệu, nhưng lại không được ủy quyền để làm điều đó

d) Cơ sở: Một tham chiếu đến tên hoặc thông tin đánh chỉ mục hữu ích khác trong việc xác định dữ liệu người dùng được truyền hay nhận. Nó bao gồm các thuộc tính an toàn kết hợp với thông tin.

e) Cơ sở: bất kỳ nỗ lực xác định nào để ngăn chặn việc truyền dữ liệu người dùng

f) Chi tiết: các kiểu và/hoặc các ảnh hưởng của bất kỳ sự thay đổi được phát hiện trong truyền dữ liệu người dùng.

10.13.6 FDP_UIT.1 Toàn vẹn trao đổi dữ liệu

Phân cấp từ: không có các thành phần nào.

Các mối phụ thuộc: [FDP_ACC.1 kiểm soát truy nhập tập con, hoặc
FDP_IFC.1 kiểm soát luồng thông tin tập con]
FDP_UIT.1 Toàn vẹn trao đổi dữ liệu, hoặc
FTP_ITC.1 Kênh tin cậy liên TSF]

10.13.6.1 FDP_UIT.1.1

TSF cần thực thi [chỉ định: *kiểm soát truy nhập SFP và/hoặc kiểm soát luồng thông tin SFP*] có thể [lựa chọn: *truyền, nhận*] dữ liệu người dùng theo cách thức được bảo vệ từ [lựa chọn: *thay đổi, xóa, chèn, lặp lại*] các lỗi.

10.13.6.2 FDP_UIT.1.2

TSF cần có khả năng quyết định nhận dữ liệu người dùng, có hay không với [lựa chọn: *thay đổi, xoát, thêm, lặp lại*] xuất hiện.

10.13.7 FDP_UIT.2 Khôi phục trao đổi dữ liệu gốc

Phân cấp từ: không có các thành phần nào.

Các mối phụ thuộc: [FDP_ACC.1 kiểm soát truy nhập tập con, hoặc
FDP_IFC.1 kiểm soát luồng thông tin tập con]
FDP_UIT.1 Toàn vẹn trao đổi dữ liệu, hoặc
FTP_ITC.1 Kênh tin cậy liên TSF]

10.13.7.1 FDP_UIT.2.1

TSF cần thực thi [chỉ định: *kiểm soát truy nhập SFP và/hoặc kiểm soát luồng thông tin SFP*] có thể khôi phục từ [chỉ thị: *danh sách của các lỗi có thể khôi phục*] với sự trợ giúp của các sản phẩm IT có nguồn gốc tin cậy.

10.13.8 FDP_UIT.3 Khôi phục trao đổi dữ liệu đích

Phân cấp từ: FDP_UIT khôi phục trao đổi dữ liệu nguồn

Các mối phụ thuộc: [FDP_ACC.1 kiểm soát truy nhập tập con, hoặc
FDP_IFC.1 kiểm soát luồng thông tin tập con]
FDP_UIT.1 Toàn vẹn trao đổi dữ liệu, hoặc
FTP_ITC.1 Kênh tin cậy liên TSF]

10.13.8.1 FDP_UIT.3.1

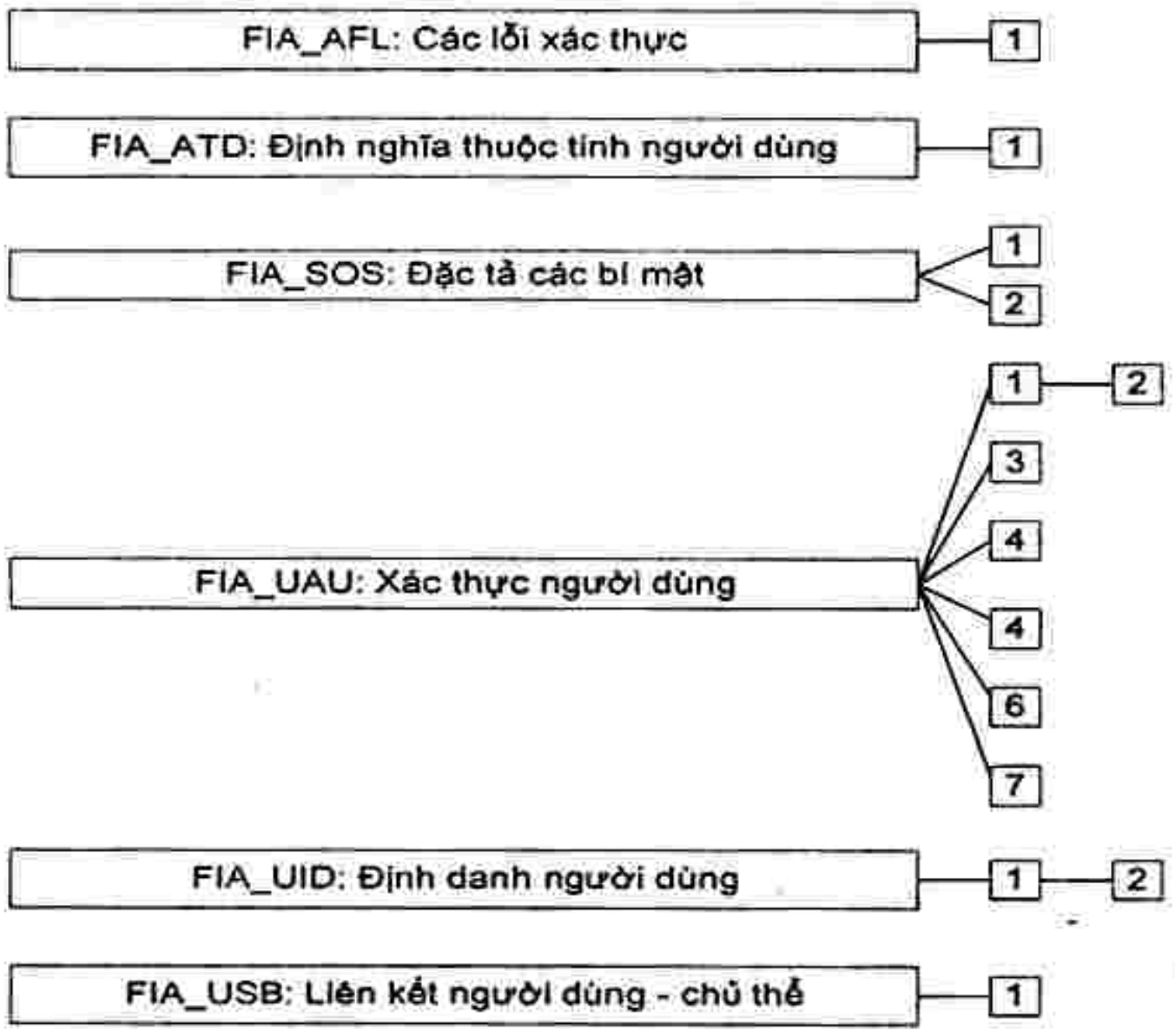
TSF cần thực thi [chỉ định: kiểm soát truy nhập SFP và/hoặc kiểm soát luồng thông tin SFP] có thể khôi phục từ [chỉ thị: danh sách của các lỗi có thể khôi phục] **không có bất kỳ sự trợ giúp nào từ** các sản phẩm IT có nguồn gốc tin cậy.

11 Lớp FIA: Định danh và xác thực

Các họ trong lớp này gửi những yêu cầu cho những chức năng để thiết lập và xác minh một định danh người dùng đã được yêu cầu.

Yêu cầu định danh và xác thực để đảm bảo rằng người dùng sẽ có các thuộc tính an toàn (ví dụ như: định danh, nhóm, các quy tắc, các mức an toàn hay toàn vẹn).

Danh tính rõ ràng của người dùng có thẩm quyền và việc kết hợp đúng các thuộc tính an toàn với người dùng và các chủ thể then chốt để bắt buộc các chính sách an ninh mong muốn. Các họ trong lớp này đề cập đến việc xác định và xác minh danh tính của người dùng, xác định người có thẩm quyền của họ để tương tác với TOE, và với việc kết hợp đúng của các thuộc tính an toàn đối với người dùng có thẩm quyền. Các lớp khác của yêu cầu (bảo vệ dữ liệu người dùng, kiểm toán an toàn) phụ thuộc vào việc định danh và xác thực chính xác người dùng thì mới có hiệu lực.



Hình 11 - Phân cấp lớp FIA: Định danh và xác thực

11.1 Các lỗi xác thực (FIA_AFL)

11.1.1 Hành xử của họ

Họ này bao gồm các yêu cầu để định nghĩa các giá trị cho một vài số lượng thử chứng thực mà không thành công và các hành động TSF trong các trường hợp lỗi thử xác thực. Những tham số, không hạn chế, bao gồm số lượng thử xác thực bị lỗi và các ngưỡng thời gian.

11.1.2 Phân mức thành phần

FIA_AFL.1 Xử lý lỗi xác thực, yêu cầu TSF có thể giới hạn các quá trình thiết lập phiên sau khi xác định được số việc thử xác thực thất bại. Sau khi giới hạn quá trình thiết lập phiên, nó cũng yêu cầu TSF có thể khóa tài khoản người dùng hoặc điểm vào (máy trạm) từ lúc thử nghiệm cho tới khi xảy ra điều kiện mà người quản trị đã định nghĩa.

11.1.3 Quản lý của FIA_AFL.1

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

a) Quản lý các ngưỡng của việc thử xác thực không thành công.

b) Quản lý các hành động được tạo ra trong sự kiện của lỗi xác thực.

11.1.4 Kiểm toán của FIA_AFL.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Đạt được ngưỡng cho việc thử xác thực không thành công và thực hiện các hành động (khóa đầu cuối), sau đó là việc phục hồi trở về trạng thái bình thường (mở lại đầu cuối).

11.1.5 Xử lý lỗi xác thực FIA_AFL.1

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: FIA_UAU.1 Định thời cho xác thực

11.1.5.1 FIA_AFL.1.1

TSF cần phát hiện [Việc lựa chọn: [ấn định: *số nguyên dương*] khi nhà quản trị thiết lập số nguyên dương với điều kiện là [chỉ định: *khoảng giá trị cho phép*] và việc thử xác thực không thành công xuất hiện liên quan tới [chỉ định: *danh sách các sự kiện xác thực*].

11.1.5.2 FIA_AFL.1.2

Khi số lượng việc thử xác thực không thành công được xác định hoặc phụ trội thì TSF sẽ thực hiện [chỉ định*: danh sách các hành động*].

11.2 Định nghĩa thuộc tính người dùng (FIA_ATD)

11.2.1 Hành xử của họ

Tất cả người dùng có thẩm quyền có thể có một tập thuộc tính an toàn, những thuộc tính khác định danh người dùng được sử dụng để thực thi TSP. Họ này xác định các yêu cầu về thuộc tính an toàn người dùng liên đới với những người dùng cần để trợ giúp TSP.

11.2.2 Phân mức thành phần

FIA_ATD.1 Xác định thuộc tính người dùng cho phép các thuộc tính an toàn người dùng đối với mỗi người dùng để duy trì một cách riêng lẻ.

11.2.3 Quản lý của FIA_ATD.1

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

a) Nếu việc ấn định quá mức ấn định, người quản trị có thẩm quyền phải định nghĩa thêm các thuộc tính an toàn cho người dùng.

11.2.4 Kiểm toán của FIA_ATD.1

Không có sự kiện có thể kiểm toán nào.

11.2.5 FIA_ATD.1 Định nghĩa thuộc tính người dùng

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

11.2.5.1 FIA_ATD.1.1

TSF cần duy trì danh sách các thuộc tính an toàn mà thuộc về người dùng riêng lẻ: [chỉ định: *danh sách các thuộc tính an toàn*].

11.3 Đặc tả các của các bí mật (FIA_SOS)

11.3.1 Hành xử của họ

Họ này định nghĩa các yêu cầu về kỹ thuật để thực thi các tỷ lệ đặc trưng được định nghĩa trong vấn đề bảo mật đã đề cập cũng như là mới phát sinh để đáp ứng tỷ lệ đã định nghĩa.

11.3.2 Phân mức thành phần

FIA_SOS.1 Thẩm tra bảo mật, yêu cầu TSF xác minh các vấn đề bảo mật được thấy trong tỷ lệ đặc trưng đã được định nghĩa.

FIA_SOS.2 TSF Tạo ra các bí mật, yêu cầu TSF có thể phát sinh các vấn đề bảo mật nhận thấy trong tỷ lệ đặc trưng đã định nghĩa.

11.3.3 Quản lý của FIA_SOS.1

Các hành động sau có thể liên quan tới các chức năng quản lý trong FMT:

a) Quản lý các tỷ lệ để xác minh vấn đề bảo mật

11.3.4 Quản lý của FIA_SOS.2

Các hành động sau có thể liên quan tới các chức năng quản lý trong FMT:

a) Quản lý các tỷ lệ để phát sinh vấn đề bảo mật

11.3.5 Kiểm toán của FIA_SOS.1, FIA_SOS.2

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Việc loại bỏ bởi TSF trong bất kỳ thử nghiệm bảo mật nào.

b) Cơ sở: Việc loại bỏ hoặc chấp nhận bởi TSF trong bất kỳ thử nghiệm bảo mật nào.

c) Chi tiết: Định danh của bất kỳ sự thay đổi tới tỷ lệ đặc trưng đã định nghĩa.

11.3.6 FIA_SOS.1 Thẩm tra của các bí mật

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc nào.

11.3.6.1 FIA_SOS.1.1

TSF cần cung cấp một cơ chế để thẩm tra các bí mật đã thỏa mãn [chỉ định: *một đơn vị đo chất lượng định nghĩa trước*].

11.3.7 FIA_SOS.2 Tạo các bí mật TSF

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: Không có sự phụ thuộc.

11.3.7.1 FIA_SOS.2.1

TSF cần cung cấp một cơ chế để thẩm tra bí mật đã thỏa mãn [chỉ định: *một đơn vị đo chất lượng định nghĩa trước*].

11.3.7.2 FIA_SOS.2.2

TSF cần có khả năng thực thi việc sử dụng các bí mật đã tạo ra cho TSF cho [chỉ định: *danh sách các chức năng của TSF*].

11.4 Xác thực người dùng (FIA_UAU)

11.4.1 Hành xử của họ

Họ này định nghĩa các kiểu cơ chế xác thực người dùng được trợ giúp bởi TSF. Họ này cũng định nghĩa các thuộc tính được yêu cầu trong cơ chế xác thực người dùng phải là các thuộc tính cơ sở.

11.4.2 Phân mức thành phần

FIA_UAU.1 Định thời cho xác thực, cho phép một người dùng thực thi ưu tiên các hành động nào đó hơn là xác thực danh tính của một người dùng.

FIA_UAU.2 Xác thực người dùng trước khi hành động, yêu cầu người dùng là phải được xác thực trước khi bất kỳ hành động nào được cho phép bởi TSF.

FIA_UAU.3 Xác thực không thể giả mạo, yêu cầu cơ chế xác thực có thể phát hiện và ngăn chặn việc sử dụng dữ liệu xác thực đã được giả mạo hay sao chép.

FIA_UAU.4 Các cơ chế xác thực dùng đơn chiếc, yêu cầu một cơ chế xác thực tính toán với dữ liệu xác thực sử dụng riêng lẻ.

FIA_UAU.5 Các cơ chế đa xác thực, yêu cầu các cơ chế xác thực khác nhau được cung cấp và được sử dụng để xác thực danh tính người dùng trong các sự kiện cụ thể.

FIA_UAU.6 Xác thực lại, yêu cầu khả năng để xác định các sự kiện cho người dùng cần được xác thực.

FIA_UAU.7 Phản hồi xác thực có bảo vệ, yêu cầu những thông tin phản hồi hạn chế được quy định cho người dùng trong việc xác thực.

11.4.3 Quản lý của FIA_UAU.1

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

a) Quản lý dữ liệu xác thực bởi người quản trị

b) Quản lý dữ liệu xác thực bởi người dùng cộng tác

c) Quản lý danh sách các hành động mà có thể được thực hiện trước khi người dùng được xác thực.

11.4.4 Quản lý của FIA_UAU.2

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

a) Quản lý dữ liệu xác thực bởi người quản trị

b) Quản lý dữ liệu xác thực bởi người dùng cộng tác với dữ liệu này.

11.4.5 Quản lý của FIA_UAU.3, FIA_UAU.4, FIA_UAU.7

Không có các hoạt động quản lý nào.

11.4.6 Quản lý của FIA_UAU.5

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

a) Quản lý các cơ chế xác thực

b) Quản lý các quy tắc xác thực

11.4.7 Quản lý của FIA_UAU.6

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

a) Nếu người quản trị có thẩm quyền có thể yêu cầu xác thực lại, việc quản lý gồm một yêu cầu xác thực lại.

11.4.8 Kiểm toán của FIA_UAU.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Sử dụng cơ chế xác thực không thành công.

b) Cơ sở: Sử dụng tất cả cơ chế xác thực.

c) Chi tiết: Tất cả các hành động trung gian TSF được thực thi trước khi xác thực người dùng.

11.4.9 Kiểm toán của FIA_UAU.2

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Sử dụng cơ chế xác thực không thành công

b) Cơ sở: Sử dụng tất cả cơ chế xác thực

11.4.10 Kiểm toán của FIA_UAU.3

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Phát hiện các dữ liệu xác thực giả mạo.

b) Cơ sở: Tất cả các độ đo trực tiếp được thực hiện và các kết quả kiểm tra trên dữ liệu giả mạo.

11.4.11 Kiểm toán của FIA_UAU.4

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Việc thử dùng lại các dữ liệu xác thực.

11.4.12 Kiểm toán của FIA_UAU.5

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: quyết định cuối cùng vào việc xác thực.

b) Cơ sở: Kết quả của mỗi cơ chế hoạt động cùng với quyết định cuối cùng.

11.4.13 Kiểm toán của FIA_UAU.6

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Lỗi xác thực lại;

b) Cơ sở: Tất cả việc thử xác thực lại.

11.4.14 Kiểm toán của FIA_UAU.7

Không có sự kiện có thể kiểm toán nào.

11.4.15 FIA_UAU.1 Định thời cho xác thực

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: FIA_UID.1 Định thời cho định danh

11.4.15.1 FIA_UAU.1.1

TSF cần cho phép [chỉ định: *danh sách các hành động trung gian TSF*] đại diện cho người dùng thực hiện trước khi người dùng được xác thực.

11.4.15.2 FIA_UAU.1.2

TSF cần yêu cầu người dùng phải xác thực thành công trước khi cho phép các hành động trung gian TSF khác đại diện cho người dùng đó.

11.4.16 FIA_UAU.2 Xác thực người dùng trước khi hành động

Phân cấp từ: FIA_UAU.1 Định thời cho xác thực

Các mối phụ thuộc: FIA_UID.1 Định thời cho định danh

11.4.16.1 FIA_UAU.2.1

TSF cần yêu cầu mỗi người dùng xác thực thành công trước khi cho phép các hành động trung gian TSF khác đại diện cho người dùng đó.

11.4.17 FIA_UAU.3 Xác thực không thể giả mạo

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: Không có sự phụ thuộc

11.4.17.1 FIA_UAU.3.1

TSF cần [lựa chọn: *phát hiện, ngăn chặn*] việc sử dụng dữ liệu xác thực đã bị giả mạo bởi một người dùng TSF nào đó.

11.4.17.2 FIA_UAU.3.2

TSF cần [lựa chọn: *phát hiện, ngăn chặn*] việc sử dụng của dữ liệu xác thực đã được sao chép từ một người dùng TSF khác.

11.4.18 FIA_UAU.4 Các cơ chế xác thực đơn

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: Không có sự phụ thuộc nào.

11.4.18.1 FIA_UAU.4.1

TSF cần ngăn chặn việc sử dụng lại dữ liệu xác thực liên quan tới [chỉ định: *cơ chế xác thực định danh*].

11.4.19 FIA_UAU.5 Cơ chế đa xác thực

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: Không có sự phụ thuộc nào

11.4.19.1 FIA_UAU.5.1

TSF cần cung cấp [Chỉ định: *danh sách cơ chế đa xác thực*] để trợ giúp xác thực người dùng.

11.4.19.2 FIA_UAU.5.2

TSF cần xác thực bất kỳ định danh yêu cầu của người dùng nào tuân theo [chỉ định: *các quy tắc miêu tả các cơ chế đa xác thực quy định việc xác thực như thế nào*].

11.4.20 FIA_UAU.6 Xác thực lại

Phân cấp từ: Không có các thành phần nào

Sự Các mối phụ thuộc: Không có sự phụ thuộc nào.

11.4.20.1 FIA_UAU.6.1

TSF cần xác thực lại người dùng dưới các điều kiện [chỉ định: *danh sách các điều kiện dưới mỗi việc xác thực lại được yêu cầu*]

11.4.21 FIA_UAU.7 Phản hồi xác thực có bảo vệ

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: FIA_UAU.1 Định thời cho xác thực

11.4.21.1 FIA_UAU.7.1

TSF cần cung cấp chỉ các [chỉ định: *danh sách phản hồi*] tới người dùng trong khi việc xác thực là đang được tiến hành.

11.5 Định danh người dùng (FIA_UID)

11.5.1 Hành xử của họ

Họ này định nghĩa các điều kiện mà người dùng sẽ được yêu cầu để định danh chúng trước khi thực hiện bất kỳ các hành động khác đã được dàn xếp bởi TSF và điều kiện này yêu cầu định danh người dùng.

11.5.2 Phân mức thành phần

FIA_UID.1 Định thời cho định danh, cho phép người dùng thực hiện các hành động chắc chắn trước khi được định danh bởi TSF.

FIA_UID.2 Định danh người dùng trước khi bất kỳ hành động, yêu cầu người dùng định danh trước khi hành động được cho phép bởi TSF.

11.5.3 Quản lý của FIA_UID.1

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

a) Quản lý định danh người dùng

b) Nếu một người quản trị có thẩm quyền có thể: thay đổi các hành động được phép trước khi định danh, quản lý các danh sách hành động.

11.5.4 Quản lý của FIA_UID.2

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

a) Quản lý định danh người dùng

11.5.5 Kiểm toán của FIA_UID.1, FIA_UID.2

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Sử dụng cơ chế định danh người dùng không thành công, bao gồm định danh người dùng được quy định.

b) Cơ sở: Tất cả sử dụng cơ chế định danh người dùng, bao gồm định danh người dùng được quy định.

11.5.6 FIA_UID.1 Định thời cho định danh

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: Không có sự phụ thuộc nào.

11.5.6.1 FIA_UID.1.1

TSF cần cho phép [chỉ định: *danh sách các hành động trung gian TSF*] trợ giúp người dùng thực hiện trước khi người dùng được định danh.

11.5.6.2 FIA_UID.1.2

TSF cần yêu cầu mỗi người dùng phải được xác định thành công trước khi cho phép các hành động trung gian TSF đại diện cho người dùng đó.

11.5.7 FIA_UID.2 Định danh người dùng trước khi hành động

Phân cấp từ: FIA_UID.1 Định thời cho định danh

Các mối phụ thuộc: Không có sự phụ thuộc nào

11.5.7.1 FIA_UID.2.1

TSF cần yêu cầu mỗi người dùng xác định danh tính trước khi cho phép bất kỳ các hành động trung gian TSF đại diện cho người dùng đó.

11.6 Liên kết chủ thể - người dùng (FIA_USB)

11.6.1 Hành xử của họ

Một người dùng được xác thực hành động đặc trưng về một chủ đích để sử dụng TOE. Các thuộc tính an toàn người dùng là được kết hợp (tổng thể hoặc từng phần) với chủ đích này. Họ này định nghĩa các yêu cầu để tạo và duy trì sự kết hợp của các thuộc tính an toàn người dùng tới một hành động chủ đích phía đại diện cho người dùng.

11.6.2 Phân mức thành phần

FIA_USB.1 Liên kết chủ thể - người dùng yêu cầu sự ấn định của bất kỳ quy tắc nào bao trùm việc trợ giúp giữa các thuộc tính người dùng và các thuộc tính chủ thể vào trong cái mà chúng được ánh xạ.

11.6.3 Quản lý của FIA_USB.1

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

a) Người quản trị có thẩm quyền có thể định nghĩa mặc định các thuộc tính an toàn chủ-thể.

b) Người quản trị có thẩm quyền có thể thay đổi các thuộc tính an toàn chủ thể.

11.6.4 Kiểm toán của FIA_USB.1

Các hành động sau nên được kiểm toán, nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đưa vào trong PP/ST:

a) Tối thiểu: Ràng buộc các thuộc tính an toàn người dùng tới một vấn đề là không thành công (ví dụ: việc tạo ra một chủ thể).

b) Cơ sở: Việc thành công hay thất bại của vấn đề ràng buộc các thuộc tính an toàn người dùng tới một chủ thể (ví dụ: việc thành công hay thất bại để tạo một chủ thể).

11.6.5 FIA_USB.1 Liên kết chủ thể - người dùng

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: FIA_ATD.1 Định nghĩa thuộc tính người dùng

11.6.5.1 FIA_USB.1.1

TSF cần kết hợp các thuộc tính an toàn người dùng với các chủ thể hành động bên phía đại diện của người dùng đó: [chỉ định: *danh sách các thuộc tính an toàn người dùng*].

11.6.5.2 FIA_USB.1.2

TSF cần thực thi các quy tắc sau dựa trên phía liên kết của các thuộc tính an toàn người dùng lúc khởi tạo với các chủ đề hành động dựa trên phía đại diện của người dùng: [chỉ định: *các quy tắc cho liên kết ban đầu của các thuộc tính*].

11.6.5.3 FIA_USB.1.3

TSF cần thực thi các quy tắc chủ yếu sau thay đổi các thuộc tính an toàn người dùng được liên kết với các chủ thể hành động bên phía đại diện người dùng:[chỉ định: *các quy tắc để thay đổi các thuộc tính*].

12 Lớp FMT: Quản lý an toàn

Lớp này được dùng để chỉ định quản lý một vài lĩnh vực của TSF: các thuộc tính an toàn, các chức năng và dữ liệu TSF. Các quy tắc quản lý khác nhau và sự tương tác giữa chúng có thể được chỉ rõ như là sự phân tách khả năng.

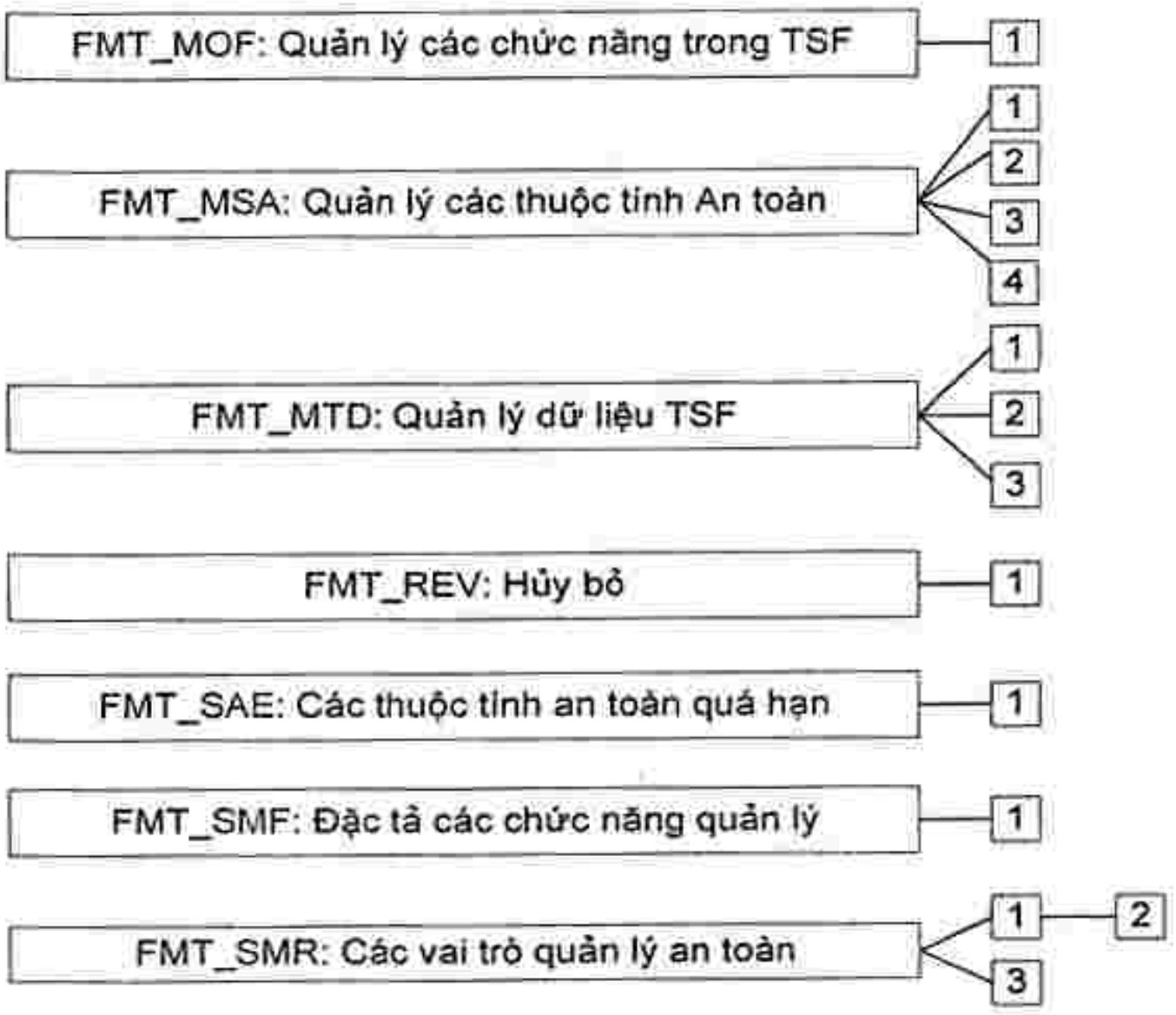
Lớp này có một vài mục tiêu sau:

a) Quản lý dữ liệu TSF, ví dụ như là: tiêu đề

b) Quản lý các thuộc tính an toàn, ví dụ như là: các Danh sách kiểm soát truy cập và danh sách Năng lực.

c) Quản lý các chức năng của TSF, ví dụ như là: việc lựa chọn các chức năng và các quy tắc hay các điều kiện tác động đến hành vi của TSF.

d) Định nghĩa các vai trò an toàn.



Hình 12 - Sự phân cấp lớp FMT: Quản lý an toàn

12.1 Quản lý các chức năng trong TSF (FMT_MOF)

12.1.1 Hành xử của họ

Họ này cho phép người dùng có thẩm quyền điều khiển thông qua việc quản lý các chức năng trong TSF. Ví dụ về các chức năng trong TSF bao gồm các chức năng kiểm tra và các chức năng đa xác thực.

12.1.2 Phân mức thành phần

FMT_MOF.1 Quản lý hành xử của các chức năng an toàn, cho phép người dùng có thẩm quyền (các quy tắc) để quản lý cơ chế hoạt động của chức năng trong TSF mà sử dụng các quy tắc hay có các điều kiện đặc biệt có thể được quản lý.

12.1.3 Quản lý của FMT_MOF.1

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

a) Quản lý nhóm các quy tắc có thể tương tác với các chức năng trong TSF.

12.1.4 Kiểm toán của FMT_MOF.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Cơ sở: tất cả sự thay đổi trong hành vi của các chức năng trong TSF.

12.1.5 FMT_MOF.1 Các cơ chế hoạt động của quản lý chức năng an toàn

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: FMT_SMR.1 Các vai trò an toàn

FMT_SMF.1 Đặc tả các chức năng quản lý

12.1.5.1 FMT_MOF.1.1

TSF cần hạn chế khả năng tới [lựa chọn: *xác định cơ chế hoạt động như là tắt, bật, thay đổi cơ chế hoạt động*] của các chức năng [chỉ định: *danh sách các chức năng] cho tới [chỉ định: các quy tắc định danh có thẩm quyền*].

12.2 Quản lý các thuộc tính an toàn (FMT_MSA)

12.2.1 Hành xử của họ

Họ này cho phép người dùng có thẩm quyền điều khiển qua việc quản lý các thuộc tính an toàn. Việc quản lý này phải bao gồm các khả năng hiển thị và thay đổi các thuộc tính an toàn.

12.2.2 Phân mức thành phần

FMT_MSA.1 Quản lý các thuộc tính an toàn, cho phép người dùng có thẩm quyền (các quy tắc) để quản lý các thuộc tính an toàn đã định rõ.

FMT_MSA.2 Các thuộc tính an toàn, đảm bảo rằng các giá trị được ấn định tới các thuộc tính an toàn là hợp lý và lưu ý tới trạng thái an toàn.

FMT_MSA.3 Khởi tạo thuộc tính tĩnh, đảm bảo rằng các giá trị mặc định của các thuộc tính an toàn hoặc là cho phép hoặc là hạn chế một cách thích hợp.

FMT_MSA.4 Kế thừa giá trị thuộc tính an toàn, cho phép quy tắc/chính sách xác định giá trị được thừa kế bởi một thuộc tính an toàn.

12.2.3 Quản lý của FMT_MSA.1

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

a) Quản lý nhóm các quy tắc mà có thể tương tác với các thuộc tính an toàn.

b) Quản lý các quy tắc xác định giá trị kế thừa bởi thuộc tính an toàn

12.2.4 Quản lý của FMT_MSA.2

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

a) Quản lý các quy tắc xác định giá trị kế thừa bởi thuộc tính an toàn

12.2.5 Quản lý của FMT_MSA.3

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

a) Quản lý nhóm các quy tắc mà có thể xác định các giá trị khởi tạo.

b) Quản lý việc thiết lập cho phép hoặc giới hạn các giá trị mặc định cho việc đưa ra điều khiển truy cập SFP.

c) Quản lý các quy tắc xác định giá trị kế thừa bởi thuộc tính an toàn

12.2.6 Quản lý của FMT_MSA.4

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

a) Đặc tả vai trò được phép thiết lập hoặc thay đổi thuộc tính an toàn.

12.2.7 Kiểm toán của FMT_MSA.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Cơ sở: Tất cả sự thay đổi các giá trị của các thuộc tính an toàn.

12.2.8 Kiểm toán của FMT_MSA.2

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Tất cả các giá trị từ chối và được quy định cho thuộc tính an toàn.

b) Chi tiết: tất cả các giá trị an toàn được quy định và chấp thuận cho thuộc tính an toàn.

12.2.9 Kiểm toán của FMT_MSA.3

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Cơ sở: Sự thay đổi các thiết lập mặc định của các quy tắc cho phép hoặc cấm.

b) Cơ sở: Tất cả sự thay đổi các giá trị khởi tạo của các thuộc tính an toàn.

12.2.10 Kiểm toán của FMT_MSA.3

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Sự thay đổi thuộc tính an toàn, có thể với và/hoặc giá trị thuộc tính an toàn đã được thay đổi.

12.2.11 FMT_MSA.1 Quản lý các thuộc tính an toàn

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc:

[FDP_ACC.1 Kiểm soát truy cập tập con, hoặc

FDP_IFC.1 Kiểm soát luồng thông tin tập con]

FMT_SMR.1 Các vai trò an toàn

FMT_SMF.1 Đặc tả các chức năng quản lý

12.2.11.1 FMT_MSA.1.1

TSF cần thực thi [chỉ định: *điều khiển truy cập SFP, điều khiển luồng thông tin SFP*] để hạn chế khả năng [lựa chọn: *thay đổi mặc định, yêu cầu, thay đổi, xóa, [chỉ định: các thuật toán khác*]] các thuộc tính an toàn [chỉ định: *danh sách các thuộc tính an toàn*] tới [chỉ định: *các vai trò đã xác định và cấp phép*].

12.2.12 FMT_MSA.2 Các thuộc tính an toàn

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: [FDP_ACC.1 Kiểm soát truy cập tập con, hoặc
FDP_IFC.1 Kiểm soát luồng thông tin tập con]
FMT_MSA.1 Quản lý các thuộc tính an toàn
FMT_SMR.1 Các vai trò an toàn

12.2.12.1 FMT_MSA.2.1

TSF cần đảm bảo rằng chỉ có những giá trị an toàn mới được chấp nhận cho [Chỉ định: *Danh sách các thuộc tính an toàn*].

12.2.13 FMT_MSA.3 Khởi tạo các thuộc tính tĩnh

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: FMT_MSA.1 Quản lý các thuộc tính an toàn
FMT_SMR.1 Các vai trò an toàn

12.2.13.1 FMT_MSA.3.1

TSF cần thực thi [chỉ định: *kiểm soát truy cập SFP, kiểmt soát luồng thông tin SFP*] để cung cấp [lựa chọn, chọn một trong: *ngăn cấm, cho phép, [chỉ định: thuộc tính khác*]] các giá trị mặc định cho các thuộc tính an toàn được sử dụng để thực thi SFP.

12.2.13.2 FMT_MSA.3.2

TSF cần cho phép [chỉ định: *các vai trò đã xác định và cấp phép*] để đặc tả các giá trị khởi tạo khác thay cho các giá trị mặc định khi một đối tượng hay thông tin được tạo.

12.2.14 FMT_MSA.4

Phân cấp từ: Không có thành phần khác

Các mối phụ thuộc: [FDP_ACC.1 Kiểm soát truy nhập tập con hoặc
FDP_IFC.1 Kiểm soát luồng thông tin tập con]

12.2.14.1 FMT_MSA.4.1

TSF cần sử dụng những quy tắc sau để thiết lập giá trị các thuộc tính an toàn: [chỉ định: *quy tắc cho các thiết lập giá trị của thuộc tính an toàn*].

12.3 Quản lý dữ liệu TSF (FMT_MTD)

12.3.1 Hành xử của họ

Họ này cho phép người dùng có thẩm quyền (các quy tắc) điều khiển qua quản lý dữ liệu TSF. Ví dụ dữ liệu TSF bao gồm thông tin kiểm toán, khóa, cấu hình hệ thống và các tham số cấu hình TSF khác.

12.3.2 Phân mức thành phần

FMT_MTD.1 Quản lý dữ liệu TSF, cho phép người dùng có thẩm quyền quản lý dữ liệu TSF.

FMT_MTD.2 Quản lý hạn chế trên dữ liệu TSF, xác định hành động được tạo ra nếu sự hạn chế dữ liệu TSF là đạt được hoặc vượt quá.

FMT_MTD.3 Dữ liệu TSF an toàn, đảm bảo rằng các giá trị được ấn định tới dữ liệu TSF là hợp lý với trạng thái an toàn.

12.3.3 Quản lý của FMT_MTD.1

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

a) Quản lý nhóm các quy tắc mà có thể tương tác với dữ liệu TSF.

12.3.4 Quản lý của FMT_MTD.2

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

a) Quản lý nhóm các quy tắc mà có thể tương tác với sự hạn chế trên dữ liệu TSF.

12.3.5 Quản lý của FMT_MTD.3

Không có các hoạt động quản lý nào.

12.3.6 Kiểm toán của FMT_MTD.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Cơ sở: Tất cả việc thay đổi giá trị của dữ liệu TSF.

12.3.7 Kiểm toán của FMT_MTD.2

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Cơ sở: Tất cả việc thay đổi tới việc hạn chế trên dữ liệu TSF.

b) Cơ sở: Tất cả việc thay đổi trong các hành động sinh ra trong trường hợp vi phạm sự hạn chế đó.

12.3.8 Kiểm toán của FMT_MTD.3

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Tất cả các giá trị bị từ chối của dữ liệu TSF

12.3.9 FMT_MTD.1 Quản lý dữ liệu TSF

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: FMT_SMR.1 Các vai trò an toàn

FMT_SMF.1 Đặc tả các chức năng quản lý

12.3.9.1 FMT_MTD.1.1

TSF cần hạn chế khả năng [sự lựa chọn: *thay đổi mặc định, thay đổi, xóa, xóa, [chỉ định: các thuật toán khác*]] [chỉ định: *danh sách dữ liệu TSF*] tới [chỉ định: *các vai trò đã xác định và cấp phép*].

12.3.10 FMT_MTD.2 Quản lý các hạn chế trên dữ liệu TSF

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: FMT_MTD.1 Quản lý dữ liệu TSF

FMT_SMR.1 Các vai trò an toàn

12.3.10.1 FMT_MTD.2.1

TSF cần hạn chế việc xác định hạn chế đối với [chỉ định: *danh sách dữ liệu TSF*] tới [chỉ định: *các vai trò đã xác định và cấp phép*]

12.3.10.2 FMT_MTD.2.2

TSF cần thực thi các hành động sau, nếu dữ liệu TSF là đạt hoặc vượt quá các hạn chế đã chỉ ra: [chỉ định: *các hành động cần được thực hiện*]

12.3.11 FMT_MTD.3 Dữ liệu TSF an toàn

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: FMT_MTD.1 Quản lý dữ liệu TSF.

12.3.11.1 FMT_MTD.3.1

TSF cần đảm bảo rằng chỉ có các giá trị an toàn mới được chấp nhận cho dữ liệu TSF.

12.4 Hủy bỏ (FMT_REV)

12.4.1 Hành xử của họ

Họ này đề cập đến việc hủy bỏ các thuộc tính an toàn đối với một vài thực thể trong TOE.

12.4.2 Phân mức thành phần

FMT_REV.1 Hủy bỏ, cung cấp cho việc hủy bỏ các thuộc tính an toàn được bắt buộc tại một vài mốc thời gian.

12.4.3 Quản lý của FMT_REV.1

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

a) Quản lý nhóm các quy tắc mà có thể giúp cho việc thu hồi các thuộc tính an toàn.

b) Quản lý danh sách người dùng, chủ đề, đối tượng và các nguồn khác cho việc có thể thu hồi.

c) Quản lý các quy tắc thụ hồi.

12.4.4 Kiểm toán của FMT_REV.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Việc thu hồi các thuộc tính an toàn là không thành công.

b) Cơ sở: Tất cả việc thử để hủy bỏ các thuộc tính an toàn

12.4.5 FMT_REV.1 Hủy bỏ

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: FMT_SMR.1 Các vai trò an toàn

12.4.5.1 FMT_REV.1.1

TSF cần hạn chế khả năng lấy lại [Chỉ định: *danh sách các thuộc tính an toàn*] liên quan tới [lựa chọn: *người dùng, chủ thể, đối tượng, [chỉ định: các tài nguyên bổ sung khác*]] dưới sự kiểm soát của TSC để [chỉ định: *các vai trò đã xác định và cấp phép*]

12.4.5.2 FMT_REV.1.2

TSF cần thực thi các quy tắc [chỉ định: *đặc tả các quy tắc hủy bỏ*]

12.5 Hết hạn thuộc tính an toàn (FMT_SAE)

12.5.1 Hành xử của họ

Họ này nhằm vào khả năng để thực thi các hạn chế về thời gian đối với giá trị các thuộc tính an toàn.

12.5.2 Phân mức thành phần

FMT_SAE.1 Giấy phép hạn chế thời gian, quy định khả năng đối với người dùng có thẩm quyền để xác định một thời gian tới hạn trên các thuộc tính an toàn đã xác định.

12.5.3 Quản lý của FMT_SAE.1

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

a) Quản lý danh sách các thuộc tính an toàn đối với giới hạn được trợ giúp.

b) Các hành động được thực hiện nếu thời gian tới hạn là đã qua

12.5.4 Kiểm toán của FMT_SAE.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Cơ sở: Xác định thời gian tới hạn đối với thuộc tính

b) Cơ sở: Hành động xảy ra đúng với giới hạn thời gian

12.5.5 FMT_SAE.1 Cấp phép hạn chế thời gian

Phân cấp từ: Không có thành phần nào khác

Các mối phụ thuộc: FMT_SMR.1 Các vai trò an toàn

FPT_STM.1 Nhãn thời gian tin cậy

12.5.5.1 FMT_SAE.1.1

TSF cần hạn chế khả năng để xác định thời gian tới hạn đối với [chỉ định: *danh sách các thuộc tính an toàn đối với giới hạn được trợ giúp*] để [chỉ định: *các vai trò đã xác định và cấp phép*]

12.5.5.2 FMT_SAE.1.2

Đối với mỗi thuộc tính an toàn này, TSF cần có khả năng [chỉ định: *danh sách các hành động thực hiện đối với mỗi thuộc tính an toàn*] sau khi thời gian tới hạn cho thuộc tính an toàn được chỉ định đã qua.

12.6 Đặc tả các chức năng quản lý (FMT_SMF)

12.6.1 Hành xử của họ

Họ này cho phép việc xác định các chức năng quản lý được quy định bởi TOE. Các chức năng quản lý TFI cho phép người quản trị xác định các tham số để điều khiển hoạt động của các lĩnh vực liên quan

đến an toàn của TOE, như là: các thuộc tính bảo vệ dữ liệu để xác định các tham số để điều khiển thuật toán lĩnh vực liên quan đến an toàn của TOE, như là: thuộc tính bảo vệ dữ liệu, thuộc tính bảo vệ TOE, thuộc tính kiểm tra, các thuộc tính xác thực và định danh. Các chức năng quản lý cũng bao gồm các chức năng đó được thực thi bởi một người điều khiển để đảm bảo rằng hành động tiếp theo của TOE, như là sao lưu và phục hồi. Họ này làm việc trong sự kết hợp với các thành phần khác trong FMT: Các lớp quản lý an toàn: thành phần trong họ này gọi là các chức năng quản lý, và các họ khác trong FMT: quản lý an toàn hạn chế khả năng sử dụng các chức năng quản lý này.

12.6.2 Phân mức thành phần

FMT_SMF.1 Đặc tả các chức năng quản lý, yêu cầu TSF cung cấp các chức năng quản lý cụ thể.

12.6.3 Quản lý của FMT_SMF.1

Không có các hoạt động quản lý nào.

12.6.4 Kiểm toán của FMT_SMF.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Sử dụng các chức năng quản lý

12.6.5 FMT_SMF.1 Định rõ các chức năng quản lý

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: Không có sự phụ thuộc nào

12.6.5.1 FMT_SMF.1.1

TSF cần có khả năng thực thi các chức năng quản lý an toàn sau: [chỉ định: *danh sách các chức năng quản lý an toàn được quy định bởi TSF*]

12.7 Các quy tắc quản lý an toàn (FMT_SMR)

12.7.1 Hành xử của họ

Họ này là được dùng để điều khiển việc ấn định các quy tắc khác nhau tới người dùng. Các khả năng của các quy tắc này với khía cạnh quản lý an toàn được miêu tả trong các họ khác trong lớp.

12.7.2 Phân mức thành phần

FMT_SMR.1 Các vai trò an toàn xác định các vai trò với các khía cạnh an toàn mà TSF thừa nhận.

FMT_SMR.2 Hạn chế về các vai trò an toàn, xác định rằng ngoài việc đặc tả các vai trò, còn có các quy tắc kiểm soát các mối quan hệ giữa các vai trò.

FMT_SMR.3 Chỉ định các vai trò, yêu cầu rõ ràng được đưa ra tới TSF để thừa nhận một quy tắc.

12.7.3 Quản lý của FMT_SMR.1

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

a) Quản lý nhóm người dùng là một phần của quy tắc.

12.7.4 Quản lý của FMT_SMR.2

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

a) Quản lý nhóm người dùng là một phần của quy tắc

b) Quản lý các điều kiện mà các quy tắc phải thỏa mãn

12.7.5 Quản lý của FMT_SMR.3

Không có các hoạt động quản lý nào.

12.7.6 Kiểm toán của FMT_SMR.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: sự thay đổi tới nhóm người dùng là một phần của quy tắc

b) Chi tiết: mọi việc sử dụng quyền lợi của quy tắc.

12.7.7 Kiểm toán của FMT_SMR.2

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: sự thay đổi các nhóm người dùng là một phần của quy tắc

b) Tối thiểu: Việc thử sử dụng các quy tắc không thành công giúp đưa ra các điều kiện trên quy tắc đó.

c) Chi tiết: mọi việc sử dụng quyền của quy tắc.

12.7.8 Kiểm toán của FMT_SMR.3

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Yêu cầu rõ ràng nhằm thừa nhận một quy tắc

12.7.9 FMT_SMR.1Các quy tắc an toàn

Phân cấp từ: Không có thành phần nào

Các mối phụ thuộc: FIA_UID.1 Định thời cho định danh

12.7.9.1 FMT_SMR.1.1

TSF cần duy trì các vai trò [chỉ định: *các vai trò đã xác định và cấp phép*]

12.7.9.2 FMT_SMR.1.2

TSF cần có khả năng liên kết người dùng với các vai trò.

12.7.10 FMT_SMR.2 Hạn chế về các vai trò an toàn

Phân cấp từ: FMT_SMR.1 Các vai trò an toàn

Các mối phụ thuộc: FIA_UID.1 Định thời cho định danh

12.7.10.1 FMT_SMR.2.1

TSF cần duy trì các vai trò : [chỉ định: *các vai trò đã xác định và **cấp phép***]

12.7.10.2 FMT_SMR.2.2

TSF cần có khả năng liên kết người dùng với vai trò.

12.7.10.3 FMT_SMR.2.3

TSF cần đảm bảo rằng các điều kiện [chỉ định: *các điều kiện cho các vai trò khác nhau*] được thỏa mãn.

12.7.11 FMT_SMR.3 Chỉ định các vai trò

Phân cấp từ: Không có thành phần nào

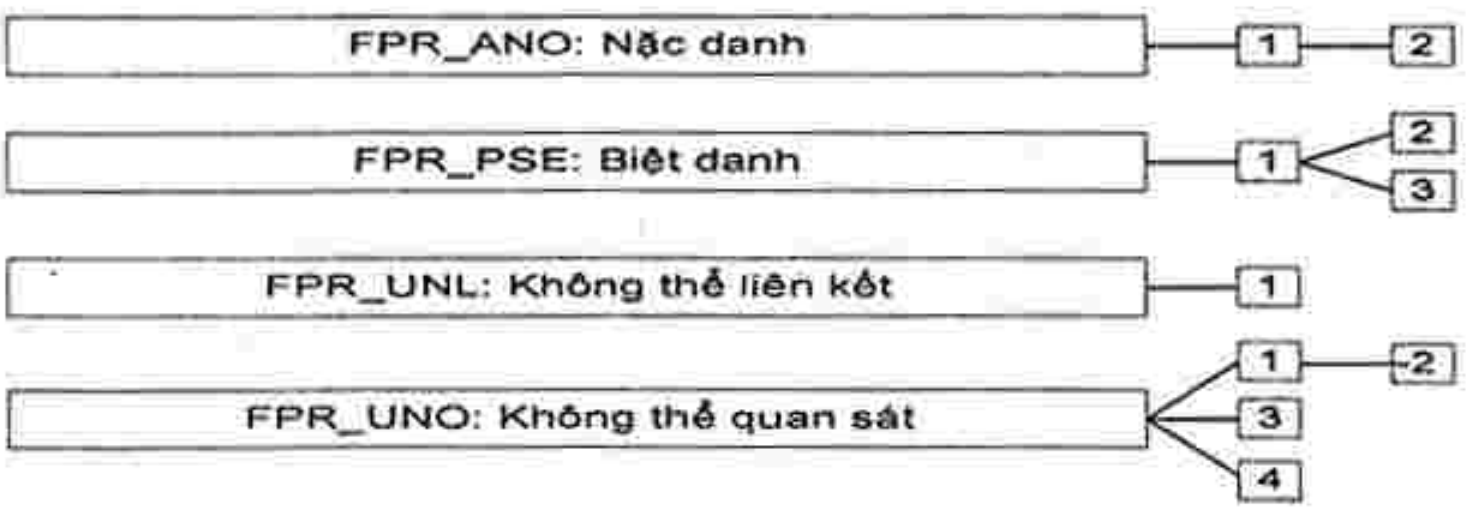
Các mối phụ thuộc: FMT_SMR.1 Các vai trò an toàn

12.7.11.1 FMT_SMR.3.1

TSF cần có một yêu cầu rõ ràng để thừa nhận các vai trò sau: [chỉ định: *các vai trò*].

13 Lớp FPR: Riêng tư

Lớp này chứa các yêu cầu riêng tư. Các yêu cầu này giúp bảo vệ người dùng chống tiết lộ và lợi dụng danh tính các người dùng khác.



Hình 13 - Phân cấp lớp FPR: Riêng tư

13.1 Nặc danh (FPR_ANO)

13.1.1 Hành xử của họ

Họ này cho phép người dùng có thể sử dụng một tài nguyên hoặc dịch vụ không cần biết định danh người dùng. Các yêu cầu nặc danh phục vụ cho bảo vệ danh tính người dùng. Nặc danh không dự tính để bảo vệ danh tính chủ thể.

13.1.2 Phân mức thành phần

FPR_ANO.1 Nặc danh, yêu cầu các người dùng khác hoặc các chủ thể khác không được có khả năng xác định danh tính một người dùng trong phạm vi một chủ thể hoặc một hoạt động.

FPR_ANO.2 Nặc danh không niu kéo thông tin, cải thiện các yêu cầu của FPR_ANO.1 Nặc danh bằng cách đảm bảo rằng TSF không hỏi danh tính người dùng.

13.1.3 Quản lý của FPR_ANO.1, FPR_ANO.2

Không có hoạt động quản lý nào.

13.1.4 Kiểm toán của FPR_ANO.1, FPR_ANO.2

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

b) Tối thiểu: Viện dẫn cơ chế nặc danh.

13.1.5 FPR_ANO.1 Nặc danh

Phân cấp tới: Không có các thành phần nào

Các mối phụ thuộc: Không có

13.1.5.1 FPR_ANO.1.1

TSF cần đảm bảo rằng [chỉ định: *tập các người dùng và/hoặc chủ thể*] không có khả năng xác định tên người dùng thật ràng buộc tới [chỉ định: *danh sách các chủ thể và/hoặc hoạt động và/hoặc đối tượng*].

13.1.6 FPR_ANO.2 Nặc danh không có thông tin níu kéo

Phân cấp tới: FPR_ANO.1 Nặc danh

Các mối phụ thuộc: Không có

13.1.6.1 FPR_ANO.2.1

TSF cần đảm bảo rằng [chỉ định: *tập các người dùng và/hoặc chủ thể*] không có khả năng xác định tên người dùng thật ràng buộc tới [chỉ định: *danh sách các chủ thể và/hoặc hoạt động và/hoặc đối tượng*].

13.1.6.2 FPR_ANO.2.2

TSF cần cho [chỉ định: *danh sách các dịch vụ*] tới [chỉ định: *danh sách các chủ thể*] không có bất kỳ tham chiếu níu kéo nào đến tên thật của người dùng.

13.2 Biệt danh (FPR_PSE)

13.2.1 Hành xử của họ

Họ này đảm bảo rằng một người dùng sử dụng một tài nguyên hoặc dịch vụ không để lộ danh tính người dùng, song vẫn có thể chịu trách nhiệm về việc sử dụng.

13.2.2 Phân mức thành phần

FPR_PSE.1 Biệt danh yêu cầu một tập các người dùng và/hoặc chủ thể không được có khả năng xác định danh tính người dùng ràng buộc bởi một chủ thể hoặc hoạt động, song người dùng này vẫn phải chịu trách nhiệm về các hành động của họ.

FPR_PSE.2 Biệt danh nghịch đảo yêu cầu TSF có năng lực xác định danh tính người dùng chính thức dựa trên một bí danh đã quy định.

FPR_PSE.3 Biệt danh dấu tên yêu cầu TSF theo dõi các quy tắc cấu trúc nhất định cho bí danh để định danh người dùng.

13.2.3 Quản lý của FPR_PSE.1, FPR_PSE.2, FPR_PSE.3

Không có các hoạt động quản lý nào.

13.2.4 Kiểm toán của FPR_PSE.1, FPR_PSE.2, FPR_PSE.3

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

b) Tối thiểu: Chủ thể/người dùng được yêu cầu kiểm toán danh tính người dùng.

13.2.5 FPR_PSE.1 Biệt danh

Phân cấp tới: Không có thành phần nào.

Các mối phụ thuộc: Không có

13.2.5.1 FPR_PSE.1.1

TSF cần đảm bảo rằng [chỉ định: *tập các người dùng và/hoặc chủ thể*] không có khả năng xác định tên người dùng thật ràng buộc tới [chỉ định: *danh sách các chủ thể và/hoặc hoạt động và/hoặc đối tượng*].

13.2.5.2 FPR_PSE.1.2

TSF cần khả năng cho [chỉ định: *số các bí danh*] bí danh của tên người dùng thật tới [chỉ định: *danh sách các chủ thể*] .

13.2.5.3 FPR_PSE.1.3

TSF cần [Chọn lựa, chọn một trong: *Xác định một bí danh cho người dùng, chấp nhận các bí danh từ người dùng và kiểm tra xem nó có tuân thủ theo [chỉ định: đơn vị bí danh*] .

13.2.6 FPR_PSE.2 Biệt danh nghịch đảo

Phân cấp tới: FPR_PSE.1 Biệt danh

Các mối phụ thuộc: FIA_UID.1 Định thời cho định danh

13.2.6.1 FPR_PSE.2.1

TSF cần đảm bảo rằng [chỉ định: *tập các người dùng và/hoặc chủ thể*] không có khả năng xác định tên người dùng thật ràng buộc với [chỉ định: *danh sách các chủ thể và/hoặc hoạt động và/hoặc đối tượng*].

13.2.6.2 FPR_PSE.2.2

TSF cần khả năng cho [chỉ định:số các bí danh] bí danh của tên người dùng thật tới [chỉ định:danh sách các chủ thể]

13.2.6.3 FPR_PSE.2.3

TSF cần [Chọn lựa, chọn một trong: *Xác định một bí danh cho người dùng, chấp nhận các bí danh từ người dùng*] và kiểm tra xem nó có tuân thủ theo [chỉ định: *đơn vị bí danh*] .

13.2.6.4 FPR_PSE.2.4

TSF cần cung cấp [Chọn lựa : *một người dùng có thẩm quyền, [chỉ định:danh sách các chủ thể tin cậy]*] có năng lực xác định danh tính người dùng dựa trên các bí danh đã quy định chỉ trong điều kiện sau [chỉ định: *danh sách các điều kiện*] .

13.2.7 FPR_PSE.3 Biệt danh bí danh

Phân cấp tới: FPR_PSE.1 Biệt danh.

Các mối phụ thuộc: Không có.

13.2.7.1 FPR_PSE.3.1

TSF cần đảm bảo rằng [chỉ định: *tập các người dùng và/hoặc chủ thể*] không có khả năng xác định tên người dùng thật ràng buộc với [chỉ định: *danh sách các chủ thể và/hoặc hoạt động và/hoặc đối tượng*].

13.2.7.2 FPR_PSE.3.2

TSF cần có khả năng cung cấp [chỉ định: *số các bí danh*] bí danh của tên người dùng thật tới [chỉ định: *danh sách các chủ thể*].

13.2.7.3 FPR_PSE.3.3

TSF cần [Chọn lựa, chọn một trong: *Xác định một bí danh cho người dùng, chấp nhận các bí danh từ người dùng*] và kiểm tra xem nó có tuân thủ theo [chỉ định: *đơn vị bí danh*].

13.2.7.4 FPR_PSE.3.4

TSF cần cung cấp một bí danh tới một tên người dùng thật và bí danh này cần trùng với bí danh cho trước theo điều kiện [chỉ định: *danh sách các điều kiện*], nếu không bí danh đã quy định cần không liên quan đến bí danh đã quy định trước đó.

13.3 Tính không thể liên kết (FPR_UNL)

13.3.1 Hành xử của họ

Họ này đảm bảo rằng một người dùng có thể sử dụng nhiều lần các tài ngiuyên và dịch vụ và không có khả năng liên kết các sử dụng đó với nhau được.

13.3.2 Phân mức thành phần

FPR_UNL.1 Tính không thể liên kết yêu cầu người dùng / chủ thể không được có khả năng xác định xem có đúng là cùng một người dùng đã gây ra các hoạt động đặc trưng xác định trong hệ thống.

13.3.3 Quản lý của FPR_UNL.1

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

b) Quản lý chức năng không thể liên kết.

13.3.4 Kiểm toán của FPR_UNL.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

b) Tối thiểu: Viện dẫn cơ chế không thể liên kết.

13.3.5 FPR_UNL1.1 Tính không thể liên kết

Phân cấp tới: Không có thành phần nào.

Các mối phụ thuộc: Không có.

13.3.5.1 FPR_UNL.1.1

TSF cần đảm bảo rằng [chỉ định: *tập các người dùng và/hoặc chủ thể*] không có khả năng xác định xem [chỉ định: *danh sách các hoạt động*][lựa chọn: *gây ra bởi cùng người dùng, liên quan như sau [chỉ định: danh sách các quan hệ]]*.

13.4 Tính không thể quan sát (FPR_UNO)

13.4.1 Hành xử của họ

Họ này đảm bảo rằng một người dùng có thể sử dụng một tài nguyên hoặc dịch vụ mà không có người nào khác, đặc biệt là đối tác thứ ba, có khả năng quan sát được tài nguyên hoặc dịch vụ đang sử dụng.

13.4.2 Phân mức thành phần

FPR_UNO.1 Tính không thể quan sát yêu cầu các người dùng và/hoặc chủ thể không được có khả năng xác định xem một hoạt động nào đang được thực hiện.

FPR_UNO.2 Tính không thể quan sát ảnh hưởng cấp phát thông tin yêu cầu TSF quy định các cơ chế xác định để tránh việc tập trung các thông tin liên quan đến sự riêng tư bên trong TOE. Sự tập trung đó có thể ảnh hưởng đến tính không thể quan sát nếu xảy ra một thỏa hiệp an toàn thông tin.

FPR_UNO.3 Tính không thể quan sát không có thông tin níu kéo yêu cầu TSF không được thử tìm cách lấy thông tin liên quan riêng tư để dùng cho thỏa hiệp tính không thể quan sát được.

FPR_UNO.4 Tính quan sát được người dùng có thẩm quyền yêu cầu TSF quy định một hoặc nhiều người dùng có thẩm quyền, có năng lực quan sát sự sử dụng các tài nguyên và/hoặc dịch vụ.

13.4.3 Quản lý của FPR_UNO.1, FPR_UNO.2

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

a) Quản lý hành vi của chức năng không thể quan sát được.

13.4.4 Quản lý của FPR_UNO.3

Không có các hành động quản lý nào.

13.4.5 Quản lý của FPR_UNO.4

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

a) Danh sách các người dùng có thẩm quyền có khả năng xác định việc xảy ra các hoạt động.

13.4.6 Kiểm toán của FPR_UNO.1, FPR_UNO.2

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Viện dẫn cơ chế cho tính không thể quan sát được.

13.4.7 Kiểm toán của FPR_UNO.3

Không có các sự kiện kiểm toán nào.

13.4.8 Kiểm toán của FPR_UNO.4

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: Quan sát việc sử dụng một tài nguyên hoặc dịch vụ bởi một người dùng hoặc một chủ thể.

13.4.9 FPR_UNO.1 Tính không thể quan sát

Phân cấp từ: Không có các thành phần nào

Các mối phụ thuộc: Không có

13.4.9.1 FPR_UNO.1.1

TSF cần đảm bảo rằng [chỉ định: *danh sách các người dùng và/hoặc chủ thể*] không có khả năng quan sát được hoạt động [chỉ định: *danh sách các hoạt động*] trên [chỉ định: *danh sách các đối tượng*] thông qua [chỉ định: *danh sách các người dùng và/hoặc chủ thể được bảo vệ*].

13.4.10 FPR_UNO.2 Tính không thể quan sát ảnh hưởng đến cấp phát thông tin

Phân cấp từ: FPR_UNO.1 Tính không thể quan sát

Các mối phụ thuộc: không có.

13.4.10.1 FPR_UNO.2.1

TSF cần đảm bảo rằng [chỉ định: *danh sách các người dùng và/hoặc chủ thể*] không có khả năng quan sát được hoạt động [Chỉ định: *danh sách các hoạt động*] trên [Chỉ định: *danh sách các đối tượng*] thông qua [Chỉ định: *danh sách các người dùng và/hoặc chủ thể được bảo vệ*].

13.4.10.2 FPR_UNO.2.2

TSF cần cấp phát [Chỉ định: *Thông tin liên quan tính không thể quan sát được*] trong số các phần của TOE sao cho điều kiện sau được giữ suốt thời gian tồn tại của thông tin [Chỉ định: *danh sách các điều kiện*].

13.4.11 FPR_UNO.3 Tính không thể quan sát không có thông tin níu kéo

Phân cấp từ: Không có thành phần nào.

Các mối phụ thuộc: FPR_UNO.1 Tính không thể quan sát.

13.4.11.1 FPR_UNO.3.1

TSF cần quy định [Chỉ định: *danh sách các dịch vụ*] cho [Chỉ định: *danh sách các chủ thể*] không níu kéo tham chiếu đến [Chỉ định: *thông tin liên quan tính riêng tư*].

13.4.12 FPR_UNO.4 Tính quan sát được người dùng có thẩm quyền

Phân cấp từ: Không có thành phần nào.

Các mối phụ thuộc: không có.

13.4.12.1 FPR_UNO.4.1

TSF cần quy định [Chỉ định: *tập các người dùng có thẩm quyền*] với năng lực quan sát việc sử dụng của [Chỉ định: *danh sách các tài nguyên và/hoặc dịch vụ*].

14 Lớp FPT: bảo vệ TSF

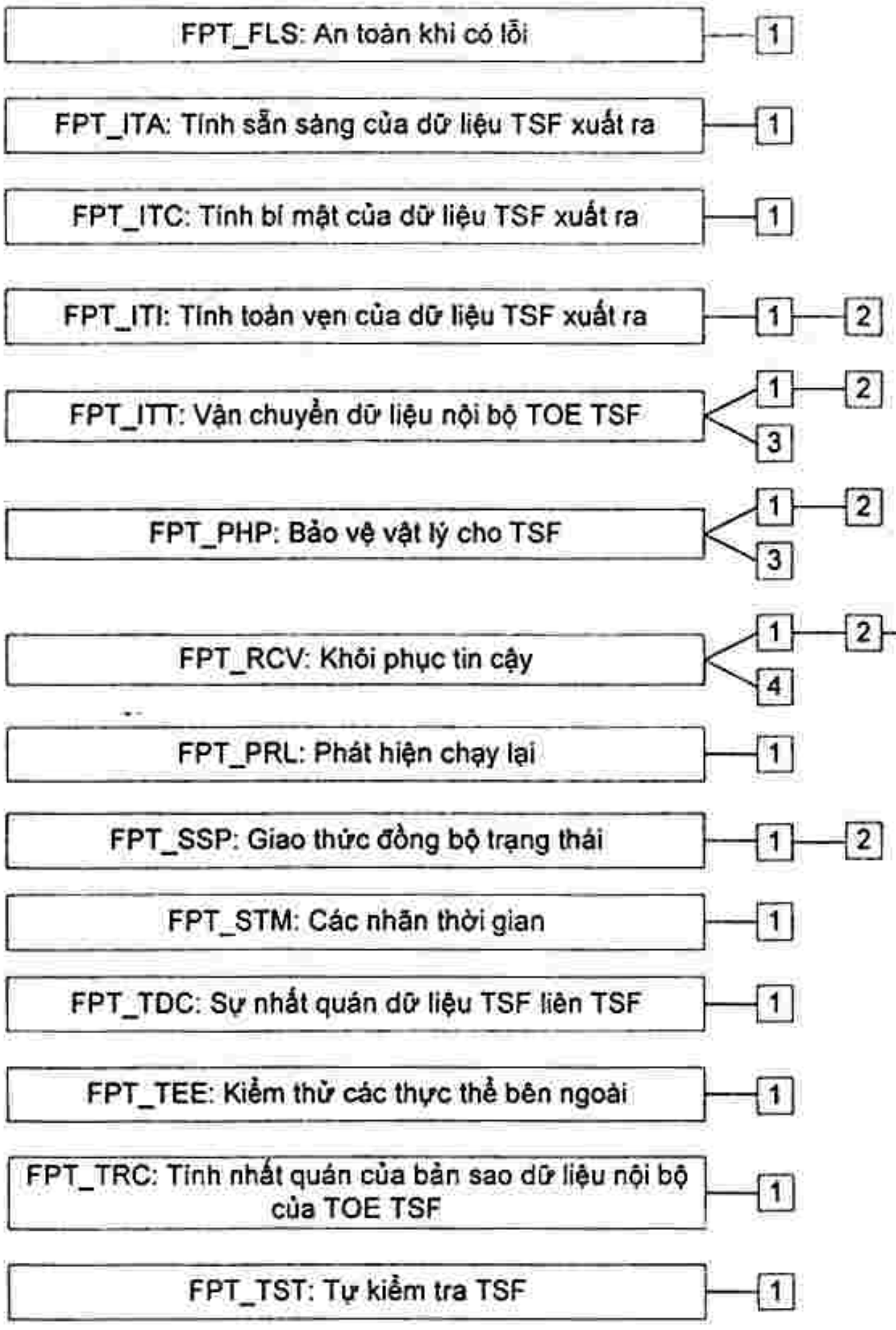
Lớp này bao gồm các họ yêu cầu chức năng liên quan đến tính toàn vẹn và sự quản lý của các cơ chế tạo thành TSF và tính toàn vẹn của dữ liệu TSF. Trong một số trường hợp, các họ trong lớp này có thể xuất hiện trong các thành phần lặp lại trong FDP: Lớp bảo vệ dữ liệu người dùng; chúng có thể được triển khai bằng việc sử dụng các cơ chế giống nhau. Mặc dù vậy, FDP: Bảo vệ dự liệu người dùng tập trung vào bảo vệ dữ liệu người dùng, trong khi FPT: bảo vệ TSF tập trung vào bảo vệ dữ liệu TSF. Thực tế, các thành phần trong FPT: Bảo vệ lớp TSF là cần thiết để đưa ra các yêu cầu mà các SFP trong TOE không thể bị xâm phạm hoặc vượt qua.

Từ việc xem xét lớp này, liên quan đến TSF, có ba phần tử quan trọng:

a) Việc triển khai TSF, trong đó thực hiện và triển khai các cơ chế để thực thi các SFR.

b) Dữ liệu TSF, đó là các cơ sở dữ liệu quản trị dùng để hướng dẫn thực thi các SFR.

c) Các thực thể bên ngoài mà TSF có thể tương tác với để thực thi các SFR.



Hình 14 – Sự phân cấp lớp FPT: Bảo vệ TSF

14.1 An toàn khi có lỗi (FPT_FLS)

14.1.1 Hành xử của họ

Các yêu cầu của họ này đảm bảo rằng TOE sẽ luôn thực thi các SFR của nó trong sự xuất hiện các danh mục lỗi trong TSF.

14.1.2 Phân mức thành phần

Họ này bao gồm chỉ một thành phần, FPT_FLS.1 Lỗi với sự bảo toàn trạng thái an toàn, yêu cầu TSF duy trì một trạng thái an toàn khi đối mặt với các lỗi được xác định.

14.1.3 Quản lý của FPT_FLS.1

Không có các hoạt động quản lý nào.

14.1.4 Kiểm toán của FPT_FLS.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Cơ sở: lỗi của TSF.

14.1.5 FPT_FLS.1 Lỗi với bảo toàn trạng thái an toàn

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

14.1.5.1 FPT_FLS.1.1

TSF cần phải duy trì một trạng thái an toàn khi xảy ra các kiểu lỗi sau: [chỉ định: *danh sách các loại lỗi trong TSF*] .

14.2 Tính sẵn sàng xuất dữ liệu TSF (FPT_ITA)

14.2.1 Hành xử của họ

Họ này định nghĩa các quy tắc cho việc duy trì tính sẵn sàng chuyển dữ liệu TSF giữa TSF và một sản phẩm IT tin cậy khác. Dữ liệu này, ví dụ là dữ liệu quan trọng của TSF như là mật khẩu, khoá, dự liệu kiểm toán hoặc mã thực thi TSF.

14.2.2 Phân mức thành phần

Họ này bao gồm chỉ một thành phần FPT_ITA.1 Tính sẵn sàng liên-TSF trong khoảng đơn vị đo tính sẵn sàng được định nghĩa trước. Thành phần này yêu cầu TSF đảm bảo, với một mức độ xác định có thể xảy ra, tính sẵn sàng của dữ liệu TSF quy định cho một sản phẩm IT tin cậy khác.

14.2.3 Quản lý của FPT_ITA.1

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

a) quản lý danh sách các loại dữ liệu TSF phản sẵn sàng đối với một sản phẩm IT tin cậy khác.

14.2.4 Kiểm toán của FPT_ITA.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: sự thiếu dữ liệu TSF khi được yêu cầu bởi một TOE.

14.2.5 FPT_ITA.1 Tính sẵn sàng liên TSF trong hệ tính sẵn sàng được định nghĩa.

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

14.2.5.1 FPT_ITA.1.1

TSF cần đảm bảo tính sẵn sàng của [chỉ định: *danh sách các kiểu dữ liệu TSF*] quy định cho một sản phẩm IT tin cậy khác trong [chỉ định: *một đơn vị đo tính sẵn sàng được định nghĩa trước*] đưa ra theo các điều kiện [chỉ định: *các điều kiện đảm bảo tính sẵn sàng*].

14.3 Tính bí mật của dữ liệu TSF xuất ra (FPT_ITC)

14.3.1 Hành xử của họ

Họ này định nghĩa các quy tắc bảo vệ dữ liệu từ việc xâm phạm không có quyền vào dữ liệu trong khi truyền giữa TSF và một sản phẩm IT tin cậy khác. Dữ liệu này có thể, ví dụ dữ liệu quan trọng của TSF như mật khẩu, mã khoá, dữ liệu kiểm toán hoặc mã thực thi TSF.

14.3.2 Phân mức thành phần

Họ này bao gồm chỉ một thành phần, FPT_ITC.1 Tính bí mật liên-TSF trong quá trình truyền tải, đòi hỏi TSF bảo đảm rằng dữ liệu được truyền giữa TSF và một sản phẩm IT tin cậy khác được bảo vệ khỏi xâm phạm trong quá trình truyền.

14.3.3 Quản lý của FPT_ITC.1

Không có các hoạt động quản lý nào.

14.3.4 Kiểm toán của FPT_ITC.1

Không có các hoạt động quản lý nào.

14.3.5 FPT_ITC.1 Độ tin cậy liên TSF trong quá trình truyền tải

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

14.3.5.1 FPT_ITC.1.1

TSF cần bảo vệ tất cả dữ liệu TSF được truyền từ TSF đến một sản phẩm IT tin cậy khác khỏi sự xâm phạm bất hợp pháp trong quá trình truyền.

14.4 Tính toàn vẹn của dữ liệu TSF xuất ra (FPT_ITI)

14.4.1 Hành xử của họ

Họ này định nghĩa các quy tắc bảo vệ khỏi sự thay đổi bất hợp pháp dữ liệu TSF trong quá trình truyền giữa TSF và một sản phẩm IT tin cậy khác. Dữ liệu này ví dụ là dữ liệu TSF quan trọng như mật khẩu, mã khoá, dữ liệu kiểm toán hoặc mã thực thi TSF.

14.4.2 Phân mức thành phần

FPT_ITI.1 Phát hiện sửa đổi liên-TSF, cung cấp khả năng phát hiện sự thay đổi dữ liệu TSF trong quá trình truyền giữa TSF và sản phẩm IT tin cậy khác, với giả thiết rằng sản phẩm IT tin cậy khác đó có nhận biết được cơ chế sử dụng.

FPT_ITI.2 Phát hiện và chỉnh sửa thay đổi liên-TSF, cung cấp khả năng cho một sản phẩm IT tin cậy khác không những phát hiện sự thay đổi mà còn sửa sự thay đổi dữ liệu với giả thiết rằng sản phẩm IT tin cậy khác đó có nhận biết được chế độ sử dụng.

14.4.3 Quản lý của FPT_ITI.1

Không có các hoạt động quản lý nào.

14.4.4 Quản lý của FPT_ITI.2

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

a) quản lý các kiểu dữ liệu TSF mà TSF có thể sửa chữa sự thay đổi trong quá trình truyền.

b) quản lý các kiểu hoạt động mà TSF có thể thực hiện nếu dữ liệu TSF bị thay đổi trong quá trình truyền.

14.4.5 Kiểm toán của FPT_ITI.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: phát hiện sự thay đổi dữ liệu TSF trong quá trình truyền.

b) Cơ sở: hoạt động đưa ra dựa trên phát hiện sự thay đổi dữ liệu TSF trong quá trình truyền.

14.4.6 Kiểm toán của FPT_ITI.2

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: phát hiện sự thay đổi dữ liệu TSF trong quá trình truyền.

b) Cơ sở: hành động đưa ra dựa theo phát hiện sự thay đổi dữ liệu TSF được truyền.

c) Cơ sở: sử dụng các cơ chế sửa lỗi.

14.4.7 FPT_ITI.1 Phát hiện sự thay đổi liên-TSF

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

14.4.7.1 FPT_ITI.1.1

TSF cần cung cấp khả năng phát hiện sự thay đổi của tất cả dữ liệu TSF trong quá trình truyền giữa TSF và một sản phẩm IT tin cậy từ xa với với hệ: [chỉ định: *một đơn vị thay đổi xác định*].

14.4.7.2 FPT_ITI.1.2

TSF cần cung cấp khả năng kiểm tra tính toàn vẹn của tất cả dữ liệu TSF được truyền giữa TSF và một sản phẩm IT tin cậy từ xa và thực hiện [chỉ định: *hoạt động cần thực hiện*] nếu sự thay đổi được phát hiện.

14.4.8 FPT_ITI.2 Phát hiện và chỉnh sửa thay đổi liên-TSF

Phân cấp từ: FPT_ITI.1 Phát hiện sự thay đổi liên-TSF

Các mối phụ thuộc: Không có sự phụ thuộc.

14.4.8.1 FPT_ITI.2.1

TSF cần cung cấp khả năng phát hiện sự thay đổi của tất cả dữ liệu TSF trong quá trình truyền giữa TSF và một sản phẩm IT tin cậy khác trong theo hệ sau: [chỉ định: *một đơn vị thay đổi xác định*]

14.4.8.2 FPT_ITI.2.2

TSF cần cung cấp khả năng kiểm tra tính toàn vẹn của tất cả dữ liệu truyền giữa TSF và một sản phẩm IT tin cậy khác và thực hiện [chỉ định: *hành động được đưa ra*] nếu phát hiện sự thay đổi.

14.4.8.3 FPT_ITI.2.3

TSF cần cung cấp khả năng sửa lỗi [chỉ định: *kiểu thay đổi*] của tất cả dữ liệu TSF được truyền giữ TSF và một sản phẩm IT tin cậy khác.

14.5 Vận chuyển dữ liệu nội bộ TOE TSF (FPT_ITT)

14.5.1 Hành xử của họ

Họ này đưa ra các yêu cầu đề cập đến việc bảo vệ dữ liệu TSFkhi nó được truyền giữa các phần khác nhau bên trong TOE qua một kênh nội bộ.

14.5.2 Phân mức thành phần

FPT_ITT.1 Bảo vệ vận chuyển dữ liệu nội bộ TSF, yêu cầu dữ liệu TSF được bảo vệ khi truyền giữa các phần khác nhau trong TOE.

FPT_ITT.2 Phân chia vận chuyển dữ liệu, yêu cầu TSF phân chia dữ liệu người dùng từ dữ liệu TSF trong quá trình truyền.

FPT_ITT.3 Giám sát tính toàn vẹn dữ liệu, yêu cầu dữ liệu TSF được truyền giữa các phần khác nhau của TOE được giám sát các lỗi về toàn vẹn xác định trước.

14.5.3 Quản lý của FPT_ITT.1

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

a) quản lý các loại chống sự thay đổi mà TSF cần bảo vệ;

b) quản lý các cơ chế sử dụng để cung cấp khả năng bảo vệ dữ liệu trong quá trình truyền giữa các phần khác nhau của TSF.

14.5.4 Quản lý của FPT_ITT.2

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

a) quản lý các loại chống lại sự thay đổi mà TSF bảo vệ.

b) quản lý các cơ chế sử dụng để cung cấp khả năng bảo vệ dữ liệu trong quá trình truyền giữa các phần khác nhau của TSF.

c) quản lý cơ chế phân chia.

14.5.5 Quản lý của FPT_ITT.3

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

a) quản lý các loại chống lại sự thay đổi mà TSF bảo vệ.

b) quản lý các cơ chế sử dụng để cung cấp khả năng bảo vệ dữ liệu trong quá trình truyền giữa các phần khác nhau của TSF.

c) quản lý các kiểu thay đổi dữ liệu TSF mà TSF cần phát hiện.

d) quản lý các hoạt động được đưa ra.

14.5.6 Kiểm toán của FPT_ITT.1, FPT_ITT.2

Không có sự kiện có thể kiểm toán nào.

14.5.7 Kiểm toán của FPT_ITT.3

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST :

a) Tối thiểu: phát hiện ra sự thay đổi dữ liệu TSF;

b) Cơ sở: đưa ra hành động dựa theo sự phát hiện lỗi toàn vẹn.

14.5.8 FPT_ITT.1 Bảo vệ vận chuyển dữ liệu nội bộ TSF cơ bản

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

14.5.8.1 FPT_ITT.1.1

TSF cần bảo vệ dữ liệu TSF từ [lựa chọn: *xâm phạm, thay đổi*] khi nó được truyền giữa các phần khác nhau của TOE.

14.5.9 FPT_ITT.2 Phân chia vận chuyển dữ liệu TSF

Phân cấp từ: FPT_ITT.1 Bảo vệ vận chuyển dữ liệu nội bộ TSF cơ bản.

Các mối phụ thuộc: Không có sự phụ thuộc.

14.5.9.1 FPT_ITT.2.1

TSF cần bảo vệ dữ liệu từ [lựa chọn: *xâm phạm, thay đổi*] khi nó được truyền giữa các phần khác nhau của TOE.

14.5.9.2 FPT_ITT.2.2

TSF cần phân tách dữ liệu người dùng từ dữ liệu TSF khi dữ liệu đó được truyền giữa các phần khác nhau của TOE.

14.5.10 FPT_ITT.3 Giám sát tính toàn vẹn dữ liệu TSF

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FPT_ITT.1 Bảo vệ vận chuyển dữ liệu nội bộ TSF cơ bản.

14.5.10.1 FPT_ITT.3.1

TSF cần có khả năng phát hiện [lựa chọn: *thay đổi dữ liệu, thay thế dữ liệu, sắp xếp lại dữ liệu, xoá dữ liệu,[chỉ định: các lỗi toàn vẹn khác]*] đối với dữ liệu TSF được truyền giữa các thành phần khác nhau của TOE.

14.5.10.2 FPT_ITT.3.2

Khi phát hiện lỗi toàn vẹn dữ liệu, TSF cần thực hiện các hành động sau: [Chỉ định: *xác định hành động cần thực hiện*].

14.6 Bảo vệ vật lý TSF (FPT_PHP)

14.6.1 Hành xử của họ

Bảo vệ các thành phần vật lý TSF tham chiếu đến giới hạn quyền truy nhập vật lý đến TSF, và sự ngăn chặn chúng, và bảo vệ trước thay đổi vật lý trái phép, hoặc thay thế trong TSF.

Các yêu cầu đối với các thành phần trọng họ này đảm bảo rằng TSF được bảo vệ khỏi sự giả mạo và sự can thiệp vật lý. Để thoả mãn các yêu cầu đó thì các kết quả các thành phần này trong TSF được đóng gói và sử dụng như là một kiểu mà sự xâm phạm vật lý được phát hiện, hoặc sự phản ứng với xâm phạm vật lý bị ngăn chặn. Không có các thành phần này, các chức năng của một TSF bị mất tác dụng trong môi trường mà ở đó sự phát huỷ vật lý không được ngăn chặn. Họ này cũng quy định các yêu cầu về cách mà TSF phản ứng lại các xâm phạm vật lý.

14.6.2 Phân mức thành phần

FPT_PHP.1 phát hiện thụ động với tấn công vật lý, cung cấp các đặc trưng chỉ ra khi một thiết bị TSF hoặc phần tử TSF là chủ thể bị xâm phạm. Tuy nhiên thông báo về xâm phạm không tự động; một người dùng được phép sẽ phải thực hiện một chức năng quản lý an toàn, hoặc thực hiện thẩm tra thủ công để xác định xem có hiện tượng xâm phạm xảy ra không.

FPT_PHP.2 Thông báo tấn công vật lý, cung cấp thông báo tự động về một tấn công với một tập các xâm phạm vật lý đã được xác định.

FPT_PHP.3 Phản ứng lại tấn công vật lý, cung cấp các đặc trưng để ngăn chặn hoặc chống lại sự xâm phạm đến các thiết bị và các phần tử TSF.

14.6.3 Quản lý của FPT_PHP.1

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

a) Quản lý người sử dụng hay các quyền mà nó xác định liệu tấn công vật lý có thể xảy ra.

14.6.4 Quản lý của FPT_PHP.2

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

a) Quản lý người sử dụng hay quyền mà họ nhận được thông báo về sự xâm nhập.

b) Quản lý danh sách các thiết bị mà nó sẽ thông báo chỉ ra người hoặc vai trò của họ về sự xâm nhập.

14.6.5 Quản lý của FPT_PHP.3

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

a) Quản lý các phản ứng tự động đối với sự xâm phạm vật lý.

14.6.6 Kiểm toán của FPT_PHP.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: nếu phát hiện bởi các phương tiện IT, sự phát hiện xâm nhập.

14.6.7 Kiểm toán của FPT_PHP.2

Các hành động sau đây có thể được kiểm toán nếu FAU_ GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: phát hiện xâm nhập.

14.6.8 Kiểm toán của FPT_PHP.3

Không có sự kiện có thể kiểm toán nào.

14.6.9 FPT_PHP.1 Phát hiện thụ động tấn công vật lý

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

14.6.9.1 FPT_PHP.1.1

TSF cần cung cấp khả năng phát hiện rõ ràng về tấn công vật lý có thể làm tổn hại đến TSF.

14.6.9.2 FPT_PHP.1.2

TSF cần cung cấp khả năng xác định liệu có xảy ra tấn công vật lý đến các thiết bị hoặc phần tử của TSF.

14.6.10 FPT_PHP.2 Thông báo tấn công vật lý

Phân cấp từ: FPT_PHP.1 Phát hiện thụ động tấn công vật lý

Các mối phụ thuộc: FMT_MOF.1 Quản lý các hành xử của chức năng an toàn.

14.6.10.1 FPT_PHP.2.1

TSF cần cung cấp khả năng phát hiện rõ ràng về tấn công vật lý có thể làm tổn hại đến TSF.

14.6.10.2 FPT_PHP.2.2

TSF cần cung cấp khả năng xác định liệu tấn công vật lý có thể xảy ra đối với các thiết bị hoặc phần tử TSF.

14.6.10.3 FPT_PHP.2.3

Với [chỉ định: *danh sách các thiết bị/phần tử TSF có yêu cầu phát hiện tích cực*], TSF cần giám sát các thiết bị và phần tử và thông báo [chỉ định: *một người sử dụng hay một vai trò đã xác định*] khi xảy ra tấn công vật lý với các thiết bị hoặc phần tử TSF.

14.6.11 FPT_PHP.3 Chống tấn công vật lý

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

14.6.11.1 FPT_PHP.3.1

TSF cần chống lại [chỉ định: *các kịch bản tấn công vật lý*] đối với [chỉ định: *danh sách các thiết bị/phần tử TSF*] bằng việc phản ứng một cách tự động sao cho TSP không bị vi phạm.

14.7 Khôi phục tin cậy (FPT_RCV)

14.7.1 Hành xử của họ

Các yêu cầu của họ này đảm bảo rằng TSF có thể xác định TOE được khởi động mà không có khả năng bảo vệ và có thể khôi phục sau khi bị ngừng hoạt động. Họ này rất quan trọng bởi vì trạng thái khởi động TSF xác định sự bảo vệ các trạng thái tiếp theo.

14.7.2 Phân mức thành phần

FPT_RCV.1 Khôi phục thủ công, cho phép một TOE quy định cơ chế can thiệp của con người vào trạng thái an toàn.

FPT_RCV.2 Tự động khôi phục, quy định tối thiểu một dạng dịch vụ khôi phục sự gián đoạn trạng thái an toàn mà không cần can thiệp của con người, khôi phục các gián đoạn khác có thể vẫn cần sự can thiệp của con người

FPT_RCV.3 Tự động khôi phục không làm tổn hại lớn cũng cung cấp khả năng khôi phục tự động nhưng nó mạnh hơn bằng cách ngăn chặn các tổn thất lớn đối với các đối tượng được bảo vệ

FPT_RCV.4 Chức năng khôi phục, cung cấp khả năng khôi phục ở mức SF đặc biệt, đảm bảo khôi phục dữ liệu TSF sang trạng thái an toàn hoàn toàn

14.7.3 Quản lý của FPT_RCV.1

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

a) Quản lý việc ai có quyền khôi phục trong chế độ bảo trì

14.7.4 Quản lý của FPT_RCV.2, FPT_RCV.3

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

a) Quản lý ai có quyền khôi phục trong chế độ bảo trì

b) Quản lý danh sách lỗi/ gián đoạn dịch vụ có thể kiểm soát thông qua các thủ tục tự động

14.7.5 Quản lý của FPT_RCV.4

Không có hoạt động quản lý nào.

14.7.6 Kiểm toán của FPT_RCV.1, FPT_RCV.2, FPT_RCV.3

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: thực tế lỗi hoặc gián đoạn dịch vụ có thể xảy ra.

b) Tối thiểu: bắt đầu hoạt động lại một cách bình thường.

c) Cơ sở: loại lỗi hoặc gián đoạn dịch vụ.

14.7.7 Kiểm toán của FPT_RCV.4

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: nếu có thể, tính không thể trở về trạng thái an toàn sau lỗi của một chức năng an toàn.

b) Cơ sở: nếu có thể, sự phát hiện lỗi của một chức năng an toàn.

14.7.8 FPT_RCV.1 Khôi phục thủ công

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: AGD_OPE.1 Hướng dẫn người dùng vận hành.

14.7.8.1 FPT_RCV.1.1

Sau khi [chỉ định: *danh sách lỗi/gián đoạn dịch vụ*] TSF cần đưa ra chế độ bảo trì mà ở đó cung cấp khả năng trở về trạng thái an toàn.

14.7.9 FPT_RCV.2 Khôi phục tự động

Phân cấp từ: FPT_RCV.1 Khôi phục thủ công

Các mối phụ thuộc: AGD_OPE.1 Hướng dẫn người dùng vận hành.

14.7.9.1 FPT_RCV.2.1

Khi tự động khôi phục từ [chỉ định: *danh sách lỗi/gián đoạn dịch vụ*] là không thể, thì TSF cần về chế độ bảo trì, có khả năng quay trở lại trạng thái an toàn.

14.7.9.2 FPT_RCV.2.2

Với [chỉ định: *danh sách lỗi/gián đoạn dịch vụ*], TSF cần bảo đảm TOE trở về trạng thái an toàn sử dụng các thủ tục tự động

14.7.10 FPT_RCV.3 Khôi phục tự động tránh tổn thất lớn

Phân cấp từ: FPT_RCV.2 Khôi phục tự động.

Các mối phụ thuộc: AGD_OPE.1 Hướng dẫn người dùng vận hành.

14.7.10.1 FPT_RCV.3.1

Khi khôi phục tự động từ [chỉ định: *danh sách lỗi/gián đoạn dịch vụ*] là không thể, TSF cần chuyển sang chế độ bảo trì, nơi có khả năng quay trở lại trạng thái an toàn.

14.7.10.2 FPT_RCV.3.2

Với [chỉ định: *danh sách lỗi/gián đoạn dịch vụ*], TSF cần đảm bảo TOE quay trở lại trạng thái an toàn sử dụng các thủ tục tự động.

14.7.10.3 FPT_RCV.3.3

Các chức năng quy định bởi TSF để khôi phục lỗi hoặc gián đoạn dịch vụ cần đảm bảo rằng trạng thái khởi động an toàn được khôi phục không vượt quá [chỉ định: *số lượng*] đối với tổn thất dữ liệu TSF hoặc đối tượng trong TSC.

14.7.10.4 FPT_RCV.3.4

TSF cần cung cấp khả năng xác định các đối tượng có hoặc không có khả năng khôi phục.

14.7.11 FPT_RCV.4 Khôi phục chức năng

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

14.7.11.1 FPT_RCV.4.1

TSF cần đảm bảo [chỉ định: *danh sách SFs và các kịch bản lỗi*] có đặc tính là hoặc SF hoàn thành thành công hoặc chỉ ra các kịch bản lỗi, khôi phục về trạng thái an toàn và phù hợp.

14.8 Phát hiện chạy lại (FPT_RPL)

14.8.1 Hành xử của họ

Họ này đề cập đến việc phát hiện và chạy lại với các loại thực thể trước đó (ví dụ: tin nhắn, yêu cầu dịch vụ, đáp ứng dịch vụ) và các hoạt động tiếp theo để sữa lỗi. Trong trường hợp này vị trí chạy lại được phát hiện và như vậy nó có thể ngăn ngừa một cách hiệu quả.

14.8.2 Phân mức thành phần

Họ này bao gồm chỉ một thành phần FPT_RPL.1 Phát hiện chạy lại, nó đòi hỏi TSF có khả năng phát hiện các thực thể xác định chạy lại.

14.8.3 Quản lý của FPT_RPL.1

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

a) quản lý danh sách các thực thể xác định được phát hiện chạy lại.

b) quản lý danh sách các hoạt động cần đưa ra trong trường hợp chạy lại.

14.8.4 Kiểm toán của FPT_RPL.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Cơ sở: phát hiện các tấn công chạy lại.

b) Chi tiết: Hoạt động đưa ra dựa trên các hoạt động cụ thể.

14.8.5 FPT_RPL.1 Phát hiện chạy lại

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

14.8.5.1 FPT_RPL.1.1

TSF cần phát hiện chạy lại theo các thực thể như sau: [chỉ định: *danh sách các thực thể xác định*].

14.8.5.2 FPT_RPL.1.2

TSF cần thực hiện [Chỉ định: *danh sách các hoạt động cụ thể*] khi phát hiện chạy lại.

14.9 Giao thức đồng bộ trạng thái (FPT_SSP)

14.9.1 Hành xử của họ

Hệ thống phân tán có thể có độ phức tạp hơn nhiều so với các hệ thống tập trung vì các trạng thái khác nhau giữa các phần của hệ thống, và vì độ trễ trong truyền thông. Trong hầu hết các trường hợp đồng bộ trạng thái giữa các chức năng phân tán cần phải có một giao thức trao đổi, không chỉ đơn giản là một hành động. Khi xuất hiện điểm yếu trong môi trường phân tán của các giao thức này thì cần có nhiều hơn các giao thức bảo vệ phức tạp hơn.

Giao thức đồng bộ trạng thái (FPT_SSP) thiết lập yêu cầu cho các chức năng an toàn trọng yếu nhất định của TSF để sử dụng giao thức tin cậy này. Giao thức đồng bộ trạng thái đảm bảo rằng hai thành phần phân tán của TOE (ví dụ như các máy chủ) được đồng bộ trạng thái sau khi có hành động an toàn thích hợp.

14.9.2 Phân mức thành phần

FPT_SSP.1 Xác nhận tin cậy đơn, đòi hỏi chỉ một xác nhận đơn giản từ phía người nhận dữ liệu.

FPT_SSP.2 Xác nhận tin cậy tương hỗ, đòi hỏi xác nhận nhận từ cả hai phía trao đổi dữ liệu.

14.9.3 Quản lý của FPT_SSP.1, FPT_SSP.2

Không có các hoạt động quản lý nào.

14.9.4 Kiểm toán của FPT_SSP.1, FPT_SSP.2

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: nhận được thông báo lỗi khi có nhu cầu

14.9.5 FPT_SSP.1 Xác nhận tin cậy một chiều (đơn)

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FPT_ITT.1 Bảo vệ vận chuyển dữ liệu nội bộ TSF cơ bản.

14.9.5.1 FPT_SSP.1.1

TSF cần xác nhận, khi có yêu cầu của một bộ phận khác trong TSF, cho nơi nhận truyền dữ liệu TSF không thay đổi.

14.9.6 FPT_SSP.2 Xác nhận tin cậy hai chiều

Phân cấp từ: FPT_SSP.1 Xác nhận tin cậy đơn giản.

Các mối phụ thuộc: FPT_ITT.1 Bảo vệ vận chuyển dữ liệu nội bộ TSF cơ bản.

14.9.6.1 FPT_SSP.2.1

TSF cần xác nhận, khi có yêu cầu của một bộ phận khác trong TSF, cho nơi nhận truyền dữ liệu TSF không thay đổi.

14.9.6.2 FPT_SSP.2.2

TSF cần đảm bảo rằng các thành phần tương ứng của TSF nhận biết được trạng thái đúng của dữ liệu truyền trong số các phần khác nhau, sử dụng các xác nhận.

14.10 Nhãn thời gian (FPT_STM)

14.10.1 Hành xử của họ

Họ này xác định các yêu cầu cho chức năng nhãn thời gian tin cậy trong TOE.

14.10.2 Phân mức thành phần

Họ này bao gồm chỉ một thành phần, FPT_STM.1 Các nhãn thời gian tin cậy, nó đòi hỏi TSF quy định các nhãn thời gian tin cậy cho các chức năng TSF.

14.10.3 Quản lý của FPT_STM.1

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

a) quản lý thời gian.

14.10.4 Kiểm toán của FPT_STM.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) tối thiểu: thay đổi thời gian.

b) chi tiết: quy định một nhãn thời gian.

14.10.5 FPT_STM.1 Thẻ thời gian tin cậy

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

14.10.5.1 FPT_STM.1.1

TSF cần có khả năng quy định các nhãn thời gian tin cậy.

14.11 Tính nhất quán dữ liệu liên-TSF (FPT_TDC)

14.11.1 Hành xử của họ

Trong môi trường hệ thống phân tán hoặc phức hợp, một TOE có thể cần trao đổi dữ liệu TSF (ví dụ các thuộc tính SFP liên quan đến dữ liệu, thông tin kiểm toán, thông tin định danh) với các sản phẩm IT tin cậy khác, họ này định nghĩa các yêu cầu cho việc chia sẻ và thể hiện tính nhất quán của các thuộc tính này giữa TSF của TOE và các sản phẩm IT tin cậy khác.

14.11.2 Phân mức thành phần

FPT_TDC.1 Tính nhất quán dữ liệu TSF cơ sở liên-TSF đòi hỏi TSF cung cấp khả năng đảm bảo tính nhất quán của các thuộc tính giữa các TSF.

14.11.3 Quản lý của FPT_TDC.1

Không có các hoạt động quản lý nào.

14.11.4 Kiểm toán của FPT_TDC.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: sử dụng thành công các cơ chế nhất quán dữ liệu TSF.

b) Cơ sở: sử dụng các cơ chế nhất quán dữ liệu TSF.

c) Cơ sở: xác định dữ liệu TSF nào được chuyển đổi.

d) Cơ sở: phát hiện thay đổi dữ liệu.

14.11.5 FPT_TDC.1 Tính nhất quán dữ liệu TSF cơ bản liên-TSF

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

14.11.5.1 FPT_TDC.1.1

TSF cần cung cấp khả năng giải nghĩa một cách nhất quán [chỉ định: *danh sách kiểu dữ liệu TSF*] khi chia sẻ giữa TSF và sản phẩm CNTT tin cậy khác.

14.11.5.2 FPT_TDC.1.2

TSF cần sử dụng [chỉ định: *danh sách các quy tắc chuyển đổi được áp dụng bởi TSF*] khi giải nghĩa dữ liệu TSF từ sản phẩm IT tin cậy khác.

14.12 Kiểm thử các thực thể bên ngoài (FPT_TEE)

14.12.1 Hành xử của họ

Họ này định nghĩa các yêu cầu cho TSF thực thi các kiểm thử trên một hoặc nhiều thực thể bên ngoài.

Thành phần này không được tính đến để áp dụng cho con người.

Các thực thể bên ngoài có thể bao gồm các ứng dụng chạy trên TOE, phần cứng hay phần mềm chạy "bên dưới" TOE (chẳng hạn như các nền tảng, các hệ điều hành v.v...) hay các ứng dụng/hộp kết nối với TOE (như các hệ thống phát hiện xâm nhập, tường lửa, các máy chủ đăng nhập, các máy chủ thời gian v.v...).

14.12.2 Phân mức thành phần

FPT_TEE.1 Kiểm thử của các thực thể bên ngoài, cung cấp các kiểm thử về các thực thể bên ngoài nhờ TSF.

14.12.3 Quản lý của FPT_TEE.1

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

a) Quản lý với các điều kiện mà theo đó các kiểm thử của các thực thể bên ngoài xảy ra, chẳng hạn như trong quá trình khởi động ban đầu, khoảng thời gian quy định, hay dưới các điều kiện đặc biệt;

b) Quản lý theo khoảng thời gian nếu thích hợp.

14.12.4 Kiểm toán cho FPT_TEE.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Cơ sở: Việc thực hiện các kiểm thử của các thực thể bên ngoài và các kết quả kiểm thử.

14.12.5 FPT_TEE.1 Kiểm thử các thực thể bên ngoài

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

6.1.1.3 FPT_TEE.1.1

TSF cần chạy một bộ các kiểm thử [lựa chọn: *trong suốt thời gian khởi động ban đầu, định kỳ trong quá trình hoạt động bình thường, tại các yêu cầu của người dùng có thẩm quyền, [chỉ định: các điều kiện khác]*] để kiểm tra việc thực hiện của [chỉ định: danh sách các thuộc tính của các thực thể bên ngoài].

6.1.1.4 FPT_TEE.1.2

Nếu các kiểm thử thất bại, TSF cần [chỉ định: *các hành động*]

14.13 Tính nhất quán bản sao dữ liệu bên trong TOE TSF (FPT_TRC)

14.13.1 Hành xử của họ

Các yêu cầu của họ này cần thiết để đảm bảo tính nhất quán của dữ liệu khi dữ liệu được sao lưu trong TOE. Dữ liệu như vậy có thể trở thành không nhất quán nếu kênh truyền bên trong giữa các bộ phận của TOE làm ngưng hoạt động. Nếu TOE được xây dựng bên trong như là một mạng và một phần các kết nối mạng TOE bị đứt thì điều này có thể xảy ra khi phần đó trở là không kích hoạt.

14.13.2 Phân mức thành phần

Họ này bao gồm chỉ một thành phần, FPT_TRC.1 - tính nhất quán trong TSF các yêu cầu này là TSF đảm bảo tính nhất quán của dữ liệu TSF khi nó được sao lưu tại nhiều nơi.

14.13.3 Quản lý của FPT_TRC.1

Không có các hoạt động quản lý nào.

14.13.4 Kiểm toán của FPT_TRC.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: Khôi phục tính nhất quán theo khôi phục kết nối.

b) Cơ sở: Phát hiện tính không nhất quán của dữ liệu TSF.

14.13.5 FPT_TRC.1 Tính nhất quán bên trong TSF

Phân cấp từ: không có thành phần khác.

Các mối phụ thuộc: FPT_ITT.1 Bảo vệ truyền dữ liệu trong TSF cơ bản.

14.13.5.1 FPT_TRC.1.1

TSF cần đảm bảo dữ liệu TSF là nhất quán khi sao chép giữa các phần của TOE.

14.13.5.2 FPT_TRC.1.2

Khi các phần của TOE chứa dữ liệu sao chép TSF bị gián đoạn, TSF cần đảm bảo tính nhất quán của dữ liệu sao chép TSF từ khi kết nối lại trước khi xử lý bất cứ yêu cầu nào cho [chỉ định: danh sách các SF phụ thuộc vào tính nhất quán sao chép dữ liệu TSF].

14.14 Tự kiểm tra TSF (FPT_TST)

14.14.1 Hành xử của họ

Họ này định nghĩa các yêu cầu cho việc tự kiểm tra TSF tập trung vào một số hoạt động chuẩn mong muốn. Ví dụ các giao diện đối với các chức năng thực thi và các hoạt động số học lấy mẫu trên cơ sở các phần quan trọng của TOE. Các kiểm tra này có thể thực hiện tại lúc khởi tạo, định kỳ, tại lúc có yêu cầu của người đủ thẩm quyền, hoặc khi thỏa mãn các điều kiện khác. Các hoạt động có thể được đưa ra bởi TOE như là kết quả của việc tự kiểm tra được định nghĩa trọng các họ khác.

Các yêu cầu của họ này cũng cần thiết để phát hiện sự gián đoạn của mã thực thi TSF (ví dụ phần mềm TSF) và dữ liệu TSF bởi các lỗi khác mà không cần thiết phải dừng hoạt động của TOE (nó được kiểm soát bởi các họ khác) các kiểm tra này phải được thực hiện bởi vì các lỗi đó có thể không cần thiết phải bảo vệ. Các lỗi như vậy có thể xảy ra hoặc vì các chế độ lỗi không được dự đoán trước hoặc liên quan đến sai sót trong thiết kế phần cứng, phần mềm, hoặc bởi vì sự gián đoạn cố ý của TSF vì không phù hợp logic và/hoặc sự bảo vệ vật lý.

14.14.2 Phân mức thành phần

FPT_TST.1 TSF kiểm tra, cung cấp khả năng kiểm tra hoạt động đúng của TSF. Các kiểm tra này có thể được thực hiện tại thời điểm khởi động, định kỳ, hoặc theo yêu cầu của người có thẩm quyền, hay khi các điều kiện khác thỏa mãn. Nó cũng cung cấp khả năng kiểm tra tính toàn vẹn của dữ liệu TSF và mã thực thi.

14.14.3 Quản lý của FPT_TST.1

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

a) Quản lý các điều kiện để TSF tự kiểm tra, ví dụ trong khi khởi động, khoảng thời gian đều đặn hoặc theo một số điều kiện cụ thể.

b) Quản lý khoảng thời gian thích hợp.

14.14.4 Kiểm toán của FPT_TST.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Cơ sở: thực hiện tự kiểm tra TSF và các kết quả kiểm tra.

14.14.5 FPT_TST.1 kiểm tra TSF

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

14.14.5.1 FPT_TST.1.1

TSF cần thực hiện một bộ các tự kiểm tra [lựa chọn: trong quá trình khởi tạo, hoạt động một cách định kỳ, tại thời điểm yêu cầu của người có thẩm quyền, ở các điều kiện *[chỉ định: các*

điều kiện cho tự kiểm tra] để chứng tỏ hoạt động của TSF là đúng đắn. [lựa chọn:*[tấn định:các bộ phận của TSF], TSF*].

14.14.5.2 FPT_TST.1.2

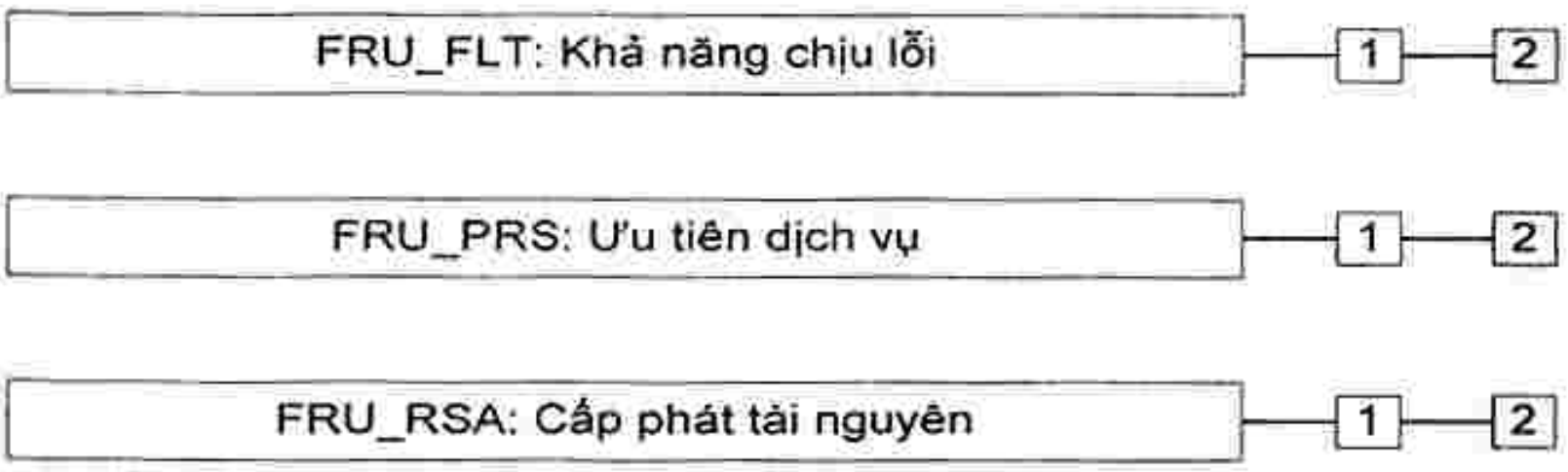
TSF cần quy định cho người sử dụng hợp pháp khả năng kiểm tra tính toàn vẹn của [lựa chọn: *[chỉ định: các bộ phận của TSF], dữ liệu TSF*].

14.14.5.3 FPT_TST.1.3

TSF cần quy định cho người sử dụng hợp pháp khả năng kiểm tra tính toàn vẹn của mã thực thi được lưu trong TSF.

15 Lớp FRU: Sử dụng tài nguyên

Lớp này giới thiệu 3 họ hỗ trợ cho tính sẵn sàng của các tài nguyên được yêu cầu, chẳng hạn như về khả năng xử lí và/hay dung lượng dữ trữ. Họ Khả năng chịu lỗi (Faul Tolerance) quy định sự bảo vệ đối với khả năng không sẵn sàng do lỗi của TOE gây ra. Họ Quyền ưu tiên của dịch vụ (Priority of Service) đảm bảo tài nguyên sẽ được cấp phát cho những nhiệm vụ quan trọng hơn và tài nguyên đó không thể giữ độc quyền bởi những nhiệm vụ có quyền ưu tiên thấp hơn. Họ Cấp phát tài nguyên (Resource Allocation) đưa ra giới hạn về việc sử dụng các tài nguyên sẵn có, vì thế sẽ ngăn chặn việc người dùng chiếm dụng độc quyền tài nguyên.



Hình 15 – Phân rã lớp FRU: Sử dụng tài nguyên

15.1 Khả năng chịu lỗi (FRU_FLT)

15.1.1 Hành xử của họ

Các yêu cầu của họ này đảm bảo rằng TOE sẽ duy trì hoạt động chính xác ngay cả khi có lỗi.

15.1.2 Phân mức thành phần

FRU_FLT.1: Khả năng chịu lỗi suy giảm, yêu cầu TOE vẫn hoạt động chính xác với những khả năng xác định trong sự kiện lỗi xác định.

FRU_FLT.2: Khả năng chịu lỗi giới hạn (Limited fault tolerance), yêu cầu TOE vẫn hoạt động chính xác ở mọi khả năng trong sự kiện lỗi xác định.

15.1.3 Quản lí của FRU_FLT.1, FRU_FLT.2

Không có các hoạt động quản lý nào.

15.1.4 Kiểm toán của FRU_FLT.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: Bất cứ lỗi nào được phát hiện bởi TSF.

b) Cơ sở: Tất cả những khả năng mà TOE bị gián đoạn do lỗi.

15.1.5 Kiểm toán của FRU_FLT.2

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: Bất cứ lỗi nào được phát hiện bởi TSF.

15.1.6 FRU_FLT.1 Khả năng chịu lỗi suy giảm

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FPT_FLS.1 Lỗi với việc bảo toàn trạng thái an toàn.

15.1.6.1 FRU_FLT.1.1

TSF cần đảm bảo hoạt động của [chỉ định: *danh sách các khả năng của TOE*] khi xuất hiện các lỗi sau: [chỉ định: *danh sách các loại lỗi*].

15.1.7 FRU_FLT.2 Khả năng chịu lỗi giới hạn

Phân cấp từ: FRU_FLT.1 Khả năng chịu lỗi suy giảm

Các mối phụ thuộc: FPT_FLS.1 Lỗi với việc bảo toàn trạng thái an toàn.

15.1.7.1 FRU_FLT.2.1

TSF cần đảm bảo hoạt động của **tất cả các khả năng của TOE** khi các lỗi sau xuất hiện: [chỉ định: *danh sách các loại lỗi*].

15.2 Ưu tiên dịch vụ (FRU_PRS)

15.2.1 Hành xử của họ

Những yêu cầu của họ này cho phép TSF kiểm soát việc sử dụng tài nguyên trong TSC bởi người dùng và các chủ thể sao cho các hoạt động ưu tiên trong TSC sẽ luôn được hoàn thành mà không bị can thiệp hay trễ quá mức do các hoạt động có độ ưu tiên thấp hơn gây ra.

15.2.2 Phân mức thành phần

FRU_PRS.1 Ưu tiên dịch vụ có giới hạn, quy định các mức ưu tiên cho một chủ thể sử dụng một tập con tài nguyên của chủ thể trong TSC.

FRU_PRS.2 Ưu tiên dịch vụ đầy đủ, quy định các mức ưu tiên cho việc sử dụng tất cả các tài nguyên của một chủ thể trong TSC.

15.2.3 Quản lý của FRU_PRS.1, FRU_PRS.2

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

a) Chỉ định các mức ưu tiên cho mỗi chủ thể trong TSF.

15.2.4 Kiểm toán của FFU_PRS.1, FRU_PRS.2

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: Từ chối hoạt động dựa trên việc sự dụng mức ưu tiên bên trong một cấp phát.

b) Cơ sở: Mọi khả năng sử dụng chức năng cấp phát liên quan đến mức ưu tiên của các chức năng dịch vụ.

15.2.5 FRU_PRS.1 Ưu tiên dịch vụ có giới hạn

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

15.2.5.1 FRU_PRS.1.1

TSF cần ấn định một mức ưu tiên cho mỗi chủ thể trong TSF.

15.2.5.2 FRU_PRS.1.2

TSF cần đảm bảo rằng mỗi truy nhập tới [chỉ định: các tài nguyên được kiểm soát] phải được dàn xếp trên cơ sở các chủ thể được ấn định quyền ưu tiên.

15.2.6 FRU_PRS.2 Quyền ưu tiên dịch vụ đầy đủ

Phân cấp từ: FRU_PRS.1 Ưu tiên dịch vụ có giới hạn.

Các mối phụ thuộc: Không có sự phụ thuộc.

15.2.6.1 FRU_PRS.2.1

TSF cần ấn định một mức ưu tiên cho mỗi chủ thể trong TSF.

15.2.6.2 FRU_PRS.2.2

TSF cần đảm bảo rằng mỗi truy nhập tới **tất cả các tài nguyên có thể chia sẻ** cần được dàn xếp trên nền tảng các chủ thể được ấn định mức ưu tiên.

15.3 Cấp phát tài nguyên (FRU_RSA)

15.3.1 Hành xử của họ

Các yêu cầu của họ này cho phép TSF kiểm soát việc sử dụng các tài nguyên bởi người dùng và các chủ thể, sao cho việc từ chối dịch vụ không xảy ra bởi sự độc chiếm không được phép của các tài nguyên.

15.3.2 Phân mức thành phần

FRU_RSA.1: Chỉ tiêu tối đa, quy định các yêu cầu cho các cơ chế định mức để đảm bảo rằng người dùng và chủ thể không độc chiếm một tài nguyên đã được kiểm soát.

FRU_RSA.2: Chỉ tiêu tối đa và tối thiểu, quy định các yêu cầu cho các cơ chế định mức để đảm bảo rằng người dùng và chủ thể sẽ luôn có ít nhất một tài nguyên cụ thể tối thiểu và họ sẽ không thể độc chiếm một tài nguyên đã được kiểm soát.

15.3.3 Quản lý của FRU_RSA.1

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

a) Định rõ những giới hạn tối đa cho một tài nguyên cho các nhóm và/hay người dùng cụ thể và/hay các chủ thể bởi nhà quản trị.

15.3.4 Quản lý của FRU_RSA.2

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

a) Định rõ các giới hạn tối đa và tối thiểu cho một tài nguyên cho các nhóm và/hay những người dùng và/hay các chủ thể bởi nhà quản trị.

15.3.5 Kiểm toán của FRU_RSA.1, FRU_RSA.2

Các hành động sau có thể được kiểm toán nếu FAU_GEN tạo dữ liệu kiểm toán an toàn chứa trong PP/ST:

a) Tối thiểu: Loại trừ hoạt động cấp phát do những giới hạn về tài nguyên

b) Cơ sở: Mọi khả năng sử dụng chức năng cấp phát dưới sự kiểm soát của TSF.

15.3.6 FRU_RSA.1 Các chỉ tiêu tối đa

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

15.3.6.1 FRU_RSA.1.1

TSF cần tuân theo các chỉ tiêu tối đa của các tài nguyên sau [chỉ định: các tài nguyên được kiểm soát] mà [lựa chọn: *người dùng cụ thể, nhóm những người dùng xác định, các chủ thể*] có thể sử dụng [lựa chọn: *đồng thời trên một khoảng thời gian cụ thể*].

15.3.7 FRU_RSA.2 Các chỉ tiêu tối đa và tối thiểu

Phân cấp tới: FRU_RSA.1 Các chỉ tiêu tối đa

Các mối phụ thuộc: Không phụ thuộc

15.3.7.1 FRU_RSA.2.1

TSF cần thực thi các chỉ tiêu tối đa của các tài nguyên sau [chỉ định: *các tài nguyên được kiểm soát*] mà [lựa chọn: *người dùng cụ thể, nhóm những người dùng xác định*] có thể sử dụng [lựa chọn: *đồng thời, trên một khoảng thời gian cụ thể*].

15.3.7.2 FRU_RSA.2.2

TSF cần đảm bảo việc quy định số lượng tối thiểu của mỗi [chỉ định: *các tài nguyên được kiểm soát*] sẵn có cho [lựa chọn: *người dùng cụ thể, nhóm những người dùng xác định, các chủ thể*] để sử dụng [lựa chọn: *đồng thời, trên một khoảng thời gian cụ thể*].

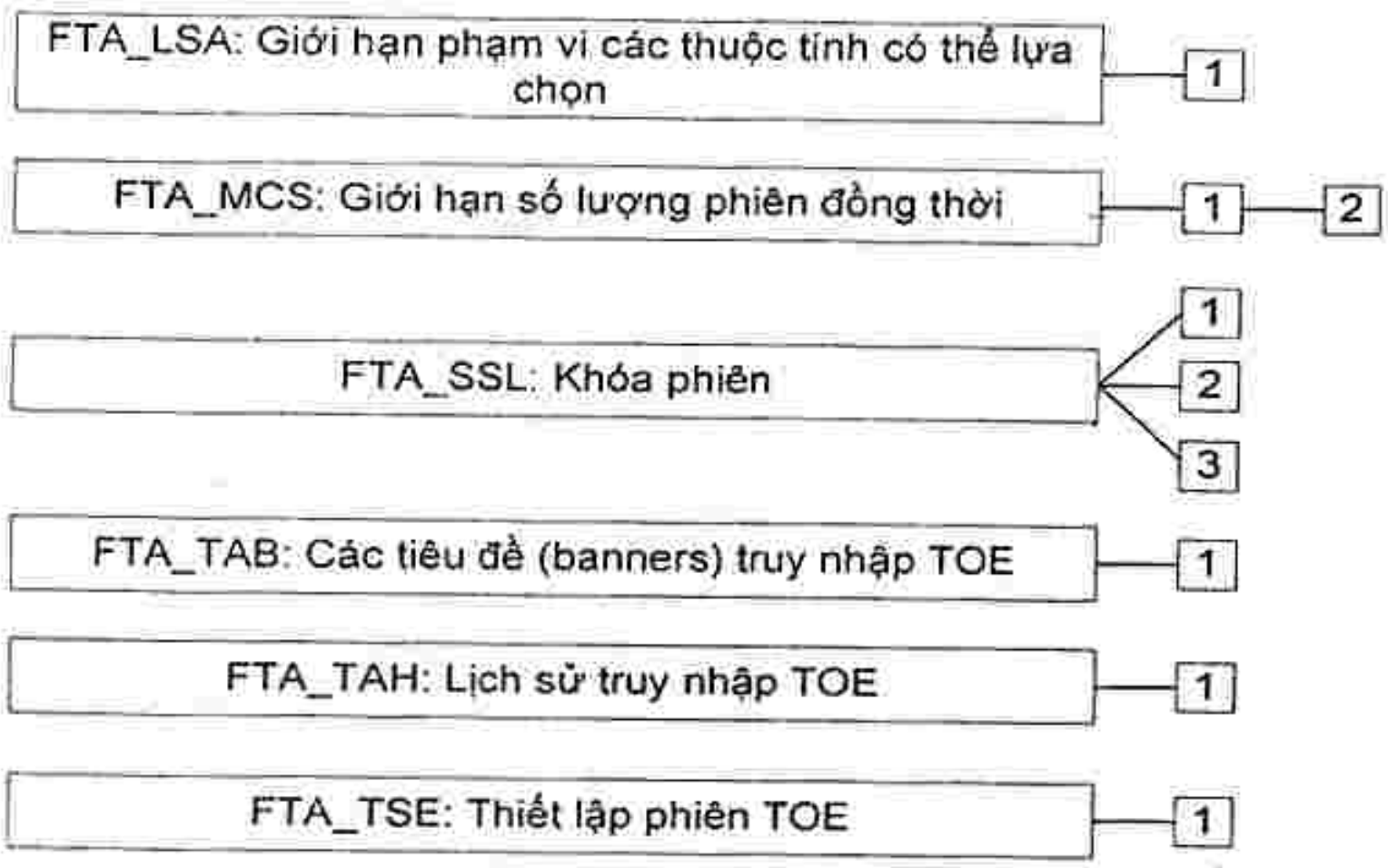
16 Lớp FTA: Truy nhập TOE

Họ này định rõ các yêu cầu về chức năng điều khiển thiết lập phiên người dùng.

16.1 Giới hạn trên phạm vi các thuộc tính có thể lựa chọn (FTA_LSA)

16.1.1 Hành xử của họ

Họ này định nghĩa những yêu cầu cho việc giới hạn phạm vi các thuộc tính an toàn phiên mà người dùng có thể lựa chọn cho một phiên.



Hình 16 – Phân rã lớp FTA: truy nhập TOE

16.1.2 Phân mức thành phần

FTA_LSA.1 Giới hạn trên phạm vi các thuộc tính có thể lựa chọn, quy định yêu cầu cho một TOE để giới hạn phạm vi các thuộc tính an toàn trong suốt quá trình thiết lập phiên.

16.1.3 Quản lý của FTA_LSA.1

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

a) Quản lí phạm vi các thuộc tính an toàn phiên bởi nhà quản trị.

16.1.4 Kiểm toán của FTA_LSA.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: Tất cả các nỗ lực không đạt được khi lựa chọn các thuộc tính an toàn phiên;

b) Cơ sở: Tất cả các cố gắng khi lựa chọn các thuộc tính an toàn phiên;

c) Chi tiết: Giữ lại các giá trị của mỗi thuộc tính an toàn phiên

16.1.5 FTA_LSA.1 Giới hạn trên phạm vi các thuộc tính có thể lựa chọn

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

16.1.5.1 FTA_LSA1.1

TSF cần hạn chế phạm vi của các thuộc tính an toàn phiên [chỉ định: *các thuộc tính an toàn phiên*], dựa trên cơ sở [chỉ định: *các thuộc tính*].

16.2 Giới hạn về nhiều phiên diễn ra đồng thời (FTA_MCS)

16.2.1 Hành xử của họ

Họ này định nghĩa các yêu cầu để đưa ra các giới hạn trên một số phiên diễn ra đồng thời thuộc cùng người dùng.

16.2.2 Phân mức thành phần

FTA_MCS.1 Giới hạn cơ sở trên đa phiên đồng thời, quy định những giới hạn áp dụng cho tất cả người dùng TSF.

FTA_MCS.2 Giới hạn thuộc tính mỗi người dùng trên cơ sở mở rộng các phiên làm việc đồng thời FTA_MCS.1 thông qua việc yêu cầu khả năng chỉ ra các giới hạn về số phiên làm việc đồng thời trên cơ sở các thuộc tính an toàn liên quan.

16.2.3 Quản lý của FTA_MCS.1

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

a) Quản lí một số lượng cho phép tối đa các phiên người dùng đồng thời bởi nhà quản trị.

16.2.4 Quản lý của FTA_MCS.2

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

a) Quản lý các quy tắc quản trị số lượng cho phép tối đa các phiên người dùng đồng thời bởi nhà quản trị.

16.2.5 Kiểm toán của FTA_MCS.1, FTA_MCS.2

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: Loại trừ một phiên mới dựa trên cơ sở giới hạn nhiều phiên đồng thời.

b) Chi tiết: Giữ lại một số phiên người dùng đang diễn ra đồng thời và các thuộc tính an toàn người dùng.

16.2.6 FTA_MCS.1 Giới hạn cơ sở trên đa phiên đồng thời

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FIA_UID.1 Định thời cho định danh..

16.2.6.1 FTA_MCS.1.1

TSF cần hạn chế số lượng tối đa các phiên đồng thời thuộc cùng người dùng.

16.2.6.2 FTA_MCS1.2

Mặc định, TSF phải tuân thủ giới hạn [chỉ định: số mặc định] phiên cho mỗi người dùng.

16.2.7 FTA_MCS.2 Giới hạn thuộc tính mỗi người dùng cho nhiều phiên đồng thời

Phân cấp từ: FTA_MCS.1 Giới hạn cơ sở trên đa phiên đồng thời

Các mối phụ thuộc: FIA_UID.1 Định thời cho định danh.

16.2.7.1 FTA_MCS.2.1

TSF cần hạn chế số lượng tối đa các phiên đồng thời thuộc cùng người dùng **theo quy tắc [chỉ định: *các quy tắc về số các phiên đồng thời tối đa*].**

16.2.7.2 FTA_MCS.2.2

Mặc định, TSF cần thực thi giới hạn [chỉ định: *số mặc định*] số phiên trên người dùng.

16.3 Khóa và chấm dứt phiên (FTA_SSL)

16.3.1 Hành xử của họ

Họ này định nghĩa những yêu cầu đối với TSF để quy định khả năng khóa, mở khóa TSF đã khởi đầu và người dùng đã khởi đầu của các phiên tương tác.

16.3.2 Phân cấp thành phần

FTA_SSL.1 Khóa phiên TSF đã khởi đầu gồm việc khóa hệ thống đã khởi đầu của một phiên tương tác sau một khoảng thời gian nhất định khi không có hoạt động người dùng.

FTA_SSL2 Khóa phiên người dùng đã khởi đầu, quy định những khả năng cho người dùng khóa hay mở khóa các phiên tương tác mà người dùng đó đang sử dụng.

FTA_SSL.3 Kết thúc TSF đã khởi đầu, quy định những yêu cầu cho phép TSF kết thúc phiên làm việc sau một khoảng thời gian không có hoạt động người dùng.

FTA_SSL.4 Kết thúc phiên người dùng đã khởi đầu, quy định khả năng cho người dùng để chấm dứt các phiên tương tác của chính người dùng.

16.3.3 Quản lý của FTA_SSL.1

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

a) Đặc tả về thời gian không có hoạt động người dùng sau khi lock-out diễn ra đối với mỗi người dùng cụ thể.

b) Đặc tả thời gian mặc định không có hoạt động người dùng sau khi lock-out diễn ra.

c) Quản lý các sự kiện diễn ra trước khi mở khóa một phiên.

16.3.4 Quản lý của FTA_SSL.2

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

a) Quản lý các sự kiện diễn ra trước khi mở khóa một phiên.

16.3.5 Quản lý của FTA_SSL.3

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

a) Đặc tả thời gian không có hoạt động người dùng sau khi kết thúc một phiên tương tác diễn ra đối với từng người dùng cụ thể.

b) Đặc tả thời gian mặc định không có người dùng sau khi kết thúc một phiên tương tác diễn ra.

16.3.6 Quản lý của FTA_SSL.4

Không có các hoạt động quản lý nào.

16.3.7 Kiểm toán của FTA_SSL.1, FTA_SSL.2

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: Khóa một phiên tương tác bởi cơ chế khóa phiên.

b) Tối thiểu: Mở khóa thành công một phiên tương tác .

c) Cơ sở: Bất kì sự nỗ lực nào để mở khóa một phiên tương tác.

16.3.8 Kiểm toán của FTA_SSL.3

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: Kết thúc một phiên tương tác nhờ cơ chế khóa phiên.

16.3.9 Kiểm toán của FTA_SSL.4

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

b) Tối thiểu: Kết thúc một phiên tương tác bởi người dùng.

16.3.10 FTA_SSL.1 Khóa phiên khởi tạo bởi TSF

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FIA_UAU.1 Định thời cho xác thực

16.3.10.1 FTA_SSL.1.1

TSF cần khóa một phiên tương tác sau [chỉ định: *khoảng thời gian không có hoạt động người dùng*] nhờ:

a) Xóa hoặc ghi đè các thiết bị hiển thị, làm cho những nội dung hiện tại không thể đọc;

b) Cấm mọi hoạt động của các thiết bị hiển thị / truy nhập dữ liệu người dùng nếu không phải là mở khóa phiên.

16.3.10.2 FTA_SSL.1.2

TSF cần yêu cầu các sự kiện sau diễn ra trước khi mở khóa phiên: [chỉ định*: các sự kiện diễn ra*].

16.3.11 FTA_SSL.2 Khóa khởi tạo bởi người dùng

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: FIA_UAU.1 Định thời cho xác thực

16.3.11.1 FTA_SSL.2.1

TSF cần cho phép việc khóa khởi tạo bởi người dùng cho phiên tương tác của chính họ thông qua:

a) Xóa hoặc ghi đè các thiết bị hiển thị, làm cho những nội dung hiện tại không thể đọc được.

b) Cấm mọi hoạt động của các thiết bị hiển thị / truy nhập dữ liệu của người dùng nếu không phải là mở khóa phiên.

16.3.11.2 FTA_SSL.2.2

TSF cần yêu cầu các sự kiện sau diễn ra trước khi mở khóa phiên: [chỉ định: *các sự kiện diễn ra*].

16.3.12 FTA_SSL.3 Kết thúc phiên khởi tạo bởi TSF

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

16.3.12.1 FTA_SSL.3.1

TSF cần kết thúc một phiên tương tác sau một khoảng [chỉ định: khoảng thời gian không có hoạt động người dùng].

16.4 Các biểu trưng truy nhập TOE (FTA_TAB)

16.4.1 Hành xử của họ

Họ này định nghĩa những yêu cầu để hiển thị bản tin cảnh báo tư vấn cấu hình cho người dùng về cách sử dụng thích hợp của TOE.

16.4.2 Phân mức thành phần

FTA_TAB.1 Các biểu trưng truy nhập TOE mặc định, quy định yêu cầu cho một biểu trưng Truy nhập TOE. Biểu trưng này được hiển thị trước khi thiết lập hội thoại cho một phiên làm việc.

16.4.3 Quản lý của FTA_TAB.1

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

a) Duy trì biểu trưng bởi nhà quản trị có thẩm quyền.

16.4.4 Kiểm toán của FTA_TAB.1

Không có sự kiện có thể kiểm toán nào.

16.4.5 FTA_TAB.1 Các biểu trưng truy nhập TOE mặc định

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

16.4.5.1 FTA_TAB.1.1

Trước khi thiết lập một phiên người dùng, TSF sẽ hiển thị một bản tin cảnh báo tư vấn về cách sử dụng không được cấp phép của TOE.

16.5 Lịch sử truy nhập TOE (FTA_TAH)

16.5.1 Hành xử của họ

Họ này định nghĩa những yêu cầu đối với TSF để hiển thị tới người dùng, sau khi thiết lập phiên thành công, một bản ghi lại những lần truy nhập thành công và không thành công vào tài khoản người.

16.5.2 Phân mức thành phần

FTA_TAH.1 Lịch sử truy nhập TOE, quy định yêu cầu đối với mỗi TOE để hiển thị thông tin liên quan đến cố gắng trước đó để thiếp lập một phiên.

16.5.3 Quản lý của FTA_TAH.1

Không có các hoạt động quản lý nào.

16.5.4 Kiểm toán của FTA_TAH.1

Không có sự kiện có thể kiểm toán nào.

16.5.5 FTA_TAH.1 Lịch sử truy nhập TOE

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

16.5.5.1 FTA_TAH.1.1

Sau khi thiết lập phiên thành công, TSF cần hiển thị [lựa chọn: ngày tháng, thời gian, phương pháp, địa điểm] của lần thiết lập phiên thành công mới đây nhất cho người dùng.

16.5.5.2 FTA_TAH.1.2

Sau khi thiết lập phiên thành công, TSF cần hiển thị [lựa chọn: *ngày tháng, thời gian, phương pháp, địa điểm*] về những cố gắng không thành công mới nhất về việc thiết lập phiên và một số các cố gắng không thành công từ lần thiết lập phiên thành công cuối cùng.

16.5.5.3 FTA_TAH.1.3

TSF cần không được xóa thông tin lịch sử truy nhập từ giao diện người dùng mà không đưa ra cho người dùng một cơ hội xem lại thông tin.

16.6 Thiết lập phiên TOE (FTA_TSE)

16.6.1 Hành xử của họ

Họ này định nghĩa các yêu cầu từ chối truy cập người dùng thiết lập một phiên với TOE.

16.6.2 Phân mức thành phần

FTA_TSE.1 Thiết lập phiên TOE, quy định những yêu cầu đối với việc từ chối truy nhập người dùng tới TOE dựa trên các thuộc tính.

16.6.3 Quản lý của FTA_TSE.1

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

a) Quản lý các trạng thái thiết lập phiên bởi nhà quản trị.

16.6.4 Kiểm toán của FTA_TSE.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: Từ chối thiết lập một phiên do cơ chế thiết lập phiên.

b) Cơ sở: Mọi cố gắng thiết lập một phiên người dùng.

c) Chi tiết: Giữ lại giá trị của các thông số truy nhập đã lựa chọn (ví dụ: địa điểm truy nhập, thời gian truy nhập).

16.6.5 FTA_TSE.1 Thiết lập phiên TOE

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

16.6.5.1 FTA_TSE.1.1

TSF cần phải có khả năng từ chối thiết lập phiên dựa trên cơ sở [chỉ định: các thuộc tính].

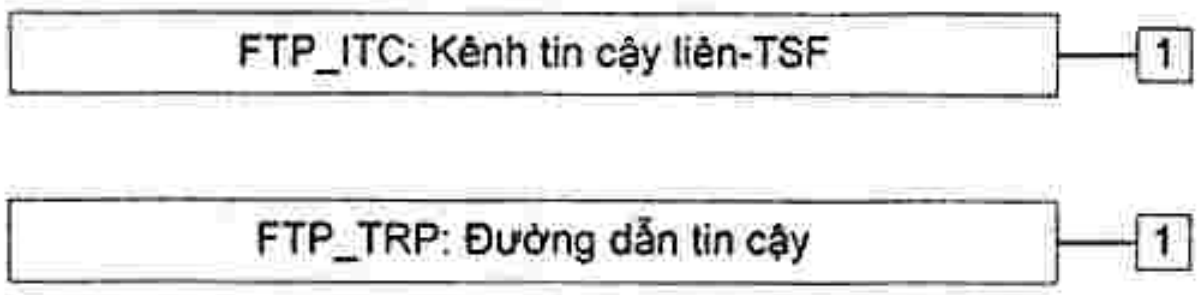
17 Lớp FTP: Đường dẫn/Kênh tin cậy

Các họ trong lớp này quy định các yêu cầu đối với tuyến truyền thông tin cậy giữa người dùng và TSF, và đối với kênh truyền thông tin cậy giữa TSF và các sản phẩm IT tin cậy khác. Các tuyến và các kênh tin cậy có những đặc điểm chung sau:

- Tuyến truyền thông tin cậy được xây dựng nhờ sử dụng các kênh truyền thông bên trong và bên ngoài (thích hợp với thành phần đó) giữ cho tập con xác định của dữ liệu và các lệnh TSF tách biệt với phần còn lại của TSF và dữ liệu người dùng.
- Việc sử dụng tuyến truyền thông có thể được khởi đầu bởi người dùng và/hay TSF (thích hợp cho thành phần đó).
- Tuyến truyền thông có khả năng quy định sự đảm bảo cho người dùng đang truyền thông với đúng TSF, và TSF đang truyền thông với đúng người dùng (thích hợp cho thành phần đó).

Ở mô hình này, một kênh tin cậy là một kênh truyền thông có thể được khởi đầu từ phía khác của kênh, và quy định những đặc điểm không từ chối đối với việc định danh các phía của kênh.

Một tuyến tin cậy quy định phương tiện cho người dùng thực hiện các chức năng thông qua tương tác trực tiếp được đảm bảo với TSF. Tuyến tin cậy thường xuyên được mong muốn đối với các hành động người dùng chẳng hạn như sự nhận dạng và/hay xác thực, nhưng cũng có thể được mong muốn ở những lần khác trong suốt một phiên người dùng. Sự trao đổi bằng tuyến tin cậy có thể được khởi đầu bởi người dùng hay TSF. Người dùng phản hồi qua một tuyến tin cậy đảm bảo tránh được sự chỉnh sửa hay bị lộ bởi những ứng dụng không đáng tin cậy.



Hình 17 – Phân cấp lớp FTP: tuyến / kênh tin cậy

17.1 Kênh tin cậy liên-TSF (FTP_ITC)

17.1.1 Hành xử của họ

Họ này định nghĩa những yêu cầu về việc tạo thành kênh tin cậy giữa TSF và các sản phẩm IT khác đối với hiệu năng các hoạt động then chốt cho an toàn. Họ này nên được kèm theo khi có những yêu cầu về truyền thông an toàn của dữ liệu người dùng hay dữ liệu TSF giữa TOE và các sản phẩm CNTT tin cậy khác.

17.1.2 Phân mức thành phần

FTP_ITC.1 kênh tin cậy liên TSF, yêu cầu TSF quy định một kênh truyền thông tin cậy giữa nó và một sản phẩm IT tin cậy khác.

17.1.3 Quản lý của FTP_ITC.1

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

a) Lập cấu hình các hành động yêu cầu kênh tin cậy, nếu được hỗ trợ.

17.1.4 Kiểm toán của FTP_ITC.1

Các hành động sau cần được kiểm tra nếu FAU_GEN tạo dữ liệu kiểm toán an toàn chứa trong PP/ST:

a) Tối thiểu: Lỗi của các chức năng kênh tin cậy.

b) Tối thiểu: Nhận dạng khởi đầu và đích của các chức năng kênh tin cậy bị lỗi.

c) Cơ sở: Mọi việc sử dụng thử các chức năng kênh tin cậy.

d) Cơ sở: Nhận dạng khởi đầu và đích của mọi chức năng kênh tin cậy.

17.1.5 FTP_ITC.1 Kênh tin cậy liên TSF

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

17.1.5.1 FTP_ITC.1.1

TSF cần quy định một kênh truyền thông tin cậy giữa nó và một sàn phẩm IT khác phân biệt về logic với các kênh truyền thông khác và quy định việc nhận dạng bảo đảm về điểm cuối của kênh và việc bảo về dữ liệu kênh khỏi sự chỉnh sửa hay bị lộ thông tin.

17.1.5.2 FTP_ITC.1.2

TSF cần cho phép [lựa chọn: *TSF, sản phẩm IT tin cậy khác*] khởi tạo truyền thông qua kênh tin cậy.

17.1.5.3 FTP_ITC.1.3

TSF cần khởi tạo truyền thông qua kênh tin cậy cho [Chỉ định: *danh sách các chức năng có yêu cầu một kênh tin cậy*].

17.2 Đường dẫn tin cậy (FTP_TRP)

17.2.1 Hành xử của họ

Họ này định nghĩa các yêu cầu thiết lập và duy trì truyền thông tin cậy đến hoặc từ người dùng và TSF. Tuyến tin cậy có thể được yêu cầu đối với bất kì sự tương tác liên quan đến an toàn. Sự trao đổi đường dẫn tin cậy có thể được khởi tạo bởi người dùng trong suốt sắc tương tác với TSF, hoặc TSF có thể thiết lập truyền thông với người dùng qua đường dẫn tin cậy.

17.2.2 Phân mức thành phần

FTP_TRP.1: Đường dẫn tin cậy, yêu cầu một đường dẫn tin cậy giữa TSF và một người dùng được quy định cho một tập các sự kiện định nghĩa bởi tác giả PP/ST. Người dùng và/hoặc TSF đều có khả năng khởi tạo Đường dẫn tin cậy.

17.2.3 Quản lý của FTP_TRP.1

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

a) Lập cấu hình các hành động yêu cầu đường dẫn tin cậy, nếu được hỗ trợ.

17.2.4 Kiểm toán của FTP_TRP.1

Các hành động sau đây có thể được kiểm toán nếu FAU_GEN Tạo dữ liệu kiểm toán an toàn được đặt trong PP/ST:

a) Tối thiểu: Lỗi của các chức năng đường dẫn tin cậy.

b) Tối thiểu: Nhận dạng người dùng liên quan đến mọi lỗi của Đường dẫn tin cậy, nếu có.

c) Cơ sở: Mọi việc sử dụng thử các chức năng đường dẫn tin cậy.

d) Cơ sở: Nhận dạng người dùng liên quan đến mọi nỉu kéo Đường dẫn tin cậy, nếu có.

17.2.5 FTP_TRP.1 Đường dẫn tin cậy

Phân cấp từ: Không có các thành phần nào.

Các mối phụ thuộc: Không có sự phụ thuộc.

17.2.5.1 FTP_TRP.1.1

TSF cần quy định một đường dẫn truyền thông giữa nó và [lựa chọn: từ xa, nội hạt] những người dùng phân biệt về logic với các Đường dẫn truyền thông khác và quy định việc nhận dạng bảo đảm về điểm cuối và việc bảo vệ dữ liệu Đường dẫn khỏi sự chỉnh sửa hay bị lộ thông tin.

17.2.5.2 FTP_TRP.1.2

TSF cần cho phép [lựa chọn: *TSF, người dùng nội hạt, người dùng từ xa*] khởi tạo truyền thông qua đường dẫn tin cậy.

17.2.5.3 FTP_TRP.1.3

TSF cần yêu cầu sử dụng đường dẫn tin cậy cho [lựa chọn: *xác thực người dùng khởi đầu, [ấn định: các dịch vụ khác đối với đường dẫn tin cậy được yêu cầu]*].

Phụ lục A
(Quy định)

Ghi chú về ứng dụng các yêu cầu chức năng an toàn

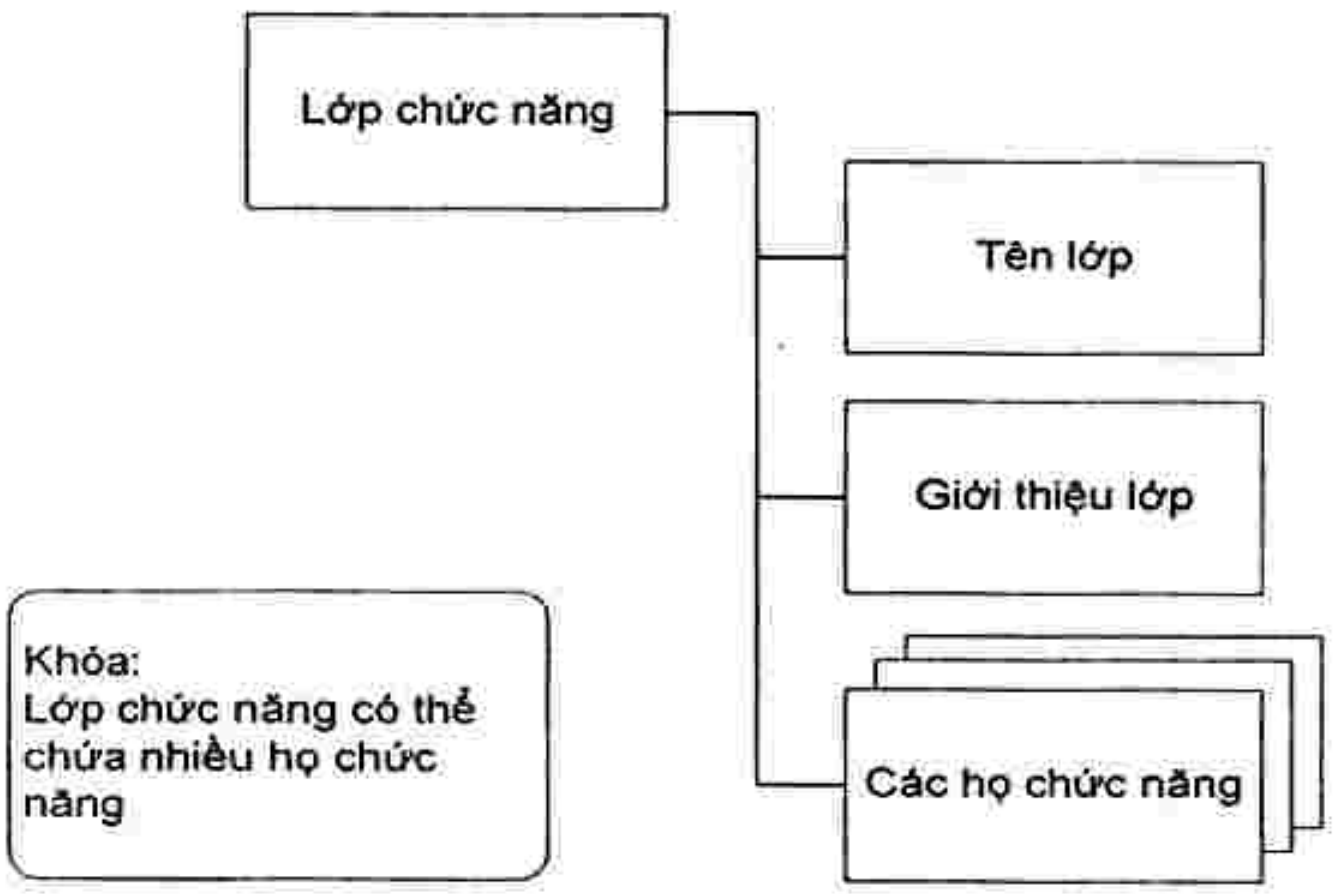
Phụ lục này bao gồm hướng dẫn bổ sung cho các họ và thành phần định nghĩa trong các phần tử của TCVN 8709 theo đó yêu cầu người sử dụng, người phát triển và đánh giá viên phải tuân theo.Để việc tìm thông tin thích hợp thuận tiện hơn, việc trình bày các lớp, họ và thành phần trong phụ lục này tương tự như sự trình bày bên trong các phần tử.

A.1 Cấu trúc phần ghi chú

Cấu trúc bản ghi chú định nghĩa nội dung và trình bày bản ghi chú liên quan đến yêu cầu chức năng của TCVN 8709.

A.1.1 Cấu trúc lớp

Hình A.1 dưới đây thể hiện cấu trúc lớp chức năng trong phụ lục này.



Hình A.1 - Cấu trúc lớp chức năng

A.1.1.1 Tên lớp

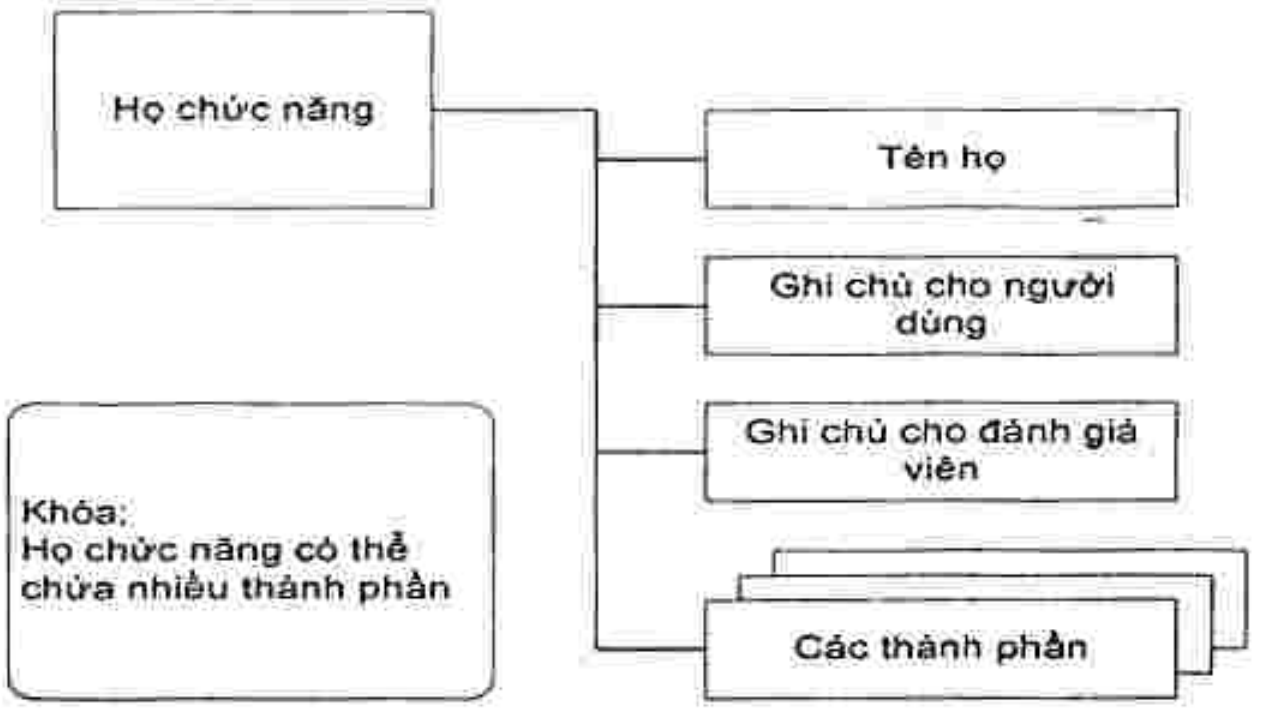
Đây là tên lớp duy nhất định nghĩa bên trong các phần tử quy chuẩn của phần TCVN 8709 này.

A.1.1.2 Giới thiệu lớp

Phần giới thiệu lớp trong phụ lục này cung cấp thông tin về việc sử dụng các họ và các thành phần của lớp. Thông tin này được hoàn thành với lược đồ mô tả tổ chức của mỗi lớp với những họ của mỗi lớp và mối liên quan giữa các thành phần trong mỗi họ.

A.1.2 Cấu trúc họ

Hình A.2 minh họa sơ đồ cấu trúc chức năng của họ cho ghi chú ứng dụng.



Hình A.2 - Cấu trúc họ chức năng cho các ghi chú ứng dụng

A.1.2.1 Tên họ

Đây là tên duy nhất của họ định nghĩa trong các phần tử quy chuẩn của phần này trong ISO /IEC 15408.

A.1.2.2 Chú thích cho người sử dụng

Chú thích cho người sử dụng bao gồm thông tin bổ sung được quan tâm bởi những người dùng tiềm năng của họ, đó có thể là PP, ST, tác giả gói chức năng hoặc những người phát triển TOE thực hiện việc tích hợp những thành phần chức năng. Sự biểu diễn cung cấp thông tin và có thể bao gồm cảnh báo về sự hạn chế của việc sử dụng và những lĩnh vực cần sự tập trung riêng khi sử dụng thành phần.

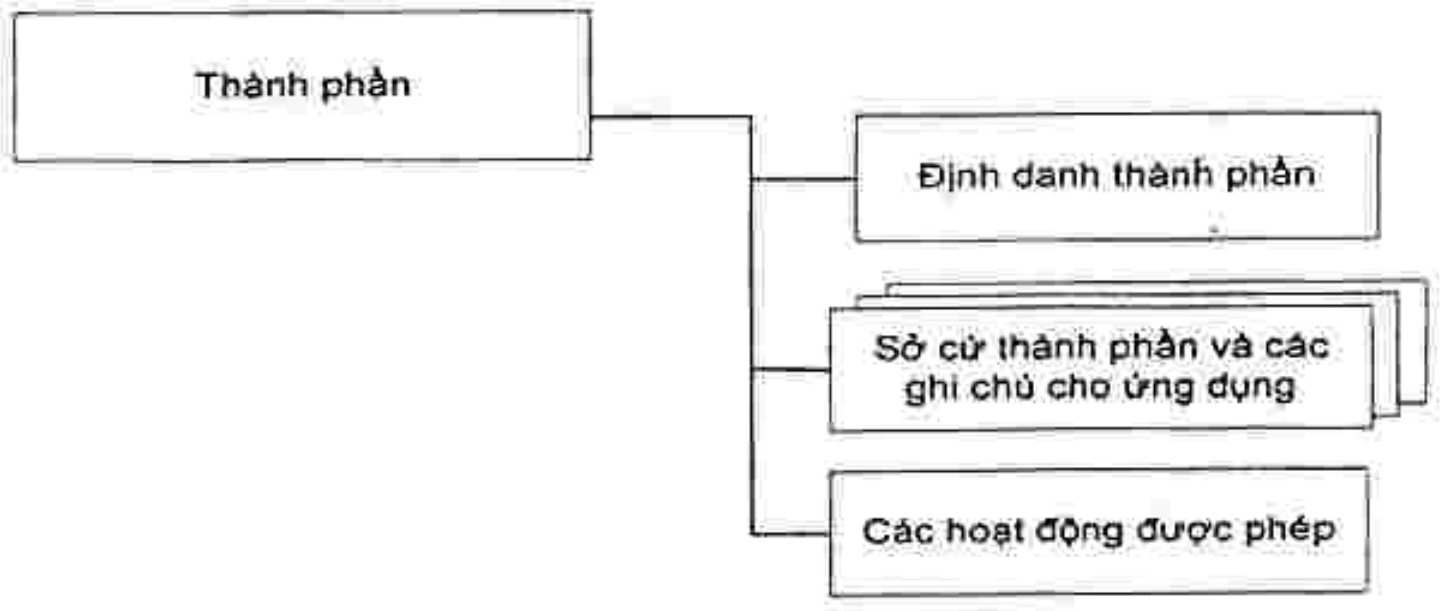
A.1.2.3 Chú thích cho đánh giá viên

Chú thích cho đánh giá viên bao gồm thông tin được quan tâm bởi những người phát triển, các đánh giá viên về một thành phần của họ. Chú thích cho đánh giá viên được trình bày trong nhiều lĩnh vực cần quan tâm riêng khi đánh giá TOE, chẳng hạn làm rõ ý nghĩa và chi tiết hóa một vấn đề cũng như cảnh báo một chi tiết cần đánh giá.

Các điều khoản về chú thích cho người sử dụng và chú thích cho đánh giá viên không bắt buộc và chỉ xuất hiện khi phù hợp.

A.1.3 Cấu trúc thành phần

Hình A.3 minh họa cấu trúc thành phần chức năng của ghi chú ứng dụng.



Hình A.3 - Cấu trúc thành phần chức năng

A.1.3.1 Định danh thành phần

Đây là tên duy nhất của thành phần định nghĩa trong phần tử quy chuẩn của TCVN 8709.

A.1.3.2 Sở cứ thành phần và các ghi chú ứng dụng

Mọi thông tin chi tiết liên quan đến thành phần có thể tìm thấy trong mệnh đề phụ sau:

- Sở cứ thành phần: bao gồm những đặc trưng của sở cứ được bổ sung chi tiết. Sở cứ thành phần chỉ xuất hiện trong lớp nào đó nếu cần thiết.
- Ghi chú ứng dụng bao gồm những bổ sung chi tiết về một thành phần nhất định. Sự bổ sung này có thể gắn liền với Chú thích cho người sử dụng và/hoặc ghi chú đánh giá viên như đã mô tả ở A.1.2. Bổ sung chi tiết có thể được sử dụng để giải thích bản chất những sự phụ thuộc (ví dụ: thông tin chia sẻ hoặc hành động chia sẻ).

Điều khoản nhỏ này không bắt buộc và chỉ xuất hiện nếu phù hợp.

A.1.3.3 Những hành động được phép

Đây là những chỉ dẫn liên quan đến những hành động được phép của thành phần.

Điều khoản nhỏ này không bắt buộc và chỉ xuất hiện nếu phù hợp.

A.2 Các bảng về mối phụ thuộc

Bảng sau đây chỉ rõ sự phụ thuộc trực tiếp, gián tiếp và tùy chọn của các thành phần chức năng. Mỗi thành phần có sự phụ thuộc liên quan đến thành phần khác được xếp vào một cột. Mỗi thành phần chức năng được xếp vào một hàng. Giá trị ký tự của ô giao giữa cột và hàng chỉ rõ sự phụ thuộc tương ứng là trực tiếp (x), gián tiếp (-) hay tùy chọn (o). Một ví dụ về thành phần với phụ thuộc tùy chọn là FDP_ETC.1 (Xuất dữ liệu người dùng không có thuộc tính bảo mật) yêu cầu hoặc FDP_ACC.1 (Điều khiển truy nhập tập con) hoặc FDP_IFC.1 (Điều khiển luồng thông tin). Do vậy nếu có FDP_ACC.1 thì sẽ không cần FDP_IFC.1 và ngược lại. Nếu không có ký tự nào xuất hiện, thành phần không có tính phụ thuộc vào thành phần nào khác.

Bảng A.1 - Bảng phụ thuộc của lớp FAU: Kiểm toán an toàn

	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FIA_UID.1	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1
FAU_ARP.1	-	X							-
FAU_GEN.1									X
FAU_GEN.2	X				X				-
FAU_SAA.1	X								-
FAU_SAA.2					X				
FAU_SAA.3									
FAU_SAA.4									
FAU_SAR.1	X								-
FAU_SAR.2	-		X						-
FAU_SAR.3	-		X						-
FAU_SEL.1	X				-	X	-	-	-
FAU_STG.1	X								-
FAU_STG.2	X								-
FAU_STG.3	-			X					-
FAU_STG.4	-			X					-

Bảng A.2 – Bảng phụ thuộc của lớp FCO: Truyền thông

	FIA_UID.1
FCO_NRO.1	X
FCO_NRO.2	X
FCO_NRR.1	X
FCO_NRR.2	X

Bảng A.3 – Bảng phụ thuộc của lớp FCS: Hỗ trợ mật mã

	ADV_SPM.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITC.2	FIA_UID.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1
FCS_CKM.1	-	-	O	X	O	-	-	-	-	-	-	-	-	X	-	-	-	-	-	-
FCS_CKM.2	-	O	-	X	-	-	-	-	-	O	O	-	-	X	-	-	-	-	-	-
FCS_CKM.3	-	O	-	X	-	-	-	-	-	O	O	-	-	X	-	-	-	-	-	-
FCS_CKM.4	-	O	-	-	-	-	-	-	-	O	O	-	-	X	-	-	-	-	-	-
FCS_COP.1	-	O	-	X	-	-	-	-	-	O	O	-	-	X	-	-	-	-	-	-

Bảng A.4 – Bảng phụ thuộc của lớp FDP: Bảo vệ dữ liệu người dùng

	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITT.1	FDP_ITT.2	FDP_UIT.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1
FDP_ACC.1	-	X	-	-				-	-	-	-	-	-		
FDP_ACC.2	-	X	-	-				-	-	-	-	-			
FDP_ACF.1	X	-	-	-				-	-	X	-	-			
FDP_DAU.1															
FDP_DAU.2								X							
FDP_ETC.1	O	-	O	-				-	-	-	-	-			
FDP_ETC.2	O	-	O	-				-	-	-	-	-			
FDP_IFC.1	-	-	-	X				-	-	-	-	-			
FDP_IFC.2	-	-	-	X				-	-	-	-	-			
FDP_IFF.1	-	-	X	-				-	-	X	-	-			
FDP_IFF.2	-	-	X	-				-	-	X	-	-			
FDP_IFF.3	-	-	X	-				-	-	-	-	-			
FDP_IFF.4	-	-	X	-				-	-	-	-	-			
FDP_IFF.5	-	-	X	-				-	-	-	-	-			
FDP_IFF.6	-	-	X	-				-	-	-	-	-			
FDP_ITC.1	O	-	O	-				-	-	X	-	-			
FDP_ITC.2	O	-	O	-				-	-	-	-	-	X	O	O
FDP_ITT.1	O	-	O	-				-	-	-	-	-			
FDP_ITT.2	O	-	O	-				-	-	-	-	-			
FDP_ITT.3	O	-	O	-	X			-	-	-	-	-			
FDP_ITT.4	O	-	O	-		X		-	-	-	-	-			
FDP_RIP.1															
FDP_RIP.2															
FDP_ROL.1	O	-	O	-				-	-	-	-	-			
FDP_ROL.2	O	-	O	-				-	-	-	-	-			
FDP_SDI.1															
FDP_SDI.2															
FDP_UCT.1	O	-	O	-				-	-	-	-	-		O	O
FDP_UIT.1	O	-	O	-				-	-	-	-	-		O	O
FDP_UIT.2	O	-	O	-			O	-	-	-	-	-		O	-
FDP_UIT.3	O	-	O	-			O	-	-	-	-	-		O	-

Bảng A.5 – Bảng phụ thuộc của lớp FIA: Định danh và xác thực

	FIA_ATD.1	FIA_UAU.1	FIA_UID.1
FIA_AFL.1		X	-
FIA_ATD.1			
FIA_SOS.1			
FIA_SOS.2			
FIA_UAU.1			X
FIA_UAU.2			X
FIA_UAU.3			
FIA_UAU.4			
FIA_UAU.5			
FIA_UAU.6			
FIA_UAU.7		X	-
FIA_UID.1			
FIA_UID.2			
FIA_USB.1	X		

Bảng A.6 – Bảng phụ thuộc của lớp FMT: Quản lý an toàn

	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1
FMT_MOF.1					-				X	X	
FMT_MSA.1	O	-	O	-	-	-	-		X	X	
FMT_MSA.2	O	-	O	-	-	X	-		-	X	
FMT_MSA.3	-	-	-	-	-	X	-		-	X	
FMT_MSA.4	O	-	O	-	-	-	-		-	-	
FMT_MTD.1					-				X	X	
FMT_MTD.2					-			X	-	X	
FMT_MTD.3					-			X	-	-	
FMT_REV.1					-					X	
FMT_SAE.1					-					X	X
FMT_SMF.1											
FMT_SMR.1					X						
FMT_SMR.2					X						
FMT_SMR.3					-					X	

Bảng A.7 – Bảng phụ thuộc của lớp FPR: Tính riêng tư

	FIA_UID.1	FPR_UNO.1
FPR_ANO.1		
FPR_ANO.2		
FPR_PSE.1		
FPR_PSE.2	X	
FPR_PSE.3		
FPR_UNL.1		
FPR_UNO.1		
FPR_UNO.2		
FPR_UNO.3		X
FPR_UNO.4		

Bảng A.8 – Bảng phụ thuộc của lớp FPT: Bảo vệ TSF

	AGD_OPE.1	FIA_UID.1	FMT_MOF.1	FMT_SMF.1	FMT_SMR.1	FPT_ITT.1
FPT_FLS.1						
FPT_ITA.1						
FPT_ITC.1						
FPT_ITI.1						
FPT_ITI.2						
FPT_ITT.1						
FPT_ITT.2						
FPT_ITT.3						X
FPT_PHP.1						
FPT_PHP.2		-	X	-	-	
FPT_PHP.3						
FPT_RCV.1	X					
FPT_RCV.2	X					
FPT_RCV.3	X					
FPT_RCV.4						
FPT_RPL.1						
FPT_SSP.1						X
FPT_SSP.2						X
FPT_STM.1						
FPT_TDC.1						
FPT_TEE.1						
FPT_TRC.1						X
FPT_TST.1						

Bảng A.9 – Bảng phụ thuộc của lớp FRU: Sử dụng tài nguyên

	FPT_FLS.1
FRU_FLT.1	X
FRU_FLT.2	X
FRU_PRS.1	
FRU_PRS.2	
FRU_RSA.1	
FRU_RSA.2	

Bảng A.10 – Bảng phụ thuộc của lớp FTA: Truy nhập TOE

	FIA_UAU.1	FIA_UID.1
FTA_LSA.1		
FTA_MCS.1		X
FTA_MCS.2		X
FTA_SSL.1	X	-
FTA_SSL.2	X	-
FTA_SSL.3		
FTA_SSL.4		
FTA_TAB.1		
FTA_TAH.1		
FTA_TSE.1		

Phụ lục B

(Quy định)

Các lớp, họ và thành phần chức năng

Các Phụ lục từ C đến M cung cấp các ghi chú cho ứng dụng cho các lớp chức năng định nghĩa trong phần nội dung chính của tập TCVN 8709 này.

Phụ lục C

(Quy định)

Lớp FAU: Kiểm toán an toàn

TCVN 8709 cho phép tác giả PP/ST được xác định những yêu cầu nhằm giám sát thao tác của người dùng và trong một số trường hợp phát hiện sự vi phạm đã, sắp hoặc có khả năng xảy ra đối với việc thực thi các SFR. Chức năng giám sát kiểm toán của TOE dùng để giám sát những sự kiện liên quan đến an toàn và đóng vai trò chống lại các vi phạm an toàn. Các yêu cầu của họ kiểm toán an toàn bao gồm những chức năng bảo vệ kiểm tra dữ liệu, định dạng dữ liệu, và lựa chọn sự kiện cũng như các công cụ phân tích, cảnh báo vi phạm và phân tích thời gian thực. Dấu vết kiểm toán cần được biểu diễn với định dạng có thể đọc được trực tiếp hoặc gián tiếp (chẳng hạn như sử dụng công cụ kiểm toán rút gọn) hoặc cả hai.

Khi phát triển các yêu cầu kiểm toán an toàn, tác giả PP/ST cần ghi chú về mối quan hệ giữa họ kiểm toán và thành phần. Khả năng này xác định tập hợp những yêu cầu kiểm toán danh sách những họ/thành phần đồng thời tạo nên kết quả là chức năng kiểm toán không hiệu quả (ví dụ chức năng kiểm toán yêu cầu tất cả các sự kiện liên quan đến an toàn phải được kiểm toán nhưng không thể điều khiển được các cá thể đơn lẻ như từng người dùng hoặc vật thể).

C.1 Các yêu cầu kiểm toán trong môi trường phân tán

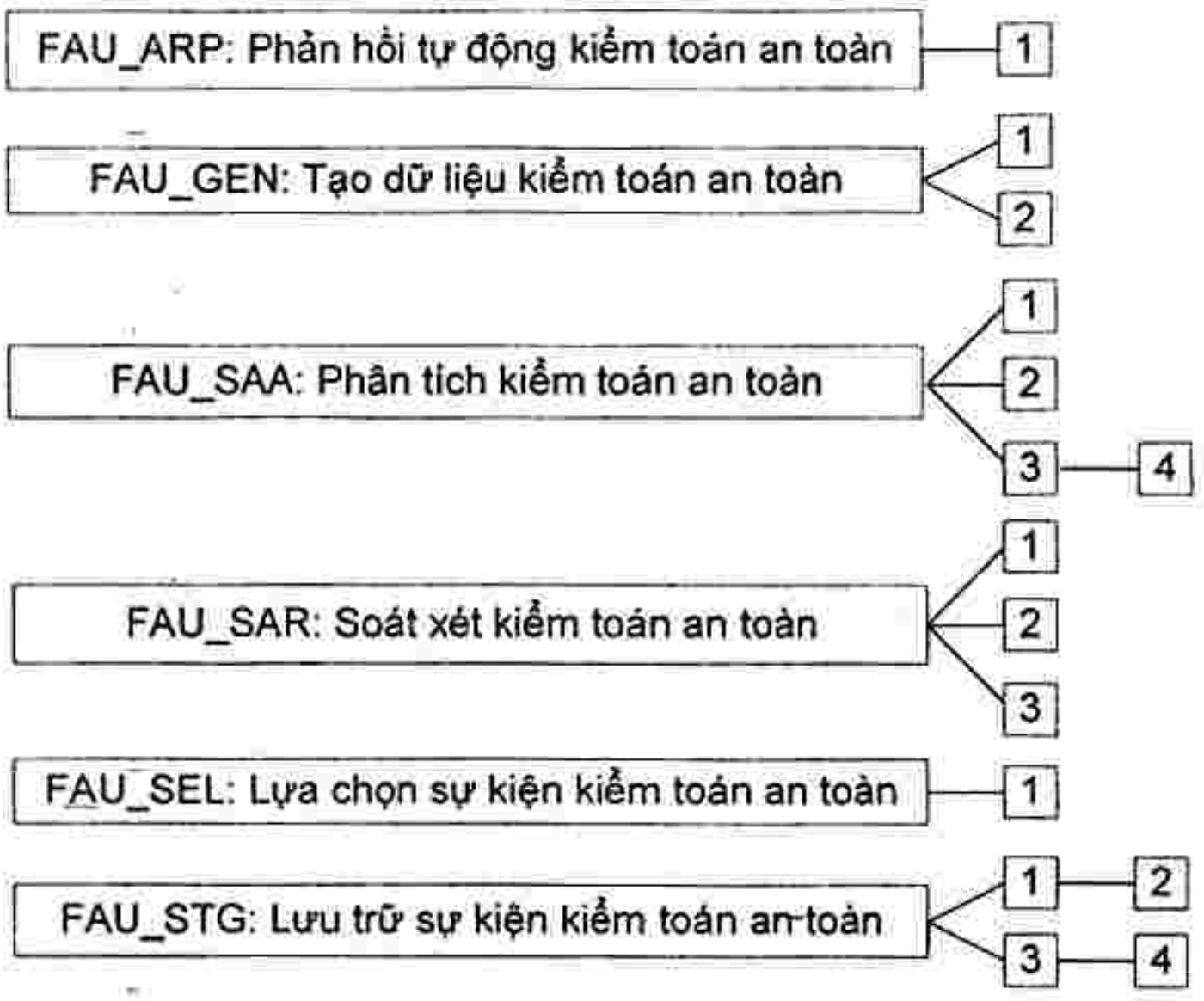
Việc thực thi các yêu cầu kiểm toán trong mạng và các hệ thống lớn có thể khác biệt nhiều so với việc thực thi cần có đối với các hệ thống độc lập. Các hệ thống lớn hơn, phức tạp và tích cực hơn, yêu cầu được quan tâm hơn liên quan đến việc thu thập dữ liệu kiểm toán nào và nó cần được quản lý thế nào do tính khả thi thấp của việc giải trình (hoặc thậm chí lưu trữ) những gì đã thu thập được. Khái niệm truyền thống về danh sách theo thứ tự thời gian hoặc "dấu vết" của các sự kiện kiểm toán có thể không áp dụng được trong một mạng tổng thể không đồng bộ với nhiều sự kiện xảy ra bất kỳ cùng một lúc.

Mặt khác, những máy tính, máy chủ khác trong một TOE phân tán có thể có những chính sách ghi danh và giá trị khác nhau. Cần có một dạng biểu diễn tên theo ký hiệu để tránh dư thừa hoặc xung đột về tên.

Một tập hợp đa đối tượng được truy nhập bởi nhiều người sử dụng có thẩm quyền cần có chức năng kiểm toán hữu ích trong các hệ thống phân tán.

Việc lạm quyền của người dùng được cấp quyền cần được đề cập đến một cách hệ thống tránh việc lưu trữ cục bộ dữ liệu kiểm toán liên quan đến các hành động của quản trị viên.

Hình C.1 minh họa sự phân tách của lớp này ra các thành phần cấu thành.



Hình C.1 –Phân cấp lớp FAU: Kiểm toán an toàn

C.2 Đáp ứng tự động kiểm toán an toàn (FAU_ARP)

C.2.1 Chú thích cho người sử dụng

Họ đáp ứng tự động kiểm toán an toàn mô tả các yêu cầu về xử lý các sự kiện kiểm toán. Yêu cầu có thể bao gồm cảnh báo hoặc những hành động TSF (đáp ứng tự động). Ví dụ, TSF có thể bao gồm việc tạo ra những cảnh báo thời gian thực, kết thúc một tiến trình xâm phạm, vô hiệu hóa một dịch vụ, ngắt kết nối hoặc làm mất hiệu lực một tài khoản người dùng.

Một sự kiện kiểm toán được xác định là "vi phạm an toàn nghiêm trọng" nếu được chỉ rõ trong thành phần phân tích kiểm toán an toàn (FAU_SAA).

C.2.2 FAU_ARP.1 Cảnh báo an toàn

C.2.2.1 Chú thích cho ứng dụng người sử dụng

Một hành động cần được thực hiện ngay sau sự kiện cảnh báo. Hành động này có thể thông báo cho người được cấp quyền cùng với một tập hợp hành động gợi ý tương ứng. Thời điểm của hành động cũng nên được xem xét bởi PP/ST.

C.2.2.2 Các hoạt động

C.2.2.2.1 Chỉ định

Trong FAU_ARP.1.1, PP/ST cần xác định hành động cần thực hiện bởi một người dùng có quyền khi xảy ra vi phạm an toàn nghiêm trọng. Ví dụ: thông báo với người có quyền, vô hiệu hóa đối tượng gây nên vi phạm an toàn.

C.3 Tạo các dữ liệu kiểm toán an toàn (FAU_GEN)

C.3.1 Chú thích cho người sử dụng

Họ tạo dữ liệu kiểm toán an toàn bao gồm những yêu cầu chỉ rõ các sự kiện kiểm toán cần được tạo ra bởi TSF cho sự kiện liên quan an toàn.

Họ này được giới thiệu ở khía cạnh tránh sự phụ thuộc vào tất cả các thành phần yêu cầu hỗ trợ kiểm toán. Mỗi thành phần gồm một mệnh đề kiểm toán trong đó sự kiện trong vùng chức năng tương ứng phải được liệt kê. Khi tác giả PP/ST lắp ghép các PP/ST, các phần tử trong vùng kiểm toán được sử dụng để tạo thành biến hoàn chỉnh của thành phần. Do vậy, đặc điểm dữ liệu của mỗi vùng chức năng được đặt trong vùng chức năng đó.

Danh sách các sự kiện có thể kiểm toán là hoàn toàn phụ thuộc vào các họ chức năng khác trong PP/PT. Mỗi định nghĩa họ do đó cần bao gồm một danh sách các sự kiện có thể kiểm toán thuộc họ cụ thể của nó. Mỗi sự kiện kiểm toán trong danh sách các sự kiện có thể kiểm toán được xác định rõ trong họ chức năng cần phù hợp với một trong các mức tạo ra sự kiện kiểm toán được ghi rõ trong họ này (nghĩa là: mức tối thiểu, cơ bản, chi tiết). Điều này cung cấp cho tác giả PP/ST thông tin cần thiết để đảm bảo rằng tất cả các sự kiện kiểm toán tương ứng đều được xác định rõ trong PP/ST. Các ví dụ sau cho thấy các sự kiện có thể kiểm toán sẽ được xác định rõ trong các họ chức năng tương ứng như thế nào:

" Các hoạt động sau cần được kiểm toán nếu tạo dữ liệu kiểm toán an toàn (FAU_GEN) có trong PP/ST:

a/ Tối thiểu: Việc sử dụng thành công các chức năng quản lý thuộc tính an toàn của người sử dụng

b/ Cơ bản: Tất cả việc sử dụng thử các chức năng quản lý thuộc tính an toàn của người sử dụng

c/ Cơ bản: Xác định thuộc tính an toàn người sử dụng nào đã sửa đổi

d/ Chi tiết: Ngoại trừ những mục dữ liệu thuộc tính nhạy cảm cụ thể (mật khẩu, mã khóa) các giá trị mới của thuộc tính cần được lấy."

Với mỗi thành phần chức năng được chọn, sự kiện kiểm toán trong thành phần đó cùng mức và dưới mức so với FAU_GEN cần phải cho phép kiểm toán. Các sự kiện kiểm toán có cấu trúc phân cấp. Ví dụ khi chọn mức kiểm toán cơ bản, tất cả các sự kiện cũng phải ở mức cơ bản hoặc tối thiểu. Mặt khác, nếu mức chi tiết được lựa chọn, các sự kiện có thể ở mức chi tiết, cơ bản hoặc tối thiểu.

Ví dụ: những sự kiện sau nên được kiểm toán trong mỗi thành phần chức năng PP/ST:

a/ Giới thiệu về đối tượng bên trong TSC đến không gian địa chỉ đối tượng

b/ Xóa đối tượng

c/ Phân phối hoặc hủy bỏ khả năng hoặc quyền truy nhập

d/ Thay đổi đối tượng hoặc thuộc tính của đối tượng

e/ Kiểm tra chính sách thực hiện bởi TSF khi có yêu cầu từ một đối tượng

f/ Sử dụng quyền truy nhập để vượt qua kiểm tra chính sách;

g/ Sử dụng định danh và xác thực;

h/ Hành động từ một người điều hành và/ hoặc người được cấp quyền.

C.3.2 FAU_GEN.1 Tạo dữ liệu kiểm toán

C.3.2.1 Chú thích cho ứng dụng người sử dụngChú thích cho ứng dụng người sử dụng

Thành phần này xác định những yêu cầu về bản ghi kiểm toán được tạo ra tương ứng với sự kiện và thông tin trong bản ghi.

Tạo dữ liệu kiểm toán FAU_GEN.1 tự nó có thể được sử dụng khi các SFR không yêu cầu định danh người dùng cụ thể kết hợp với sự kiện kiểm toán. Nó có thể là thích hợp khi PP/ST cũng chứa các yêu cầu tính riêng tư. Nếu phải kết hợp định danh người dùng thì có thể cần sử dụng thêm liên kết định danh người dùng FAU_GEN 2.

Nếu chủ thể là một người dùng thì định danh người dùng có thể được ghi lại như định danh chủ thể. Định danh người dùng có thể không được kiểm lại nếu Xác thực người dùng (FIA_UAU) không được áp dụng. Do đó trong trường hợp một đăng nhập không hợp lệ định danh người dùng được yêu cầu cần được ghi lại. Có thể xem xét để thấy khi nào một định danh đã lưu là chưa được xác thực.

C.3.2.2 Chú thích cho đánh giá viên

TOE có sự phụ thuộc vào nhãn thời gian (Time stamp – FPT_STM). Nếu độ chính xác của thời gian không phải vấn đề, có thể bỏ qua sự phụ thuộc này.

C.3.2.3 Các hoạt động

C.3.2.3.1 Phép chọn

Trong FAU_GEN.1.1, PP/ST cần lựa chọn mức độ của sự kiện kiểm toán trong mệnh đề con của các thành phần chức năng khác bao gồm trong PP/ST. Cấp độ này bao gồm: tối thiểu, cơ bản, chi tiết và không xác định.

C.3.2.3.2 Chỉ định

Trong FAU_GEN.1.1, PP/ST cần Chỉ định những sự kiện kiểm toán khác trong danh sách những sự kiện kiểm toán. Có thể không Chỉ định gì cả hoặc Chỉ định những sự kiện mức cao hơn yêu cầu cũng như các sự kiện được tạo ra qua giao diện lập trình ứng dụng (API).

Trong FAU_GEN.1.2, PP/ST cần Chỉ định những thông tin liên quan nếu có trong mỗi sự kiện kiểm toán bao gồm trong PP/ST.

C.3.3 FAU_GEN.2 Kết hợp định danh người dùng

C.3.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này liên quan tới những sự kiện kiểm toán tài khoản của người dùng và cần sử dụng kết hợp với FAU_GEN.1

Giữa yêu cầu kiểm toán và tính riêng tư có sự mâu thuẫn. Với mục đích kiểm toán cần biết ai thực hiện một hành động nào đó. Người dùng có thể lưu giữ các hành động của mình và không bị nhận biết bởi những người khác. Hoặc có thể yêu cầu trong chính sách an toàn sự bảo vệ định danh của người dùng. Trong những trường hợp đó, đối tượng kiểm toán và sự riêng tư có thể mâu thuẫn với nhau. Do vậy, nếu lựa chọn yêu cầu này và sự riêng tư là quan trọng cần cân nhắc bí danh của người dùng. Yêu cầu xác định tên thật của người dùng dựa trên bí danh được xác định trong lớp riêng.

Nếu định danh người dùng chưa được kiểm lại qua việc xác thực, thì trường hợp đăng nhập không hợp lệ thì định danh người dùng được yêu cầu nên được lưu lại. Cần xem xét để thấy khi nào một định danh đã lưu là chưa được xác thực.

C.4 Phân tích kiểm toán an toàn (FAU_SAA)

C.4.1 Chú thích cho người sử dụng

Họ này xác định những yêu cầu về việc tự động phân tích Hoạt động của hệ thống và dữ liệu kiểm toán nhằm phát hiện ra những sự vi phạm có thể hoặc đã xảy ra. Sự phân tích có thể thực hiện với sự hỗ trợ của phát hiện xâm nhập hoặc tự động phản ứng với sự vi phạm an toàn sắp xảy ra.

Hành động được thực hiện bởi TSF khi phát hiện ra sự vi phạm sẽ hoặc có nguy cơ xảy ra được định nghĩa trong các thành phần Phản hồi tự động kiểm toán an toàn (FAU_ARP).

Khi phân tích thời gian thực, dữ liệu kiểm toán có thể chuyển thành những dạng phù hợp với việc xử lý tự động hoặc ở dạng xem lại được với người dùng có quyền.

C.4.2 FAU_SAA.1 Phân tích khả năng vi phạm

C.4.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này được sử dụng để xác định một tập hợp các sự kiện kiểm toán liên quan đến sự vi phạm tiềm năng trong TSP và mọi luật được dùng để thực hiện phân tích vi phạm.

C.4.2.2 Các hoạt động

C.4.2.2.1 Chỉ định

Trong FAU_SAA.1.2, tác giả PP/ST cần chỉ rõ tập con của những sự kiện kiểm toán đã định nghĩa mà sự xảy ra hoặc xảy ra tích lũy của chúng cần được phát hiện là dấu hiệu vi phạm tiềm năng việc thi hành của các SFR.

Trong FAU_SAA.1.2 tác giả PP/ST cần chỉ rõ bất cứ qui định nào khác mà TSF cần sử dụng trong phân tích dấu vết kiểm chứng. Những luật này có thể bao gồm những yêu cầu cụ thể thể hiện nhu cầu đối với các sự kiện xảy ra trong một khoảng thời gian nhất định (có nghĩa trong khoảng của ngày, một thời kỳ). Nếu không có những qui định bổ sung mà TSF có thể sử dụng trong phân tích dấu vết kiểm chứng thì sự chỉ định này sẽ được hoàn thành với "không" ("none").

C.4.3 FAU_SAA.2 Phát hiện bất thường dựa trên mô tả tóm tắt

C.4.3.1 Chú thích cho ứng dụng người sử dụng

Tiểu sử là một cấu trúc mô tả biểu hiện của người sử dụng hoặc đối tượng, biểu diễn bằng cách nào người sử dụng hoặc đối tượng tương tác với TSF. Mẫu sử dụng được xây dựng với nhiều kiểu hoạt động mà người sử dụng hoặc đối tượng tham gia (Ví dụ các mẫu về xuất hiện ngoại lệ, tận dụng tài nguyên như thế nào, khi nào). Phương thức những hoạt động khác nhau được ghi lại trong tiểu sử (ví dụ tính toán tài nguyên, bộ đếm sự kiện, thời gian) được gọi là thuộc tính tiểu sử.

Mỗi tiểu sử thể hiện mẫu sử dụng của thành viên trong nhóm tiểu sử mục tiêu. Mẫu sử dụng có thể dựa trên quá khứ hoặc sự sử dụng thông thường của người dùng trong các nhóm tương tự nhau. Một nhóm tiểu sử mục tiêu là một hoặc nhiều hơn những người dùng tương tác với TSF. Hoạt động của mỗi thành viên trong nhóm tiểu sử được sử dụng bởi công cụ phân tích để xây dựng mẫu sử dụng trong nhóm tiểu sử đó. Sau đây là các ví dụ về nhóm tiểu sử mục tiêu:

a/ **Tài khoản người dùng**: mỗi người dùng có một tiểu sử

b/ **Định danh nhóm hoặc tài khoản nhóm**: một tiểu sử cho tất cả người dùng với cùng định danh nhóm hoặc tài khoản nhóm

c/ **Vai trò vận hành**: một tiểu sử cho tất cả người dùng có chung một vai trò vận hành.

d/ **Hệ thống**: một tiểu sử cho tất cả người dùng trong một hệ thống

Mỗi thành viên của một nhóm tiểu sử mục tiêu được gán một tỷ lệ nghi ngờ thể hiện mức độ tương ứng của những hành động gần đây nhất của người dùng với mẫu sử dụng trong nhóm tiểu sử.

Mức độ tinh vi của những công cụ phát hiện bất thường được xác định phần lớn dựa trên số lượng tiểu sử nhóm mục tiêu và độ phức tạp của thông số tiểu sử.

Thành phần này được sử dụng để xác định tập hợp các sự kiện kiểm toán có khả năng vi phạm với TSP và những công cụ dùng để phân tích sự vi phạm. Tập hợp những sự kiện và luật này có thể thay đổi bởi người dùng có quyền, chẳng hạn thêm, sửa hoặc xóa sự kiện hoặc luật.

PP/ST cần liệt kê chi tiết những hoạt động nào cần giám sát và/hoặc phân tích bởi TSF. PP/ST cũng cần xác định những thông tin liên quan để tạo nên tiểu sử sử dụng.

FAU_SAA.2 **Phát hiện bất thường dựa trên mô tả tóm tắt** yêu cầu TSF phải duy trì tiểu sử sử dụng của hệ thống. Điều này có nghĩa là sự phát hiện bất thường sẽ chủ động cập nhật tiểu sử sử dụng dựa trên những hành động của những thành viên trong nhóm tiểu sử. Điều quan trọng ở đây là thông số biểu diễn hành động của người dùng được định nghĩa trong PP/ST. Ví dụ, có thể có hàng nghìn hành động được cho phép thực hiện với mỗi người dùng nhưng sự phát hiện bất thường chỉ giám sát một tập hợp con của những hành động đó. Những hành động bất thường diễn ra trong thời gian dài có thể sẽ trở thành bình thường với người dùng nhất định nào đó và TSF sẽ không nên giám sát những hành động này nữa.

C.4.3.2 Các hoạt động

C.4.3.2.1 Chỉ định

Trong FAU_SAA.2.1, PP/ST cần xác định nhóm tiểu sử mục tiêu. Một PP/ST có thể gồm nhiều nhóm tiểu sử mục tiêu.

Trong FAU_SAA.2.3, PP/ST cần xác định điều kiện trong đó những hành động bất thường được thông báo qua TSF. Điều kiện có thể bao gồm tỷ lệ nghi ngờ đạt đến một mức nhất định hoặc kiểu của hành động bất thường.

C.4.4 FAU_SAA Thử nghiệm tấn công đơn giản

C.4.4.1 Chú thích cho ứng dụng người sử dụng

Trong thực tế, rất ít khi một công cụ phân tích phát hiện ra sự vi phạm an ninh sắp xảy ra. Tuy nhiên, một số sự kiện hệ thống rất quan trọng cần được xem xét độc lập. Ví dụ những sự kiện liên quan đến xóa một tệp chứa khóa dữ liệu an toàn TSF (mật khẩu) hoặc hành động người dùng từ xa cố gắng chiếm quyền quản lý. Những sự kiện đó gọi là sự kiện dấu hiệu mà sự xuất hiện của chúng được coi như hành động xâm nhập.

Sự phức tạp của một công cụ sẽ phụ thuộc rất lớn vào sự chỉ định của PP/ST khi định danh tập hợp những sự kiện dấu hiệu.

PP/ST cần liệt kê chi tiết những sự kiện cần giám sát bởi TSF để thực hiện phân tích. PP/ST cần định danh những thông tin liên quan cần thiết đến một sự kiện nhằm xác định sự kiện đó có phải là sự kiện dấu hiệu không.

Những thông báo quản trị cần cung cấp sao cho người dùng có quyền hiểu được ý nghĩa sự kiện và có những phản hồi thích hợp.

Cần có những phương pháp để có thể giám sát thao tác hệ thống mà không hoàn toàn phụ thuộc vào dữ liệu kiểm toán. Ví dụ có thể sử dụng những công cụ phát hiện xâm nhập hiện có hoặc trước đây không sử dụng dữ liệu kiểm toán.

Phần tử trong FAU_SAA.3 Phát hiện tấn công đơn giản không yêu cầu TSF thực hiện trong cùng TSF đang được giám sát thao tác. Do vậy, có thể phát triển một thành phần phát hiện xâm nhập độc lập với hệ thống đang được giám sát.

C.4.4.2 Các hoạt động

C.4.4.2.1 Chỉ định

Trong FAU_SAA.3.1, người biên soạn PP/ST cần nhận dạng một tập con gốc các sự kiện hệ thống mà sự xuất hiện của chúng tách biệt với những hành động hệ thống khác, có thể cho thấy sự vi phạm thi hành của các SFR. Chúng gồm các sự kiện mà bản thân thể hiện rõ sự vi phạm việc thi hành của các SFR, hoặc sự xảy ra của chúng đáng kể đến nỗi có thể bảo đảm có hành động.

Trong FAU_SAA.3.2, PP/ST cần xác định thông tin được sử dụng để giám sát hoạt động hệ thống. Thông tin này là dữ liệu đầu vào được công cụ phân tích sử dụng để tìm những hành động hệ thống xuất hiện trong TOE. Dữ liệu này bao gồm dữ liệu kiểm toán, dữ liệu kiểm toán kết hợp với dữ liệu hệ thống khác hoặc những dữ liệu khác với dữ liệu kiểm toán. PP/ST cần xác định chính xác những sự kiện hệ thống và thuộc tính hệ thống được sử dụng để giám sát dữ liệu đầu vào.

C.4.5 FAU_SAA.4 Thử nghiệm tấn công phức tạp

C.4.5.1 Chú thích cho ứng dụng người sử dụng

Trong thực tế, rất ít khi một công cụ phân tích phát hiện ra sự vi phạm an ninh sắp xảy ra. Tuy nhiên, một số sự kiện hệ thống rất quan trọng cần được xem xét độc lập. Ví dụ những sự kiện liên quan đến xóa một tệp chứa khóa dữ liệu an toàn TSF (mật khẩu) hoặc hành động người dùng từ xa cố gắng chiếm quyền quản lý. Những sự kiện đó gọi là sự kiện dấu hiệu mà sự xuất hiện của chúng được coi như hành động xâm nhập.

Sự phức tạp của một công cụ sẽ phụ thuộc rất lớn vào sự chỉ định của PP/ST khi định danh tập hợp những sự kiện dấu hiệu.

PP/ST cần liệt kê chi tiết những sự kiện cần giám sát bởi TSF để thực hiện phân tích. PP/ST cần định danh những thông tin liên quan cần thiết đến một sự kiện nhằm xác định sự kiện đó có phải là sự kiện dấu hiệu không.

Những thông báo quản trị cần cung cấp sao cho người dùng có quyền hiểu được ý nghĩa sự kiện và có những phản hồi thích hợp.

Cần có những phương pháp để có thể giám sát hoạt động hệ thống mà không hoàn toàn phụ thuộc vào dữ liệu kiểm toán. Ví dụ có thể sử dụng những công cụ phát hiện xâm nhập hiện có hoặc trước

đây không sử dụng dữ liệu kiểm toán. Vì vậy, PP/ST được yêu cầu phải xác định dữ liệu đầu vào để giám sát hoạt động hệ thống.

Phần tử trong Phát hiện tấn công phức tạp FAU_SAA.4 không yêu cầu TSF thực hiện trong cùng TSF đang được giám sát hoạt động. Do vậy, có thể phát triển một thành phần phát hiện xâm nhập độc lập với hệ thống đang được giám sát.

C.4.5.2 Các hoạt động

C.4.5.2.1 Chỉ định

Trong FAU_SAA.4.1, PP/ST cần định danh một tập hợp gốc danh sách của chuỗi những sự kiện hệ thống mà sự xuất hiện của chúng được coi là kịch bản xâm nhập đã biết trước. Mỗi sự kiện trong chuỗi được gắn với một sự kiện hệ thống đã giám sát.

Trong FAU_SAA.4.1, người biên soạn PP/ST nên định danh tập con cơ sở của những sự kiện hệ thống mà sự xuất hiện của chúng tách biệt với những hoạt động hệ thống khác, có thể chỉ ra sự vi phạm việc thi hành của các SFR. Chúng gồm các sự kiện mà bản thân thể hiện rõ sự vi phạm việc thi hành của các SFR, hoặc sự xảy ra của chúng đáng kể đến nỗi có thể bảo đảm có hành động.

Trong FAU_SAA.4.2, PP/ST cần xác định thông tin được sử dụng để xác định hoạt động của hệ thống. Thông tin này là dữ liệu đầu vào cho các công cụ phân tích để tìm ra những hành động hệ thống xuất hiện trong TOE. Dữ liệu này có thể bao gồm dữ liệu kiểm toán, hoặc sự kết hợp của dữ liệu kiểm toán với những dữ liệu khác. PP/ST cũng cần định nghĩa chính xác những sự kiện hệ thống và thuộc tính sự kiện đang được giám sát với dữ liệu đầu vào.

C.5 Soát xét kiểm toán an toàn (FAU_SAR)

C.5.1 Chú thích cho người sử dụng

Họ xem xét lại kiểm chứng an toàn định nghĩa các yêu cầu liên quan đến sự xem xét lại thông tin kiểm chứng.

Những chức năng này nên cho phép lưu trữ trước hoặc lưu trữ sau lựa chọn kiểm toán để xem xét lại trong đó có thể bao gồm:

- Hành động của người sử dụng (các hành động liên quan đến định danh, nhận thực, cổng vào TOE và điều khiển truy nhập;
- Hành động thực hiện trên một đối tượng nhất định hoặc tài nguyên TOE;
- Tất cả những ngoại lệ kiểm toán của một tập hợp nhất định;
- Hành động liên quan đến một thuộc tính của TSP

Sự khác biệt giữa những xem xét lại kiểm chứng dựa vào tính chức năng. Xem xét lại kiểm chứng (duy chỉ) bao hàm khả năng xem lại dữ liệu kiểm chứng. Xem xét lại có thể lựa chọn thì phức tạp hơn, và đòi hỏi khả năng lựa chọn tập con dữ liệu kiểm chứng dựa trên tiêu chí đơn hoặc đa tiêu chí với các quan hệ logic (có nghĩa: và/ hoặc), và sắp xếp dữ liệu kiểm chứng trước khi nó được xem xét lại.

C.5.2 FAU_SAR.1 Soát xét kiểm toán

C.5.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cung cấp cho những người dùng được ủy quyền có quyền khả năng thu thập và dịch thông tin. Trong trường hợp con người sử dụng, thông tin này cần biểu diễn ở dạng cho con người hiểu được. Trong trường hợp với các thực thể IT khác, thông tin này cần biểu diễn ở dạng điện tử rõ ràng.

C.5.2.2 Các hoạt động

C.5.2.2.1 Chỉ định

Trong FAU_SAR.1.1, người biên soạn PP/ST cần xác định người quản trị có thể sử dụng khả năng này. Nếu thích hợp, người biên soạn PP/ST nên bao gồm vai trò an toàn (xem vai trò an toàn FMT-SMR.1)

Trong FAU_SAR.1.1, người biên soạn PP/ST cần qui định rõ kiểu loại thông tin mà người dùng danh nghĩa được phép lấy từ bản ghi dữ liệu kiểm toán. Ví dụ là "tất cả" ("all"), "định danh chủ thể" ("subject identify"), "tất cả thông tin thuộc về bản ghi kiểm toán tham khảo người dùng này" ("all information belonging to audit records referencing this user"). Khi sử dụng SFR, RAU_SAR.1, không cần phải lặp lại, một cách hoàn toàn chi tiết, danh sách thông tin kiểm chứng được qui định ban đầu trong FAU_GEN.1. Việc sử dụng thuật ngữ như là "tất cả" hoặc "tất cả thông tin kiểm chứng" giúp hạn chế tình trạng tối nghĩa và việc cần phân tích so sánh thêm giữa hai yêu cầu an toàn.

C.5.3 FAU_SAR.2 Soát xét kiểm toán có hạn chế

C.5.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này xác định những người sử dụng không có định danh trong FAU_SAR.1 sẽ không được đọc bản ghi dữ liệu kiểm toán.

C.5.4 FAU_SAR.3 Soát xét kiểm toán có chọn lựa

C.5.4.1 Chú thích cho ứng dụng người sử dụng

Thành phần này được sử dụng để xác định rằng có thể lựa chọn dữ liệu kiểm toán để xem lại. Nếu có nhiều tiêu chuẩn lựa chọn, mối quan hệ giữa chúng cần phải logic (dưới dạng and, or) và công cụ cần cung cấp khả năng để xử lý dữ liệu kiểm toán (sắp xếp, lọc).

C.5.4.2 Các hoạt động

C.5.4.2.1 Phép chọn

Trong FAU_SAR.3.1, người biên soạn PP/ST cần qui định rõ những khả năng nào để lựa chọn và/hoặc dữ liệu kiểm toán thứ tự nào được yêu cầu từ TSF.

Trong FAU_SAR.3.1, người biên soạn PP/ST cần chỉ định tiêu chí, có thể bằng các mối quan hệ logic, được sử dụng để lựa chọn dữ liệu kiểm toán xem lại. Các mối quan hệ logic này nhằm để qui định rõ hoạt động có thể trên một thuộc tính riêng lẻ hay là trên một tập hợp các thuộc tính. Một ví dụ về sự chỉ định này là: "ứng dụng, tài khoản người dùng và/hoặc vị trí" ("application, user account and/or location"). Trong trường hợp này hoạt động có thể được qui định rõ bằng việc sử dụng bất cứ liên hợp nào của ba thuộc tính: ứng dụng, tài khoản người dùng và vị trí.

C.6 Lựa chọn sự kiện kiểm toán an toàn (FAU_SEL)

C.6.1 Chú thích cho người sử dụng

Họ lựa chọn sự kiện kiểm toán an toàn cung cấp yêu cầu liên quan đến khả năng những sự kiện kiểm toán nào có thể kiểm toán được. Sự kiện kiểm toán được định nghĩa trong họ FAU_GEN, nhưng những sự kiện đó cần được định nghĩa một cách chọn lọc trong thành phần này để kiểm toán.

Họ này đảm bảo rằng có thể không sử dụng những dữ liệu kiểm toán quá dài bằng cách định nghĩa thuộc tính thích hợp trong những sự kiện kiểm toán an toàn được lựa chọn.

C.6.2 FAU_SEL.1 Kiểm toán lựa chọn

C.6.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này định nghĩa tiêu chuẩn lựa chọn được sử dụng và những tập hợp con kết quả đã được kiểm toán của tập hợp tất cả các sự kiện có thể kiểm toán, dựa trên các thuộc tính người dùng, các thuộc tính chủ thể, các thuộc tính đối tượng hoặc các kiểu loại sự kiện.

Sự tồn tại của định danh người dùng không bao gồm trong thành phần này. Điều này cho phép những TOE như bộ định tuyến có thể không cần hỗ trợ khái niệm người dùng.

Đối với môi trường phân tán, định danh của máy trạm có thể sử dụng như lựa chọn cho những sự kiện kiểm toán.

Chức năng quản lý dữ liệu TSF (FMT_MTD.1) sẽ xử lý quyền của người quản trị khi truy vấn hoặc sửa đổi lựa chọn.

C.6.2.2 Các hoạt động

C.6.2.2.1 Phép chọn

Trong FAU_SEL.1.1, PP/ST cần lựa chọn mối quan hệ của thuộc tính an toàn để kiểm toán dựa trên định danh đối tượng, định danh người dùng, định danh máy trạm hoặc kiểu sự kiện.

C.6.2.2.2 Chỉ định

Trong FAU_SEL.1.1, PP/ST cần xác định những thuộc tính bổ sung liên quan đến sự lựa chọn kiểm toán. Nếu không có cũng cần Chỉ định rõ là "không có".

C.7 Lưu trữ sự kiện kiểm toán an toàn (FAU_STG)

C.7.1 Chú thích cho người sử dụng

Họ lưu trữ sự kiện kiểm toán an toàn mô tả các yêu cầu lưu trữ dữ liệu kiểm toán để dùng lại sau đó, trong đó bao gồm điều khiển thất thoát thông tin kiểm toán do lỗi TOE, tấn công và/hoặc hết dung lượng lưu trữ.

C.7.2 FAU_STG.1 Lưu trữ các vết kiểm toán có bảo vệ

C.7.2.1 Chú thích cho ứng dụng người sử dụng

Trong môi trường phân tán, do nơi lưu trữ dữ liệu kiểm toán trong TSC nhưng không cần thiết phải trong cùng nơi tạo ra dữ liệu, PP/ST có thể yêu cầu nhận thực về nguồn gốc của bản ghi kiểm toán trước khi lưu bản ghi đó.

TSF sẽ bảo vệ dữ liệu kiểm toán đã lưu trữ trong dấu vết kiểm toán khỏi những hành động xóa hoặc sửa đổi không được phép. Lưu ý rằng trong một số TOE (vai trò) người kiểm toán có thể không được phép xóa bản ghi kiểm toán trong một khoảng thời gian nhất định.

C.7.2.2 Các hoạt động

C.7.2.2.1 Phép chọn

Trong FAU_STG.1.2, người biên soạn PP/ST cần qui định TSF sẽ ngăn chặn hoặc chỉ có thể phát hiện sự thay đổi của các dữ liệu kiểm toán đã lưu trữ trong dấu vết kiểm toán. Chỉ một tùy chọn được lựa chọn.

C.7.3 FAU_STG.2 Đảm bảo sự sẵn sàng của dữ liệu kiểm toán

C.7.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cho phép PP/ST xác định những thông số mà dữ liệu kiểm toán cần đáp ứng.

Trong môi trường phân tán, do nơi lưu trữ dữ liệu kiểm toán trong TSC nhưng không cần thiết phải trong cùng nơi tạo ra dữ liệu, PP/ST có thể yêu cầu nhận thực về nguồn gốc của bản ghi kiểm toán trước khi lưu bản ghi đó.

C.7.3.2 Các hoạt động

C.7.3.2.1 Phép chọn

Trong FAU_STG.2.2, người biên soạn PP/ST cần qui định rõ TSF sẽ ngăn chặn hoặc chỉ có thể phát hiện sự thay đổi của bản ghi kiểm toán đã lưu trữ trong dấu vết kiểm toán. Chỉ một tùy chọn được lựa chọn.

C.7.3.2.2 Chỉ định

Trong FAU_STG.2.3, tác giả PP/ST cần chỉ rõ thông số mà TSF phải đảm bảo đối với bản ghi kiểm toán lưu trữ. Thông số này giới hạn dữ liệu thất thoát dựa trên số lượng bản ghi phải được duy trì hoặc thời gian bản ghi được đảm bảo duy trì. Ví dụ, thông số là "100,000" có nghĩa là 100,000 bản ghi kiểm toán cần được lưu giữ.

C.7.3.2.3 Phép chọn

Trong FAU_STG.2.3, tác giả PP/ST cần xác định điều kiện trong đó TSF nào vẫn có thể duy trì được một lượng dữ liệu kiểm toán đã thiết lập trước. Điều kiện này có thể như sau: không gian lưu trữ bị cạn kiệt, hỏng hoặc tấn công.

C.7.4 FAU_STG.3 Hành động trong trường hợp có thể mất mát dữ liệu kiểm toán

C.7.4.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu hành động sẽ phải thực hiện khi dữ liệu kiểm toán vượt quá giới hạn đã thiết lập trước.

C.7.4.2 Các hoạt động

C.7.4.2.1 Chỉ định

Trong FAU_STG.3.1, PP/ST cần xác định giới hạn thiết lập trước. Nếu chức năng quản lý thông báo rằng con số này có thể thay đổi bởi người dùng được cấp quyền thì giá trị là giá trị mặc định. PP/ST nên cho phép người dùng được cấp quyền thiết lập giới hạn này.

Trong FAU_STG.3.1, PP/ST cần xác định hành động cần thực hiện trong trường hợp nơi lưu trữ dữ liệu kiểm toán sắp bị hỏng dựa trên sự thông báo vượt qua mức ngưỡng. Hành động nên bao gồm thông báo cho người được cấp quyền.

C.7.5 FAU_STG.4 Ngăn chặn mất mát dữ liệu kiểm toán

C.7.5.1 Chú thích cho ứng dụng người dùng

Thành phần này chỉ rõ ứng xử của TOE khi dấu vết kiểm toán bị đầy: hoặc là các bản ghi kiểm toán bị bỏ qua hoặc TOE bị "đông cứng" đến nỗi không có sự kiện kiểm toán nào có thể xảy ra được. Các yêu cầu cũng chỉ ra rằng bất cứ yêu cầu là như thế nào, thì người dùng được cấp phép với các quyền cụ thể đối với kết quả này đều có thể tiếp tục tạo ra sự kiện kiểm toán (các hành động). Lý do là mặt khác thì người dùng được cấp quyền thậm chí cũng không thể khởi động lại TOE. Cần cân nhắc lựa chọn hành động do TSF thực hiện trong trường hợp cạn kiệt lưu trữ kiểm toán, như bỏ qua các sự kiện, mà cung cấp khả năng sẵn sàng của TOE tốt hơn, cũng sẽ cho phép các hành động được thực hiện mà không ghi lại và không theo dõi được người sử dụng.

C.7.5.2 Các hoạt động

C.7.5.2.1 Phép chọn

Trong FAU_STG.4.1, PP/ST cần lựa chọn TSF sẽ bỏ qua những hành động có thể kiểm toán hoặc những bản ghi lâu nhất được ghi đè khi TSF không thể ghi tiếp. Chỉ một tùy chọn được phép sử dụng.

C.7.5.2.2 Chỉ định

Trong FAU_STG.4.1, PP/ST cần xác định những hành động được thực hiện khi nơi lưu trữ dữ liệu kiểm toán bị hỏng, ví dụ thông báo với người dùng được cấp quyền. Nếu không, sự Chỉ định phải ghi rõ là "không có".

Phụ lục D

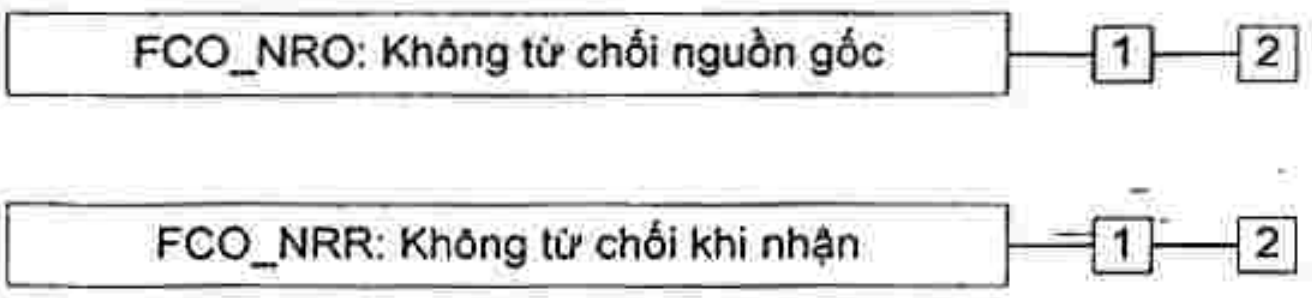
(Quy định)

Lớp FCO: Truyền thông

Lớp này mô tả các yêu cầu đặc biệt quan tâm đối với các TOE dùng cho việc vận chuyển thông tin. Các họ trong lớp này liên quan việc không từ chối.

Trong lớp này khái niệm "thông tin" được sử dụng. Thông tin này cần được dịch như là đối tượng đang được truyền thông; và có thể bao gồm một thông điệp thư điện tử, tệp hoặc một tập hợp kiểu thuộc tính đã xác định.

Hình D.1 mô tả thành phần của lớp này:



Hình D.1 –Phân cấp lớp FCO: Truyền thông

D.1 Không chối bỏ nguồn gốc (FCO_NRO)

D.1.1 Chú thích cho người sử dụng

Nguồn gốc không thể phủ nhận định nghĩa yêu cầu để cung cấp bằng chứng cho người sử dụng/đối tượng về định danh người khởi tạo ra một số thông tin. Người khởi tạo không thể phủ nhận những thông tin đã gửi vì bằng chứng về nguồn gốc (ví dụ chữ ký số) khẳng định mối liên kết giữa người đó và thông tin đã gửi đi. Người nhận hoặc một người thứ ba có thể xác nhận bằng chứng về nguồn gốc này. Bằng chứng này cần không làm giả được.

Nếu thông tin hoặc những thuộc tính liên quan bị thay đổi theo bất kỳ cách nào, tính hợp lệ của bằng chứng về nguồn gốc là thất bại. Do đó PP/ST cần cân nhắc bao gồm cả yêu cầu toàn vẹn như FDP_UIT.1.

Không thể phủ nhận bao gồm một số vai trò khác nhau có thể kết hợp trong đối tượng:

- Vai trò thứ nhất là một đối tượng yêu cầu bằng chứng về nguồn gốc (chỉ có trong FCO_NRO.1),
- Vai trò thứ hai là là người nhận và/hoặc những đối tượng khác được cung cấp bằng chứng
- Vai trò thứ ba là một đối tượng yêu cầu kiểm tra lại nguồn gốc của bằng chứng

PP/ST cần xác định điều kiện cần thiết để kiểm tra tính hợp lệ của bằng chứng. Một ví dụ về điều kiện này là sự kiểm tra bằng chứng phải xảy ra trong vòng 24 giờ. Những điều kiện này do vậy cho phép thay đổi yêu cầu hợp lệ, ví dụ có thể cung cấp bằng chứng trong một vài năm.

Trong phần lớn trường hợp, định danh của người nhận sẽ là người nhận sự truyền tin. Trong một số trường hợp PP/ST không muốn định danh người dùng xuất ra. Trong trường hợp đó, PP/ST cần cân nhắc bao gồm cả lớp này hoặc có nên sử dụng định danh của người cung cấp dịch vụ hay định danh của máy trạm không.

Ngoài ra, PP/ST cần xem xét đến thời gian thông tin được truyền đi. Ví dụ, yêu cầu khuyến nghị phải được truyền đi trước ngày nào đó. Trong trường hợp như vậy, những yêu cầu này có thể tùy biến nhằm cung cấp một sự chỉ thị về mốc thời gian (thời gian gốc).

D.1.2 FCO_NRO.1 Lựa chọn kiểm chứng nguồn gốc

D.1.2.1 Các hoạt động

D.1.2.1.1 Chỉ định

Trong FCO_NRO.1.1, PP/ST cần điền kiểu thông tin về đối tượng trong chức năng bằng chứng về nguồn gốc, ví dụ thông điệp thư điện tử.

D.1.2.1.2 Phép chọn

Trong FCO_NRO.1.1, PP/ST cần xác định người dùng/ đối tượng có thể yêu cầu bằng chứng về nguồn gốc.

D.1.2.1.3 Chỉ định

Trong FCO_NRO.1.1, PP/ST dựa trên sự lựa chọn cần xác định những đối tác thứ ba có thể yêu cầu bằng chứng về nguồn gốc. Một đối tác thứ ba có thể là trọng tài, quan tòa hoặc một đối tượng hợp lệ.

Trong FCO_NRO.1.2, PP/ST cần điền danh sách những thuộc tính sẽ liên kết với thông tin, ví dụ định danh người khởi tạo, thời gian gốc, và vị trí gốc.

Trong FCO_NRO.1.2, PP/ST cần điền danh sách những trường thông tin mang những thuộc tính cung cấp bằng chứng về nguồn gốc, ví dụ nội dung của một thông điệp.

D.1.2.1.4 Phép chọn

Trong FCO_NRO.1.3, PP/ST cần xác định người dùng/ đối tượng có thể thẩm tra bằng chứng về nguồn gốc.

D.1.2.1.5 Chỉ định

Trong FCO_NRO.1.3, PP/ST cần điền danh sách những giới hạn mà bằng chứng có thể thẩm tra. Ví dụ, bằng chứng chỉ có thể thẩm tra trong 24 giờ. Một Chỉ định "ngay tức thì" hoặc "không xác định" có thể được chấp nhận.

Trong FCO_NRO.1.3, PP/ST dựa trên sự lựa chọn cần xác định những đối tác thứ ba có thể thẩm tra bằng chứng về nguồn gốc.

D.1.3 FCO_NRO.2 Thực thi kiểm chứng nguồn gốc

D.1.3.1 Các hoạt động

D.1.3.1.1 Chỉ định

Trong FCO_NRO.2.1, PP/ST cần điền những kiểu thông tin đối tượng trong chức năng bằng chứng nguồn gốc, ví dụ thông điệp thư điện tử.

Trong FCO_NRO.2.2, PP/ST cần điền danh sách những thuộc tính sẽ liên kết với thông tin, ví dụ định danh người khởi tạo, thời gian gốc, và vị trí gốc.

Trong FCO_NRO.2.2, PP/ST cần điền danh sách những trường thông tin mang những thuộc tính cung cấp bằng chứng về nguồn gốc, ví dụ nội dung của một thông điệp.

D.1.3.1.2 Phép chọn

Trong FCO_NRO.2.3, PP/ST cần xác định người dùng/đối tượng có thể thẩm tra bằng chứng về nguồn gốc.

D.1.3.1.3 Chỉ định

Trong FCO_NRO.1.3, PP/ST cần điền danh sách những giới hạn mà bằng chứng có thể thẩm tra. Ví dụ, bằng chứng chỉ có thể thẩm tra trong 24 giờ. Một Chỉ định "ngay tức thì" hoặc "không xác định" có thể được chấp nhận.

Trong FCO_NRO.1.3, PP/ST dựa trên sự lựa chọn cần xác định những đối tác thứ ba có thể thẩm tra bằng chứng về nguồn gốc. Đối tác thứ ba có thể là một trọng tài, quan tòa hoặc một đối tượng hợp lệ.

D.2 Không thể từ chối của bên nhận (FCO_NRR)

D.2.1 Chú thích cho người sử dụng

FCO_NRR định nghĩa yêu cầu để cung cấp bằng chứng cho những người dùng/ đối tượng khác rằng thông tin được nhận bởi người nhận.Người nhận không thể từ chối thành công đã nhận thông tin bởi bằng chứng biên nhận (ví dụ chữ ký điện tử) khẳng định mối liên kết giữa thuộc tính người nhận và thông tin. Người khởi tạo hoặc đối tác thứ ba có thể thẩm tra bằng chứng biên nhận. Bằng chứng này cần không làm giả được.

Lưu ý rằng sự bằng chứng cung cấp không cần thiết gợi ý rằng thông tin đã được đọc hoặc lĩnh hội mà chỉ nhận được.

Nếu thông tin hoặc những thuộc tính liên quan được thay đổi theo cách nào đó, tính hợp lệ của bằng chứng biên nhận so với thông tin gốc là thất bại. Do vậy PP/ST cần cân nhắc yêu cầu về tính toàn vẹn như FDP_UIT.1

Trong không thể phủ định bao gồm một số vai trò khác nhau có thể kết hợp trong đối tượng:

- Vai trò thứ nhất là một đối tượng yêu cầu bằng chứng về nguồn gốc (chỉ có trong FCO_NRO.1),
- Vai trò thứ hai là là người nhận và/hoặc những đối tượng khác được cung cấp bằng chứng, ví dụ công chứng viên
- Vai trò thứ ba là một đối tượng yêu cầu thẩm tra lại nguồn gốc của bằng chứng ví dụ như trọng tài

PP/ST cần xác định điều kiện cần thiết để thẩm tra tính hợp lệ của bằng chứng. Một ví dụ về điều kiện này là sự thẩm tra bằng chứng phải xảy ra trong vòng 24 giờ. Những điều kiện nầy do vậy cho phép thay đổi yêu cầu hợp lệ, ví dụ có thể cung cấp bằng chứng trong một vài năm.

Trong phần lớn trường hợp, định danh của người nhận sẽ là người nhận sự truyền tin. Trong một số trường hợp PP/ST không muốn định danh người dùng xuất ra. Trong trường hợp đó, PP/ST cần cân nhắc bao gồm cả lớp này hoặc có nên sử dụng định danh của người cung cấp dịch vụ hay định danh của máy trạm không.

Ngoài ra, PP/ST cần xem xét đến thời gian thông tin được truyền đi. Ví dụ, yêu cầu khuyến nghị phải được truyền đi trước ngày nào đó. Trong trường hợp như vậy, những yêu cầu này có thể tùy biến nhằm cung cấp một sự chỉ thị về mốc thời gian (thời gian gốc).

D.2.2 FCO_NRR.1 Lựa chọn kiểm chứng bên nhận

D.2.2.1 Các hoạt động

D.2.2.1.1 Chỉ định

Trong FCO_NRR.1.1, PP/ST cần điền vào kiểu thông tin đối tượng cho bằng chứng biên nhận, vi dụ, thông điệp thư điện tử.

D.2.2.1.2 Phép chọn

Trong FCO_NRR.1.1, PP/ST cần xác định người dùng/đối tượng có thể yêu cầu bằng chứng biên nhận.

D.2.2.1.3 Chỉ định

Trong FCO_NRR.1.1, PP/ST dựa vào sự lựa chọn cần xác định những đối tác thứ ba có thể yêu cầu bằng chứng biên nhận. Đối tác thứ ba có thể là trọng tài, quan tòa hoặc đối tượng hợp lệ.

Trong FCO_NRR.1.2, PP/ST cần điền danh sách những thuộc tính sẽ liên kết với thông tin; ví dụ định danh người nhận, thời gian nhận, địa điểm nhận.

Trong FCO_NRR.1.2, PP/ST cần điền danh sách các trường thông tin trong đó có những thuộc tính cung cấp bằng chứng biên nhận, vi dụ nội dung của một thông điệp.

D.2.2.1.4 Phép chọn

Trong FCO_NRR.1.3, PP/ST cần xác định những người dùng/ đối tượng có thể thẩm tra bằng chứng biên nhận.

D.2.2.1.5 Chỉ định

Trong FCO_NRR.1.3, PP/ST cần điền danh sách những sự hạn chế mà dựa vào đó bằng chứng có thể thẩm tra. Ví dụ bằng chứng chỉ có thể thẩm tra trong vòng 24 giờ. Một sự Chỉ định "ngay lập tức" hoặc "không xác định" là chấp nhận được.

Trong FCO_NRR.1.3, PP/ST cần dựa trên sự lựa chọn để xác định những đối tác thứ ba có thể thẩm tra bằng chứng biên nhận.

D.2.3 FCO_NRR.2 Thực thi kiểm chứng bên nhận

D.2.3.1 Các hoạt động

D.2.3.1.1 Chỉ định

Trong FCO_NRR.2.1, PP/ST cần điền vào kiểu thông tin đối tượng cho bằng chứng biên nhận, vi dụ, thông điệp thư điện tử.

Trong FCO_NRR.2.2, PP/ST cần điền danh sách những thuộc tính sẽ liên kết với thông tin; ví dụ định danh người nhận, thời gian nhận, địa điểm nhận.

Trong FCO_NRR.2.2, PP/ST cần điền danh sách các trường thông tin trong đó có những thuộc tính cung cấp bằng chứng biên nhận, vi dụ nội dung của một thông điệp.

D.2.3.1.2 Phép chọn

Trong FCO_NRR.2.3, PP/ST cần xác định những người dùng/ đối tượng có thể thẩm tra bằng chứng biên nhận.

D.2.3.1.3 Chỉ định

Trong FCO_NRR.1.3, PP/ST cần điền danh sách những sự hạn chế mà dựa vào đó bằng chứng có thể thẩm tra. Ví dụ bằng chứng chỉ có thể thẩm tra trong vòng 24 giờ. Một sự Chỉ định "ngay lập tức" hoặc "không xác định" là chấp nhận được.

Trong FCO_NRR.1.3, PP/ST cần dựa trên sự lựa chọn để xác định những đối tác thứ ba có thể thẩm tra bằng chứng biên nhận. Đối tác thứ ba có thể là một trọng tài, quan tòa hoặc đối tượng hợp lệ.

Phụ lục E

(Quy định)

Lớp FCS: Hỗ trợ mật mã

TSF có thể tận dụng chức năng mật mã để hỗ trợ cho những mục đích an toàn ở mức cao. Chức năng này có thể bao gồm (nhưng không giới hạn bởi) : định danh và nhận thực, không phủ định, đường tin cậy, kênh tin cậy và tách dữ liệu. Lớp này được sử dụng khi TOE thực hiện chức năng mật mã, có thể trong phần cứng, phần sụn hoặc phần mềm.

FCS bao gồm hai họ: Quản lý khóa mật mã (FCS_CKM) và Thao tác mật mã (FCS_COP). FCS_CKM chú trọng vào vấn đề quản lý khóa mật mã trong khi FCS_COP liên quan đến sự sử dụng những khóa mật mã đó.

Với mỗi phương thức tạo khóa mật mã thực hiện bởi TOE nếu có, PP/ST cần lựa chọn thành phần Tạo khóa mật mã FCS_CKM.1

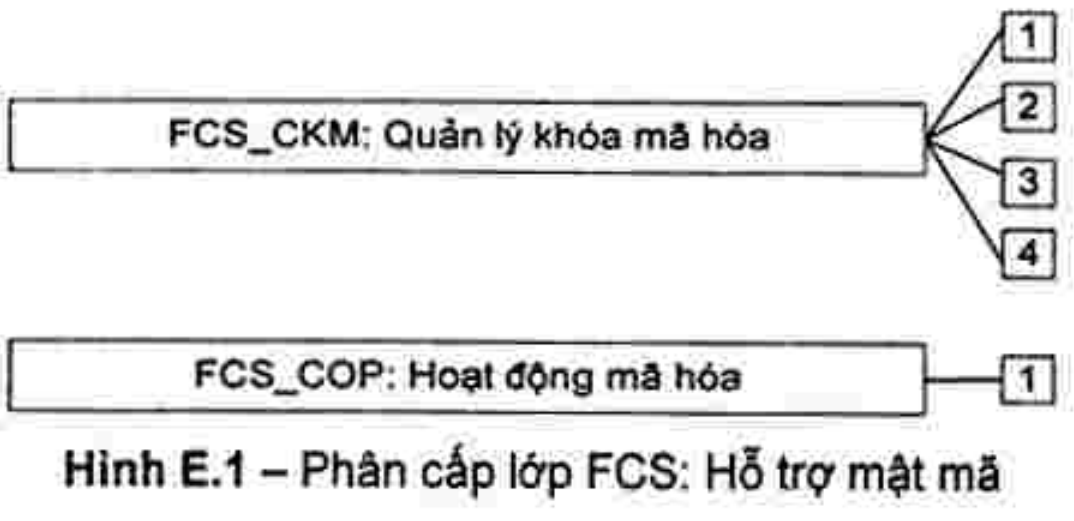
Với mỗi phương thức phân phối khóa mật mã thực hiện bởi TOE nếu có, PP/ST cần lựa chọn thành phần Phân phối khóa mật mã FCS_CKM.2

Với mỗi phương thức truy nhập khóa mật mã thực hiện bởi TOE nếu có, PP/ST cần lựa chọn thành phần Truy nhập khóa mật mã FCS_CKM.3

Với mỗi phương thức hủy khóa mật mã thực hiện bởi TOE nếu có, PP/ST cần lựa chọn thành phần Hủy khóa mật mã FCS_CKM.4

Chức năng mật mã có thể sử dụng để đáp ứng mục tiêu trong lớp FCO - Trao đổi thông tin và trong các họ Nhận thực dữ liệu (FDP_DAU), Tính toàn vẹn dữ liệu lưu trữ (FDP_SDI), Bảo vệ chuyển giao bí mật dữ liệu người dùng giữa TSF (FDP_UIT), Đặc tính bí mật (FIA_SOS), Nhận thực người dùng (FIA_UAU) để đáp ứng nhiều mục tiêu khác nhau. Trong trường hợp chức năng mật mã được sử dụng để đáp ứng mục tiêu cho các lớp khác, những thành phần chức năng riêng lẻ xác định những mục tiêu đó phải đáp ứng chức năng mật mã. Mục tiêu trong lớp FCS cần được sử dụng khi chức năng mật mã của TOE được yêu cầu từ khách hàng.

Hình E.1 minh họa các thành phần của lớp FCS.



Hình E.1 – Phân cấp lớp FCS: Hỗ trợ mật mã

E.1 Quản lý khóa mật mã (FCS_CKM)

E.1.1 Chú thích cho người sử dụng

Khóa mật mã phải được quản lý trong suốt thời gian tồn tại của khóa. Những sự kiện thường gặp trong chu kỳ sống của khóa mật mã bao gồm (nhưng không giới hạn bởi): tạo, phân phối, lưu giữ, truy nhập và hủy khóa.

Số trạng thái của khóa phụ thuộc vào chiến lược quản lý khóa đang triển khai do TOE không cần thiết tham gia vào tất cả trong chu kỳ sống của khóa (ví dụ TOE chỉ tạo và phân phối khóa)

Họ này nhằm hỗ trợ chu kỳ sống của khóa và do đó định nghĩa yêu cầu cho những thao tác sau: Tạo khóa, phân phối khóa và hủy khóa. Họ này cần sử dụng khi có yêu cầu chức năng về quản lý khóa mật mã.

Nếu FAU_GEN bao gồm trong PP/ST thì trong ngữ cảnh của sự kiện đang kiểm toán:

a/ Thuộc tính của mục đích có thể bao gồm người dùng đã gán cho khóa mật mã, vai trò của người dùng, thao tác sử dụng khóa mật mã, định danh khóa mật mã và khoảng thời gian hợp lệ của khóa mật mã.

b/ Giá trị của mục đích có thể bao gồm giá trị của khóa mật mã và tham số không kể đến những thông tin nhạy cảm (ví dụ khóa mật mã bí mật hoặc riêng tư).

Thông thường, số ngẫu nhiên được sử dụng để tạo khóa mật mã. Trong trường hợp đó, FCS_CKM.1 cần được dùng thay cho FIA_SOS.2. FIA_SOS.2 được sử dụng trong trường hợp việc tạo mã ngẫu nhiên yêu cầu mục đích khác.

E.1.2 FCS_CKM.1 Tạo khóa mật mã

E.1.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu xác định độ dài khóa mật mã và phương thức tạo khóa (có thể tuân theo một tiêu chuẩn Chỉ định). Chỉ cần một đối tượng của thành phần cho cùng một phương thức và những độ dài mã khác nhau. Độ dài mã có thể dùng chung hoặc khác nhau với các thực thể, có thể là đầu vào hoặc đầu ra của phương thức.

E.1.2.2 Các hoạt động

E.1.2.2.1 Chỉ định

Trong FCS_CKM.1.1, tác giả PP/ST nên xác định thuật toán tạo khóa mật mã được sử dụng.

Trong FCS_CKM.1.1, tác giả PP/ST nên xác định độ dài khóa mật mã được sử dụng. Độ dài khóa cần thích hợp với thuật toán và mục đích sử dụng.

Trong FCS_CKM.1.1, tác giả PP/ST nên xác định tiêu chuẩn được chỉ định để tạo khóa mật mã. Tiêu chuẩn chỉ định có thể không có hoặc nhiều hơn một tiêu chuẩn đã công bố quốc tế, trong nước hoặc một tổ chức.

E.1.3 FCS_CKM.2 Phân phối khóa mật mã

E.1.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu các phương pháp được sử dụng để phân phối các khóa mật mã được quy định, điều này có thể phù hợp với một tiêu chuẩn được chỉ định.

E.1.3.2 Các hoạt động

E.1.3.2.1 Chỉ định

Trong FCS_CKM.2.1, tác giả PP/ST nên xác định phương pháp phân phối khóa mật mã được sử dụng.

Trong FCS_CKM.2.1, tác giả PP/ST nên xác định tiêu chuẩn được chỉ định để tạo các khóa mật mã. Tiêu chuẩn chỉ định có thể không có hoặc nhiều hơn một tiêu chuẩn đã công bố quốc tế, trong nước hoặc một tổ chức.

E.1.4 FCS_CKM.3 Truy nhập khóa mật mã

E.1.4.1 Chú thich cho ứng dụng người sử dụng

Thành phần này yêu cầu phương pháp được sử dụng để truy cập các khóa mật mã quy định, điều này có thể phù hợp với tiêu chuẩn được chỉ định.

E.1.4.2 Các hoạt động

E.1.4.2.1 Chỉ định

Trong FCS_CKM.3.1, tác giả PP/ST nên xác định loại truy cập khóa mật mã đang sử dụng. Ví dụ về loại truy cập khóa mật mã gồm (nhưng không hạn chế) sao lưu khóa mật mã và phục hồi khóa mật mã.

Trong FCS_CKM.3.1, tác giả PP/ST nên xác định phương pháp truy cập khóa mật mã được sử dụng.

Trong FCS_CKM.3.1, tác giả PP/ST nên xác định tiêu chuẩn được chỉ định để tạo các khóa mật mã. Tiêu chuẩn chỉ định có thể không có hoặc nhiều hơn một tiêu chuẩn đã công bố quốc tế, trong nước hoặc một tổ chức.

E.1.5 FCS_CKM.4 Hủy bỏ khóa mật mã

E.1.5.1 E.1.5.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu phương pháp được sử dụng để phá hủy các khóa mật mã quy định, điều này có thể phù hợp với tiêu chuẩn được chỉ định.

E.1.5.2 Các hoạt động

E.1.5.2.1 Chỉ định

Trong FCS_CKM.4.1, tác giả PP/ST nên xác định phương pháp phá hủy khóa được sử dụng cho việc phá hủy các khóa mật mã.

Trong FCS_CKM.4.1, tác giả PP/ST nên xác định tiêu chuẩn được chỉ định để tạo các khóa mật mã. Tiêu chuẩn chỉ định có thể không có hoặc nhiều hơn một tiêu chuẩn đã công bố quốc tế, trong nước hoặc một tổ chức.

E.2 Hoạt động mật mã (FCS_COP)

E.2.1 Chú thích cho người sử dụng

Thao tác mật mã có thể gắn liền với những chế độ mật mã. Khi đó chế độ mật mã phải được xác định.

Thao tác mật mã có thể hỗ trợ một hoặc một vài dịch vụ an toàn TOE. Thành phần FCS_COP có thể cần lặp lại hơn một lần dựa trên:

a/ Ứng dụng người dùng mà trên đó dịch vụ an toàn được sử dụng

b/ Sự sử dụng những thuật toán và độ dài khóa mật mã khác nhau

c/ Kiểu dữ liệu đang sử dụng

Nếu trong PP/ST bao gồm cả FAU_GEN thì trong ngữ cảnh của thao tác mật mã đang kiểm tra:

a/ Thao tác mật mã có thể bao gồm tạo và (hoặc) kiểm tra chữ ký số, tạo mã kiểm tra toàn vẹn và kiểm tra lại, tính hàm băm, mã hóa và giải mã dữ liệu, mã hóa và giải mã khóa mật mã, thỏa thuận khóa mật mã và tạo số ngẫu nhiên.

b/ Thuộc tính đối tượng có thể bao gồm vai trò đối tượng và người dùng gắn liền với đối tượng đó.

c/ Thuộc tính của đối tượng có thể bao gồm người dùng Chỉ định cho khóa mật mã, vai trò người dùng và thời gian hợp lệ của khóa mật mã.

E.2.2 FCS_COP.1 Hoạt động mật mã

E.2.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu thuật toán mật mã và độ dài khóa được sử dụng cho thao tác mật mã có thể dựa trên một tiêu chuẩn Chỉ định.

E.2.2.2 Các hoạt động

E.2.2.2.1 Chỉ định

Trong FCS_COP.1.1, PP/ST cần xác định thao tác mật mã đang thực hiện. Những thao tác mật mã thông thường bao gồm tạo và (hoặc) kiểm tra chữ ký số, tạo mã kiểm tra toàn vẹn và kiểm tra lại, tính hàm băm, mã hóa và giải mã dữ liệu, mã hóa và giải mã khóa mật mã, thỏa thuận khóa mật mã và tạo số ngẫu nhiên. Thao tác mật mã có thể được thực hiện trên dữ liệu người dùng hoặc dữ liệ TSF.

Trong FCS_COP.1.1, PP/ST cần xác định thuật toán mật mã được sử dụng; có thể bao gồm (nhưng không giới hạn bởi) DES, RSA và IDEA.

Trong FCS_COP.1.1, PP/ST cần xác định độ dài khóa mật mã được sử dụng. Độ dài khóa cần thích hợp với thuật toán và mục tiêu sử dụng.

Trong FCS_COP.1.1, PP/ST cần xác định tiêu chuẩn Chỉ định trong đó có dẫn chứng tài liệu về phương thức thao tác mật mã. Tiêu chuẩn Chỉ định có thể không có, có một hoặc nhiều hơn tiêu chuẩn đã công bố quốc tế, trong nước hoặc trong một tổ chức.

Phụ lục F

(Quy định)

Lớp FDP: Bảo vệ dữ liệu người dùng

Lớp này chứa các họ chỉ rõ các yêu cầu liên quan việc bảo vệ dữ liệu người sử dụng. Lớp này khác với FIA và FPT trong FDP đó: việc bảo vệ dữ liệu người dùng chỉ rõ các thành phần bảo vệ dữ liệu người dùng, FIA chỉ rõ các thành phần bảo vệ các thuộc tính liên kết với người dùng, và FPT chỉ rõ các thành phần bảo vệ thong tin TSF

Lớp FDP không chứa các yêu cầu rõ ràng cho các kiểm soát truy nhập bắt buộc truyền thống (Mandatory Access Controls – MAC) hoặc các kiểm soát truy nhập rời rạc truyền thống (Discretionary Access Controls – DAC); Tuy nhiên, các yêu cầu đó có thể được thiết kế qua các thành phần của lớp này.

Lớp FDP không đề cập rõ ràng đến tính bí mật, toàn vẹn, hoặc khả dụng, tuy cả ba tính chất này thường gắn liền trong chính sách và các cơ chế. Tuy nhiên, chính sách an toàn TOE phải bao trùm cả ba mục tiêu này trong PP/ST.

Một khía cạnh khác của lớp này là nó quy định kiểm soát truy nhập dưới dạng "các thao tác". Một thao tác được xác định là một kiểu truy nhập cụ thể tới một đối tượng cụ thể. Nó phụ thuộc vào mức độ trừu tượng của chủ thể PP/ST, hoặc các thao tác được mô tả là các thao tác "đọc" hay "viết", hoặc là các thao tác phức tạp hơn ví dụ như "Cập nhật cơ sở dữ liệu".

Các chính sách kiểm soát truy nhập là các chính sách dùng để kiểm soát truy nhập tới một kho chứa thông tin. Các thuộc tính biểu thị thuộc tính của kho chứa. Một khi thông tin ra khỏi kho chứa, tác nhân truy nhập sẽ tùy ý sửa đổi thông tin, bao gồm cả việc viết thông tin vào một kho chứa khác với các thuộc tính khác. Trái lại, các chính sách cho một luồng tin kiểm soát truy nhập tới thông tin, độc lập với kho chứa. Các thuộc tính của thông tin, có thể liên đới với các thuộc tính của kho chứa (hoặc không liên đới, như trường hợp một cơ sở dữ liệu đa cấp), chúng sẽ gắn liền với thông tin khi di chuyển. Tác nhân truy nhập không có khả năng, trường hợp thiếu chủ quyền rõ ràng, để thay đổi các thuộc tính thông tin.

Lớp FDP không có nghĩa là một bảng phân loại tổng hợp các chính sách truy nhập CNTT, như có thể hình dung đối với các lớp khác. Các chính sách bao hàm ở đây chỉ đơn giản là các chính sách mà theo kinh nghiệm đối với các hệ thống thực tế, cung cấp cơ sở cho việc quy định rõ các yêu cầu. Có thể có các nghĩa khác không thuộc vào các định nghĩa ở đây.

Ví dụ, giả sử muốn có các kiểm soát có áp đặt của người dùng (hoặc do người dùng xác định) tới luồng tin. Các khái niệm đó có thể được xử lý như các bổ sung chi tiết, hoặc các mở rộng của các thành phần FDP.

Cuối cùng, điều quan trọng là khi xem xét các thành phần trong FDP là phải ghi nhớ rằng các thành phần này là các yêu cầu đối với các chức năng có thể được thực thi bởi một cơ chế để phục vụ hoặc có thể phục vụ mục đích khác. Ví dụ, có thể thiết lập một chính sách kiểm soát truy nhập (Chính sách kiểm soát truy nhập FDP_ACC) có sử dụng các nhãn (các thuộc tính an toàn đơn giản FDP_IF.1) như là cơ sở cho cơ chế kiểm soát truy nhập.

Một tập hợp các SFR có thể chứa đựng nhiều chính sách chức năng an toàn (SFP), mỗi cái được xác định bởi hai thành phần định hướng chính sách FDP_ACC, và chính sách kiểm soát luồng tin

(FDP_IFC). Các chính sách này thường xem xét tính bí mật, tính toàn vẹn và tính khả dụng theo như yêu cầu để thỏa mãn các yêu cầu TOE. Cần thận trọng để đảm bảo rằng mọi mục tiêu sẽ đạt được bởi ít nhất một SFP và không có xung đột xuất hiện khi thực thi nhiều SFP.

Khi thiết lập một PP/ST với các thành phần của FDP, thông tin tiếp theo cung cấp hướng dẫn về việc thấy nó ở đâu và chọn lựa gì từ lớp này.

Các yêu cầu trong lớp FDP được định nghĩa thông qua một tập hợp các SFR mà sẽ thực thi một SFP. Do một TOE có thể thực thi đồng thời nhiều SFP, tác giả PP/ST phải quy định rõ tên của mỗi SFP, do đó nó có thể được tham chiếu từ các họ khác. Tên này sẽ được dùng trong mỗi thành phần được chọn để chỉ ra rằng nó đang được sử dụng như một phần của định nghĩa các yêu cầu cho chức năng này. Điều đó cho phép tác giả dễ dàng chỉ ra phạm vi các thao tác, ví dụ các mục tiêu bao hàm, các thao tác bao hàm, các người dùng có thẩm quyền,..

Mỗi bản sao của một thành phần có thể áp dụng chỉ cho một SFP. Bởi vậy nếu một SFP được quy định trong một thành phần thì SFP này sẽ áp dụng cho mọi phần tử trong thành phần này. Các thành phần có thể tạo thành bản sao nhiều lần bên trong một PP/ST để diễn giải cho các chính sách khác nhau như mong muốn.

Mấu chốt để chọn các thành phần từ họ này là cần có một chính sách an toàn TOE xác định rõ để cho phép chọn chính xác các thành phần từ hai thành phần chính sách: Chính sách kiểm soát truy nhập FDP_ACC và chính sách kiểm soát luồng tin FDP_IFC. Trong chính sách kiểm soát truy nhập FDP_ACC và chính sách kiểm soát luồng tin tương ứng, mọi chính sách kiểm soát truy nhập và chính sách kiểm soát luồng tin được đặt tên. Ngoài ra phạm vi kiểm soát của các thành phần này dưới dạng chủ thể, đối tượng và thao tác được chứa trong chức năng an toàn này. Tên của các chính sách này có nghĩa được dùng suốt trong phần còn lại của các thành phần chức năng mà có một thao tác gọi đến một phép gán hoặc chọn một "SFP kiểm soát truy nhập", hoặc một "SFP kiểm soát luồng tin". Các quy tắc này xác định chức năng của các SFP kiểm soát truy nhập và kiểm soát luồng tin đã đặt tên, chúng sẽ được xác định trong các họ chức năng kiểm soát truy nhập (FDP_ACF) và các họ chức năng kiểm soát luồng tin (FDP_IFF) một cách tương ứng.

Các bước sau hướng dẫn việc áp dụng lớp này trong việc thiết kế một PP/ST:

a) Xác định chính sách cần thực hiện từ các họ chính sách kiểm soát truy nhập (FDP_ACC) và chính sách kiểm soát luồng tin (FDP_IFC). Các họ này xác định phạm vi kiểm soát cho chính sách, mức độ thô của việc kiểm soát và có thể xác định một số quy tắc đi kèm theo chính sách.

b) Xác định các thành phần và thực hiện mọi thao tác có thể áp dụng được trong các thành phần chính sách. Các thao tác gán có thể được thực hiện tổng quát (tương tự như với công bố "tất cả các tệp") hoặc chỉ rõ (tệp "A", "B", v.v.) tùy thuộc vào mức độ chi tiết đã biết.

c) Xác định mọi thành phần chức năng có thể áp dụng được từ họ các chức năng kiểm soát truy nhập (FDP_ACF) và các chức năng kiểm soát luồng tin (FDP_IFF) để định rõ các họ chính sách từ chính sách kiểm soát truy nhập (FDP_ACC) và chính sách kiểm soát luồng tin (FDP_IFC). Thực hiện các thao tác để tạo các thành phần là định nghĩa các quy tắc cần thực thi bởi các chính sách đã Chỉ định. Điều đó khiến cho các thành phần đáp ứng được các yêu cầu của chức năng đã chọn hoặc cần được tạo ra.

d) Xác định ai có khả năng kiểm soát và thay đổi các thuộc tính của chức năng, ví dụ như duy nhất chỉ người quản trị bảo mật, chỉ chủ sở hữu của đối tượng, v.v. Chọn các thành phần tương ứng

từ FMT: quản lý an toàn và thực hiện các thao tác. Việc bổ sung chi tiết có thể hữu ích nhằm xác định ra các đặc tính còn thiếu, ví dụ như một số hoặc tất cả sự thay đổi cần phải thực hiện qua kênh tin cậy.

e) Xác định mọi thành phần tương ứng từ FMT: quản lý an toàn cho các giá trị khởi đầu cho các đối tượng và chủ thể mới.

f) Xác định mọi thành phần quay lại trạng thái từ họ Rollback (FDP_ROL).

g) Xác định mọi yêu cầu bảo vệ thông tin dư thừa có thể áp dụng từ họ bảo vệ thông tin dư thừa (FDP_RIP).

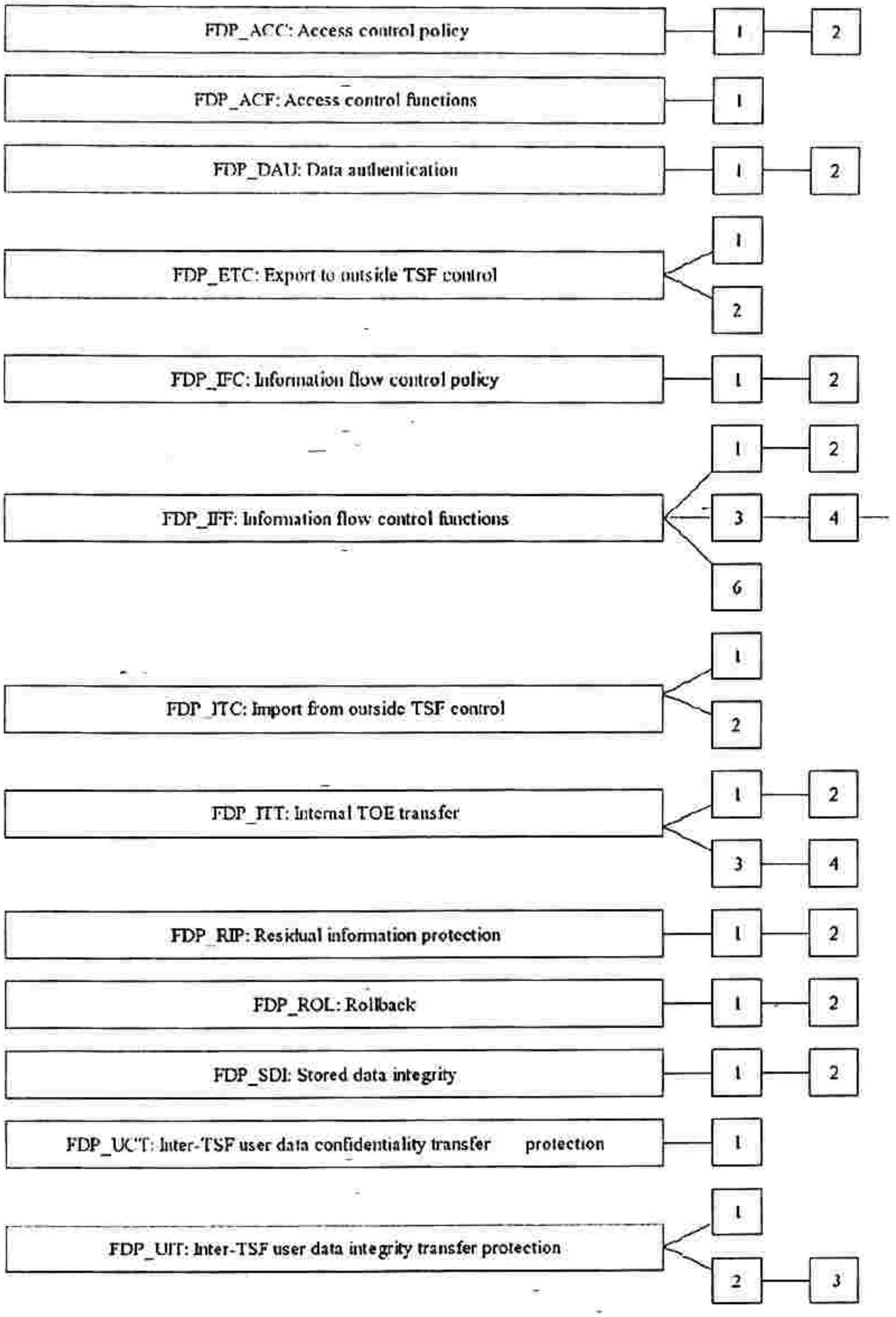
h) Xác định mọi thành phần nhập / xuất có thể áp dụng, và cách thức xử lý các thuộc tính an toàn trong quá trình nhập / xuất, qua quá trình nhập từ bên ngoài các họ kiểm soát TSF (FDP_ITC) và xuất ra bên ngoài các họ kiểm soát TOE (FDP_ETC).

i). Xác định mọi thành phần truyền thông TOE nội bộ áp dụng được từ họ truyền tải TOE nội bộ (FDP_ITT).

j) Xác định mọi yêu cầu đối với việc bảo vệ toàn vẹn các thông tin lưu trữ từ họ lưu giữ toàn vẹn dữ liệu (FDP_SDI)

k) Xác định mọi thành phần truyền thông liên TSF từ các họ bảo vệ truyền tải bí mật dữ liệu người dùng giữa các TSF hoặc các họ bảo vệ truyền tải toàn vẹn dữ liệu người dùng giữa các TSF.

Hình F.1 chỉ ra việc phân tách lớp này ra các thành phần cấu trúc của nó.



Hình F.1 – Phân cấp lớp FDP: Bảo vệ dữ liệu người dùng

Chính sách kiểm soát truy nhập (FDP_ACC)

F.1.1 Chú thích cho người sử dụng

Họ này dựa trên mô hình các kiểm soát tùy ý tương tác của các chủ thể và đối tượng. Phạm vi và mục đích của các kiểm soát là dựa trên các thuộc tính của bộ truy nhập (chủ thể), thuộc tính của khối được truy nhập (đối tượng), các động tác (thao tác) và mọi quy tắc kiểm soát truy nhập liên quan.

Các thành phần trong họ này có khả năng xác định ra các SFP kiểm soát truy nhập (qua tên) được thực thi bởi các cơ chế kiểm soát truy nhập rời rạc truyền thông (Discretionary Access Control – DAC). Ngoài ra, nó chỉ ra các chủ thể, đối tượng và các thao tác có trong các SFP kiểm soát truy nhập xác định. Các quy tác định ra chức năng của một SFP kiểm soát truy nhập sẽ được định nghĩa bởi các họ khác, như là các chức năng kiểm soát truy nhập (FDP_ACF) và Xuất từ TOE (FDP_ETC). Tên của các SFP kiểm soát truy nhập được định nghĩa trong chính sách kiểm soát truy nhập (FDP_ACC) có nghĩa được sử dụng trong suốt phần còn lại của các thành phần chức năng có chứa một thao tác gọi đến tính năng Chỉ định hoặc chọn một " SFP kiểm soát truy nhập"

Kiểm soát truy nhập SFP bao hàm một tập bộ ba: chủ thể, đối tượng và các thao tác. Bởi vậy một chủ thể có thể được chứa trong nhiều SFP kiểm soát truy nhập, song chỉ có liên quan đến một thao tác khác, hoặc một đối tượng khác. Dĩ nhiên là tương tự với các đối tượng và các thao tác.

Một điểm quan trọng đối với chức năng kiểm soát truy nhập thực thi một SFP kiểm soát truy nhập là khả năng người dùng có thể thay đổi các thuộc tính liên quan đến các quyết định kiểm soát truy nhập. Họ chính sách kiểm soát truy nhập (FDP_ACC) không Chỉ định các điểm này. Một số yêu cầu không được xác đinh, song có thể bổ sung như các bổ sung chi tiết. Trong khi đó, một số yêu cầu khác có thể chứa đâu đó trong các họ khác hoặc lớp khác, ví dụ như họ quản lý an toàn FMT.

Không có các yêu cầu kiểm toán trong chính sách kiểm soát truy nhập (FDP_ACC) do họ này định rõ các yêu cầu kiểm soát truy nhập SFP. Các yêu cầu kiểm toán nằm trong các họ đặc tả các chức năng thỏa mãn kiểm soát truy nhập SFP chỉ ra trong họ này.

Họ này cung cấp cho tác nhân PP/ST khả năng định rõ một số chính sách, ví dụ là một SFP kiểm soát truy nhập cố định có thể áp dụng cho một phạm vi kiểm soát, một SFP kiểm soát truy nhập động có thể được định nghĩa cho một phạm vi kiểm soát khác. Để chỉ rõ nhiều chính sách kiểm soát truy nhập, các thành phần của họ này cần lặp lại nhiều lần trong mỗi PP/ST trong các tập con của các thao tác và các đối tượng. Điều này làm cho các TOE đa chính sách có thể định rõ một tập cụ thể các thao tác và đối tượng. Nói cách khác, chủ thể PP/ST cần định ra các thông tin cần thiết trong thành phần ACC cho mỗi SFP kiểm soát truy nhập mà TSF phải thực thi. Ví dụ, một TOE có thể tập hợp 3 SFP kiểm soát truy nhập, mỗi cái chỉ chứa một tập các đối tượng, chủ thể và các thao tác bên trong TOE, chứa một tập con FDP_ACC.1 thành phần kiểm soát truy nhập cho 1 trong 3 SFP kiểm soát truy nhập cần cho toàn thể 3 thành phần kiểm soát truy nhập tập con FDP_ACC.1.

F.1.2 FDP_ACC.1 Kiểm soát truy nhập tập con

F.1.2.1 Chú thích cho ứng dụng người sử dụng

Các khái niệm chủ thể và đối tượng chỉ các phần tử chung trong TOE. Để thực thi được một chính sách, các phần tử cần được định rõ. Đối với một PP, các đối tượng và thao tác có thể được biểu thị với các kiểu như: đối tượng có tên, nơi chứa dữ liệu, các truy nhập quan sát, v.v. Đối với một hệ thống xác định, các khái niệm chung này (đối tượng, chủ thể) cần phải được định rõ, ví dụ các tệp, bản ghi, cổng, miền, lời gọi hệ thống...

Thành phần này định rõ chính sách bao gồm một số tập thao tác xác định cho một số tập con các đối tượng. Không có ràng buộc nào cho các thao tác bên ngoài tập – kể cả các thao tác cho đối tượng được giám sát bởi các thao tác khác.

F.1.2.2 Các hoạt động

F.1.2.2.1 Chỉ định

Trong FDP_ACC.1.1, chủ thể PP/ST cần chỉ ra một kiểm soát truy nhập có tên duy nhất SFP cần thực thi bởi TSF.

Trong FDP_ACC.1.1, chủ thể PP/ST cần chỉ ra danh sách các chủ thể, đối tượng, các thao tác ứng với chủ thể và đối tượng bao hàm trong SFP.

F.1.3 FDP_ACC.2 Kiểm soát truy nhập toàn bộ

F.1.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu mọi thao tác khả thi cho đối tượng chứa trong SFP cần chứa trong một kiểm soát truy nhập SFP.

Chủ thể PP/ST cần phải chỉ ra mỗi tổ hợp của đối tượng và chủ thể được bao hàm trong một kiểm soát truy nhập SFP.

F.1.3.2 Các hoạt động

F.1.3.2.1 Chỉ định

Trong FDP_ACC.2.1, chủ thể PP/ST cần chỉ ra một kiểm soát truy nhập có tên duy nhất SFP cần thực thi bởi TSF.

Trong FDP_ACC.1.1, chủ thể PP/ST cần chỉ ra danh sách các chủ thể, đối tượng bao hàm trong SFP. Mọi thao tác ứng với chủ thể và đối tượng cần được bao hàm trong SFP.

F.2 Các chức năng kiểm soát truy nhập (FDP_ACF)

F.2.1 Chú thích cho người sử dụng

Họ này mô tả các quy tắc cho các chức năng xác định có thể thực thi một chính sách kiểm soát truy nhập được ghi danh trong FDP_ACC Chính sách kiểm soát truy nhập, chỉ ra phạm vi dk chính sách.

Họ này cung cấp cho chủ thể PP/ST khả năng mô tả các quy tắc cho kiểm soát truy nhập. Các kết quả trong một hệ thống không thay đổi. Một ví dụ là đối tượng: "Bản tin ngày" có thể đọc bởi tất cả, song chỉ người quản trị được phép thay đổi nó. Họ này cũng cung cấp cho chủ thể PP/ST khả năng mô tả các quy tắc về ngoại lệ cho các quy tắc kiểm soát truy nhập chung. Các ngoại lệ này có thể là việc cho phép rõ ràng hoặc từ chối quyền truy nhập đến một đối tượng.

Không có thành phần rõ ràng nào định rõ các chức năng khác, vi như kiểm soát kép, quy tắc chuỗi thao tác, các kiểm soát loại trừ. Tuy nhiên, các cơ chế này cũng như các cơ chế DAC truyền thống khác, có thể đặc trưng với các thành phần đang có, có thể sửa đổi theo các quy tắc kiểm soát truy nhập.

Trong họ này có một loạt các kiểm soát truy nhập chấp nhận được SFP có thể chỉ ra là:

- Các danh sách kiểm soát truy nhập (Access Control Lists – ACLs)
- Các đặc tả kiểm soát truy nhập dựa thời gian

- Các đặc tả kiểm soát truy nhập dựa chủ gốc
- Các kiểm soát truy nhập được chủ thể giám sát.

F.2.2 Kiểm soát truy nhập dựa trên thuộc tính an toàn FDP_AFC.1

F.2.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cung cấp các yêu cầu về một cơ chế làm trung gian cho kiểm soát-truy nhập dựa trên các thuộc tính an toàn liên quan đến các chủ thể và đối tượng. Mỗi chủ thể và đối tượng có một tập các thuộc tính liên quan như vị trí, thời điểm cấu thành, quyền truy nhập (ví dụ các danh sách kiểm soát truy nhập ACL).

mọi thao tác khả thi cho đối tượng chứa trong SFP cần chứa trong một kiểm soát truy nhập SFP.

Chủ thể PP/ST cần phải chỉ ra mỗi tổ hợp của đối tượng và chủ thể được bao hàm trong một kiểm soát truy nhập SFP. Thành phần này cho phép chủ thể PP/ST định rõ các thuộc tính dùng làm trung gian cho kiểm soát truy nhập. Thành phần này cho phép định ra các quy tắc kiểm soát truy nhập có sử dụng các thuộc tính này.

Các ví dụ về thuộc tính mà một chủ thể PP/ST có thể Chỉ định được trình bày trong các phần tiếp theo. Một thuộc tính định danh có thể liên quan đến người dùng, chủ thể, đối tượng được dùng làm trung gian. Ví dụ về các thuộc tính này có thể là tên của phần chương trình dùng để tạo ra chủ thể hoặc một thuộc tính an toàn Chỉ định cho phần chương trình.

Một thuộc tính thời gian có thể dùng để chỉ ra rằng truy nhập sẽ được cấp quyền trong một khoảng thời gian nhất định trong ngày/tuần/hoặc năm.

Một thuộc tính vị trí có thể chỉ ra vị trí yêu cầu chức năng, vị trí chức năng được thực thi hoặc cả hai. Nó có thể dựa trên một bảng nội bộ để chuyển đổi giao diện logic sang các vị trí TSF ví dụ thông qua vị trí đấu nối, vị trí CPU,...

Một thuộc tính nhóm cho phép một nhóm người dùng liên hệ đến một thao tác với mục đích kiểm soát truy nhập. Nếu cần, một thao tác bổ sung sẽ được dùng để chỉ ra số nhóm tối đa, số thành viên tối đa của nhóm, số nhóm tối đa mà một người dùng có liên hệ đồng thời.

Thành phần này đồng thời cũng cung cấp các yêu cầu cho các chức năng kiểm soát truy nhập để chấp thuận hoặc từ chối truy nhập đến một đối tượng trên cơ sở các thuộc tính an toàn. Chức năng này có thể dùng để cấp đặc quyền truy nhập, chủ quyền truy nhập trong TOE. Những đặc quyền, quyền hoặc chủ quyền đó có thể áp dụng cho người dùng, đối tượng và chủ thể (đại diện cho người dùng hoặc ứng dụng).

F.2.2.2 Các hoạt động

F.2.2.2.1 Chỉ định

Trong FDP_ACF.1.1, chủ thể PP/ST cần phải chỉ ra một tên chức năng kiểm soát truy nhập SFP mà TSF phải thực thi. Tên của kiểm soát truy nhập SFP, phạm vi kiểm soát cho chính sách này được định ngiã trong các thành phần của FDP_ACC Chính sách kiểm soát truy nhập.

Trong FDP_ACF.1.1, chủ thể PP/ST cần định rõ, đối với mỗi chủ thể và đối tượng được kiểm soát, các thuộc tính an toàn và/hoặc các nhóm định danh thuộc tính an toàn mà chức năng sẽ sử dụng khi mô tả các quy tắc.

Ví dụ, các thuộc tính có thể là định danh người dùng, định danh chủ thể, thời điểm, vị trí, ACLs, hoặc mọi thuộc tính khác chỉ ra bởi chủ thể PP/ST. Các nhóm định danh thuộc tính an toàn có thể định rõ để cung cấp một phương thức thuận tiện để tham chiếu tới nhiều thuộc tính an toàn. Các nhóm định danh có thể cung cấp một cách thức hữu hiệu để gắn kết các vai trò (roles) định nghĩa trong các vai trò quản lý an toàn (FMT_SMR) và mọi thuộc tính liên quan đến chúng với các chủ thể. Nói cách khác, mỗi vai trò có thể liên quan đến một nhóm định danh thuộc tính.

Trong FDP_ACF.1.2, chủ thể PP/ST cần định rõ các quy tắc SFP quản trị truy nhập theo các chủ thể được giám sát và các đối tượng được giám sát thông qua các thao tác kiểm soát trên các đối tượng. Các quy tắc này chỉ ra rằng truy nhập được cho phép hoặc từ chối. Chúng có thể chỉ ra các chức năng kiểm soát truy nhập chung (ví dụ như các bit cho phép đặc trưng), hoặc các chức năng kiểm soát truy nhập thô hơn (ví dụ ACLs).

Trong FDP_ACF.1.3, chủ thể PP/ST cần định rõ các quy tắc, trên cơ sở thuộc tính an toàn, dùng cho cấp chủ quyền rõ ràng về việc truy nhập của các chủ thể tới các đối tượng. Các quy tắc này bổ sung cho các quy tắc chỉ ra trong FDP_ACF.1.1. Chúng thuộc FDP_ACF.1.3, với chủ ý bổ sung các ngoại lệ cho các quy tắc trong FDP_ACF.1.1. Một ví dụ về các quy tắc cho cấp quyền rõ ràng cho truy nhập là dựa trên vec tơ đặc quyền cho một chủ thể luôn có quyền truy nhập tới các đối tượng mà kiểm soát truy nhập SFP đã xác định rõ. Nếu điều này không mong muốn thì chủ thể PP/ST cần định rõ giá trị là "none".

Trong FDP_ACF.1.4, chủ thể PP/ST cần định rõ các quy tắc, trên cơ sở thuộc tính an toàn, dùng cho cấp chủ quyền rõ ràng về việc truy nhập của các chủ thể tới các đối tượng. Các quy tắc này bổ sung cho các quy tắc chỉ ra trong FDP_ACF.1.1. Chúng thuộc FDP_ACF.1.4, với chủ ý bổ sung các ngoại lệ cho các quy tắc trong FDP_ACF.1.1. Một ví dụ về các quy tắc cho cấp quyền rõ ràng cho truy nhập là dựa trên vec tơ đặc quyền cho một chủ thể luôn có quyền từ chối truy nhập tới các đối tượng mà kiểm soát truy nhập SFP đã xác định rõ. Nếu điều này không mong muốn thì chủ thể PP/ST cần định rõ giá trị là "none".

F.3 Xác thực dữ liệu (FDP_DAU)

F.3.1 Chú thích cho người sử dụng

Họ này mô tả các chức năng đặc trưng dùng để xác thực các dữ liệu tĩnh (static). Các thành phần trong họ này dùng khi có một yêu cầu xác thực các dữ liệu tĩnh (static), nghĩa là khi dữ liệu cần được ký nhận chứ không phải chuyển đi. (Lưu ý là họ không khước từ nguồn gốc (Non-repudiation of origin – FCO_NRO) cho thông tin về việc khước từ nguồn gốc trong quá trình trao đổi dữ liệu.

F.3.2 Xác thực dữ liệu cơ sở FDP_DAU.1

F.3.2.1 Chú thích cho người sử dụng

Thành phần này có thể thỏa mãn bằng các hàm băm một chiều (lấy tổng kiểm tra mật mã, vân tay, kê bản tin), để tạo ra một giá trị hàm băm cho một tài liệu xác định, để có tể dùng cho việc kiểm tra, thẩm định hoặc xác thực nội dung thông tin.

F.3.2.2 Các hoạt động

F.3.2.2.1 Chỉ định

Trong FDP_DAU.1.1, chủ thể PP/ST cần phải chỉ ra danh sách các đối tượng hoặc kiểu thông tin có thể áp dụng cho TSF để tạo ra các bằng chứng xác thực dữ liệu.

Trong FDP_DAU.1.2, chủ thể PP/ST cần phải chỉ ra danh sách các chủ thể có khả năng kiểm định các bằng chứng xác thực dữ liệu cho các đối tượng đã xác định trong phần tử trước đó. Danh sách các chủ thể có thể rất rõ ràng, nếu chủ thể đã biết, hoặc khá chung chung và tham chiếu đến một kiểu chủ thể ví dụ như vai trò đã biết.

F.3.3 FDP_DAU.2 Xác thực dữ liệu với định danh người đảm bảo

F.3.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này có thể yêu cầu thêm khả năng kiểm chứng danh định người dùng đã cấp xác thực có đảm bảo (ví dụ một đối tác tin cậy thứ 3).

F.3.3.2 Các hoạt động

F.3.3.2.1 Chỉ định

Trong FDP_DAU.2.1, chủ thể PP/ST cần phải chỉ rõ danh sách các đối tượng hoặc kiểu thông tin có thể áp dụng cho TSF để tạo ra các bằng chứng xác thực dữ liệu.

Trong FDP_DAU.2.2, chủ thể PP/ST cần phải chỉ ra danh sách các chủ thể có khả năng kiểm định các bằng chứng xác thực dữ liệu cho các đối tượng đã xác định trong phần tử trước đó cũng như định danh người dùng có thể tạo ra bằng chứng xác thực dữ liệu.

F.4 Xuất dữ liệu ra ngoài TOE (FDP_ETC)

F.4.1 Chú thích cho người sử dụng

Họ này định nghĩa các chức năng kết xuất dữ liệu người dùng từ TOE sao cho các thuộc tính an toàn của nó hoặc được bảo quản rõ ràng, hoặc có thể bỏ qua sau khi chúng đã được kết xuất. Tính nhất quán của các thuộc tính an toàn được chỉ ra bởi sự nhất quán dữ liệu TSF bên trong-TSF (FPT_TDC).

Kết xuất từ TOE (FDP_ETC) liên quan đến các giới hạn về kết xuất và tổ hợp các thuộc tính an toàn cùng dữ liệu người dùng.

Họ này và việc nhập họ tương ứng từ bên ngoài của TOE (FDP_ITC) chỉ ra TOE xử lý dữ liệu người dùng được chuyển bên trong bên ngoài kiểm soát thế nào. Về nguyên tắc, họ này gắn liền với kết xuất trung gian TSF của dữ liệu người dùng và các thuộc tính an toàn liên quan.

Một số thao tác có thể có là:

a) Kết xuất dữ liệu người dùng không có thuộc tính an toàn

b) Kết xuất dữ liệu người dùng có thuộc tính an toàn, trong đó thuộc tính an toàn thể hiện dữ liệu người dùng kết xuất.

Nếu có nhiều SFP (kiểm soát luồng tin, và/hoặc kiểm soát truy nhập) thì chúng cần lặp các thành phần này cho mỗi SFP.

F.4.2 FDP_ETC.1 Xuất dữ liệu người dùng không có các thuộc tính an toàn

F.4.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này dùng để chỉ ra kết xuất trung gian-TSF của dữ liệu người dùng không có kết xuất thuộc tính an toàn.

F.4.2.2 Các hoạt động

F.4.2.2.1 Chỉ định

Trong FDP_ETC.1.1, chủ thể PP/ST cần phải chỉ rõ các kiểm soát truy nhập SFP và/hoặc các SFP kiểm soát luồng tin khi thực thi kết xuất dữ liệu người dùng. Dữ liệu người dùng được kết xuất thuộc phạm vi Chỉ định bởi các SFP này.

F.4.3 FDP_ETC.2 Xuất dữ liệu người dùng với thuộc tính an toàn

F.4.3.1 Chú thích cho ứng dụng người sử dụng

Dữ liệu người dùng được kết xuất cùng với các thuộc tính an toàn. Có một số cách kết hợp thuộc tính an toàn với dữ liệu người dùng. Một cách thực hiện là thông qua sắp xếp vật lý dữ liệu người dùng và các thuộc tính an toàn (ví dụ cùng một đĩa mềm), hoặc thông qua các kỹ thuật mật mã như chữ ký an toàn để kết hợp dữ liệu người dùng và các thuộc tính.

Kênh tin cậy liên TSF (FTP_ITC) có thể dùng để đảm bảo rằng các thuộc tính được nhận chính xác ở phía sản phẩm CNTT tin cậy khác, trong khi tính nhất quán của dữ liệu liên TSF (FTP_TDC) có thể dùng để đảm bảo rằng các thuộc tính này được diễn tả chính xác. Ngoài ra, tuyến tin cậy (FPT_TRP) có thể dùng để đảm bảo rằng việc kết xuất đang được người dùng hợp thức tạo ra.

F.4.3.2 Các hoạt động

F.4.3.2.1 Chỉ định

Trong FDP_ETC.2.1, chủ thể PP/ST cần phải chỉ rõ các kiểm soát truy nhập SFP và/hoặc các SFP kiểm soát luồng tin khi thực thi kết xuất dữ liệu người dùng. Dữ liệu người dùng được kết xuất thuộc phạm vi Chỉ định bởi các SFP này.

Trong FDP_ETC.2.4, chủ thể PP/ST cần phải chỉ ra mọi quy tắc kết xuất bổ sung hoặc "none" nếu như không có quy tắc kết xuất bổ sung nào. Các quy tắc này được thực thi bởi TSF bổ sung thêm cho SFP kiểm soát truy nhập và/hoặc SFP kiểm soát luồng tin đã chọn trong FDP_ETC.2.1.

F.5 Chính sách kiểm soát luồng tin (FDP_IFC)

F.5.1 Chú thích cho người sử dụng

Họ này bao gồm việc định danh các SFP kiểm soát luồng tin; và, đối với mỗi chúng, nó chỉ ra phạm vi kiểm soát của SFP.

Các thành phần trong họ này có thể định danh các SFP kiểm soát luồng tin để chúng thực thi bởi các cơ chế kiểm soát truy nhập bắt buộc truyền thống có sẵn trong một TOE. Tuy nhiên, chúng nằm ngoài phạm vi các cơ chế MAC truyền thống và có thể dùng để xác định và mô tả các chính sách không đan xen và các dịch chuyển trạng thái. Ngoài ra, nó định nghĩa các chủ thể chịu sự giám sát của chính sách, thông tin chịu giám sát của chính sách và các thao tác phát sinh các thông tin có kiểm soát vào/ra các chủ thể được giám sát đối với mỗi SFP kiểm soát luồng tin trong TOE. Chức năng định ra các quy tắc cho một SFP kiểm soát luồng tin được định nghĩa bởi các họ khác, ví dụ như các chức năng kiểm soát luồng tin (FDP_IFF) và bảo vệ thông tin thường trú (FDP_RIP). SFP kiểm soát luồng tin ghi danh trong chính sách kiểm soát luồng tin (FDP_IFC) được dùng trong suốt phần còn lại của các thành phần chức năng có các thao tác gọi hàm tới phép chỉ định hoặc chọn lựa một "SFP kiểm soát luồng tin".

Các thành phần này khá mềm dẻo. Chúng cho phép chỉ rõ miền kiểm soát luồng tin và không yêu cầu cơ chế phải được đánh dấu. Các phần tử khác của các thành phần kiểm soát luồng tin còn cho phép các mức ngoại lệ khác nhau đối với chính sách.

Mỗi SFP gồm cụm ba: chủ thể, thông tin, các thao tác cho phép thông tin vào /ra các chủ thể. Một số chính sách kiểm soát luồng tin có thể rất chi tiết mức thấp và mô tả rõ ràng các chủ thể dưới dạng các tiến trình của một hệ điều hành. Các chính sách kiểm soát luồng tin khác có thể ở mức cao, mô tả các chủ thể dưới dạng tổng quát là người dùng hay các kênh vào/ra.

Nếu chính sách kiểm soát luồng tin ở mức quá cao, không chi tiết, nó có thể không định nghĩa rõ ràng các chức năng an toàn CNTT. Trong trường hợp này, cần chỉ ra chính xác và mô tả các chính sách kiểm soát luồng tin như các mục tiêu.

Các chức năng an toàn CNTT mong muốn có thể được xác định như những hỗ trợ cho các mục tiêu này.

Trong thành phần thứ hai (FDP_IFC.2 kiểm soát luồng tin toàn diện), mỗi SFP kiểm soát luồng tin sẽ bao gồm mọi thao tác có thể SFP gây ra việc chuyển thông tin ra vào chủ thể.

Ngoài ra, mọi luồng tin sẽ cần được chứa trong một SFP. Bởi vậy, đối với mỗi thao tác làm cho chuyển tin đến luồng, cần phải có một tập các quy tắc nhằm xác định hành vi có được phép không. Nếu có nhiều SFP và chúng đều có thể áp dụng cho một luồng tin nào đó, thì mọi SFP liên quan phải cho phép luồng tin này trược khi nó thực thi việc cho phép.

Một SFP kiểm soát luồng tin chứa một tập thao tác xác định trước. Miền của các SFP có thể phủ kín đối với một số luồng tin, hoặc nó có thể chỉ liên quan đến một số thao tác có ảnh hưởng đến luồng tin.

Một SFP kiểm soát truy nhập sẽ kiểm soát truy nhập đến các đối tượng chứa thông tin. Một SFP kiểm soát luồng tin kiểm soát truy nhập đến luồng tin, không phụ thuộc vào ngăn chứa thông tin. Các thuộc tính của thông tin có liên quan đến các thuộc tính của ngăn chứa (hoặc có thể không, ví như trong cơ sở dữ liệu nhiều lớp) sẽ gắn kèm với thông tin khi di chuyển. Các thiết bị truy nhập không có khả năng (nếu không có thẩm quyền rõ ràng) thay đổi các thuộc tính của thông tin.

Các luồng tin và các thao tác có thể biểu thị ở nhiều mức. Trong trường hợp một ST, Các luồng tin và các thao tác có thể định rõ ở mức đặc trưng hệ thống: ví dụ các gói tin TCP/IP chuyển qua một bức tường lửa theo các địa chỉ IP đã biết. Đối với PP, Các luồng tin và các thao tác có thể biểu thị theo kiểu: email, kho chứa dữ liệu, các truy nhập quan sát được, ...

Các thành phần trong họ này có thể áp dụng nhiều lần trong một PP/ST cho các tập con khác nhau của các thao tác và đối tượng. Chúng trợ giúp những TOE đa chính sách, mỗi cái đề cập đến một tập cụ thể các đối tượng, chủ thể và các thao tác.

F.5.2 FDP_IFC.1 Kiểm soát luồng thông tin tập con

F.5.2.1 Chú thích cho người sử dụng

Thành phần này yêu cầu một chính sách kiểm soát luồng tin áp dụng cho một tập con các thao tác khả thi trong TOE.

F.5.2.2 Các hoạt động

F.5.2.2.1 Chỉ định

Trong FDP_IFC.1.1, chủ thể PP/ST cần phải chỉ rõ một SFP kiểm soát luồng tin ghi danh duy nhất cần thực hiện bởi TSF.

Trong FDP_IFC.1.1, chủ thể PP/ST cần phải chỉ rõ một danh sách các chủ thể, thông tin và các thao tác gây ra sự chuyển dịch thông tin đã kiểm soát vào ra các chủ thể được kiểm soát bao trùm bởi SFP. Như đã nêu ở trên, danh sách các chủ thể có thể chi tiết tùy vào sự cần thiết của chủ thể PP/ST. Có thể chỉ ra người dùng, máy tính, hoặc các tiến trình máy. Thông tin có thể tham chiếu đến dữ liệu ví như email, các giao thức mạng, hay các đối tượng đặc trưng tương tự như những gì chỉ ra trong một chính sách kiểm soát truy nhập. Nếu thông tin chỉ ra chứa trong một đối tượng và là chủ thể của một chính sách kiểm soát truy nhập, thì cả chính sách kiểm soát truy nhập và chính sách kiểm soát luồng tin đều phải thực thi trước khi thông tin đó được chuyển vào / ra đối tượng.

F.5.3 FDP_IFC.2 Kiểm soát luồng tin đầy đủ

F.5.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu mọi thao tác khả thi gây ra di chuyển thông tin vào /ra các chủ thể chứa trong SFP đều phải chứa trong một SFP kiểm soát luồng tin.

Chủ thể PP/ST phải trình bày được rằng mọi tổ hợp luồng tin và chủ thể đều chứa trogn một SFP kiểm soát luồng tin.

F.5.3.2 Các hoạt động

F.5.3.2.1 Chỉ định

Trong FDP_IFC.2.1, chủ thể PP/ST cần phải chỉ rõ một SFP kiểm soát luồng tin ghi danh duy nhất cần thực hiện bởi TSF.

Trong FDP_IFC.1.1, chủ thể PP/ST cần phải chỉ rõ một danh sách các chủ thể, thông tin chứa trong SFP. Mọi thao tác gây ra sự chuyển dịch thông tin vào ra các chủ thể được bao trùm bởi SFP. Như đã nêu ở trên, danh sách các chủ thể có thể chi tiết tùy vào sự cần thiết của chủ thể PP/ST. Có thể chỉ ra người dùng, máy tính, hoặc các tiến trình máy. Thông tin có thể tham chiếu đến dữ liệu ví như email, các giao thức mạng, hay các đối tượng đặc trưng tương tự như những gì chỉ ra trong một chính sách kiểm soát truy nhập. Nếu thông tin chỉ ra chứa trong một đối tượng và là chủ thể của một chính sách kiểm soát truy nhập, thì cả chính sách kiểm soát truy nhập và chính sách kiểm soát luồng tin đều phải thực thi trước khi thông tin đó được chuyển vào / ra đối tượng.

F.6 Các chức năng kiểm soát luồng tin (FDP_IFF)

F.6.1 Chú thích cho người sử dụng

Họ này mô tả các quy tắc cho các chức năng đặc trưng có thể cài đặt trong các SFP kiểm soát luồng tin ghi danh trong chính sách kiểm soát luồng tin (FDP_IFC), và cũng chỉ ra phạm vi kiểm soát các chính sách.

Nó chứa hai "cây": Một đề cập đến các vấn đề chức năng kiểm soát luồng tin chung, và một chứa các luồng tin trái phép (ví dụ các kênh chuyển đổi) ứng với một hoặc nhiều SFP kiểm soát luồng tin. Việc phân chia này xuất phát từ các vấn đề liên quan đến các luồng tin trái phép, nói cách khác, trái ngược với phần còn lại của một SFP. Các luồng tin trái phép là những luồng tin vi phạm chính sách. Chúng không phải vấn đề đối với chính sách.

Để triển khai bảo vệ tốt hơn việc khai phá, sửa đổi khi có các phần mềm không tin cậy, cần có kiểm soát luồng tin. Việc kiểm soát truy nhập không thể đủ vì chúng chỉ kiểm soát các truy nhập tới ngăn chứa thông tin, cho phép thông tin chuyển tới các luồng tin, không qua kiểm soát đi thông qua hệ thống.

Trong họ này, cụm từ "Các kiểu luồng tin trái phép" được sử dụng. Cụm từ này dùng để chỉ đến một kiểu các luồng tin như "Các kênh lưu trữ" hoặc các "kênh định thời", hoặc chúng tham chiếu tới các phân loại cải tiến phản ánh nhu cầu của một chủ thể PP/ST.

Mức độ mềm dẻo của các thành phần này cho phép định nghĩa một chính sách đặc quyền trong các thuộc tính an toàn đơn FDP_IFF.1 và FDP_IFF.2. Các thuộc tính an toàn phân lớp cho phép vượt qua một hoặc mọi phần của một SFP cụ thể. Nếu như có nhu cầu vượt qua một SFP định trước, chủ thể PP/ST sẽ phải xem xét việc đưa vào một chính sách đặc quyền.

F.6.2 FDP_IFF.1 Các thuộc tính an toàn đơn giản

F.6.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu mọi thuộc tính an toàn của thông tin và của chủ thể gây ra di chuyển thông tin vào /ra các chủ thể là các bộ tiếp nhận thông tin này. Các thuộc tính của ngăn chứa thông tin cần được xem xét như mong muốn để chúng đóng một vai trò quyết định cho kiểm soát luồng tin hoặc nếu chúng được bao bởi một chính sách kiểm soát truy nhập. Thành phần này chỉ rõ các quy tắc chủ yếu cần thực thi và mô tả cách nhận được các thuộc tính an toàn.

Thành phần này không chỉ ra chi tiết cách một thuộc tính an toàn được Chỉ định (ví như người dùng – tiến trình). Sự mềm dẻo trong chính sách được cho bởi việc Chỉ định, cho phép chỉ ra chính sách và các yêu cầu chức năng bổ sung nếu cần.

Thành phần này cũng cho ra các yêu cầu đối với chức năng kiểm soát luồng tin dùng để cấp phép rõ ràng hoặc từ chối luồng tin trên cơ sở các thuộc tính an toàn. Chúng được dùng để thực hiện một chính sách đặc quyền, bao gồm cả các ngoài lệ đối với chính sách cơ sở định nghĩa trong thành phần này.

F.6.2.2 Các hoạt động

F.6.2.2.1 Chỉ định

Trong FDP_IFF.1.1, chủ thể PP/ST cần phải chỉ rõ một SFP kiểm soát luồng tin thực thi bởi TSF. Tên của SFP kiểm soát luồng tin, phạm vi kiểm soát cho chính sách này được định nghĩa trong các thành phần thuộc chính sách kiểm soát luồng tin (FDP_IFC).

Trong FDP_IFF.1.1, chủ thể PP/ST cần phải chỉ rõ, đối với mỗi kiểu chủ thể và thông tin được kiểm soát, các thuộc tính an toàn tương ứng với đặc tả của các quy tắc SFP. Ví dụ, các thuộc tính an toàn có thể là định danh chủ thể, nhãn độ nhạy chủ thể, nhãn độ trống của chủ thể, nhãn độ nhạy thông tin... Các kiểu thuộc tính an toàn cần phải đủ khả năng hỗ trợ các yêu cầu của môi trường.

Trong FDP_IFF.1.2, chủ thể PP/ST cần phải chỉ rõ đối với mỗi thao tác, mối quan hệ trên cơ sở các thuộc tính an toàn cần được duy trì giữa chủ thể và các thuộc tính an toàn thông tin mà TSF sẽ thực hiện.

Trong FDP_IFF.1.3, Tác giả PP/ST cần phải chỉ rõ mọi quy tắc SFP kiểm soát luồng tin bổ sung để TSF được thực thi. Đó là bao gồm tất cả các qui tắc của SFP mà hoặc là không dựa trên các thuộc

tính an toàn của thông tin và chủ thể hoặc là các qui tắc mà tự động sửa đổi các thuộc tính an toàn của thông tin hay chủ thể như một qui tắc của một thao tác truy cập. Một ví dụ cho trường hợp đầu tiên là một qui tắc của SFP kiểm soát một giá trị ngưỡng cho các kiểu thông tin cụ thể, Đây có thể là ví dụ cho trường hợp khi SFP luồng thông tin chứa các qui tắc về truy cập dữ liệu thống kê nơi mà một chủ thể chỉ được phép truy cập kiểu thông tin này đến một mức cụ thể các truy cập. Một ví dụ cho trường hợp thứ hai là một qui tắc được nêu ra trong các điều kiện và các thuộc tính an toàn của một chủ thể hoặc đối tượng thay đổi như thế nào như là kết quả của một thao tác truy cập. Một số chính sách luồng thông tin trong ví dụ có thể giới hạn số thao tác truy cập vào thông tin với các thuộc tính an toàn cụ thể. Nếu không có quy tắc bổ sung nào, chủ thể PP/ST cần phải chỉ rõ "none".

Trong FDP_IFF.1.4, tác giả PP/ST cần phải chỉ rõ các qui tắc, dựa trên các thuộc tính an toàn, mà xác thực các luồng thông tin. Các qui tắc này được bổ sung thêm vào các qui tắc được chỉ rõ trong các thành phần nói trước. Chúng có trong FDP_IFF 1.4 bởi vì chúng dự định chứa các ngoại trừ đối với các qui tắc trong các thành phần trước đó. Một ví dụ về các qui tắc xác quyền rõ ràng luồng thông tin được dựa trên véc-tơ ưu tiên liên kết với một chủ thể mà luôn cho phép chủ thể khả năng tạo ra luồng thông tin đối với thông tin được bao hàm bởi SFP cụ thể. Nếu không cần khả năng như vậy thì tác giả PP/ST cần phải chỉ rõ "none".

Trong FDP_IFF.1.5, chủ thể PP/ST cần phải chỉ rõ các quy tắc dựa trên các thuộc tính an toàn, mà từ chối luồng tin rõ ràng. Các quy tắc này bổ sung cho các quy tắc đã chỉ ra trong các phần từ trước đó. Chúng có trong FDP_IFF.1.5, dự định chứa các ngoại lệ đối với các quy tắc trong các thành phần trước đó. Một ví dụ về các quy tắc từ chối rõ ràng cho các luồng tin là dựa trên vectơ đặc quyền liên kết đến một chủ thể mà luôn từ chối chủ thể khả năng tạo ra luồng tin bao bởi SFP đã định trước. Nếu không cần năng lực bổ sung như vậy, tác giả PP/ST cần phải chỉ rõ "none".

F.6.3 FDP_IFF.2 Các thuộc tính an toàn phân cấp

F.6.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu mọi SFP kiểm soát luồng tin trong TSP sử dụng các thuộc tính an toàn phân lớp tạo thành một tấm lưới.

Điều quan trọng cần lưu ý là các yêu cầu về quan hệ phân lớp đã xác định trong FDP_IFF.2.4 chỉ cần áp dụng cho các thuộc tính an toàn kiểm soát luồng tin đối với các SFP kiểm soát luồng tin đã xác định trong FDP_IFF.2.1. Thành phần này không chủ ý áp dụng cho các SFP khác, ví dụ như các SFP kiểm soát truy nhập.

FDP_IFF 2.6 cho thấy các yêu cầu đối với tập hợp các thuộc tính an toàn để tạo ra một tấm lưới. Một số chính sách luồng thông tin định nghĩa trong văn học và thực hiện trong các sản phẩm IT là dựa trên tập hợp các thuộc tính an toàn mà tạo ra tấm lưới. FDP_IFF 2.6 đặc biệt được bao gồm để chỉ rõ loại chính sách luồng thông tin.

Giống thành phần trước, thành phần này có thể áp dụng để thực hiện một chính sách đặc quyền bao các quy tắc cho phép cấp quyền rõ ràng hoặc từ chối các luồng tin.

Nếu là trường hợp nhiều SFP kiểm soát luồng tin, và nếu mỗi SFP này có các thuộc tính an toàn riêng của nó không liên quan đến các thuộc tính khác, thì chủ thể PP/ST cần phải lặp lại thành phần này cho mỗi SFP. Nếu không sẽ có xung đột xảy ra với các nội dung chi tiết trong FDP_IFF.2.4, vì thiếu các mối quan hệ cần thiết.

F.6.3.2 Các hoạt động

F.6.3.2.1 Chỉ định

Trong FDP_IFF.2.1, chủ thể PP/ST cần phải chỉ rõ các SFP kiểm soát luồng tin thực thi bởi TSF. Tên của SFP kiểm soát luồng tin, phạm vi kiểm soát cho chính sách này được định nghĩa trong các thành phần thuộc chính sách kiểm soát luồng tin (FDP_IFC).

Trong FDP_IFF.2.1, chủ thể PP/ST cần phải chỉ rõ, đối với mỗi kiểu chủ thể và thông tin được kiểm soát, các thuộc tính an toàn tương ứng với đặc tả của các quy tắc SFP. Ví dụ, các thuộc tính an toàn có thể là định danh chủ thể, nhãn độ nhạy chủ thể, nhãn độ trống của chủ thể, nhãn độ nhạy thông tin... Các kiểu thuộc tính an toàn cần phải đủ khả năng hỗ trợ các yêu cầu của môi trường.

Trong FDP_IFF.2.2, chủ thể PP/ST cần phải chỉ rõ đối với mỗi thao tác, mối quan hệ trên cơ sở các thuộc tính an toàn cần được duy trì giữa chủ thể và các thuộc tính an toàn thông tin mà TSF sẽ thực hiện. Các mối quan hệ này cần dựa trên cơ sở các mối quan hệ có sắp xếp của các thuộc tính an toàn.

Trong FDP_IFF.2.3, tác giả PP/ST cần phải chỉ rõ mọi quy tắc SFP kiểm soát luồng tin bổ sung để TSF được thực thi. Nó bao gồm các qui tắc của SFP mà hoặc là không dựa vào các thuộc tính an toàn của thông tin và chủ thể hoặc qui tắc tự động sửa các thuộc tính an toàn của thông tin hay chủ thể như là kết quả của một thao tác truy cập. Một ví dụ về trường hợp đầu là một qui tắc của SFP kiểm soát giá trị ngưỡng cho các loại thông tin cụ thể. Cũng có thể cho ví dụ trong trường hợp SFP luồng thông tin chứa các qui tắc truy cập vào vào dữ liệu phân tích nơi mà chủ thể chỉ được phép truy cập kiểu thông tin đó với số lần truy cập nhất định. Một ví dụ cho trường hợp thứ hai có thể là một qui tắc chỉ ra trong điều kiện nào và các thuộc tính an toàn của một chủ thể và đối tượng thay đổi như là kết quả của thao tác truy cập như thế nào. Một số chính sách luồng thông tin ví dụ có thể giới hạn số thao tác truy cập vào thông tin với các thuộc tính an toàn cụ thể. Nếu không có quy tắc bổ sung nào, chủ thể PP/ST cần phải chỉ rõ "none".

Trong FDP_IFF.2.4, tác giả PP/ST cần phải chỉ rõ mọi qui tắc, dựa trên các thuộc tính an toàn, mà cấp phép rõ ràng cho luồng thông tin. Các qui tắc này được bổ sung vào các qui tắc đã ghi rõ trong các thành phần trước đó. Chúng có trong FDP_IFF 2.4 bởi vì chúng dự định chứa các ngoại trừ đối với các qui tắc trong thành phần trước đó. Một ví dụ về các qui tắc cấp phép luồng thông tin rõ ràng dựa trên vec-tơ ưu tiên liên kết với một chủ thể mà luôn cấp cho chủ thể khả năng tạo ra luồng thông tin cho thông tin mà được bao hàm bởi SFP đã được xác định. Nếu không có năng lực bổ sung nào, chủ thể PP/ST cần phải chỉ rõ "none".

Trong FDP_IFF.2.5, chủ thể PP/ST cần phải chỉ rõ các quy tắc, dựa trên các thuộc tính an toàn, mà từ chối rõ ràng cho luồng tin. Các quy tắc này bổ sung cho các quy tắc đã chỉ ra trong các phần tử trước đó. Chúng chứa trong FDP_IFF.2.5, có chứa các ngoại lệ đối với các quy tắc đó. Một ví dụ về các quy tắc từ chối rõ ràng cho các luồng tin là dựa trên vectơ đặc quyền liên quan đến một chủ thể, luôn từ chối chủ thể khả năng tạo ra luồng tin bao bởi SFP đã định trước. Nếu không có năng lực bổ sung nào, chủ thể PP/ST cần phải chỉ rõ "none".

F.6.4 FDP_IFF.3 Giới hạn các luồng thông tin bất hợp pháp

F.6.4.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cần được dùng khi tối thiểu một trong số SFP có yêu cầu kiểm soát các luồng tin trái phép mà không yêu cầu giảm bớt luồng tin.

Để chỉ ra các luồng tin trái phép, cần có các năng lực tối đa nhất định. Ngoài ra, một chủ thể PP/ST có khả năng chỉ ra việc các luồng tin trái phép có phải kiểm toán hay không.

F.6.4.2 Các hoạt động

F.6.4.2.1 Chỉ định

Trong FDP_IFF.3.1, chủ thể PP/ST cần phải chỉ rõ một SFP kiểm soát luồng tin thực thi bởi TSF. Tên của SFP kiểm soát luồng tin, phạm vi kiểm soát cho chính sách này được định nghĩa trong các thành phần thuộc chính sách kiểm soát luồng tin (FDP_IFC).

Trong FDP_IFF.3.1, chủ thể PP/ST cần phải chỉ rõ các kiểu luồng tin trái phép trong phạm vi dung lượng tối đa.

Trong FDP_IFF.3.1, chủ thể PP/ST cần phải chỉ rõ dung lượng tối đa cho phép cho các kiểu luồng tin trái phép đã xác định.

F.6.5 FDP_IFF.4 Loại trừ từng phần các luồng thông tin bất hợp pháp

F.6.5.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cần được dùng khi mọi SFP yêu cầu kiểm soát các luồng tin trái phép có yêu cầu loại trừ một số luồng tin trái phép (song không bắt buộc loại trừ tất cả).

F.6.5.2 Các hoạt động

F.6.5.2.1 Chỉ định

Trong FDP_IFF.4.1, chủ thể PP/ST cần phải chỉ rõ một SFP kiểm soát luồng tin thực thi bởi TSF. Tên của SFP kiểm soát luồng tin, phạm vi kiểm soát cho chính sách này được định nghĩa trong các thành phần thuộc chính sách kiểm soát luồng tin (FDP_IFC).

Trong FDP_IFF.4.1, chủ thể PP/ST cần phải chỉ rõ các kiểu luồng tin trái phép trong phạm vi dung lượng tối đa.

Trong FDP_IFF.4.1, chủ thể PP/ST cần phải chỉ rõ dung lượng tối đa cho phép cho các kiểu luồng tin trái phép đã xác định.

Trong FDP_IFF.4.1, chủ thể PP/ST cần phải chỉ rõ các kiểu luồng tin trái phép cần được loại trừ. Danh sách này có thể không trống vì thành phần này có yêu cầu loại trừ một số luồng tin trái phép.

F.6.6 FDP_IFF.5 Không có các luồng thông tin bất hợp pháp

F.6.6.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cần được dùng khi các SFP có yêu cầu kiểm soát các luồng tin trái phép yêu cầu loại trừ mọi luồng tin trái phép. Tuy nhiên, chủ thể PP/ST cần xem xét kỹ lưỡng ảnh hưởng của việc loại trừ mọi luồng tin trái phép có thể có đối với thao tác bình thường của TOE.

Nhiều ứng dụng thực tế đã chỉ ra rằng có một mối quan hệ gián tiếp giữa các luồng tin trái phép và chức năng bình thường trong TOE. Việc loại trừ mọi luồng tin trái phép có thể dẫn đến thiểu năng TOE.

F.6.6.2 Các hoạt động

F.6.6.2.1 Chỉ định

Trong FDP_IFF.5.1, chủ thể PP/ST cần phải chỉ rõ ra SFP kiểm soát luồng tin cần loại trừ luồng tin trái phép. Tên của SFP kiểm soát luồng tin, phạm vi kiểm soát cho chính sách này được định nghĩa trong các thành phần thuộc chính sách kiểm soát luồng tin (FDP_IFC).

F.6.7 FDP_IFF.6 Giám sát luồng thông tin bất hợp pháp

F.6.7.1 Chú thích cho ứng dụng người sử dụng

Họ này định nghĩa các cơ chế để nhập TSF- trung dữ liệu người dùng từ bên ngoài TOE vào TOE để các thuộc tính an toàn dữ liệu người dùng có thể được bảo toàn. Tính chắc chắn của các thuộc tính an toàn này được chỉ rõ bởi tính chắc chắn dữ liệu TSF TSF- liên kết (FPT-TDC).

Nhập từ bên ngoài TOE (FDP_ITC) liên quan đến các giới hạn về nhập khẩu, đặc điểm người dùng của các thuộc tính an toàn, và liên kết các thuộc tính an toàn với dữ liệu người dùng.

Họ này, và họ xuất tương ứng EXPORT từ TOE (FDP_ETC), chỉ ra TOE liên quan với dữ liệu người dùng bên ngoài kiểm soát của nó thế nào. Họ này liên quan đến việc chỉ định và tách thuộc tính an toàn dữ liệu người dùng.

Các hoạt động khác nhau có thể liên quan ở đây:

a) Nhập khẩu dữ liệu người dùng từ môi trường chưa định dạng (có nghĩa, đĩa mềm, băng, máy quét, video, hoặc tín hiệu kiểm tra), mà không có bất cứ thuộc tính an toàn nào, và đánh dấu theo cách vật lý môi trường chỉ ra nội dung của nó;

b) Nhập khẩu dữ liệu, gồm các thuộc tính an toàn, từ một môi trường và phân loại ra các thuộc tính an toàn đối tượng nào là tương ứng;

c) Nhập khẩu dữ liệu người dùng, gồm các thuộc tính an toàn, từ một môi trường sử dụng kỹ thuật đánh dấu mã hóa để bảo vệ liên hợp dữ liệu người dùng và các thuộc tính an toàn.

Họ này không liên quan với việc xác định dữ liệu người dùng có được nhập khẩu hay không. Nó liên quan đến các dữ liệu của các thuộc tính an toàn để liên kết với dữ liệu người dùng đã được nhập.

Thành phần này cần được dùng khi muốn rằng TSF có thể giám sát các luồng tin trái phép sử dụng một dung lượng vượt quá mức cho phép. Nếu cần kiểm chứng các luồng tin này, thành phần này có thể giúp cung cấp nguồn thông tin kiểm chứng được lấy từ họ FAU_GEN tạo dữ liệu kiểm toán an toàn.

F.6.7.2 Các hoạt động

F.6.7.2.1 Chỉ định

Trong FDP_IFF.6.1, chủ thể PP/ST cần phải chỉ rõ một SFP kiểm soát luồng tin thực thi bởi TSF. Tên của SFP kiểm soát luồng tin, phạm vi kiểm soát cho chính sách này được định nghĩa trong các thành phần thuộc chính sách kiểm soát luồng tin (FDP_IFC).

Trong FDP_IFF.6.1, chủ thể PP/ST cần phải chỉ rõ các kiểu luồng tin trái phép cần được giám sát khi có dung lượng vượt quá mức tối đa.

Trong FDP_IFF.6.1, chủ thể PP/ST cần phải chỉ rõ dung lượng tối đa mà TSF dùng để giám sát các luồng tin trái phép.

F.7 Nhập dữ liệu từ bên ngoài TOE (FDP_ITC)

F.7.1 Chú thich cho người sử dụng

Họ này định nghĩa các cơ chế để nhập TSF- trung gian dữ liệu người dùng từ bên ngoài TOE vào TOE để các thuộc tính an toàn dữ liệu người dùng có thể được bảo toàn. Tính chắc chắn của các thuộc tính an toàn này được chỉ rõ bởi tính chắc chắn dữ liệu TSF TSF- liên kết (FPT-TDC).

Nhập từ bên ngoài TOE (FDP_ITC) liên quan đến các giới hạn về nhập khẩu, đặc điểm người dùng của các thuộc tính an toàn, và liên kết các thuộc tính an toàn với dữ liệu người dùng.

Họ này, và họ xuất tương ứng EXPORT từ TOE (FDP_ETC), chỉ ra TOE liên quan với dữ liệu người dùng bên ngoài kiểm soát của nó thế nào. Họ này liên quan đến việc chỉ định và tách thuộc tính an toàn dữ liệu người dùng.

Một số thao tác có thể có là:

a) Nhập dữ liệu người dùng từ một môi trường chưa định dạng (đĩa từ, băng từ, bộ quét, video hay tín hiệu kiểm chứng) không có chứa một thuộc tính an toàn nào, và đánh dấu vật lý để biểu thị nội dung.

b) Nhập dữ liệu người dùng có thuộc tính an toàn từ một môi trường và kiểm tra các thuộc tính an toàn cho đối tượng có chính xác không.

c) Nhập dữ liệu người dùng, bao gồm cả thuộc tính an toàn từ một môi trường có sử dụng kỹ thuật mật mã để bảo vệ mối quan hệ giữa thuộc tính an toàn và dữ liệu người dùng.

Họ này không liên quan đến việc xác định xem dữ liệu người dùng có được nhập liệu không. Nó chỉ liên quan đến các giá trị của thuộc tính an toàn kết hợp với dữ liệu người dùng được nhập.

Có hai khả năng nhập liệu người dùng: hoặc dữ liệu người dùng có kết hợp với các thuộc tính an toàn tin cậy (các giá trị và ý nghĩa của thuộc tính an toàn không bị sửa đổi), hoặc không có các thuộc tính an toàn tin cậy (hoặc không có thuộc tính an toàn nào) có thể nhận được từ nguồn nhập liệu. Họ này đề cập đến cả hai trường hợp trên.

Nếu có sẵn các thuộc tính an toàn tin cậy, chúng có thể kết hợp với dữ liệu người dùng bằng phương thức vật lý (các thuộc tính an toàn thường trên cùng phương tiện), hoặc qua logic (các thuộc tính an toàn được cấp riêng, song có gắn liền định danh đối tượng, ví dụ tổng kiểm tra mật mã).

Họ này có liên quan đến việc nhập TSF-trung gian dữ liệu người dùng và duy trì sự kết hợp của các thuộc tính an toàn như SFP yêu cầu. Các họ khác liên quan đến các khía cạnh khác ví dụ như tính nhất quán, kênh tin cậy, tính vẹn toàn nằm ngoài phạm vi họ này. Ngoài ra, nhập liệu từ bên ngoài kiểm soát TSF (FDP_ITC) chỉ liên quan đến giao diện môi trường nhập liệu. Kết xuất ra kiểm soát TSF bên ngoài (FDP_ETC) chịu trách nhiệm đối với môi trường phía đầu kia (nguồn phát).

Một số yêu cầu nhập liệu quen thuộc là:

a) Nhập dữ liệu người dùng không có thuộc tính an toàn;

b) Nhập dữ liệu người dùng có thuộc tính an toàn, trong đó cả hai kết hợp với nhau và các thuộc tính an toàn biểu diễn phần nào thông tin đang được nhập.

Các yêu cầu nhập liệu này có thể xử lý bởi TSF với hoặc không có can thiệp của con người, tùy theo những hạn chế CNTT và chính sách an toàn của tổ chức. Ví dụ, nếu dữ liệu người dùng nhận được qua kênh "mật", các thuộc tính an toàn của các đối tượng được đặt thành "mật".

Nếu có nhiều SFP (kiểm soát luồng tin, và/hoặc kiểm soát truy nhập) thì chúng cần lặp các thành phần này cho mỗi SFP.

F.7.2 FDP_ITC.1 Nhập dữ liệu người dùng không có các thuộc tính an toàn

F.7.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này dùng để chỉ ra việc nhập dữ liệu người dùng không có thuộc tính an toàn tin cậy nào gắn liền theo. Chức năng này yêu cầu các thuộc tính an toàn cho dữ liệu người dùng được nhập cần được khởi tạo bên trong TSF. Đây cũng có thể là trường hợp chủ thể PP/ST chỉ ra các quy tắc cho nhập liệu. Đúng hơn, trong một số trường hợp, cần yêu cầu các thuộc tính này được cung cấp qua các kênh tin cậy hoặc các cơ chế kênh tin cậy.

F.7.2.2 Các hoạt động

F.7.2.2.1 Chỉ định

Trong FDP_ITC.1.1, chủ thể PP/ST cần phải chỉ rõ các kiểm soát truy nhập SFP và/hoặc các SFP kiểm soát luồng tin khi thực thi nhập dữ liệu người dùng. Dữ liệu người dùng được nhập vào thuộc phạm vi Chỉ định bởi các SFP này.

Trong FDP_ITC.1.3, chủ thể PP/ST cần phải chỉ ra mọi quy tắc kết xuất bổ sung hoặc "none" nếu như không có quy tắc kết xuất bổ sung nào. Các quy tắc này được thực thi bởi TSF bổ sung thêm cho SFP kiểm soát truy nhập và/hoặc SFP kiểm soát luồng tin đã chọn trong FDP_ITC.1.1.

F.7.3 Nhập liệu dữ liệu người dùng với các thuộc tính an toàn FDP_ITC.2

F.7.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này dùng để chỉ ra việc nhập dữ liệu người dùng với các thuộc tính an toàn tin cậy kết hợp với chúng.

Chức năng này dựa vào các thuộc tính an toàn có kết hợp chính xác và rõ ràng với các đối tượng của môi trường nhập liệu. Khi đã được nhập liệu, các đối tượng này sẽ có cùng các thuộc tính như vậy. Điều này đòi hỏi sự nhất quán dữ liệu TSF giữa các TSF (FPT_TDC) để đảm bảo tính nhất quán của dữ liệu. Đây có thể là trường hợp chủ thể PP/ST chỉ rõ các quy tắc nhập liệu.

F.7.3.2 Các hoạt động

F.7.3.2.1 Chỉ định

Trong FDP_ITC.2.1, tác giả PP/ST cần phải chỉ rõ một SFP kiểm soát truy cập và/hoặc các SFP kiểm soát luồng thông tin cần thực thi khi nhập dữ liệu người dùng từ bên ngoài TOE. Dữ liệu người dùng mà chức năng này nhập liệu được thông qua việc Chỉ định các SFP.

Trong FDP_ETC.2.4, chủ thể PP/ST cần phải chỉ ra mọi quy tắc luồng tin bổ sung hoặc "none" nếu như không có quy tắc luồng tin bổ sung nào. Các quy tắc này được thực thi bởi TSF bổ sung thêm cho SFP kiểm soát truy nhập và/hoặc SFP kiểm soát luồng tin đã chọn trong FDP_ITC.2.1.

F.8 Vận chuyển nội bộ TOE (FDP_ITT)

F.8.1 Chú thích cho người sử dụng

Họ này cung cấp các yêu cầu liên quan đến việc bảo vệ dữ liệu người dùng khi vận chuyển qua các phần của một TOE xuyên qua một kênh nội bộ. Việc vận chuyển này trái ngược với họ bảo vệ vận chuyển bí mật dữ liệu người dùng giữa các TSF (FDP_UCT) và họ bảo vệ vận chuyển đảm bảo vẹn

toàn dữ liệu người dùng giữa các TSF (FDP_UIT), trong đó có sự bảo vệ dữ liệu người dùng khi vận chuyển qua các TSF khác nhau thông qua kênh bên ngoài và kết xuất từ TOE (FDP_ETC), và nhập liệu từ bên ngoài TOE (FDP_ITC), chỉ rõ việc vận chuyển TSF-trung gian tới hoặc từ bên ngoài TOE.

Các yêu cầu trong họ này cho phép chủ thể PP/ST chỉ ra độ an toàn mong muốn cho dữ liệu người dùng khi vận chuyển bên trong TOE. Tính an toàn có thể là bảo vệ chống khai phá, sửa đổi, mất tính sẵn sàng.

Việc xác định mức độ phân tách về vật lý mà họ này cần áp dụng tùy thuộc vào môi trường sử dụng. Trong môi trường máy chủ, có thể xuất hiện các nguy cơ khi vận chuyển dữ liệu giữa các phần của TOE tách biết nhau qua BUS hệ thống. Trong các môi trường an toàn khác, việc vận chuyển có thể qua các phương tiện kết nối mạng truyền thống.

Nếu có nhiều SFP (kiểm soát luồng tin, và/hoặc kiểm soát truy nhập) thì chúng cần lặp các thành phần này cho mỗi SFP.

F.8.2 FDP_ITT.1 Bảo vệ chuyển giao cơ sở bên trong

F.8.2.1 Các hoạt động

F.8.2.1.1 Chỉ định

Trong FDP_ITC.1.1, chủ thể PP/ST cần phải chỉ rõ các kiểm soát truy nhập SFP và/hoặc các SFP kiểm soát luồng tin bao hàm các thông tin đang vạn chuyển.

F.8.2.1.2 Phép chọn

Trong FDP_ITC.1.1, chủ thể PP/ST cần phải chỉ rõ các kiểu lỗi truyền tải để TSF cần phải tránh khi vận chuyển dữ liệu người dùng. Các tùy chọn là để lộ, sửa đổi, mất khả năng dùng.

F.8.3 FDP_ITT.2 Phân tách truyền tải bởi các thuộc tính

F.8.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này có thể dùng, ví dụ để cung cấp các mẫu khác nhau cho việc bảo vệ thông tin với các mức rõ ràng khác nhau.

Một cách để tách biệt dữ liệu khi vận chuyển là thông qua việc sử dụng tách biệt các kênh vật lý hoặc logic.

F.8.3.2 Các hoạt động

F.8.3.2.1 Chỉ định

Trong FDP_ITC.2.1, chủ thể PP/ST cần phải chỉ rõ các kiểm soát truy nhập SFP và/hoặc các SFP kiểm soát luồng tin bao hàm thông tin đang được truyền tải.

F.8.3.2.2 Phép chọn

Trong FDP_ITC.2.1, chủ thể PP/ST cần phải chỉ rõ các kiểu lỗi truyền tải để TSF cần phải tránh khi vận chuyển dữ liệu người dùng. Các tùy chọn là để lộ, sửa đổi, mất khả năng dùng.

F.8.3.2.3 Chỉ định

Trong FDP_ITC.2.2, chủ thể PP/ST cần phải chỉ rõ các thuộc tính an toàn, các giá trị mà TSF dùng để xác định khi nào cần tách biệt dữ liệu đang truyền tải giữa các phần vật lý tách biệt của TOE.

Một ví dụ là nếu dữ liệu người dùng kết hợp với định danh của một chủ sở hữu được truyền tải tách biệt với dữ liệu người dùng có kết hợp với định danh của một chủ sở hữu khác. Trong trường hợp này,

giá trị định danh của chủ sở hữu dữ liệu là giá trị cần dùng để xác định khi nào cần tách biệt dữ liệu vận chuyển.

F.8.4 FDP_ITT.3 Giám sát toàn vẹn

F.8.4.1 Chú thích cho ứng dụng người sử dụng

Thành phần này dùng kết hợp với hoặc là FDP_ITT.1phần bảo vệ vận chuyển nội bộ cơ bản hoặc FDP_ITT.2 phần tách biệt vận chuyển qua thuộc tính. Nó đảm bảo rằng TSF kiểm tra dữ liệu người dùng nhận được (và các thuộc tính của nó) về tính toàn vẹn.

FDP_ITT.1 phần bảo vệ vận chuyển nội bộ cơ bản hoặc phần tách biệt vận chuyển qua thuộc tính FDP_ITT.2 sẽ cung cấp dữ liệu theo cách sao cho nó được bảo vệ chống sửa đổi (do đó FDP_ITT.3 giám sát tính toàn vẹn có thể phát hiện ra bất kỳ sự sửa đổi nào).

Chủ thể PP/ST cũng cần phải chỉ ra các kiểu lỗi có thể phát hiện. Chủ thể PP/ST cần phải xem xét: sự sửa đổi dữ liệu, thay thế dữ liệu, thay đổi thứ tự dữ liệu, phát lại dữ liệu, dữ liệu không toàn vẹn... ngoài các lỗi toàn vẹn khác.

Chủ thể PP/ST phải chỉ ra các thao tác mà TSF cần có để phát hiện ra lỗi. Ví dụ: bỏ qua dữ liệu người dùng, yêu cầu lại dữ liệu, thông báo quản trị có thẩm quyền, định tuyến lại lưu lượng tới các tuyến khác.

F.8.4.2 Các hoạt động

F.8.4.2.1 Chỉ định

Trong FDP_ITT.3.1, chủ thể PP/ST cần phải chỉ rõ các kiểm soát truy nhập SFP và/hoặc các SFP kiểm soát luồng tin bao hàm thông tin đang được chuyển tải và giám sát về các lỗi toàn vẹn.

Trong FDP_ITT.3.1, chủ thể PP/ST cần phải chỉ rõ các kiểu lỗi toàn vẹn cần được guám sát trong khi truyền tải dữ liệu người dùng.

Trong FDP_ITT.3.2, chủ thể PP/ST cần phải chỉ rõ các thao tác mà TSF cần có khi xảy ra lỗi toàn vẹn. Một ví dụ là TSF cần yêu cầu phát lại dữ liệu người dùng. Các SFP chỉ ra trong FDP_ITT.3.1 sẽ thực thi như thao tác cần thực hiện bởi TSF.

F.8.5 FDP_ITT.4 Giám sát toàn vẹn dựa trên thuộc tính

F.8.5.1 Chú thích cho ứng dụng người sử dụng

Thành phần này dùng kết hợp với phần tách biệt vận chuyển qua thuộc tính FDP_ITT.2. Nó đảm bảo rằng TSF kiểm tra dữ liệu người dùng nhận được với việc truyền tải thông qua các kênh tách biệt (dựa trên các giá trị thuộc tính an toàn đã chỉ ra) đảm bảo tính vẹn toàn. Nó cho phép chủ thể PP/ST chỉ ra các thao tác cần có để phát hiện lỗi toàn vẹn. Ví dụ, thành phần này có thể dùng cho việc phát hiện lỗi toàn vẹn khác nhau và thao tác cho thông tin ở các mức toàn vẹn khác nhau.

Chủ thể PP/ST cần phải chỉ ra các kiểu lỗi cần được phát hiện. Chủ thể PP/ST cần xem xét: sự sửa đổi dữ liệu, thay thế dữ liệu, thay đổi thứ tự dữ liệu, phát lại dữ liệu, dữ liệu không toàn vẹn... ngoài các lỗi toàn vẹn khác.

Chủ thể PP/ST phải chỉ ra các thuộc tính (và các kênh truyền liên quan) cần cho giám sát lỗi toàn vẹn.

Chủ thể PP/ST phải chỉ ra các thao tác mà TSF cần có để phát hiện ra lỗi. Ví dụ: bỏ qua dữ liệu người dùng, yêu cầu lại dữ liệu, thông báo quản trị có thẩm quyền, định tuyến lại lưu lượng tới các tuyến khác.

F.8.5.2 Các hoạt động

F.8.5.2.1 Chỉ định

Trong FDP_ITT.4.1, chủ thể PP/ST cần phải chỉ rõ các SFP kiểm soát truy nhập và/hoặc các SFP kiểm soát luồng tin bao hàm thông tin đang được chuyển tải và giám sát về các lỗi toàn vẹn.

Trong FDP_ITT.4.1, chủ thể PP/ST cần phải chỉ rõ các kiểu lỗi toàn vẹn cần được guám sát trong khi truyền tải dữ liệu người dùng.

Trong FDP_ITT.4.1, chủ thể PP/ST cần phải chỉ rõ danh sách các thuộc tính an toàn cần có để phân biệt các kênh truyền. Danh sách này dùng để xác định dữ liệu người dùng nào cần được giám sát lỗi toàn vẹn, trên cơ sở các thuộc tính an toàn và kênh truyền tải của nó. Phần tử này liên quan trực tiếp đến việc phân tách truyền tải FDP_ITT.2 qua các thuộc tính.

Trong FDP_ITT.4.2, chủ thể PP/ST cần phải chỉ rõ các thao tác mà TSF cần có khi xảy ra lỗi toàn vẹn. Một vi dụ là TSF cần yêu cầu phát lại dữ liệu người dùng. Các SFP chỉ ra trong FDP_ITT.3.1 sẽ thực thi như thao tác cần thực hiện bởi TSF.

F.9 Bảo vệ thông tin dư thừa (FDP_RIP)

F.9.1 Chú thích cho người sử dụng

Họ này xét nhu cầu cần đảm bảo rằng các tài nguyên TSF-kiểm soát, khi đã bị đưa ra khỏi một đối tượng và trước khi chúng được đặt lại vào một đối tượng khác, được TSF xử lý theo cách có thể để tái cấu trúc tất cả hoặc một phần dữ liệu chứa trong tài nguyên trước khi nó được định vị lại.

Một TOE thường có một số chức năng mà có tiềm năng đưa tài nguyên ra khỏi đối tượng và cũng có thể đặt lại những tài nguyên này vào các đối tượng. Một số, nhưng không phải tất cả các tài nguyên có thể được dùng để lưu trữ dữ liệu trọng yếu từ lần dùng tài nguyên trước và đối với các FDP_RIP tài nguyên này yêu cầu chúng được chuẩn bị để tái sử dụng. Việc tái sử dụng đối tượng áp dụng để làm rõ yêu cầu của đối tượng hoặc người dùng để cho phép các tài nguyên cũng như các thao tác ẩn của TSF mà ảnh hưởng trong việc bỏ ra ngoài và tái định vị sau đó các tài nguyên để phân biệt các đối tượng. Các ví dụ về yêu cầu rõ ràng là việc xóa hoặc cắt bớt một tệp hoặc để ra một khoảng bộ nhớ chính. Các ví dụ về thao tác ẩn của TSF là việc bỏ ra và tái định vị các khu vực bí mật.

Các yêu cầu tái sử dụng đối tượng liên quan đến nội dung của tài nguyên thuộc về một đối tượng, không phải tất cả thông tin về tài nguyên hoặc đối tượng mà có thể lưu trữ ở nơi nào đó trong TSF. Một vi dụ thỏa mãn yêu cầu FDP_RIP đối với các tệp khi đối tượng yêu cầu tất cả các phần tạo ra tệp cần được chuẩn bị để tái sử dụng.

Họ này cũng áp dụng cho các tài nguyên có thể sử dụng lại tuần tự bởi các chủ thể trong hệ thống. Ví dụ, đa số hệ điều hành thường dựa trên các thanh ghi phần cứng (tài nguyên) để hỗ trợ các tiến trình trong hệ thống.Khi các tiến trình chuyển từ trạng thái "run" sang "sleep" (hoặc ngược lại), các thanh ghi trên sẽ được sử dụng lại tuần tự bởi các chủ thể khác. Trong khi thao tác "chuyển đổi" (swapping) không được coi lá cấp phát hoặc giải phóng tài nguyên.Bảo vệ thông tin dư thừa (FDP_RIP) có thể áp dụng cho các sự kiện và tài nguyên.

Bảo vệ thông tin dư thừa (FDP_RIP) thường kiểm soát truy nhập tới thông tin không phải là một phần của đối tượng đang xác định hoặc đang được truy nhập. Tuy nhiên, trong một số trường hợp, điều này không hoàn toàn đúng. Lấy ví dụ, đối tượng "A" là một tệp, đối tượng B là một đĩa nơi lưu giữ tệp. Nếu đối tượng A bị xóa, thông tin về đối tượng A sẽ bị kiểm soát bởi phần bảo vệ thông tin dư thừa (FDP_RIP) ngay cả khi nó vẫn còn là một phần của đối tượng B.

Điều quan trọng cần lưu ý là phần bảo vệ thông tin dư thừa (FDP_RIP) chỉ áp dụng cho các đối tượng trực tuyến (on-line) chứ không cho các đối tượng ngoại tuyến (off-line) vì như những gì backup trên băng từ. Lấy ví dụ, nếu 1 tệp bị xóa trong TOE, phần bảo vệ thông tin dư thừa (FDP_RIP) sẽ có thể yêu cầu không có thông tin dư thừa sau khi giải phóng. Tuy nhiên TSF không thể mở rộng phép thực hiện này cho cùng một tệp tồn tại ở dạng backup ngoại tuyến. Bởi vậy, chính tệp đó vẫn dùng được. Nếu đây là mối nghi ngại thì chủ thể PP/ST cần đảm bảo rằng các đối tượng môi trường phù hợp được đặt ra để hỗ trợ quản trị các đối tượng ngoại tuyến.

Bảo vệ thông tin dư thừa (FDP_RIP) và Rollback (FDP_ROL) có thể xung đột khi Bảo vệ thông tin dư thừa (FDP_RIP) thực hiện yêu cầu xóa thông tin dư thừa tại thời điểm ứng dụng giải phóng đối tượng đến TSF (nghĩa là giải phóng tài nguyên). Bởi vậy việc chọn chức năng "Deallocation" của Bảo vệ thông tin dư thừa (FDP_RIP) cần không được sử dụng với Rollback (FDP_ROL) do không có thông tin cần lấy lại. Việc chọn lựa khác là "không sẵn sàng khi cấp phát" có thể dùng với Rollback (FDP_ROL), tuy nhiên có nguy cơ là tài nguyên đang giữ thông tin đã được cấp phát cho đối tượng mới trước khi rollback có tác dụng. Khi xảy ra điều đó, rollback sẽ không thể thực hiện được.

Trong Bảo vệ thông tin dư thừa (FDP_RIP) không có các yêu cầu kiểm toán, bởi vì đó không phải chức năng được người dùng thực hiện. Kiểm toán các tài nguyên đã cấp phát hoặc giải phóng có thể thực thi trong các thao tác của SFP kiểm soát truy nhập hoặc SFP kiểm soát luồng tin.

Họ này cần được áp dụng cho các đối tượng đã chỉ ra trong SFP kiểm soát truy nhập hoặc SFP kiểm soát luồng tin như đã chỉ ra bởi chủ thể PP/ST.

F.9.2 FDP_RIP.1 Bảo vệ thông tin dư thừa tập con

F.9.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu cho mỗi tập con đối tượng trong TOE là TSF sẽ đảm bảo rằng không có thông tin dư thừa dùng được chứa trong một tài nguyên đã được cấp phát hoặc đã giải phóng cho các đối tượng đó.

F.9.2.2 Các hoạt động

F.9.2.2.1 Chỉ định

Trong FDP_RIP.1.1, chủ thể PP/ST cần phải chỉ rõ sự kiện, việc cấp phát hoặc giải phóng tài nguyên gọi đến chức năng Bảo vệ thông tin dư thừa.

F.9.2.2.2 Chỉ định

Trong FDP_RIP.1.1, chủ thể PP/ST cần phải chỉ rõ danh sách các đối tượng cho phần bảo vệ thông tin dư thừa.

F.9.3 FDP_RIP.2 Bảo vệ thông tin dư thừa đầy đủ

F.9.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu cho mọi đối tượng trong TOE là TSF sẽ đảm bảo rằng không có thông tin dư thừa dùng được chứa trong một tài nguyên đã được cấp phát hoặc đã giải phóng cho các đối tượng đó.

F.9.3.2 Các hoạt động

F.9.3.2.1 Phép chọn

Trong FDP_RIP.2.1, chủ thể PP/ST cần phải chỉ rõ sự kiện, việc cấp phát hoặc giải phóng tài nguyên gọi đến chức năng bảo vệ thông tin dư thừa.

F.10 Khôi phục (FDP_ROL)

F.10.1 Chú thích cho người sử dụng

Họ này chỉ nhu cầu cần quay trở lại một trạng thái hợp lệ định trước, ví dụ như nhu cầu của một người dùng muốn hoàn lại những sửa đổi trong tệp, hoặc hoàn lại các giao dịch trong trường hợp chuỗi giao dịch chưa hoàn thiện khi thao tác với cơ sở dữ liệu.

Họ này nhằm hỗ trợ người dùng hoàn lại một trạng thái hợp lệ định trước sau khi người dùng đã hoàn lại các thao tác, hoặc trong một cơ sở dữ liệu phân tán, hoàn lại mọi bản sao phân bố của cơ sở dữ liệu về trang thái trước khi xảy ra thao tác lỗi.

Bảo vệ thông tin dư thừa (FDP_RIP) và Hoàn lại (FDP_ROL) xung đột khi bảo vệ thông tin dư thừa (FDP_RIP) thực thi với việc nội dung không còn khả dụng tại thời điểm một tài nguyên được giải phóng khỏi một đối tượng. Bởi vậy, việc sử dụng chức năng bảo vệ thông tin dư thừa (FDP_RIP) không thể kết hợp với chức năng Hoàn lại Rollback (FDP_ROL) vì không còn thông tin để hoàn lại. Bảo vệ thông tin dư thừa (FDP_RIP) có thể chỉ sử dụng với Hoàn lại (FDP_ROL) khi thực thi với điều kiện nội dung thông tin sẽ không còn khả dụng ở thời điểm tài nguyên được cấp phát tới một đối tượng khác. Lý do là cơ chế hoàn lại (FDP_ROL) sẽ có một cơ hội truy nhập thông tin trước đó vẫn có thể còn có trong TOE để thực thi thành côgn việc hoàn lại thao tác. Yêu cầu để hoàn lại được giới hạn bởi một số hạn định. Ví dụ, một bộ soạn thảo văn bản thường chỉ cho phép hoàn lại một số lệnh nhất định. Một ví dụ khác là backup. Nếu băng từ backup bị quay chiều, sau khi băng từ đã được sử dụng lại, thì không còn có thể gọi lại thông tin. Đó cũng là giới hạn đối với yêu cầu hoàn lại.

F.10.2 FDP_ROL.1 Khôi phục cơ bản

F.10.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cho phép một người dùng hay chủ thể được hoàn lại một tập các thao tác trên một tập đối tượng định trước. Phép hoàn lại chỉ có thể trong hạn định, ví dụ cho tới một lượng ký tự hoặc tới một hạn định thời gian.

F.10.2.2 Các hoạt động

F.10.2.2.1 Chỉ định

Trong FDP_ROL.1.1, chủ thể PP/ST cần phải chỉ rõ các SFP kiểm soát truy nhập và/hoặc các SFP kiểm soát luồng tin cần thực thi khi thực hiện các thao tác hoàn lại. Điều này cần thiết để đảm bảo rằng việc hoàn lại không dùng để phá vỡ các SFP đã cho.

Trong FDP_ROL.1.1, chủ thể PP/ST cần phải chỉ rõ danh sách các thao tác có thể hoàn lại.

Trong FDP_ROL.1.1, chủ thể PP/ST cần phải chỉ rõ thông tin và/hoặc danh sách các đối tượng dùng trong chinh sách hoàn lại.

Trong FDP_ROL.1.2, chủ thể PP/ST cần phải chỉ rõ giới hạn chặn cho các thao tác hoàn lại. Giới hạn có thể chỉ ra là một khoảng thời gian định trước, vi dụ, các thao tác có thể hoàn lại khi đã thực thi trong vòng 2 phút trở lại. Các giới hạn khác có thể được xác định là số tối đa các thao tác cho phép, hoặc kích thức bộ đệm.

F.10.3.1 FDP_ROL.2 Khôi phục cải tiến Chú thich cho ứng dụng người sử dụng

Thành phần này buộc TSF cung cấp khả năng hoàn lại mọi thao tác. Tuy nhiên, người dùng có thể chọn hoàn lại chỉ là một phần của chúng.

F.10.3.2 Các hoạt động

F.10.3.2.1 Chỉ định

Trong FDP_ROL.2.1, chủ thể PP/ST cần phải chỉ rõ các SFP kiểm soát truy nhập và/hoặc các SFP kiểm soát luồng tin cần thực thi khi thực hiện các thao tác hoàn lại. Điều này cần thiết để đảm bảo rằng việc hoàn lại không dùng để phá vỡ các SFP đã cho.

Trong FDP_ROL.2.1, chủ thể PP/ST cần phải chỉ rõ danh sách các đối tượng dùng trong chính sách hoàn lại.

Trong FDP_ROL.2.2, chủ thể PP/ST cần phải chỉ rõ hạn định về giới hạn mà các thao tác hoàn lại có thể thực thi. Giới hạn có thể được chỉ ra là một khoảng thời gian định trước, vi dụ, các thao tác có thể hoàn lại khi đã thực thi trong vòng 2 phút trở lại. Các giới hạn khác có thể được xác định là số tối đa các thao tác cho phép, hoặc kích thức bộ đệm.

F.11 Toàn vẹn dữ liệu lưu trữ (FDP_SDI)

F.11.1 Chú thích cho người sử dụng

Họ này cung cấp các yêu cầu về việc bảo vệ dữ liệu người dùng trong khi chúng được lưu giữ trong khoang chứa do TSF kiểm soát.

Các bất ổn hoặc lỗi phần cứng có thể ảnh hưởng đến dữ liệu đã lưu trong bộ nhớ. Họ này cho các yêu cầu nhằm phát hiện các lối không định trước này. Sự toàn vẹn của dữ liệu người dùng khi lưu giữ trong các thiết bị nhớ do TSF kiểm soát cũng được xét đến trong họ này.

Để tránh cho một chủ thể sửa đổi dữ liệu, các chức năng kiểm soát luồng tin (FDP_IFF) hoặc các họ chức năng kiểm soát truy nhập (FDP_ACF) được yêu cầu.

Họ này khác với phép vận chuyển TOE nội bộ (FDP_ITT) là nó nó bảo vệ dữ liệu người dùng khỏi các lỗi toàn vẹn khi truyền tải dữ liệu bên trong TOE.

F.11.2 FDP_SDI.1 Giám sát toàn vẹn lưu trữ dữ liệu

F.11.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này giám sát các lỗi toàn vẹn cho dữ liệu đã lưu trong phương tiện lưu trữ. Chủ thể PP/ST có thể chỉ ra các loại thuộc tính dữ liệu người dùng khác nhau để dùng làm cơ sở cho việc giám sát.

F.11.2.2 Các hoạt động

F.11.2.2.1 Chỉ định

Trong FDP_SDI.1.1, chủ thể PP/ST cần phải chỉ ra các lỗi toàn vẹn mà TSF có thể phát hiện.

Trong FDP_SDI.1.1, chủ thể PP/ST cần phải chỉ ra các thuộc tính dữ liệu người dùng có thể sử dụng làm cơ sở cho việc giám sát.

F.11.3 FDP_SDI.2 Giám sát toàn vẹn dữ liệu lưu trữ và hành động

F.11.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này giám sát các lỗi toàn vẹn cho dữ liệu đã lưu trong phương tiện lưu trữ. Chủ thể PP/ST có thể chỉ ra thao tác nào cần thực hiện khi phát hiện có lỗi toàn vẹn.

F.11.3.2 Các hoạt động

F.11.3.2.1 Chỉ định

Trong FDP_SDI.2.1, chủ thể PP/ST cần phải chỉ ra các lỗi toàn vẹn mà TSF có thể phát hiện.

Trong FDP_SDI.2.1, chủ thể PP/ST cần phải chỉ ra các thuộc tính dữ liệu người dùng có thể sử dụng làm cơ sở cho việc giám sát.

Trong FDP_SDI.2.2, chủ thể PP/ST cần phải chỉ ra các thao tác cần có khi phát hiện có lỗi toàn vẹn.

F.12 Bảo vệ vận chuyển bí mật dữ liệu người dùng liên-TSF (FDP_UCT)

F.12.1 Chú thích cho người sử dụng

Họ này xác định các yêu cầu để đảm bảo tính bí mật của dữ liệu người dùng khi truyền tải qua một kênh bên ngoài giữa TOE và sản phẩm CNTT tin cậy khác. Tính bí mật cần thực hiện bằng việc cấm khai phá không có thẩm quyền dữ liệu người dùng trong quá trình truyền giữa hai đầu cuối. Các đầu cuối có thể là một TSF hoặc một người dùng.

Họ này cung cấp yêu cầu bảo vệ dữ liệu người dùng khi truyền tải. Ngược lại, chức năng bí mật của dữ liệu TSF được kết xuất (FPT_ITC) xử lý dữ liệu TSF.

F.12.2 FDP_UCT.1 Bí mật trao đổi dữ liệu cơ bản

F.12.2.1 Chú thích cho ứng dụng người sử dụng

TSF có khả năng bảo vệ dữ liệu người dùng chống khai phá trong khi chúng được trao đổi.

F.12.2.2 Các hoạt động

F.12.2.2.1 Chỉ định

Trong FDP_UCT.1.1, chủ thể PP/ST cần phải chỉ rõ các SFP kiểm soát truy nhập và/hoặc các SFP kiểm soát luồng tin cần được thực hiện khi trao đổi dữ liệu người dùng. Các chính sách đã Chỉ định sẽ được thực thi để ra quyết định về việc ai có thể trao đổi dữ liệu và dữ liệu nào có thể được trao đổi.

F.12.2.2.2 Phép chọn

Trong FDP_UCT.1.1, chủ thể PP/ST cần phải chỉ rõ phần tử này được áp dụng cho một cơ chế truyền tải hay thu nhận dữ liệu người dùng.

F.13 Bảo vệ vận chuyển toàn vẹn dữ liệu người dùng liên-TSF (FDP_UIT)

F.13.1 Chú thích cho người sử dụng

Họ này xác định các yêu cầu đối với việc đảm bảo toàn vẹn cho dữ liệu người dùng khi truyền tải giữa TSF và sản phẩm CNTT tin cậy khác, và khôi phục lại từ các lỗi có thể phát hiện được. Ít nhất, họ này giám sát sự toàn vẹn của dữ liệu người dùng chống sự sửa đổi. Ngoài ra, họ này hỗ trợ các cách khác nhau để sửa các lỗi toàn vẹn đã phát hiện ra.

Họ này xác định các yêu cầu đảm bảo toàn vẹn cho dữ liệu người dùng khi đang truyền, trong khi đó chức năng toàn vẹn dữ liệu kết xuất TSF (FPT_ITI) xử lý dữ liệu TSF.

Chức năng bảo vệ truyền tải toàn vẹn dữ liệu người dùng liên TSF (FDP_UIT) và bảo vệ truyền tải bí mật dữ liệu người dùng liên TSF (FDP_UCT) đi đôi với nhau, vì chức năng bảo vệ truyền tải bí mật dữ liệu người dùng liên TSF (FDP_UCT) xét tính bí mật của dữ liệu người dùng. Bởi vậy, cơ chế tương tự thực thi bảo vệ truyền tải toàn vẹn dữ liệu người dùng liên TSF (FDP_UIT) có thể dùng được để thực thi các họ khác như bảo vệ truyền tải bí mật dữ liệu người dùng liên TSF (FDP_UCT) và họ nhập liệu từ bên ngoài kiểm soát TSF (FDP_ITC).

F.13.2 FDP_UIT.1 Toàn vẹn trao đổi dữ liệu

F.13.2.1 Chú thích cho ứng dụng người sử dụng

TSF có khả năng cơ bản là gửi hoặc nhận dữ liệu người dùng theo cách phát hiện được sự sửa đổi dữ liệu người dùng. Không cần có yêu cầu nào cho một cơ chế TSF để khôi phục sửa đổi đó.

F.13.2.2 Các hoạt động

F.13.2.2.1 Chỉ định

Trong FDP_UIT.1.1, chủ thể PP/ST cần phải chỉ rõ các SFP kiểm soát truy nhập và/hoặc các SFP kiểm soát luồng tin cần được thực hiện khi truyền hoặc nhận dữ liệu người dùng. Các chính sách đã Chỉ định sẽ được thực thi để ra quyết định về việc ai có thể gửi hoặc nhận dữ liệu và dữ liệu nào có thể được gửi hoặc nhận.

F.13.2.2.2 Phép chọn

Trong FDP_UIT.1.1, chủ thể PP/ST cần phải chỉ rõ phần tử này được áp dụng cho một cơ chế truyền tải hay thu nhận các đối tượng.

Trong FDP_UIT.1.1, chủ thể PP/ST cần phải chỉ rõ dữ liệu cần phải được bảo vệ chống sửa đổi, xóa, chèn thêm hoặc phát lại.

Trong FDP_UIT.1.2, chủ thể PP/ST cần phải chỉ rõ lỗi các kiểu như: sửa đổi, xóa, chèn thêm hay phát lại được phát hiện.

F.13.3 FDP_UIT.2 Khôi phục trao đổi dữ liệu gốc

F.13.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cung cấp khả năng khôi phục từ một tập các lỗi truyền đã xác định, nếu cần thiết, sử dụng sựu trợ giúp của sản phẩm CNTT tin cậy khác.

Do sản phẩm CNTT tin cậy khác nằm ngoài TSC, TSF không thể kiểm soát hành vi của nó. Tuy nhiên, nó có thể cung cấp các chức năng có khả năng hợp tác với sản phẩm CNTT tin cậy khác để nhằm mục đích khôi phục. Ví dụ, TSF có thể chứa các chức năng tùy theo nguồn phát sản phẩm CNTT tin cậy khác để gửi lại dữ liệu khi phát hiện có lỗi xảy ra.

Thành phần này liên quan đến khả năng TSF xử lý khôi phục lỗi như vậy.

F.13.3.2 Các hoạt động

F.13.3.2.1 Chỉ định

Trong FDP_UIT.2.1, chủ thể PP/ST cần phải chỉ rõ các SFP kiểm soát truy nhập và/hoặc các SFP kiểm soát luồng tin cần thực thi khi khôi phục dữ liệu. Các chính sách đã Chỉ định sẽ được thực thi để ra quyết định về việc dữ liệu nào có thể khôi phục và cách thức có thể khôi phục nó.

Trong FDP_UIT.2.1, chủ thể PP/ST cần phải chỉ rõ danh sách các lỗi toàn vẹn mà TSF với trợ giúp của nguồn phát sản phẩm CNTT tin cậy khác có thể khôi phục lại dữ liệu người dùng ban đầu.

F.13.4 FDP_UIT.3 Khôi phục trao đổi dữ liệu đích

F.13.4.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cung cấp khả năng khôi phục từ một tập các lỗi truyền đã xác định. Nó hoàn tất nhiệm vụ mà không cần có sự trợ giúp của sản phẩm CNTT tin cậy khác. Ví dụ, nếu phát hiện ra lỗi nào đó, giao thức truyền tải cần phải đủ mạnh để cho phép TSF khôi phục lại lỗi dựa trên cơ sở tổng kiểm tra và các thông tin khả dụng khác trong giao thức.

F.13.4.2 Các hoạt động

F.13.4.2.1 Chỉ định

Trong FDP_UIT.3.1, chủ thể PP/ST cần phải chỉ rõ các SFP kiểm soát truy nhập và/hoặc các SFP kiểm soát luồng tin cần thực thi khi khôi phục dữ liệu. Các chính sách đã Chỉ định sẽ được thực thi để ra quyết định về việc dữ liệu nào có thể khôi phục và cách thức có thể khôi phục nó.

Trong FDP_UIT.3.1, chủ thể PP/ST cần phải chỉ rõ danh sách các lỗi toàn vẹn mà chỉ bản thân TSF nguồn thu có khả năng khôi phục lại dữ liệu người dùng ban đầu.

Phụ lục G

(Quy định)

Lớp FIA: Định danh và xác thực

Một yêu cầu bảo mật thông thường là để xác nhận rõ người dùng, thực thể thực hiện các chức năng trong một TOE. Điều này không chỉ là xác minh định danh yêu cầu của mỗi người dùng mà còn xác nhận mỗi người dùng đó có thực là người mà họ yêu cầu không. Điều này được thực hiện bằng cách yêu cầu người dùng cung cấp TSF về một vài thông tin cái mà được biết như là TSF dùng để liên kết với người dùng trong câu hỏi.

Các họ trong lớp này gửi các yêu cầu cho các chức năng để thiết lập và xác minh một định danh người dùng được yêu cầu. Định danh và xác thực được yêu cầu để đảm bảo rằng người dùng được liên kết (được trợ giúp) với các thuộc tính an toàn thích hợp (vd như định danh, nhóm, quy tắc, bảo mật hoặc các mức toàn vẹn).

Việc định danh rõ ràng của người dùng có thẩm quyền và sự liên kết (trợ giúp) đúng của các thuộc tính an toàn với người dùng và các đối tượng (subject) là điều kiện để áp đặt các chính sách an toàn.

Họ định danh người dùng (FIA_UID) thực hiện (gửi) việc xác định định danh của một người dùng.

Họ xác thực người dùng (FIA_UAU) thực hiện việc xác thực định danh một người dùng.

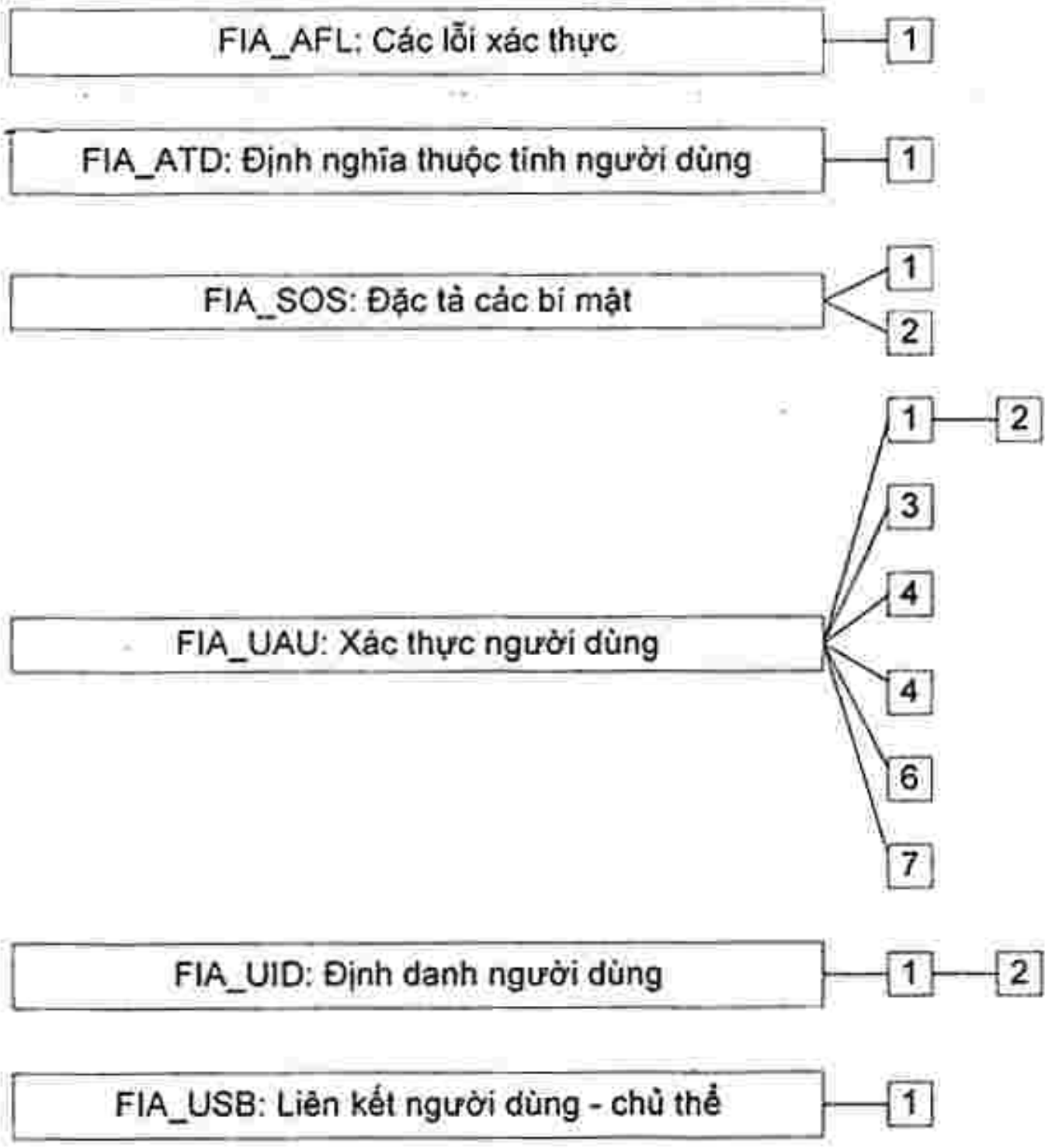
Họ lỗi xác thực (FIA_AFL) thực hiện việc định nghĩa hạn chế lặp lại việc thử xác thực không thành công.

Họ định nghĩa thuộc tính người dùng (FIA_ATD) thực hiện việc định nghĩa các thuộc tính người dùng mà được sử dụng trong việc bắt buộc của TSP.

Họ ràng buộc đối tượng người dùng (FIA_USB) thực hiện việc liên kết đúng của các thuộc tính an toàn cho mỗi người dùng có thẩm quyền.

Họ miêu tả các vấn đề bảo mật (FIA_SOS) thực hiện việc phát sinh và xác minh các vấn đề bảo mật mà thỏa mãn một tập đã định nghĩa.

Hình G1 chỉ ra sự tách lớp này thành các thành phần hợp thành



Hình G1- Sự phân cấp lớp FIA: định danh và xác thực

G.1 Các lỗi xác thực (FIA_AFL)

G.1.1 Chú thích cho người sử dụng

Họ này gửi những yêu cầu về định nghĩa các giá trị đối với việc thử xác thực và các hành động TSF trong trường hợp lỗi thử xác thực. Các tham số như là số lần thử và ngưỡng thời gian là không hạn chế.

Tiến trình thiết lập phiên là sự tương tác với người dùng để thực thi việc thiết lập phiên độc lập với thực thi hành động. Nếu số lần thử xác thực không thành công vượt quá ngưỡng đã Chỉ định hoặc tài khoản người dùng hoặc thiết bị đầu cuối (hoặc cả 2) thì sẽ bị khóa. Nếu tài khoản người dùng bị khóa, người dùng không thể đăng nhập vào hệ thống. Nếu thiết bị đầu cuối bị khóa, thiết bị đầu cuối (hay địa chỉ của thiết bị đó) không được sử dụng cho bất kỳ lần đăng nhập nào. Duy trì cả 2 trường hợp này cho đến khi thỏa mãn điều kiện thiết lập lại.

G.1.2 FIA_AFL.1 Xử lý lỗi xác thực

G.1.2.1 Chú thích cho ứng dụng người sử dụng

Tác giả PP/ST có thể định nghĩa số lần thử xác thực không thành công hoặc có thể chọn để giúp nhà phát triển TOE hoặc người dùng có thẩm quyền định nghĩa số này. Việc thử xác thực không thành công không cần phải liên tục, nhưng đúng hơn là có sự liên quan tới một sự kiện xác thực. Như vậy một sự kiện xác thực có thể được tính toán từ phiên thiết lập thành công trước ở một thiết bị đầu cuối đã xác định.

Tác giả PP/ST có thể xác định một danh sách các hành động mà TSF sẽ thực thi trong trường hợp lỗi xác thực. Một người quản trị có thẩm quyền có thể cũng được phép quản lý các sự kiện, nếu được phép của tác giả PP/ST. Các sự kiện đó có thể là các hành động: khởi tạo hành động đầu cuối, khởi tạo tài khoản người dùng hoặc đưa ra cảnh báo với người quản trị. Các điều kiện dưới trạng thái nào mà sẽ được lưu trữ một cách thông thường phải được xác định trên hành động đó.

Để ngăn chặn từ chối dịch vụ, TOE luôn đảm bảo rằng có ít nhất một tài khoản người dùng không bị khóa.

Hơn nữa các hành động cho TSF có thể xác định bởi tác giả PP/ST gồm các quy tắc cho việc khởi tạo lại quy trình thiết lập phiên người dùng, hoặc gửi một cảnh báo tới người quản trị. Ví dụ các hành động này là: cho tới khi thời gian Chỉ định trôi qua, cho tới khi người quản trị có thẩm quyền khích hoạt lại tài khoản hoặc thiết bị đầu cuối, một lần thử trước đó bị lỗi (tất cả các lần thử mà bị lỗi, 2 lần lien tiếp ngắt kích hoạt).

G.1.2.2 Các hoạt động

G.1.2.2.1 Phép chọn

Trong FIA_AFL.1.1, tác giả PP/ST nên chọn hoặc là gán một số nguyên hoặc cụm từ sau "Người quản trị nhập số nguyên dương" và đưa ra dải giá trị chấp nhận được.

G.1.2.2.2 Chỉ định

Trong FIA_AFL.1.1, tác giả PP/ST nên chỉ rõ các sự kiện xác thực. Ví dụ các sự kiện xác thực này là: việc thử xác thực không thành công kể từ xác thực thành công cuối cùng đối với định danh người dùng đã chỉ ra, các lần thử xác thực không thành công kể từ xác thực thành công cuối cùng cho thiết bị đầu cuối hiện tại, số lần thử xác thực không thành công trong 10 phút vừa qua. Có ít nhất một sự kiện xác thực phải được xác định.

Trong FIA_AFL.1.1, nếu việc gán số nguyên dương mà được chọn, tác giả PP/ST xác định số mặc định (số nguyên dương) của lần thử xác thực không thành công, khi bằng hoặc lớn hơn, cái mà sẽ gây ra các sự kiện.

Trong FIA_AFL.1.1, nếu một người quản trị khai báo số nguyên dương là được chọn, tác giả PP/ST nên xác định dải giá trị chấp nhận được từ cái mà người quản trị của TOE có thể khai báo số lần thử xác thực không thành công. Số lần thử xác thực nên ít hơn hoặc bằng giá trị cận trên và lớn hơn hoặc bằng giá trị cận dưới.

Trong FIA_AFL.1.2, tác giả PP/ST nên xác định các hành động để thực thi trong trường hợp bằng hoặc lớn hơn ngưỡng. Các hành động này có thể sẽ khóa tài khoản trong 5 phút, khóa thiết bị đầu cuối cho một lần tăng (2 hoặc nhiều hơn số lần thử không thành công trong 1 giây), hoặc khóa tài khoản cho tới khi bị khóa bởi người quản trị và khai báo đồng thời tới người quản trị. Các hành động nên xác định phép đo và nếu khoảng đo là thích hợp (hoặc cận dưới của phép đo).

G.1.2.2.3 Phép chọn

Trong FIA_AFL. 1.2, tác giả PP/ST cần chọn hoặc sự kiện gặp gỡ hoặc vượt quá số lượng đã xác định các thử xác thực không thành công sẽ thúc đẩy TSF thao tác.

G.1.2.2.4 Chỉ định

Trong FIA_AFL.1.2, tác giả PP/ST cần chỉ rõ các thao tác được thực hiện trong trường hợp ngưỡng được đáp ứng hoặc bị vượt quá hoặc được lựa chọn. Các thao tác này có thể bị vô hiệu hóa trong 5 giây, vô hiệu giới hạn số lần gia tăng (2 mũ số lần thử không thành công tính theo giây), hoặc vô hiệu tài khoản đến khi quản trị mở khóa và đồng thời thông báo với quản trị.

Các thao tác cần chỉ rõ các biện pháp và nếu có thể áp dụng thì là khoảng thời gian của biện pháp (hoặc các điều kiện trong đó các biện pháp nào sẽ kết thúc).

G.2 Định nghĩa thuộc tính người dùng (FIA_ATD)

G.2.1 Chú thích cho người sử dụng

Tất cả người dùng có thẩm quyền có thể có một tập các thuộc tính an toàn, không phải là định danh người dùng, mà nó được dùng để bắt buộc các SFR. Họ này định nghĩa các yêu cầu cho việc liên kết các thuộc tính an toàn người dùng với các người dùng mà cần để trợ giúp TSF trong việc ra quyết định an toàn.

Có sự phụ thuộc vào các định nghĩa chính sách an toàn riêng biệt. Những định nghĩa riêng này nên chứa danh sách các thuộc tính mà cần thiết cho việc bắt buộc chính sách.

G.2.2 Xác định thuộc tính người dùng FIA_ATD.1

G.2.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này xác định các thuộc tính an toàn mà nên được duy trì tại mức của người dùng. Điều này có nghĩa là các thuộc tính an toàn đã liệt kê được gán và có thể được thay đổi tại mức người dùng. Bên cạnh đó, việc thay đổi thuộc tính an toàn trong danh sách này liên kết với một người dùng không nên có ảnh hưởng tới các thuộc tính an toàn của bất kỳ người dùng khác.

Trong trường hợp các thuộc tính an toàn thuộc về nhóm các người dùng (như là danh sách các khả năng đối với một nhóm), người dùng sẽ cần có một tham chiếu (như thuộc tính an toàn) tới nhóm có liên quan.

G.2.2.2 Các hoạt động

G.2.2.2.1 Chỉ định

Trong FIA_ATD.1.1, tác giả PP/ST nên xác định các thuộc tính an toàn mà được liên kết tới một người dùng riêng. Ví dụ như một danh sách là {"thông hành", "định danh nhóm", "quyền"}.

G.3 Đặc tả các bí mật (FIA_SOS)

G.3.1 Chú thích cho người sử dụng

Họ này định nghĩ các yêu cầu đối với các cơ chế mà bắt buộc tập đặc tính đã xác định trên các vấn đề bảo mật đã được cung cấp, và phát sinh vấn đề bảo mật để thỏa mãn tập đã xác định. Ví dụ như các cơ chế có thể bao gồm việc kiểm tra mật khẩu người dùng tự động, hoặc sự phát sinh mật khẩu tự động.

Một vấn đề bảo mật có thể được phát sinh bên ngoài TOE (vd được chọn bởi người dùng và được giới thiệu trong hệ thống). Như trong trường hợp, việc xác minh thành phần bảo mật FIA_SOS.1 có thể được sử dụng để đảm bảo rằng vấn đề bảo mật được phát sinh mở rộng tham gia tới các chuẩn nhất định, vi dụ một kich cỡ tối thiểu có thể không được sử dụng trước đó mà không xuất hiện trong từ điển.

Vấn đề bảo mật cũng có thể được sinh bởi TOE. Trong trường hợp đó, sự phát sinh thành phần bảo mật FIA_SOS.2 TSF có thể được sử dụng để yêu cầu TOE đảm bảo rằng các vấn đề bảo mật sẽ tham gia tới một vài tập đã xác định.

Các vấn đề bảo mật chứa dữ liệu xác thực cung cấp bởi người dùng cho cơ chế xác thực mà được dựa trên hiểu biết chủ động của người dùng. Khi khóa mật mã được áp dụng, lớp FCS: việc trợ giúp mật mã nên được sử dụng thay cho họ này.

G.3.2 Thẩm tra các bí mật FIA_SOS.1

G.3.2.1 Chú thích cho ứng dụng người sử dụng

Các vấn đề bảo mật có thể được phát sinh bởi người dùng. Thành phần này đảm bảo rằng các vấn đề phát sinh bởi người dùng đó có thể được xác minh theo tập đặc tính nhất định.

G.3.2.2 Các hoạt động

G.3.2.2.1 Chỉ định

Trong FIA_SOS.1.1, tác giả PP/ST nên cung cấp một tập đặc tính đã xác định. Việc xác định tập đặc tính có thể đơn giản như việc miêu tả việc kiểm tra đặc tính được thực hiện, hoặc thông dụng như một tham chiếu tới chuẩn mà một quốc gia công bố để định nghĩa tập đặc tính mà các vấn đề bảo mật phải tuân theo. Ví dụ tập đặc tính có thể bao gồm một miêu tả cấu trúc bảng chữ cái của các vấn đề bảo mật được chấp nhận và/hoặc khoảng không gian mà các vấn đề bảo có thể chấp nhận phải tuân theo.

G.3.3 FIA_SOS.Tạo các bí mật TSF

G.3.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cho phép TSF phát sinh các vấn đề bảo mật cho các chức năng đặc trưng như là xác thực bằng mật khẩu.

Khi nào thì bộ phát sinh số ngẫu nhiên được sử dụng trong một thuật toán phát sinh bảo mật, nên chấp nhận nó như đầu vào là số ngẫu nhiên mà đầu ra là một kết quả hoàn toàn không thể đoán trước. Dữ liệu ngẫu nhiên này có thể nhận được từ một số tham số sẵn sàng như đồng hồ hệ thống, đăng ký hệ thống, ngày, thời gian,... Các tham số nên được chọn để đảm bảo rằng số dữ liệu duy nhất có thể được phát sinh từ đầu vào này nên là ít hơn hoặc bằng số tối thiểu vấn đề bảo mật phải được phát sinh.

G.3.3.2 Các hoạt động

G.3.3.2.1 Chỉ định

Trong FIA_SOS.2.1, tác giả PP/ST nên cung cấp một tập đặc tính đã xác định. Việc xác định tập đặc tính có thể đơn giản như miêu tả sự kiểm tra đặc tính để thực hiện hoặc thông thường như tham chiếu tới chuẩn quốc gia mà định nghĩa các tập đặc tính các vấn đề bảo mật phải tuân theo. Ví dụ tập đặc tính có thể bao gồm một miêu tả cấu trúc bảng chữ cái về các vấn đề bảo mật chấp nhận được và/hoặc không gian mà các vấn đề bảo mật chấp nhận phải tuân theo.

Trong FIA_SOS.2.2, tác giả PP/ST nên cung cấp một danh sách các chức năng TSF cho cái mà vấn đề phát sinh TSF phải được sử dụng. Ví dụ như chức năng có thể bao gồm một mật khẩu dựa trên cơ chế xác thực.

G.4 Xác thực người dùng (FIA_UAU)

G.4.1 Chú thích cho người sử dụng

Họ này định nghĩa các kiểu của cơ chế xác thực người dùng được trợ giúp bởi TSF. Họ này định nghĩa các thuộc tính yêu cầu trên cái mà cơ chế xác thực người dùng dựa vào.

G.4.2 FIA_UAU.1 Định thời cho xác thực

G.4.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu rằng tác giả PP/ST định nghĩa các hành động trung gian TSF có thể được thực thi bởi TSF thay cho người dùng trước khi định danh yêu cầu của người dùng được xác thực. Các hành động trung gian TSF không có khái niệm bảo mật với người dùng một cách sai để định danh chúng ưu tiên hơn việc xác thực. Đối với tất cả các hành động trung gian TSF không nằm trong danh sách, người dùng phải được xác thực trước khi hành động được thực thi bởi TSF thay cho người dùng.

Thành phần này không thể điều khiển mặc dù các hành động có thể thực thi trước khi thực hiện phần định danh. Điều này yêu cầu sử dụng hoặc thời gian định danh FIA_UID.1 và định danh người dùng FIA_UID.2 trước khi có bất kỳ hành động với chỉ định thích hợp.

G.4.2.2 Các hoạt động

G.4.2.2.1 Chỉ định

Trong FIA_UAU.1.1, tác giả PP/ST nên xác định danh sách các hành động trung gian TSF mà có thể thực thi bởi TSF thay cho người dùng trước khi định danh yêu cầu của người dùng được xác thực. Danh sách này có thể không rỗng. Nếu không hành động nào là thích hợp, thành phần xác thực người dùng FIA_UAU.2 trước khi có bất kỳ hành động nào nên được sử dụng để thay thế. Một ví dụ như hành động có thể bao gồm yêu cầu trợ giúp thủ tục đăng nhập.

G.4.3 FIA_UAU.2 Xác thực người dùng trước khi hành động

G.4.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu người dùng được xác thực trước khi bất kỳ hành động trung gian TSF có thể thực hiện thay cho người dùng đó.

G.4.4 FIA_UAU.3 Xác thực không thể giả mạo

G.4.4.1 Chú thích cho ứng dụng người sử dụng

Thành phần này gửi các yêu cầu cho cơ chế để cung cấp việc bảo vệ dữ liệu xác thực. Dữ liệu xác thực được chép từ người khác, hoặc bằng cách xây dựng nên được bảo vệ hoặc bị từ chối. Các cơ chế này cung cấp sự tin tưởng cái mà người dùng xác thực bởi TSF thực sự là người mà họ yêu cầu.

Thành phần này chỉ sử dụng được với cơ chế xác thực dựa trên xác thực dữ liệu mà không thể chia sẻ (ví dụ như sinh học). TSF có thể bảo vệ hoặc ngăn chặn việc chia sẻ mật khẩu bên ngoài điều khiển TSF một cách dễ dàng.

G.4.4.2 Các hoạt động

G.4.4.2.1 Phép chọn

Trong FIA_UAU.3.1, tác giả PP/ST nên xác định nơi TSF sẽ tìm thấy, ngăn chặn, hoặc bảo vệ và ngăn chặn việc giả mạo của xác thực dữ liệu.

Trong FIA_UAU.3.2, tác giả PP/ST nên xác định nơi TSF sẽ dò tìm, ngăn chặn, hoặc bảo vệ và ngăn chặn việc sao chép xác thực dữ liệu.

G.4.5 FIA_UAU.4 Các cơ chế sử dụng xác thực đơn

G.4.5.1 Chú thích cho ứng dụng người sử dụng

Thành phần này gửi các yêu cầu cho cơ chế xác thực dựa trên dữ liệu sử dụng xác thực đơn. Dữ liệu sử dụng xác thực đơn có thể là một vài thứ mà người dùng có hoặc biết chứ không phải thứ mà người dùng là nó. Ví dụ dữ liệu sử dụng xác thực đơn bao gồm sử dụng mật khẩu đơn, thời gian mã hóa, và/hoặc số ngẫu nhiên tra cứu từ bảng bảo mật.

Tác giả PP/ST có thể xác định cơ chế xác thực nào mà yêu cầu này áp dụng.

G.4.5.2 Các hoạt động

G.4.5.2.1 Chỉ định

Trong FIA_UAU.4.1, tác giả PP/ST nên xác định danh sách các cơ chế xác thực tới cái mà yêu cầu này áp dụng tới. chỉ định này có thể là "tất cả các cơ chế xác thực". Ví dụ chỉ định này có thể là "cơ chế xác thực ứng dụng tới người xác thực trên mạng ngoài".

G.4.6 FIA_UAU.5 Cơ chế đa xác thực

G.4.6.1 Chú thích cho ứng dụng người sử dụng

Sử dụng thành phần này cho phép xác định các yêu cầu cho hơn một cơ chế xác thực được sử dụng với TOE. Đối với mỗi cơ chế lọc, các yêu cầu ứng dụng phải được chọn từ FIA: Lớp định danh và xác thực được ứng dụng tới từng cơ chế. Cùng thành phần có thể được chọn nhiều lần để phản ánh các yêu cầu khác nhau cho việc sử dụng cơ chế xác thực khác nhau.

Các chức năng quản lý trong lớp FMT có thể cung cấp các khả năng duy trì cho tập các cơ chế xác thực, như là các vai trò xác định nơi việc xác thực thành công.

Cho phép người dùng nặc danh tương tác với TOE, một cơ chế xác thực "không" có thể là được hợp nhất. Sử dụng truy cập nên được giả thích rõ ràng trong các vai trò của FIA_UAU.5.2.

G.4.6.2 Các hoạt động

G.4.6.2.1 Chỉ định

Trong FIA_UAU.5.1, tác giả PP/ST nên định nghĩa cơ chế xác thực có thể dùng được. Một ví dụ danh sách có thể là: "không, cơ chế mật khẩu, sinh học (quét võng mạc), cơ chế S/key".

Trong FIA_UAU.5.2, tác giả PP/ST nên xác định các vai trò miêu tả cơ chế xác thực cung cấp việc xác thực như thế nào và mỗi cơ chế được sử dụng khi nào. Điều này có nghĩa là phải miêu tả mỗi vị trí của tập cơ chế mà có thể được sử dụng cho việc xác thực người dùng. Một ví dụ danh sách các vai trò là: "nếu người dùng có quyền sửu dụng cả hai cơ chế mật khẩu đặc biệt và một cơ chế sinh học, thành công khi cả hai thành công; đối với tất cả người dùng khác cơ chế mật khẩu sẽ được sử dụng".

Tác giả PP/ST có thể đưa ra các biên cái mà người quản trị có thẩm quyền có thể xác định các vai trò riêng biệt. Một ví dụ về vai trò là: "người dùng luôn phải được xác thực bởi phương pháp thẻ bài; người quản trị có thể định rõ việc thêm các cơ chế xác thực được sử dụng." Tác giả PP/ST không những phải chọn để xác định biên bất kỳ mà còn bỏ hoàn toàn cơ chế xác thực và vai trò của chúng cho người quản trị có thẩm quyền.

G.4.7 FIA_UAU.6 Xác thực lại

G.4.7.1 Chú thích cho ứng dụng người sử dụng

Thành phần này gửi các nhu cầu tiềm năng để xác thực lại người dùng tại thời điểm được định nghĩa. Cái này có thể bao gồm các yêu cầu người dùng đối với TSF để thực thi các hành động liên quan đến bảo mật, giống như các yêu cầu từ thực thể mà không có TSF cho việc xác thực lại (ví dụ máy chủ ứng dụng yêu cầu TSF xác thực lại máy khách mà nó phục vụ).

G.4.7.2 Các hoạt động

G.4.7.2.1 Chỉ định

Trong FIA_UAU.6.1, tác giả PP/ST nên xác định danh sách các điều kiện yêu cầu xác thực lại. Danh sách này có thể bao gồm khoảng thời gian không thao tác của một người dùng xác định, người dùng yêu cầu một sự thay đổi trong thao tác của các thuộc tính an toàn, hoặc người dùng yêu cầu TSF thực thi một vài chức năng giới hạn an toàn.

Tác giả PP/ST có thể đưa ra các biên nơi mà việc xác thực lại có thể xuất hiện và để việc xác định cho người quản trị có thẩm quyền. Một ví dụ về vai trò là: "người dùng luôn phải được xác thực lại ít nhất một lần trong ngày; người quản trị có thể chỉ rõ việc xác thực lại nên xảy ra thường xuyên hơn chứ không phải là một lần trong 10 phút".

G.4.8 FIA_UAU.7 Phản hồi xác thực có bảo vệ

G.4.8.1 Chú thích cho ứng dụng người sử dụng

Thành phần này gửi phản hồi trong tiến trình xác thực cái mà sẽ cung cấp tới người dùng. Trong một vài hệ thống phản hồi bao gồm chỉ dẫn nhiều ký tự được gõ như thế nào nhưng không chỉ ra các ký tự đó, trong hệ thống khác thậm chí thông tin này có thể là không thích hợp.

Thành phần này yêu cầu dữ liệu xác thực là không được cung cấp như là việc phản hồi tới người dùng. Trong môi trường máy trạm, nó có thể hiển thị một "ký tự thay thế" (chẳng hạn như ký tự sao) cho mỗi ký tự mật khẩu, và không phải là ký tự thực.

G.4.8.2 Các hoạt động

G.4.8.2.1 Chỉ định

Trong FIA_UAU.7.1, tác giả PP/ST nên xác định việc phản hồi liên quan tới quy trình xác thực cái mà sẽ được cung cấp tới người dùng. Ví dụ về một sự phản hồi chỉ định là "số ký tự được gõ", kiểu phản hồi khác là "cơ chế xác thực gây lỗi xác thực".

G.5 Định danh người dùng (FIA_UID)

G.5.1 Chú thích cho người sử dụng

Họ này định nghĩa các điều kiện cái mà người dùng được yêu cầu để định danh chúng trước khi thực thi bất kỳ các hành động nào khác được làm trung gian bởi TSF và yêu cầu định danh người dùng.

G.5.2 FIA_UID.1 Định thời cho định danh

G.5.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này đưa ra các yêu cầu cho người dùng để được định danh. Tác giả PP/ST có thể chỉ rõ các hành động có thể được thực thi trước khi việc định danh xảy ra.

- Nếu thời gian định danh FIA_UID.1 được sử dụng, các hành động trung gian TSF đề cập trong Thời gian định danh FIA_UID.1 cũng nên xuất hiện trong thời gian xác thực FIA_UAU.1 này.

G.5.2.2 Các hoạt động

G.5.2.2.1 Chỉ định

Trong FIA_UID.1.1, tác giả PP/ST nên xác định danh sách các hành động trung gian TSF mà có thể được thực thi bởi TSF thay cho người dùng trước khi người dùng phải định danh. Nếu không có hành động nào thích hợp, thành phần định danh người dùng FIA_UID.2 trước khi có bất kỳ hành động nào được sử dụng thay thế. Một ví dụ như một hành động có thể bao gồm yêu cầu cho trợ giúp quá trình đăng nhập.

G.5.3 FIA_UID.2 Định danh người dùng trước khi hành động

G.5.3.1 Chú thích cho ứng dụng người sử dụng

Trong thành phần này người dùng sẽ được định danh. Một người dùng không được phép bởi TSF để thực thi bất kỳ hành động nào trước khi định danh.

G.6 Liên kết chủ thể - người dùng (FIA_USB)

G.6.1 Chú thích cho người sử dụng

Một người dùng được xác thực, để sử dụng TOE, đặc biệt là hành động một đối tượng. Các thuộc tính an toàn người dùng là được liên kết với đối tượng này (toàn bộ hoặc một phần). Họ này định nghĩa các yêu cầu để tạo và duy trì sự liên kết của các thuộc tính an toàn người dùng để đối tượng thao tác trên quyền của người dùng.

G.6.2 FIA_USB.1 Liên kết chủ thể - người dùng

G.6.2.1 Chú thích cho ứng dụng người sử dụng

Câu " hành động thay cho" chứng tỏ để là một phát hành lien tiếp trong nguồn tiêu chuẩn. Muốn nói rằng một đối tượng là hành động thay cho người dùng người mà gây ra đối tượng thuộc về hoặc được hành động để thực thi một nhiệm vụ xác định.

Qua đó, khi một đối tượng được tạo ra, đối tượng đó đang hành động thay cho người dùng người mà khởi tạo việc tạo. Trong nhiều trường hợp nơi mà tình trạng giả mạo được sử dụng, đối tượng vẫn thao tác thay cho người dùng, nhưng định danh của người dùng đó là không được biết. Một chủ đề đặc biệt của đối tượng là các đối tượng đó phụ vụ nhiều người dùng (ví dụ một tiến trình tại máy chủ). Trong nhiều trường hợp người dùng tạo đối tượng này được thừa nhận để là "người sở hữu".

G.6.2.2 Các hoạt động

G.6.2.2.1 Chỉ định

Trong FIA_USB.1.1, tác giả PP/ST nên xác định danh sách các thuộc tính an toàn người dùng mà được giới hạn tới các đối tượng.

Trong FIA_USB.1.2, tác giả PP/ST nên xác định bất kỳ các vai trò mà được áp dụng lên sự liên kết khởi tạo của các thuộc tính với các đối tượng, hoặc "không".

Trong FIA_USB.1.3, tác giả PP/ST nên xác định bất kỳ các vai trò nào mà được áp dụng khi thay đổi được tạo ra để các thuộc tính an toàn người dùng liên kết với các đối tượng hành động thay cho người dùng hoặc "không".

Phụ lục H

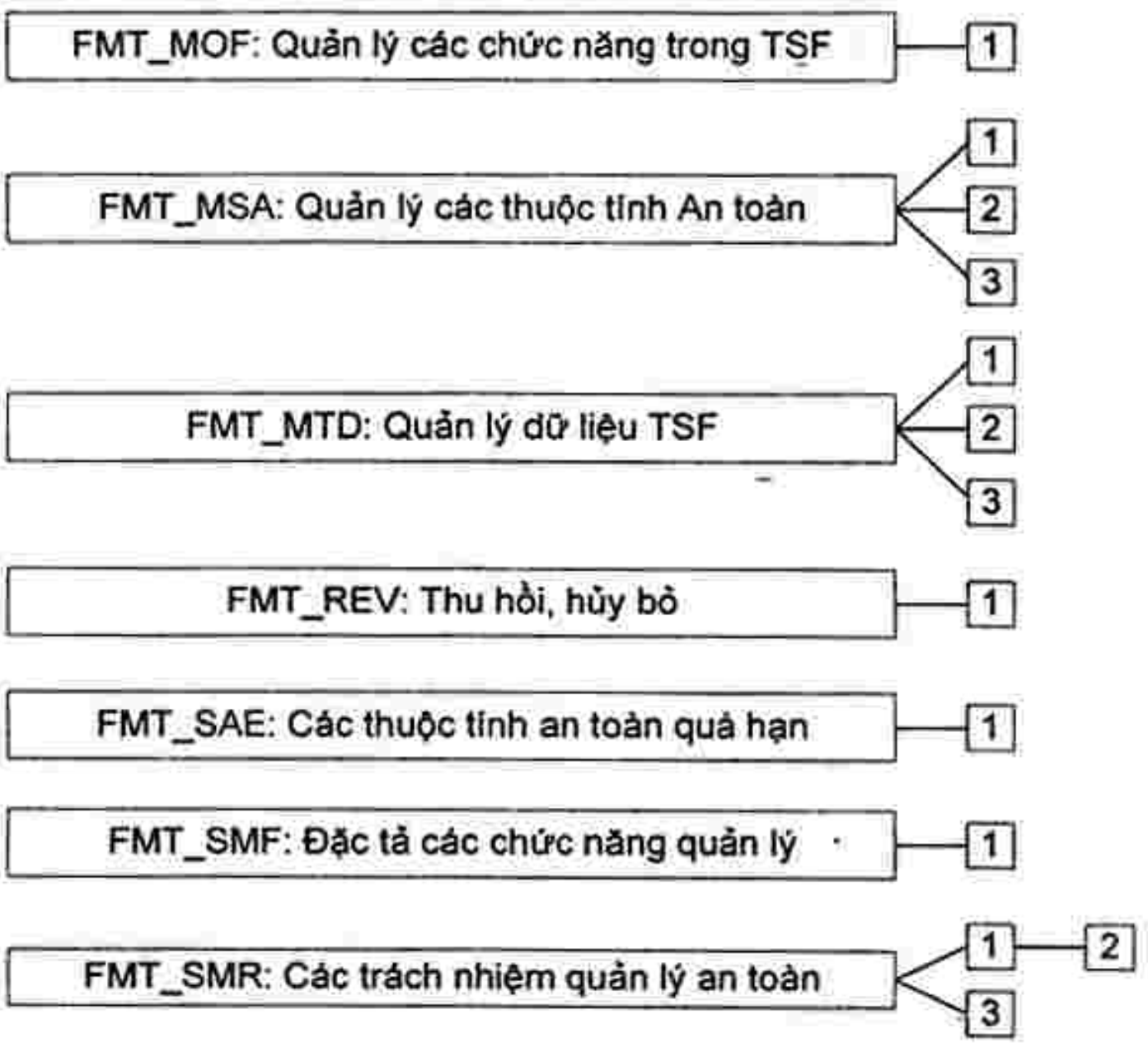
(Quy định)

Lớp FMT: Quản lý an toàn

Lớp này xác định việc quản lý một vài lĩnh vực của TSF: các thuộc tính an toàn, dữ liệu TSF và các chức năng trong TSF. Các vai trò quản lý khác nhau và sự tương tác của chúng cũng có thể được xác định, như là sự phân tách khả năng.

Trong môi trường nơi TOE được tạo ra từ nhiều phần vật lý riêng biệt mà hình thức một hệ thống phân tán, thời gian tranh luận với mối liên quan để lan truyền các thuộc tính an toàn, dữ liệu TSF, và sự thay đổi chức năng trở nên rất phức tạp, đặc biệt nếu thông tin được yêu cầu để thay thế một phần của TOE. Cái này nên được quan tâm khi lựa chọn các thành phần như sự thu hồi FMT_REV.1, hoặc quyền hạn thời gian FMT_SAE.1, nơi cơ chế là bị suy yếu.Trong trường hợp, sử dụng các thành phần từ bên trong TOE TSF bao gồm cả sựu thay thế dữ liệu (FPT_TRC) là thích hợp.

Hình H.1 chỉ ra sự phân tách của lớp này vào trong các thành phần hợp thành của nó.



Hình H.1 - Phân cấp lớp FMT: Quản lý an toàn

H.1 Quản lý các chức năng trong TSF (FMT_MOF)

H.1.1 Chú thích cho người sử dụng

Các chức năng quản lý TSF sẵn sàng với người dùng có thẩm quyền để cài đặt và điều khiển thao tác bảo mật của TOE. Các chức năng quản trị này đặc biệt là một trong số các chủ đề khác nhạu như sau:

a) Các chức năng quản lý liên quan tới điều khiển truy cập, tính toán và điều khiển xác thực bắt buộc bởi TOE. Ví dụ, định nghĩa và cập nhật các thuộc tính an toàn người dùng (ví dụ định danh duy nhất liên quan tới tên người dùng, tài khoản người dùng, tham số nhập hệ thống) hoặc định nghĩa và cập nhật kiểm toán điều khiển hệ thống (ví dụ sự lựa chọn các sự kiện kiểm toán, quản lý vết kiểm toán,

phân tích vết kiểm toán, và sinh báo cáo kiểm toán), định nghĩa và cập nhật các thuộc tính chính sách người dùng (như xóa người dùng), định nghĩa các tên điều khiển truy cập hệ thống được biết, điều khiển và quản lý nhóm người dùng.

b) Các chức năng quản lý liên quan tới tính sẵn sàng điều khiển. Ví dụ, định nghĩa và cập nhật các tham số sẵn sàng hoặc hạn nghạch nguồn tài nguyên.

c) Các chức năng quản lý mà liên quan tới sự cài đặt và cấu hình chung. Ví dụ, cấu hình TOE, khôi phục thủ công, cài đặt cố định an toàn TOE (nếu có thể), sửa và cài đặt lại phần cứng.

d) Các chức năng quản lý mà liên quan tới điều khiển công việc lặp đi lặp lại và duy trì nguồn tài nguyên TOE. Ví dụ, bật và tắt thiết bị phần cứng, lắp thiết bị lưu trữ ngoài, lưu trữ và khôi phục đối tượng.

Chú ý rằng các chức năng này cần được thể hiện trong TOE dựa trên các họ bao gồm trong PP hoặc ST. Trách nhiệm của tác giả PP/ST để đảm bảo rằng các chức năng tương ứng sẽ được cung cấp để quản lý TOE một cách an toàn.

TSF có thể chứa các chức năng mà có thể được điều khiển bởi người quản trị. Ví dụ, tắc các các chức năng kiểm toán, bật đồng bộ thời gian, và thay đổi cơ chế xác thực.

H.1.2 FMT_MOF.1 Các cơ chế hoạt động của quản lý chức năng an toàn

H.1.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cho phép các vai trò đã định danh để quản lý các chức năng an toàn của TSF. Điều này có thể thu được trạng thái hiện tại của chức năng an toàn, bật hoặc tắt chức năng an toàn, hoặc thay đổi cơ chế của chức năng an toàn. Ví dụ thay đổi cơ chế của các chức năng an toàn là thay đổi cơ chế xác thực.

H.1.2.2 Các hoạt động

H.1.2.2.1 Phép chọn

Trong FMT_MOF.1.1, tác giả PP/ST nên chọn vai trò có thể xác định cơ chế tắt hoặc ẩn và thay đổi cơ chế của các chức năng an toàn.

H.1.2.2.2 Chỉ định

Trong FMT_MOF.1.1, tác giả PP/ST nên xác định các chức năng mà có thể được thay đổi bởi các vai trò định danh. Ví dụ bao gồm kiểm toán và xác định thời gian.

Trong FMT_MOF.1.1, tác giả PP/ST nên xác định các vai trò mà được phép thay đổi các chức năng trong TSF. Các vai trò có thể được xác định trong các vai trò an toàn FMT_SMR.1.

H.2 Quản lý các thuộc tính an toàn (FMT_MSA)

H.2.1 Chú thích cho người sử dụng

Họ này định nghĩa các yêu cầu trong việc quản lý các thuộc tính an toàn.

Các thuộc tính an toàn ảnh hưởng hành vi của TSF. Các mẫu thuộc tính an toàn là một nhóm mà người dùng thuộc vào đó, vai trò mà anh ta đảm nhận, quyền ưu tiên của một quá trình (chủ thể), và các quyền thuộc về một vai trò hoặc một người dùng. Các thuộc tính an toàn này có thể cần được quản lý bởi người dùng, một chủ thể, một người dùng được cấp quyền cụ thể (người dùng với các

quyền nhất định đối với việc quản lý này) hoặc các giá trị được tiếp nhận theo một chính sách hoặc một tập hợp các qui tắc nhất định.

Lưu ý rằng quyền gán cho người dùng là thuộc tính an toàn của nó và đối tượng tiềm năng để quản lý bởi việc quản lư các thuộc tính an toàn FMT_MSA.1.

Các thuộc tính an toàn FMT_MSA.2 có thể được dùng để đảm bảo rằng bất kỳ sự kết hợp của các thuộc tính an toàn được chấp nhận là một trạng thái an toàn. Định nghĩa "đảm bảo an toàn" có nghĩa là gì, có trong hướng dẫn TOE.

Trong một vài trường hợp các đối tượng, các đối tượng hoặc tài khoản người dùng được tạo. Nếu các giá trị đưa ra là không rõ ràng cho các thuộc tính an toàn liên quan khi đó các giá trị mặc định cần được sử dụng. Quản lý các thuộc tính an toàn FMT_MSA.1 có thể được sử dụng để định rõ quản lý các giá trị mặc định này được quản lý.

H.2.2 FMT_MSA.1 Quản lý các thuộc tính an toàn

H.2.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cho phép người dùng thao tác trong các vai trò nào đó để quản lý các thuộc tính an toàn đã định danh. Người dùng được gán một vai trò trong thành phần các vai trò an toàn FMT_SMR.1.

Giá trị mặc định của tham số là giá trị tham số có được khi nó xảy ra mà không có các giá trị được gán chính xác. Một giá trị khởi tạo được cung cấp trong khi khởi tạo một tham số, và chèn giá trị mặc định.

H.2.2.2 Các hoạt động

H.2.2.2.1 Chỉ định

Trong FMT_MSA.1.1, tác giả PP/ST nên liệt kê truy cập điều khiển SFP hoặc điều khiển luồng thông tin SFP cho các thuộc tính an toàn nào được áp dụng.

H.2.2.2.2 Phép chọn

Trong FMT_MSA.1.1, tác giả PP/ST nên xác định các thao tác có thể được áp dụng tới các thuộc tính an toàn đã định danh. Tác giả PP/ST có thể xác định vai trò có thể thay đổi giá trị mặc định (thay_đổi_mặc_định), yêu cầu, thay đổi thuộc tính an toàn, xóa hoàn toàn các thuộc tính an toàn hoặc định nghĩa thao tác của chúng.

H.2.2.2.3 Chỉ định

Trong FMT_MSA.1.1, tác giả PP/ST nên xác định các thuộc tính an toàn mà có thể thao tác bởi các vai trò đã định danh. Dễ dàng cho tác giả PP/ST để xác định giá trị mặc định như là quyền truy cập mặc định có thể được quản lý. Ví dụ của các thuộc tính an toàn này là xóa người dùng, độ ưu tiên mức dịch vụ, danh sách điều khiển truy cập, quyền truy cập mặc định.

Trong FMT_MSA.1.1, tác giả PP/ST nên xác định các vai trò mà được phép thao tác trên các thuộc tính an toàn. Các vai trò có thể là được xác định trong các vai trò an toàn FMT_SMR.1

Trong FMT_MSA.1.1, nếu lựa chọn, tác giả PP/ST nên xác định các thao tác khác nào mà vai trò có thể thực thi. Ví dụ như một thao tác có thể được tạo ra.

H.2.3 FMT_MSA.2 Đảm bảo các thuộc tính an toàn

H.2.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này chứa các yêu cầu về các giá trị có thể được gán tới các thuộc tính an toàn. Các giá trị được gán như là TOE sẽ còn lại trong trạng thái an toàn.

Sự định nghĩa "đảm bảo an toàn" là gì là không có câu trả lời trong thành phần này nhưng có thể thấy trong sự phát triển của TOE và các thông tin kết quả trong hướng dẫn. Ví dụ có thể là nếu một tài khoản người dùng được tạo, nó có thể có một mật khẩu không tầm thường.

H.2.3.2 Các hoạt động

H.2.3.2.1 Chỉ định

Trong FMT_MSA.2.1, tác giả PP/ST cần chỉ rõ danh sách các thuộc tính an toàn mà yêu cầu chỉ cung cấp các giá trị đảm bảo an toàn.

H.2.4 FMT_MSA.3 Khởi tạo thuộc tính tĩnh

H.2.4.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu TSF cung cấp các giá trị mặc định cho các thuộc tính an toàn của đối tượng thích hợp, cái mà có thể được ghi đè lên bởi giá trị khởi tạo. Nó vẫn có thể cho một đối tượng mới để có các thuộc tính an toàn khác khi tạo, nếu có một cơ chế tồn tại để xác định các quyền khi tạo.

H.2.4.2 Các hoạt động

H.2.4.2.1 Chỉ định

Trong FMT_MSA.3.1, tác giả PP/ST nên liệt kê điều khiển truy cập SFP hoặc điều khiển luồng thông tin SFP cho cái mà các thuộc tính an toàn áp dụng.

H.2.4.2.2 Phép chọn

Trong FMT_MSA.3.2, tác giả PP/ST nên chọn tài sản ngầm định các thuộc tính kiểm soát truy cập sẽ bị hạn chế, cho phép hay là tài sản khác. Chỉ một trong các tùy chọn này được chọn.

H.2.4.2.3 Chỉ định

Trong FMT_MSA.3.1, nếu tác giả PP/ST chọn tài sản khác, thì tác giả PP/ST cần chỉ rõ các đặc tính của các giá trị mặc định.

Trong FMT_MSA.3.2, tác giả PP/ST nên chỉ rõ những vai trò được phép sửa đổi các giá trị của các thuộc tính an toàn. Các vai trò có thể được chỉ rõ trong các vai trò An toàn FMT_SMR.1

H.2.5 FMT_MSA Kế thừa giá trị thuộc tính an toàn

H.2.5.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu đặc tính của tập hợp các qui tắc thông qua đó thuộc tính an toàn thừa kế các giá trị và các điều kiện được đáp ứng cho các qui tắc được áp dụng.

H.2.5.2 Các hoạt động

H.2.5.2.1 Chỉ định

Trong FMT_MSA.4.1, tác giả PP/ST chỉ rõ các qui tắc điều hành giá trị mà sẽ được thừa kế bởi thuộc tính an toàn xác định, gồm các điều kiện mà có thể đáp ứng đối với các qui tắc được áp dụng. Ví dụ,

nếu một tệp mới hoặc đường dẫn được tạo (trong một hệ thống tệp đa cấp), nhãn hiệu của nó là nhãn hiệu mà tại đó người dùng đăng nhập đúng lúc nó tạo ra.

H.3 Quản lý dữ liệu TSF (FMT_MTD)

H.3.1 Chú thích cho người sử dụng

Thành phần này áp đặt các yêu cầu lên việc quản lý dữ liệu TSF. Ví dụ dữ liệu TSF là lần hiện thời và vết kiểm toán. Vì vậy, ví dụ, họ này cho phép việc xác định người nào có thể đọc, xóa, hoặc tạo vết kiểm toán.

H.3.2 FMT_MTD.1 Quản lý dữ liệu TSF

H.3.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cho phép người dùng với một vai trò nào đó để quản lý các giá trị dữ liệu TSF. Người dùng được gán tới một vai trò bên trong thành phần các vai trò an toàn FMT_SMR.1.

Giá trị mặc định của một tham số là các giá trị tham số tạo ra khi mà nó không được gán các giá trị xác định. Một giá trị khởi tạo được cung cấp trong suốt quá trình khởi tạo của tham số và ghi chèn lên giá trị mặc định.

H.3.2.2 Các hoạt động

H.3.2.2.1 Phép chọn

Trong FMT_MTD.1.1, tác giả PP/ST nên xác định các thao tác mà có thể được áp dụng tới dữ liệu TSF định danh. Tác giả PP/ST có thể xác định vai trò có thể thay đổi giá trị mặc định (thay_đổi_mặc_định), xóa, hỏi hay thay đổi dữ liệu TSF, hoặc xóa hoàn toàn dữ liệu TSF. Nếu được yêu cầu tác giả PP/ST có thể xác định bất kỳ kiểu thao tác nào. Để lọc "dữ liệu TSF sạch" có nghĩa là nội dung của dữ liệu TSF sẽ bị xóa hẳn, nhưng thực thể mà lưu trữ dữ liệu TSF thì vẫn còn trong TOE

H.3.2.2.2 Chỉ định

Trong FMT_MTD.1.1, tác giả PP/ST nên xác định dữ liệu TSF có thể được thao tác dựa trên các vai trò định danh. Dễ dàng cho tác giả PP/ST xác định giá trị mặc định có thể được quản lý.

Trong FMT_MTD.1.1, tác giả PP/ST nên xác định các vai trò mà được phép tạo trên dữ liệu TSF. Các vai trò có thể được xác định trong các vai trò an toàn FMT_SMR.1.

Trong FMT_MTD.1.1, nếu được chọn, tác giả PP/ST nên xác định vai trò có thể thực thi trên các thao tác khác nào. Ví dụ có thể là "tạo"

H.3.3 FMT_MTD.2 Quản lý hạn chế trên dữ liệu TSF

H.3.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này xác định sự hạn chế trên dữ liệu TSF, và các hành động có thể được tạo ra nếu sự hạn chế này là bị vượt quá. Thành phần này, ví dụ, sẽ cho phép sự hạn chế kích cỡ vết kiểm toán được định nghĩa, và xác định các hành động được tạo ra khi sự hạn chế này là bị vượt quá.

H.3.3.2 Các hoạt động

H.3.3.2.1 Chỉ định

Trong FMT_MTD.2.1, tác giả PP/ST nên xác định dữ liệu TSF có thể có sự hạn chế, và giá trị của sự hạn chế đó. Ví dụ như dữ liệu TSF là số người dùng đăng nhập.

Trong FMT_MTD.2.1, tác giả PP/ST nên xác định các vai trò mà được phép thay đổi sự hạn chế trên dữ liệu TSF và các hành động được thực hiện. Các vai trò có thể là được xác định trong các vai trò an toàn FMT_SMR.1.

Trong FMT_MTD.2.2, tác giả PP/ST nên xác định các hành động được thực hiện nếu hạn chế được xác định trên dữ liệu TSF xác định là bị vượt quá. Ví dụ như hành động TSF khai báo người dùng có thẩm quyền và phát sinh bản ghi kiểm toán.

H.3.4 FMT_MTD.3 Dữ liệu TSF an toàn

H.3.4.1 Chú thích cho ứng dụng người sử dụng

Thành phần này bao gồm các yêu cầu các giá trị mà có thể được gán tới dữ liệu TSF. Các giá trị được gán nên như là TOE vẫn còn trong trạng thái an toàn.

Định nghĩa "đảm bảo an toàn" có nghĩa là gì không được trả lời trong thành phần này nhưng có trong sự phát triển của TOE và thông tin kết quả trong hướng dẫn

H.3.4.2 Các hoạt động

H.3.4.2.1 Chỉ định

Trong FMT_MTD.3.1 tác giả PP/ST cần chỉ rõ dữ liệu TSF nào yêu cầu chỉ các giá trị đảm bảo an toàn được chấp nhận.

H.4 Hủy bỏ (FMT_REV)

H.4.1 Chú thích cho người sử dụng

Họ này gửi sự thu hồi các thuộc tính an toàn cho một vài thực thể bên trong TOE.

H.4.2 FMT_REV.1 Hủy bỏ

H.4.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này xác định các yêu cầu trong việc thu hồi các quyền. Nó yêu cầu việc xác định các vai trò thu hồi. Ví dụ:

Sự thu hồi sẽ chiếm không gian trên lần đăng nhập sau của người dùng;

Sự thu hồi sẽ chiếm không gian trên việc thử mở tài liệu đó trong lần sau;

Sự thu hồi sẽ chiếm không gian trong một lần cố định. Cái này có nghĩa rằng tất cả kết nối mở là được đánh giá lại trong mỗi phút.

H.4.2.2 Các thao tác

H.4.2.2.1 Phép chọn

Trong FMT_REV.1.1, tác giả PP/ST nên chỉ rõ các thuộc tính an toàn nào sắp bị thu hồi khi có thay đổi với các đối tượng, chủ thể, người dùng, các tài nguyên khác liên kết.

H.4.2.2.2 Phép chọn

Trong FMT_REV.1.1, tác giả PP/ST nên chỉ rõ khả năng thu hồi các thuộc tính an toàn từ người dùng, các chủ thể, đối tượng, hoặc bất cứ tài nguyên bổ sung nào do TSF cung cấp hay không.

H.4.2.2.3 Chỉ định

Trong FMT_REV.1.1, tác giả PP/ST nên xác định các vai trò mà được phép thay đổi các chức năng trong TSF. Các vai trò có thể được xác định trong các vai trò an toàn FMT_SMR.1.

Trong FMT_REV.1.1, nếu thêm nguồn tài nguyên được lựa chọn , tác giả PP/ST nên xác định hay không khả năng thu hồi các thuộc tính an toàn của chúng sẽ được cung cấp bởi TSF.

Trong FMT_REV.1.2, tác giả PP/ST nên xác định các vai trò thu hồi. Ví dụ các vai trò này có thể bao gồm: "ưu tiên thao tác tiếp theo trên nguồn tài nguyên liên quan" hoặc "cho tất cả việc tạo đối tượng mới"

H.5 Hết hạn thuộc tính an toàn (FMT_SAE)

H.5.1 Chú thích cho ứng dụng người sử dụng

Họ này gửi các chức năng để bắt buộc sự hạn chế thời gian cho tính hợp lệ của các thuộc tính an toàn. Họ này có thể được áp dụng để xác định các yêu cầu tới hạn cho các thuộc tính điều khiển truy cập, các thuộc tính định danh và xác thực, chứng chỉ (chứng chỉ khóa như ANSI X509 là một ví dụ), các thuộc tính kiểm toán,..

H.5.2 FMT_SAE.1 Cấp phép hạn chế thời gian

H.5.2.1 Các hoạt động

H.5.2.1.1 Chỉ định

Trong FMT_SAE.1.1, tác giả PP/ST nên cung cấp danh sách các thuộc tính an toàn cho sự tới hạn nào được trợ giúp. Ví dụ như một thuộc tính phải là khoảng an toàn của người dùng.

Trong FMT_SAE.1.1, tác giả PP/ST nên xác định các vai trò mà được phép để thay đổi các thuộc tính an toàn trong TSF. Các vai trò có thể được xác định trong các vai trò an toàn FMT_SMR.1.

Trong FMT_SAE.1.2, tác giả PP/ST nên cung cấp một danh sách các hành động để thực hiện cho mỗi thuộc tính an toàn khi nó hết hạn. Một ví dụ có thể là khoảng trống an toàn của người dùng, khi nó hết hạn, được thiết lập khoảng trống cho phép thấp nhất trên TOE. Nếu việc thu hồi ngay lập tức được yêu cầu bởi PP/ST, hành động "việc thu hồi ngay lập tức" nên được xác định.

H.6 Đặc tả các chức năng quản lý (FMT_SMF)

H.6.1 Chú thích cho người sử dụng

Họ này cho phép sự xác định các chức năng quản lý để được cung cấp bởi TOE. Mỗi chức năng quản lý an toàn không những là được liệt kê trong việc thi hành chỉ định mà còn là quản lý thuộc tính an toàn, quản lý dữ liệu TSF, hoặc quản lý chức năng an toàn.

H.6.2 FMT_SMF.1 Định rõ các chức năng quản lý

H.6.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này xác định các chức năng quản lý để được cung cấp .

Tác giả PP/ST nên đưa ra kết quả mệnh đề miêu tả "quản lý" cho các thành phần bao gồm trong PP/ST của chúng để cung cấp cơ bản cho các chức năng quản lý được liệt kê qua thành phần này.

H.6.2.2 Các hoạt động

H.6.2.2.1 Chỉ định

Trong FMT_SMF.1.1, tác giả PP/ST nên xác định các chức năng quản lý được cung cấp bởi TSF, hoặc quản lý thuộc tính an toàn, quản lý dữ liệu an toàn TSF, hoặc quản lý chức năng an toàn.

H.7 Các quy tắc quản lý an toàn (FMT_SMR)

H.7.1 Chú thích cho người sử dụng

Họ này giảm khả năng kết quả làm hỏng từ người sử dụng quyền của họ bằng cách thực thi các hành động bên ngoài sự phản hồi chức năng được gán cho họ. Nó cũng gửi đi luồng mà cơ chế không tương xứng được cung cấp để quản trị an toàn tới TSF.

Họ này yêu cầu thông tin được duy trì định danh người dùng nào có thẩm quyền để sử dụng một chức năng quản trị liên quan đến an toàn.

Một vài hành động quản lý có thể được thực thi bởi người dùng, còn lại thực hiện bởi người được Chỉ định với tổ chức. Họ này cho phép định nghĩa các vai trò khác nhau, như là quyền sở hữu, quyền biên soạn, quyền quản trị, quản lý hàng ngày.

Các vai trò này được sử dụng trong họ này là các vai trò liên quan đến an toàn. Mỗi vai trò có thể bao gồm một tập mở rộng các khả năng (vd như thư mục gốc trong UNIX), hoặc có thể là một quyền đơn lẻ (ví dụ quyền đọc một đối tượng đơn như là tài liệu tra cứu).

Họ này định nghĩa các vai trò. Các khả năng của vai trò được định nghĩa trong quản lý các chức năng trong TSF (EMT_MOF), quản lý các thuộc tính an toàn (FMT_MSA) và quản lý dữ liệu TSF (FMT_MTD).

Một vài kiểu vai trò có thể là loại trừ lẫn nhau. Ví dụ quản lý hàng ngày có thể là được định nghĩa và người dùng thao tác, nhưng không thể xóa người dùng (Cái nào là vai trò đảo ngược tới người quản trị). Lớp này sẽ cho phép các chính sách như là điều khiển 2 người được xác định.

H.7.2 FMT_SMR.1 Các quy tắc an toàn

H.7.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này xác định các vai trò khác mà TSF nên công nhận. Thông thường hệ thống lọc ra sự khác nhau giữa người quản lý thực thể, người quản trị và người dùng khác.

H.7.2.2 Các hoạt động

H.7.2.2.1 Chỉ định

Trong FMT_SMR.1.1, tác giả PP/ST nên xác định các vai trò mà được thừa nhận bởi hệ thống. Có các vai trò mà người dùng làm xuất hiện để đánh giá về an toàn. Ví dụ: quyền sở hữu, quyền soạn thảo và quyền quản trị.

H.7.3 FMT_SMR.2 Hạn chế về các vai trò an toàn

H.7.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này xác định các vai trò khác mà TSF nên thừa nhận, và các điều kiện trên các vai trò đó được quản lý như thế nào. Thông thường hệ thống lọc ra được sự khác nhau giữa người sở hữu thực thể, nhà quản trị và người dùng khác.

Các điều kiện trên các vai trò đó xác định mối liên hệ giữa các vai trò khác như là sự hạn chế trên khi vai trò có thể được thừa nhận bởi người dùng.

H.7.3.2 Các hoạt động

H.7.3.2.1 Chỉ định

Trong FMT_SMR.2.1, tác giả PP/ST nên xác định các vai trò mà được thừa nhận bởi hệ thống. Có các vai trò mà người dùng làm xuất hiện để đánh giá về vấn đề an toàn. Ví dụ: người sở hữu, nhà soạn thảo, nhà quản trị.

Trong FMT_SMR.2.3, tác giả PP/ST nên xác định các điều kiện mà ảnh hưởng chỉ định các vai trò. Ví dụ các điều kiện này là: "một tài khoản không thể có cả 2 vai trò soạn thảo và quản trị" hoặc "một người dùng liên quan tới vai trò sở hữu".

H.7.4 FMT_SMR.3 Chỉ định các vai trò

H.7.4.1 Chú thích cho ứng dụng người sử dụng

Thành phần này xác định một yêu cầu rõ ràng phải được đưa ra để thừa nhận vai trò xác định.

H.7.4.2 Các hoạt động

H.7.4.2.1 Chỉ định

Trong FMT_SMR.3.1, tác giả PP/ST nên xác định các vai trò mà yêu cầu rõ ràng là được công nhận. Ví dụ: Soạn thảo và quản trị.

Phụ lục I

(Quy định)

Lớp FPR: Riêng tư

Lớp này mô tả các yêu cầu có thể thu thập nhằm thỏa mãn các nhu cầu riêng tư của người dùng, trong khi đó vẫn cho phép hệ thống mềm dẻo như có thể được để duy trì việc kiểm soát thỏa đáng hoạt động của hệ thống.

Trong các thành phần của lớp này có sự linh hoạt về việc người dùng có thẩm quyền hay không được thể hiện bởi các chức năng an toàn cần thiết. Ví dụ, một tác giả PP/ST có thể xem xét phù hợp về việc có cần bảo vệ tính riêng tư của các người dùng đối với một người dùng có thẩm quyền phù hợp.

Lớp này cùng với các lớp khác (ví dụ các lớp liên quan đến kiểm toán, kiểm soát truy nhập, tuyến tin cậy, hoặc không chối bỏ) cung cấp độ mềm dẻo trong xác định hành vi riêng tư. Mặt khác, các yêu cầu trong lớp này có thể ẩn chứa các giới hạn về việc sử dụng các thành phần của cacs lớp khác, ví dụ như FIA: Nhận dạng và Xác thực hoặc FAU: Kiểm toán an toàn. Lấy ví dụ, nếu các người dùng có thẩm quyền không được phép xem danh tính người dùng (ví dụ Nặc danh hoặc Biệt hiệu), rõ ràng là không thể duy trì các người dùng cá nhân có trách nhiệm cho mọi hành động liên quan đến an toàn mà họ thực hiện thể hiện các nhu cầu riêng tư. Tuy nhiên, vẫn có thể đặt các yêu cầu kiểm toán trong một PP/ST, trong đó một sự kiện liên quan đến an toàn cụ thể xảy ra quan trọng hơn là biết xem ai là người chịu trách nhiệm đối với nó.

Thông tin bổ sung được cung cấp trong lưu ý ứng dụng cho lớp FAU: Kiểm toán an toàn, trong đó giải thích về định nghĩa của "Danh tính" trong ngữ cảnh kiểm toán có thể cũng là một bí danh hoặc các thông tin các có thể định danh một người dùng.

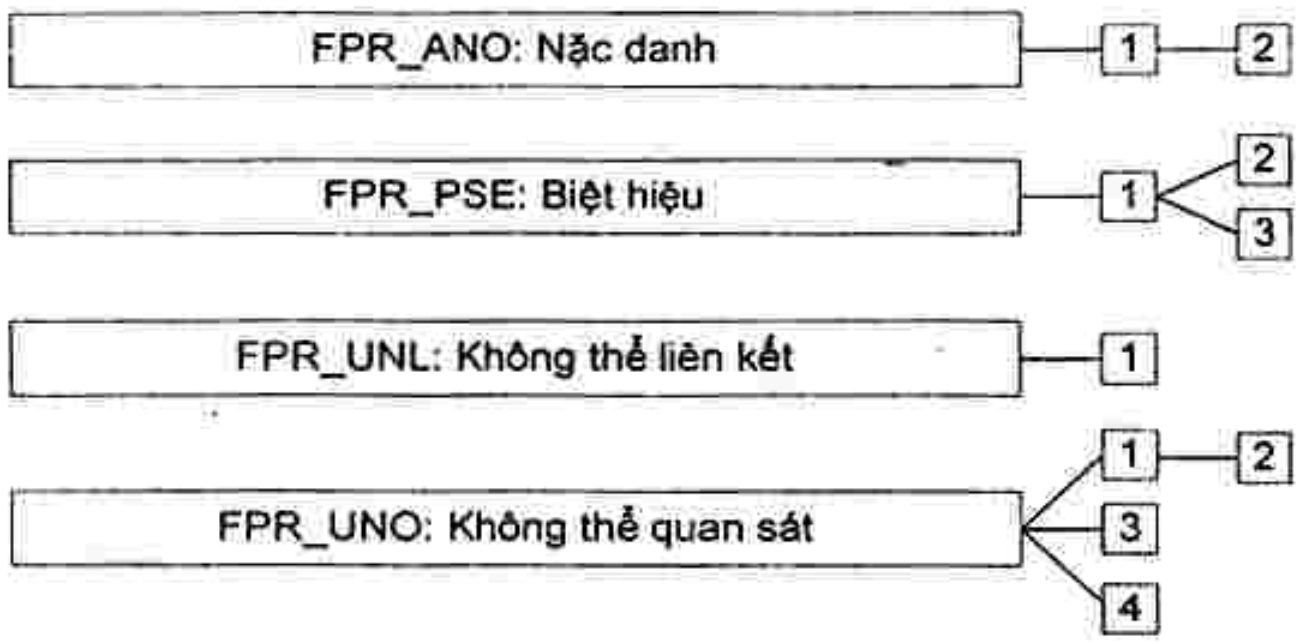
Lớp này mô tả 4 họ: Nặc danh, Biệt hiệu, Tính không thể kết nối và Tính không thể quan sát. Nặc danh, Biệt hiệu, Tính không thể kết nối có mối quan hệ liên kết phức tạp. Khi chọn một họ, sự chọn lựa nên tùy thuộc vào các mối đe dọa xác định. Đối với một số kiểu đe dọa tính riêng tư, biệt hiệu (Pseudonymity) sẽ là phù hợp hơn Nặc danh (ví dụ nếu như có yêu cầu kiểm toán). Ngoài ra, một số kiểu đe dọa tính riêng tư được ngăn chặn tốt nhất bằng tổ hợp các thành phần từ một số họ.

Tất cả các họ đều giả thiết rằng một người dùng không thực hiện rõ ràng một hành động làm lộ danh tính bản thân họ. Ví dụ, TSF không dự kiến giám sát tên người dùng trong các bản tin điện tử hoặc cơ sở dữ liệu.

Tất cả các họ trong lớp này đều có các thành phần có thể thấy được thông qua các thao tác. Các thao tác này cho phép tác giả PP/ST định rõ các người dùng/chủ thể phối hợp mà TSF phải đối mặt. Một ví dụ về thể hiện của Nặc danh có thể là: "TSF cần phải đảm bảo rằng các người dùng và/hoặc chủ thể cần không thể xác định ra danh tính người dùng trong phạm vi ứng dụng tư vấn từ xa.

Lưu ý rằng TSF nên không chỉ quy định việc bảo vệ chống lại các người dùng riêng lẻ, mà còn phải chống lại việc các người dùng phối hợp nhằm nhận được thông tin.

Hình I.1 chỉ ra sự phân tách lớp này thành những thành phần hợp thành.



Hình I.1 – Phân cấp lớp FPR: Riêng tư

I.1 Nặc danh (FPR_ANO)

I.1.1 Chú thích cho người sử dụng

Nặc danh đảm bảo rằng một chủ thể có thể sử dụng một tài nguyên hoặc dịch vụ mà không lộ danh tính người dùng nó.

Mục đích của họ này là chỉ rõ ra một người dùng hoặc chủ thể có thể thực hiện hành động mà không hé lộ danh tính người dùng cho các người dùng, chủ thể và các đối tượng khác. Họ này cung cấp cho tác giả PP/ST một phương tiện để nhận dạng tập các người dùng không có khả năng định danh ra một ai đó đang thực hiện những hành động xác định.

Do vậy, nếu một chủ thể, sử dụng nặc danh, thực hiện một hành động, một chủ thể khác sẽ không thể xác định danh tính hoặc thậm chí cả sự tham chiếu tới danh tính của người dùng đang chiếm dụng chủ thể đó. Nặc danh tập trung vào việc bảo vệ danh tính của người dùng, không tập trung vào bảo vệ danh tính chủ thể; do đó, danh tính của các chủ thể không tránh được việc bị tiết lộ.

Mặc dù danh tính của chủ thể không bị đưa ra cho các chủ thể hay người dùng khác, nhưng TSF không bị ngăn cấm rõ ràng việc lấy được danh tính người dùng. Trong trường hợp TSF không được phép biết danh tính của người dùng, FPR_ANO.2 Nặc danh không kèm thông tin yêu cầu sẽ có thể sử dụng. Trong trường hợp đó, TSF đó không cần yêu cầu thông tin người dùng.

Giải nghĩa từ "xác định" nên được xem xét theo nghĩa rộng nhất của từ..

Phân mức thành phần phân biệt giữa người dùng và người dùng có thẩm quyền. Một người dùng có thẩm quyền thường bị loại trừ khỏi thành phần, và do đó, được phép gọi danh tính của người dùng. Tuy nhiên, không có yêu cầu đặc biệt về việc người dùng có thẩm quyền phải có khả năng xác định danh tính người dùng. Đối với tính riêng tư cao nhất, các thành phần được sử dụng để chỉ rằng không có người dùng hay người dùng được cấp quyền nào có khả năng xem được danh tính của bất kì ai khi đang thực hiện một hành động nào đó.

Mặc dù một số hệ thống sẽ quy định tính nặc danh cho tất cả các dịch vụ mà nó đưa ra, các hệ thống còn lại quy định tính nặc danh cho một số các chủ thể/hoạt động. Để cung cấp khả năng linh hoạt này, một hoạt động được đưa vào khi định nghĩa phạm vi cho yêu cầu. Nếu tác giả PP/ST muốn đề cập đến tất cả các chủ thể/hoạt động, các từ "tất cả các chủ thể/hoạt động" cần được quy định.

Các ứng dụng có thể có, bao gồm khả năng tạo ra truy vấn có tính mật tới cơ sở dữ liệu công cộng, phản hồi các điều tra điện tử, hoặc thanh toán hay đóng góp mang tính nặc danh.

Các ví dụ về những người dùng hay các chủ thể thù địch tiềm ẩn là những nhà cung cấp, vận hành hệ thống, các đối tác truyền thông và những người dùng có ý lén đưa những phần mềm độc hại (vi dụ

như Trojan Horses) vào hệ thống. Tất cả những người dùng này có thể thẩm tra cách thức sử dụng (ví dụ, ai đã sử dụng dịch vụ gì) và lạm dụng thông tin này.

I.1.2 FPR_ANO.1 Nặc danh

I.1.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này đảm bảo rằng danh tính của một người dùng được bảo vệ chống bị lộ. Tuy nhiên, có thể có những trường hợp một người dùng có thẩm quyền cho trước có thể xác định ra ai đã thực hiện một số hành động nhất định nào đó. Thành phần này cho khả năng linh hoạt bắt giữ hoặc một hoặc toàn bộ chính sách riêng tư.

I.1.2.2 Các hoạt động

I.1.2.2.1 Chỉ định

Trong FPR_ANO.1.1, tác giả PP/ST nên định rõ tập các người dùng và/hoặc chủ thể mà TSF cần phải bảo vệ. Ví dụ, ngay cả khi tác giả PP/ST chỉ rõ một vai trò người dùng riêng lẻ hoặc một chủ thể, TSF phải không chỉ bảo vệ chống lại từng người dùng hoặc chủ thể đơn lẻ, mà còn phải bảo vệ trước sự phối hợp của nhiều người dùng và/hoặc chủ thể. Ví dụ, một tập các người dùng có thể tạo một nhóm người dùng và có thể hoạt động với cũng một vai trò hoặc có thể cũng sử dụng một hoặc nhiều tiến trình.

Trong FPR_ANO.1.1, tác giả PP/ST nên định danh ra danh sách các người dùng và/hoặc chủ thể và/hoặc đối tượng mà danh tính người dùng thật của chủ thể cần được bảo vệ, ví dụ "ứng dụng bỏ phiếu".

I.1.3 FPR_ANO.2 Nặc danh không có thông tin niu kéo

I.1.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này đảm bảo rằng TSF không được phép biết danh tính người dùng.

I.1.3.2 Các hoạt động

I.1.3.2.1 Chỉ định

Trong FPR_ANO.2.1, tác giả PP/ST nên định rõ tập các người dùng và/hoặc chủ thể mà TSF cần phải bảo vệ. Ví dụ, ngay cả khi tác giả PP/ST chỉ rõ một vai trò người dùng riêng lẻ hoặc một chủ thể, TSF phải không chỉ bảo vệ chống lại từng người dùng hoặc chủ thể đơn lẻ, mà còn phải bảo vệ trước sự phối hợp của nhiều người dùng và/hoặc chủ thể. Ví dụ, một tập các người dùng có thể tạo một nhóm người dùng và có thể hoạt động với cũng một vai trò hoặc có thể cũng sử dụng một hoặc nhiều tiến trình.

Trong FPR_ANO.2.1, tác giả PP/ST nên định danh ra danh sách các người dùng và/hoặc chủ thể và/hoặc đối tượng mà danh tính người dùng thật của chủ thể cần được bảo vệ, ví dụ "ứng dụng bỏ phiếu".

Trong FPR_ANO.2.2, tác giả PP/ST nên định danh ra danh sách các dịch vụ ràng buộc với yêu cầu nặc danh, ví dụ "truy nhập các thông tin về công việc".

Trong FPR_ANO.2.2, tác giả PP/ST nên định danh ra danh sách các chủ thể cần được bảo vệ danh tính người dùng thật của chủ thể cần được bảo vệ, khi các dịch vụ xác định được cung cấp.

I.2 Biệt danh (FPR_PSE)

I.2.1 Chú thích cho người sử dụng

Biệt hiệu đảm bảo rằng một người dùng có thể sử dụng một tài nguyên hoặc dịch vụ mà không lộ danh tính người dùng nó, song vẫn phải chịu trách nhiệm về việc sử dụng. Người dùng có thể chịu trách nhiệm thông qua việc liên quan trực tiếp đến một bí danh tham chiếu lưu trong TSF, hoặc qua việc cung cấp một bí danh được dùng cho các mục đích xử lý, ví dụ một số tài khoản.

Trong một vài khía cạnh, biệt hiệu giống với nặc danh. Cả biệt hiệu giống và nặc danh đều bảo vệ cho danh tính của người dùng, nhưng trong biệt hiệu mỗi tham chiếu đến danh tính người dùng được duy trì đối với trách nhiệm giải trình hoặc các mục đích khác.

Thành phần biệt hiệu FPR_PSE.1 không chỉ rõ các yêu cầu về tham chiếu tới danh tính người dùng. Đối với mục đích chỉ rõ các yêu cầu về tham chiếu này có 2 tập yêu cầu: Biệt hiệu nghịch đảo FPR_PSE.2 và Biệt hiệu bí danh FPR_PSE.3.

Một cách để sử dụng tham chiếu là khả năng nhận được danh tính người dùng nguyên gốc. Ví dụ, trong môi trường tiền điện tử, có thuận lợi là có thể dò tìm ra danh tính người dùng khi tấm séc được phát hành ra nhiều lần (tức là có gian lận). Nhìn chung, danh tính người dùng cần được gọi ra trong các điều kiện cụ thể. Tác giả PP/ST có thể muốn kết hợp biệt hiệu nghịch đảo được FPR_PSE.2 để mô tả các dịch vụ này.

Cách sử dụng khác của tham chiếu là dùng một bí danh cho mỗi người dùng. Ví dụ, người dùng nào không muốn bị nhận dạng, có thể cung cấp một tài khoản với việc tính phí sử dụng tài nguyên. Trong những trường hợp như vậy, tham chiếu đến danh tính người dùng là bí danh cho người dùng đó, còn những người dùng hay các chủ thể khác có thể sử dụng bí danh để thực thi các chức năng của họ mà không cần danh tính người dùng (ví dụ, các hoạt động thống kê về việc sử dụng hệ thống). Trong trường hợp này, tác giả PP/ST có thể mong muốn kết hợp biệt biệu bí danh FPR_PSE.3 để chỉ rõ các quy tắc mà tham chiếu phải tuân thủ theo.

Nhờ sử dụng các cấu trúc ở trên, tiền điện tử có thể được tạo ra với biệt hiệu nghịch đảo được FPR_PSE.2 chỉ rõ danh tính người dùng sẽ được bảo vệ và, nếu được chỉ ra trong điều kiện là sẽ có một yêu cầu dò tìm ra danh tính người dùng nếu tiền điện tử được lấy ra 2 lần. Khi người dùng trung thực, thì danh tính người dùng được bảo vệ, nếu người dùng tìm cách lừa đảo, thì danh tính sẽ bị truy dò ra.

Một loại khác của hệ thống có thể là một thẻ tín dụng điện tử, nơi người dùng sẽ cung cấp một biệt hiệu để chỉ báo một tài khoản từ tiền mặt có thể bị trừ. Trong những trường hợp như thế, ví dụ, FPR_PSE.3 Alias pseudonymity có thể được sử dụng. Thành phần này sẽ chỉ rõ danh tính người dùng được bảo vệ và, hơn nữa, chỉ rõ cùng một người dùng sẽ được ấn định cho các giá trị mà họ đã được cung cấp tiền (nếu được chỉ rõ trong các điều kiện).

Nên nhận biết rõ rằng, các thành phần mang tính chất nghiêm ngặt hơn không thể kết hợp với các yêu cầu khác, chẳng hạn như, nhận dạng và chứng thực hay kiểm tra. Sự giải thích về "quyết định danh tính" nên được đưa ra ở ý nghĩa rộng nhất của từ ngữ. Thông tin không được cung cấp bởi TSF trong suốt quá trình hoạt động, cũng không thể quyết định toàn bộ chủ thể hay người sở hữu của chủ thể yêu cầu hoạt động đó, TSF cũng không ghi lại thông tin, sẵn có đối với những người dùng hay các chủ thể, cái mà có thể nhận ra định danh người dùng trong tương lai.

Mục đích đó là TSF không biểu lộ bất kì thông tin nào sẽ làm hại đến danh tính người dùng, ví dụ, danh tính của các chủ thể hành động với tư cách người dùng. Thông tin được xem là nhạy cảm phụ thuộc vào sự cố gắng mà kẻ tấn công có khả năng thực hiện.

Các ứng dụng có thể có gồm những dịch vụ có thể tính cước người gọi đối với dịch vụ điện thoại mà không để lộ danh tính của họ, hoặc được tính cước đối với việc sử dụng anonymous của hệ thống thanh toán điện tử.

Ví dụ về những người dùng thù địch tiềm ẩn là những nhà cung cấp, những nhân viên vận hành hệ thống, những đối tác truyền thông và những người sử dụng, những người lén đưa những đoạn mã độc (ví dụ: Trojan Horses) vào hệ thống. Tất cả những kẻ tấn công có thể kiểm tra những gì mà người dùng đã sử dụng ở những dịch vụ đó và lạm dụng thông tin chúng lấy được. Ngoài những dịc vụ Anonymity, những dịch vụ Pseudonymity bao gồm những phương pháp cấp phép mà không cần xác minh, đặc biệt đối với thanh toán anonymous ("Tiền số"). Điều này giúp những nhà cung cấp thu phí một cách an toàn trong khi duy trì anonymity khách hàng.

I.2.2 FPR_PSE.1 Biệt danh

I.2.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này đảm bảo rằng việc định danh một người dùng được bảo vệ chống lộ. Người dùng sẽ vẫn phải chịu trách nhiệm về hành động của họ.

I.2.2.2 Các hoạt động

I.1.2.2.1 Chỉ định

Trong FPR_PSE.1.1, tác giả PP/ST nên định rõ tập các người dùng và/hoặc chủ thể mà TSF cần phải bảo vệ. Ví dụ, ngay cả khi tác giả PP/ST chỉ rõ một vai trò người dùng riêng lẻ hoặc một chủ thể, TSF phải không chỉ bảo vệ chống lại từng người dùng hoặc chủ thể đơn lẻ, mà còn phải bảo vệ trước sự phối hợp của nhiều người dùng và/hoặc chủ thể. Ví dụ, một tập các người dùng có thể tạo một nhóm người dùng và có thể hoạt động với cũng một vai trò hoặc có thể cũng sử dụng một hoặc nhiều tiến trình.

Trong FPR_PSE.1.1, tác giả PP/ST nên định danh ra danh sách các chủ thể và/hoặc hoạt động và/hoặc đối tượng mà danh tính người dùng thật của chủ thể nên được bảo vệ, ví dụ "truy nhập các thông tin về công việc".

Trong FPR_PSE.1.2, tác giả PP/ST nên định danh ra một hoặc nhiều số các bí danh mà TSF có thể cung cấp.

Trong FPR_PSE.1.2, tác giả PP/ST nên định danh ra danh sách các chủ thể mà TSF có thể cung cấp một bi danh.

I.1.2.2.2 Phép chọn

Trong FPR_PSE.1.3, tác giả PP/ST nên chỉ ra hoặc bí danh người dùng được tạo bởi TSF, hoặc cung cấp bởi người dùng. Chỉ có thể chọn một trong các tùy chọn này.

I.1.2.2.3 Chỉ định

Trong FPR_PSE.1.3, tác giả PP/ST nên định danh ra đại lượng mà bí danh do người dùng tạo ra hoặc TSF tạo ra cần được tuân thủ theo.

I.2.3 FPR_PSE.2 Biệt danh nghịch đảo

I.2.3.1 Chú thích cho ứng dụng người sử dụng

Trong thành phần này, TSF cần đảm bảo trong các điều kiện xác định, danh tính người dùng liên quan tới một tham chiếu quy định có thể được xác định.

Trong FPR_PSE.1, TSF cần phải quy định một bí danh thay vì danh tính người dùng. Khi các điều kiện đặc trưng được thỏa mãn, danh tính người dùng ứng với bí danh có thể được xác định.

I.2.3.2 Các hoạt động

I.2.3.2.1 Chỉ định

Trong FPR_PSE.2.1, tác giả PP/ST nên định rõ tập các người dùng và/hoặc chủ thể mà TSF cần phải bảo vệ. Ví dụ, ngay cả khi tác giả PP/ST chỉ rõ một vai trò người dùng riêng lẻ hoặc một chủ thể, TSF phải không chỉ bảo vệ chống lại từng người dùng hoặc chủ thể đơn lẻ, mà còn phải bảo vệ trước sự phối hợp của nhiều người dùng và/hoặc chủ thể. Ví dụ, một tập các người dùng có thể tạo một nhóm người dùng và có thể hoạt động với cũng một vai trò hoặc có thể cũng sử dụng một hoặc nhiều tiến trình.

Trong FPR_PSE.2.1, tác giả PP/ST nên định danh ra danh sách các người dùng và/hoặc chủ thể và/hoặc đối tượng mà danh tính người dùng thật của chủ thể cần được bảo vệ, ví dụ "ứng dụng bỏ phiếu".

Trong FPR_PSE.2.2, tác giả PP/ST nên định danh ra danh sách các dịch vụ ràng buộc với yêu cầu nặc danh, ví dụ "truy nhập các thông tin về công việc".

Trong FPR_PSE.2.2, tác giả PP/ST nên định danh ra danh sách các chủ thể cần được bảo vệ danh tính người dùng thật của chủ thể cần được bảo vệ, khi các dịch vụ xác định được cung cấp.

I.2.3.2.2 Phép chọn

Trong FPR_PSE.2.3, tác giả PP/ST nên chỉ ra hoặc bí danh người dùng được tạo bởi TSF, hoặc cung cấp bởi người dùng. Chỉ có thể chọn một trong các tùy chọn này.

I.2.3.2.3 Chỉ định

Trong FPR_PSE.2.3, tác giả PP/ST nên định danh ra đại lượng mà bí danh do người dùng tạo ra hoặc TSF tạo ra cần được tuân thủ theo.

I.2.3.2.4 Phép chọn

Trong FPR_PSE.2.4, tác giả PP/ST nên chỉ ra hoặc bí danh người dùng được tạo bởi TSF, hoặc cung cấp bởi người dùng. Chỉ có thể chọn một trong các tùy chọn này.

I.2.3.2.5 Chỉ định

Trong FPR_PSE.2.4, tác giả PP/ST nên định danh ra đại lượng mà bí danh do người dùng tạo ra hoặc TSF tạo ra cần được tuân thủ theo.

I.2.4 FPR_PSE.3 Biệt danh bí danh

I.2.4.1 Chú thích cho ứng dụng người sử dụng

Trong thành phần này, TSF cần đảm bảo trong các điều kiện xác định, danh tính người dùng liên quan tới một tham chiếu quy định có thể được xác định.

Nếu một người dùng muốn sử dụng các tài nguyên đĩa mà không lộ danh tính, biệt hiệu có thể dùng được. Tuy nhiên, mỗi khi người dùng truy nhập hệ thống, cần sử dụng đúng bí danh đó. Các điều kiện này có thể chỉ rõ trong thành phần này.

I.2.4.2 Các hoạt động

I.2.4.2.1 Chỉ định

Trong FPR_PSE.3.1, tác giả PP/ST nên định rõ tập các người dùng và/hoặc chủ thể mà TSF cần phải bảo vệ. Ví dụ, ngay cả khi tác giả PP/ST chỉ rõ một vai trò người dùng riêng lẻ hoặc một chủ thể, TSF phải không chỉ bảo vệ chống lại từng người dùng hoặc chủ thể đơn lẻ, mà còn phải bảo vệ trước sự phối hợp của nhiều người dùng và/hoặc chủ thể. Ví dụ, một tập các người dùng có thể tạo một nhóm người dùng và có thể hoạt động với cũng một vai trò hoặc có thể cũng sử dụng một hoặc nhiều tiến trình.

Trong FPR_PSE.3.1, tác giả PP/ST nên định danh ra danh sách các người dùng và/hoặc chủ thể và/hoặc đối tượng mà danh tính người dùng thật của chủ thể cần được bảo vệ, ví dụ "ứng dụng bỏ phiếu".

Trong FPR_PSE.3.2, tác giả PP/ST nên định danh ra danh sách các dịch vụ ràng buộc với yêu cầu nặc danh, ví dụ "truy nhập các thông tin về công việc".

Trong FPR_PSE.3.2, tác giả PP/ST nên định danh ra danh sách các chủ thể cần được bảo vệ danh tính người dùng thật của chủ thể cần được bảo vệ, khi các dịch vụ xác định được cung cấp.

I.2.4.2.2 Phép chọn

Trong FPR_PSE.3.3, tác giả PP/ST nên chỉ ra hoặc bí danh người dùng được tạo bởi TSF, hoặc cung cấp bởi người dùng. Chỉ có thể chọn một trong các tùy chọn này.

I.2.4.2.3 Chỉ định

Trong FPR_PSE.3.3, tác giả PP/ST nên định danh ra đại lượng mà bí danh do người dùng tạo ra hoặc TSF tạo ra cần được tuân thủ theo.

Trong FPR_PSE.3.4, tác giả PP/ST nên định danh ra đại lượng mà bí danh do người dùng tạo ra hoặc TSF tạo ra cần được tuân thủ theo.

I.3 Tính không thể liên kết (FPR_UNL)

I.3.1 Chú thích cho người sử dụng

Tính không thể liên kết đảm bảo rằng một người dùng có thể sử dụng các tài nguyên hoặc dịch vụ mà không có khả năng liên kết các việc sử dụng với nhau. Không thể liên kết khác với biệt hiệu ở chỗ, mặc dù ở biệt hiệu, không biết ai dùng song vẫn có mối quan hệ giữa các hành động.

Những yêu cầu đối với tính không thể liên kết được định ra để bảo vệ danh tính người dùng chống lại việc sử dụng profiling của các hoạt động. Ví dụ, khi một thẻ điện thoại thông minh được gắn một số duy nhất, thì công ty điện thoại có thể xác định hành vi của người dùng thẻ đó. Khi hồ sơ điện thoại của những người dùng được biết đến, thì thẻ có thể được liên kết với một người dùng cụ thể. Việc ẩn giấu đi mối quan hệ giữa các viện dẫn khác nhau của một dịch vụ hay một truy nhập sẽ ngăn chặn các kiểu thu thập thông tin.

Như là một kết quả, một yêu cầu cho tính không thể liên kết có thể gợi ra rằng định danh chủ thể và người dùng của một hoạt động phải được bảo vệ. Vì thế thông tin này có thể được sử dụng để liên kết tới những hoạt động với nhau.

Tính không thể liên kết yêu cầu các hoạt động khác nhau không có khả năng liên quan đến nhau. Mối quan hệ này đưa ra các dạng. Ví dụ, người dùng đã liên kết với một hoạt động, hay một đầu cuối đã

khởi đầu một hành động, hay thời gian mà hành động được thực hiện. Tác giả PP/ST có thể xác định rõ loại quan hệ nào được trình bày là phải phù hợp.

Các ứng dụng có thể có gồm khả năng tạo nhiều cách sử dụng một pseudonym mà không cần tạo ra một mẫu dùng thông thường, cái có thể làm lộ danh tính người dùng.

Ví dụ về những chủ thể và người dùng thù địch tiềm ẩn là những nhà cung cấp, những nhân viên vận hành hệ thống, những đối tác truyền thông và những người sử dụng, những người lén đưa những đoạn mã độc (ví dụ: Trojan Horses) vào hệ thống, chúng không hoạt động nhưng lại muốn nhận thông tin. Tất cả những kẻ tấn công có thể kiểm tra (ví dụ: những gì người dùng sử dụng những dịch vụ đó) và lạm dụng thông tin chúng lấy được. Unlinkability bảo vệ người dùng khỏi các nối kết được tạo ra giữa các hành động của khách hàng. Một ví dụ như một chuỗi các cuộc gọi mà các khách hàng anonymous thực hiện với các đối tác khác nhau, nơi mà sự kết hợp những danh tính của các đối tác có thể làm lộ danh tính của khách hàng đó.

I.3.2 FPR_UNL.1 Tính không thể liên kết

I.3.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này đảm bảo rằng người dùng không thể liên kết các hoạt động khác nhau trong hệ thống để lấy thông tin.

I.3.2.2 Các hoạt động

I.3.2.2.1 Chỉ định

Trong FPR_UNL.1.1, tác giả PP/ST nên định rõ tập các người dùng và/hoặc chủ thể mà TSF cần phải bảo vệ. Ví dụ, ngay cả khi tác giả PP/ST chỉ rõ một vai trò người dùng riêng lẻ hoặc một chủ thể, TSF phải không chỉ bảo vệ chống lại từng người dùng hoặc chủ thể đơn lẻ, mà còn phải bảo vệ trước sự phối hợp của nhiều người dùng và/hoặc chủ thể. Ví dụ, một tập các người dùng có thể tạo một nhóm người dùng và có thể hoạt động với cũng một vai trò hoặc có thể cũng sử dụng một hoặc nhiều tiến trình.

Trong FPR_UNL.1.1, tác giả PP/ST nên định danh ra danh sách các hoạt động liên quan đến yêu cầu không thể liên kết, ví dụ "gửi thư".

I.3.2.2.2 Phép chọn

Trong FPR_UNL.1.1, tác giả PP/ST nên chọn các mối quan hệ. Việc lựa chọn cho phép xác định danh tính người dùng hoặc chỉ định các mối quan hệ.

I.3.2.2.3 Chỉ định

Trong FPR_UNL.1.1, tác giả PP/ST nên định danh ra danh sách các quan hệ cần bảo vệ, ví dụ "cùng xuất phát từ một terminal".

I.4 Tính không thể quan sát (FPR_UNO)

I.4.1 Chú thích cho người sử dụng

Tính không thể quan sát đảm bảo rằng một người dùng có thể sử dụng các tài nguyên hoặc dịch vụ mà những người khác, đặc biệt là đối tác thứ ba, không có khả năng quan sát được các dịch vụ hoặc tài nguyên đang được dùng.

Tính không thể quan sát tiếp cận danh tính người dùng từ hướng khác so với những cách tiếp cận quen thuộc trước đó của Nặc danh, Biệt hiệu và tính không thể quan sát. Trong trường hợp này, mục

đích đó là để che giấu đi việc sử dụng tài nguyên hay dịch vụ chứ không nhằm vào việc che giấu định danh của người dùng.

Các kĩ thuật có thể được thêm vào để thực thi tính không thể quan sát. Ví dụ về các kĩ thuật đưa ra cho Tính không thể quan sát là:

a) Tính không thể quan sát ảnh hưởng đến cấp phát thông tin: Thông tin liên quan Tính không thể quan sát (ví dụ: thông tin mô tả một hoạt động đã diễn ra) có thể được định phần ở các vị trí bên trong TOE. Thông tin này có thể được định phần tới một phần được lựa chọn ngẫu nhiên khiến kẻ tấn công không biết tấn công vào phần nào của TOE. Một hệ thống luân phiên có thể phân phối thông tin đến mức không phần nào của TOE có đủ thông tin đó, nếu bị phá vỡ, tính riêng tư của người dùng sẽ bị thoả hiệp. Kĩ thuật này rõ ràng được nhắm đến trong Tính không thể quan sát ảnh hưởng đến cấp phát thông tin FPR_UNO.2.

b) Quảng bá: Khi thông tin được quảng bá (ví dụ: ethrnet, radio), những người dùng không có khả năng xác định được người thực sự nhận và sử dụng thông tin đó.

c) Sự bảo vệ bằng mật mã và chèn bản tin: Giám sát một luồng bản tin có thể thu được thông tin từ việc bản tin được chuyển đi và từ thuộc tính trên bản tin đó. Nhờ chèn lưu lượng, chèn bản tin và mã hoá luồng bản tin, sẽ bảo vệ được việc phát bản tin và thuộc tính của nó đi.

Đôi khi, người dùng không nên xem việc sử dụng một tài nguyên, nhưng một người dùng có thẩm quyền thì phải được phép xem việc sử dụng tài nguyên đó để thực hiện nhiệm vụ của của mình. Trong trường hợp đó, Tính quan sát được người dùng có thẩm quyền (FPR_UNO.4) được sử dụng, quy định khả năng cho một hoặc nhiều người dùng có quyền để quan sát việc sử dụng.

Họ này sử dụng khái niệm "các phần của TOE". Đó là bất kì phần nào của TOE, phân chia hoặc theo vật lý hoặc theo logic các phần khác của TOE. Trường hợp phân chia logic có thể liên quan đến Phân chia tên miền (FPT_SEP).

Tính không thể quan sát về truyền thông có thể là một nhân tố quan trọng trong nhiều khu vực, chẳng hạn như sự thực thi các điều trong hiến pháp, các chính sách tổ chức, hay trong các ứng dụng liên quan tới quân đội.

I.4.2 FPR_UNO.1 Tính không thể quan sát

I.4.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu rằng việc sử dụng một chức năng hoặc tài nguyên không thể bị người dùng không được phép theo dõi.

I.4.2.2 Các hoạt động

I.4.2.2.1 Chỉ định

Trong FPR_UNO.1.1, tác giả PP/ST nên định rõ tập các người dùng và/hoặc chủ thể mà TSF cần phải bảo vệ. Ví dụ, ngay cả khi tác giả PP/ST chỉ rõ một vai trò người dùng riêng lẻ hoặc một chủ thể, TSF phải không chỉ bảo vệ chống lại từng người dùng hoặc chủ thể đơn lẻ, mà còn phải bảo vệ trước sự phối hợp của nhiều người dùng và/hoặc chủ thể. Ví dụ, một tập các người dùng có thể tạo một nhóm người dùng và có thể hoạt động với cũng một vai trò hoặc có thể cũng sử dụng một hoặc nhiều tiến trình.

Trong FPR_UNO.1.1, tác giả PP/ST nên định danh ra danh sách các hoạt động liên quan đến yêu cầu không thể quan sát. Những người dùng/chủ thể khác sẽ không thể quan sát được các hoạt động trên các đối tượng trực thuộc trong danh sách xác định (ví dụ đọc / ghi đối tượng).

Trong FPR_UNO.1.1, tác giả PP/ST nên định danh ra danh sách các đối tượng được quy định trong yêu cầu không thể quan sát. Một ví dụ có thể là một mail server hoặc một ftp site xác định.

Trong FPR_UNO.1.1, tác giả PP/ST nên định ra tập các người dùng /chủ thể cần bảo vệ chống bị quan sát. Một ví dụ có thể là: "Người dùng đang truy nhập hệ thống thông qua Internet".

I.4.3 FPR_UNO.2 Tính không thể quan sát ảnh hưởng đến cấp phát thông tin

I.4.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu việc sử dụng một chức năng hoặc tài nguyên không thể quan sát được bởi những người dùng hoặc chủ thể xác định. Ngoài ra, thành phần này chỉ ra thông tin liên quan đến tính riêng tư của người dùng được phân bố trong TOE và kẻ tấn công không thể biết phần nào của TOE là mục tiêu hoặc chúng sẽ phải tấn công tới nhiều phần trong TOE.

Ví dụ về việc sử dụng thành phần này là việc sử dụng nút được cấp phát ngẫu nhiên cung cấp một chức năng. Trong trường hợp đó, thành phần đó có thể yêu cầu rằng tính riêng tư có liên quan thông tin không chỉ cần có sẵn với mỗi phần được nhận dạng của TOE, và sẽ không truyền thông được với bên ngoài phần này của TOE.

Một ví dụ phức tạp hơn được biết đến là trong các "thuật toán bỏ phiếu". Các phần của TOE sẽ được gọi trong dịch vụ đó, nhưng không phần riêng rẽ nào của TOE sẽ có thể vi phạm chính sách đó. Vì mỗi người có thể bỏ ra một phiếu (hoặc không) mà không cần TOE quyết định liệu phiếu đó đã được bỏ chưa hay chuyện gì đã xảy ra cho cái phiếu đó (trừ khi phiếu đó đã được nhất trí).

I.4.3.2 Các hoạt động

I.4.3.2.1 Chỉ định

Trong FPR_UNO.2.1, tác giả PP/ST nên định rõ tập các người dùng và/hoặc chủ thể mà TSF cần phải bảo vệ. Ví dụ, ngay cả khi tác giả PP/ST chỉ rõ một vai trò người dùng riêng lẻ hoặc một chủ thể, TSF phải không chỉ bảo vệ chống lại từng người dùng hoặc chủ thể đơn lẻ, mà còn phải bảo vệ trước sự phối hợp của nhiều người dùng và/hoặc chủ thể. Ví dụ, một tập các người dùng có thể tạo một nhóm người dùng và có thể hoạt động với cũng một vai trò hoặc có thể cũng sử dụng một hoặc nhiều tiến trình.

Trong FPR_UNO.2.1, tác giả PP/ST nên định danh ra danh sách các hoạt động liên quan đến yêu cầu không thể quan sát. Những người dùng/chủ thể khác sẽ không thể quan sát được các hoạt động trên các đối tượng trực thuộc trong danh sách xác định (ví dụ đọc / ghi đối tượng).

Trong FPR_UNO.2.1, tác giả PP/ST nên định danh ra danh sách các đối tượng được quy định trong yêu cầu không thể quan sát. Ví dụ có thể là một máy chủ thư điện tử hoặc một ftp site xác định.

Trong FPR_UNO.2.1, tác giả PP/ST nên định ra tập các người dùng /chủ thể cần bảo vệ chống bị quan sát. Một ví dụ có thể là: "Người dùng đang truy nhập hệ thống thông qua Internet".

Trong FPR_UNO.2.2, tác giả PP/ST nên nhận dạng thông tin nào có liên quan đến riêng tư nên được phân phối trong một cách thức được kiểm soát. Ví dụ những thông tin này có thể là: địa chỉ IP của chủ thể, địa chỉ IP của đối tượng, thời gian, các khoá mã hoá được sử dụng.

Trong FPR_UNO.2.2, tác giả PP/ST nên xác định rõ những điều kiện để thông tin nên gắn vào. Những điều kiện này nên được duy trì thông suốt thời gian sống của thông tin có liên quan đến tính riêng tư của mỗi trường hợp. Ví dụ những điều kiện này có thể là: "thông tin chỉ cần trình bày ở các phần riêng biệt của TOE mà không cần truyền thông ra bên ngoài phần đó của TOE.", "Thông tin chỉ cần đặt ở

từng phần cụ thể của TOE, nhưng cần được chuyển tới phần khác của TOE một cách định kì", "Thông tin cần được phân phối giữa các phần khác nhau của TOE chẳng hạn như sự thoả hiệp của 5 phần bất kì nào của TOE sẽ không thoả hiệp chính sách an toàn".

I.4.4 FPR_UNO.3 Tính không thể quan sát không có thông tin niu kéo

I.4.4.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu TSF không được thử lấy thông tin vi phạm tính không thể quan sát khi cung cấp các dịch vụ xác định. Do đó, TSF không yêu cầu (ví dụ thử lấy từ các thực thể khác) mọi thông tin có thể vi phạm tính không thể quan sát.

I.4.4.2 Các hoạt động

I.4.4.2.1 Chỉ định

Trong FPR_UNO.3.1, tác giả PP/ST nên định danh ra danh sách các dịch vụ liên quan đến yêu cầu không thể quan sát, ví dụ "truy nhập thông tin việc làm".

Trong FPR_UNO.3.1, tác giả PP/ST nên định danh ra danh sách các chủ thể mà các thông tin liên quan riêng tư cần được bảo vệ khi cung cấp các dịch vụ.

Trong FPR_UNO.3.1, tác giả PP/ST nên định ra thông tin liên quan đến riêng tư cần được bảo vệ trước các chủ thể xác định. Các ví dụ bao gồm việc nhận dạng chủ thể đã sử dụng dịch vụ và định lượng một dịch vụ đã sử dụng ví dụ như sử dụng tài nguyên bộ nhớ.

I.4.5 FPR_UNO.4 Tính quan sát được người dùng có thẩm quyền

I.4.5.1 Chú thích cho ứng dụng người sử dụng

Thành phần này dùng để yêu cầu sẽ có một hoặc nhiều người dùng có thẩm quyền có quyền xem mức sử dụng tài nguyên. Nếu không có thành phần này, việc xem lại được cho phép, song không bắt buộc.

I.4.5.2 Các hoạt động

I.4.5.2.1 Chỉ định

Trong FPR_UNO.4.1, tác giả PP/ST nên định ra tập những người dùng có phép được TSF cung cấp khả năng quan sát mức sử dụng tài nguyên. Một tập người dùng có quyền, ví dụ có thể tạo thành nhóm người dùng có quyền có thể hoạt động với cùng một vai trò hoặc có thể sử dụng cùng một hoặc nhiều tiến trình.

Trong FPR_UNO.4.1, tác giả PP/ST nên định ra tập các tài nguyên và/hoặc dịch vụ mà người dùng có thẩm quyền phải có khả năng quan sát.

Phụ lục J

(Quy định)

Lớp FPT: Bảo vệ TSF

Lớp này bao gồm các họ yêu cầu chức năng liên quan tới tính toàn vẹn và việc quản lý các cơ chế cung cấp TSF và liên quan tới tính toàn vẹn của dữ liệu TSF. Trong một số ý nghĩa, các họ trong lớp này có thể xuất hiện để sao lại các thành phần trong FDP: Lớp bảo vệ dữ liệu người sử dụng; chúng thậm chí có thể được thực thi bằng những cơ chế giống nhau. Tuy nhiên, FDP: Bảo vệ dữ liệu người sử dụng tập trung vào việc bảo vệ dữ liệu của người sử dụng, trong khi đó FPT: Bảo vệ của TSF lại tập trung vào việc bảo vệ dữ liệu TSF. Trên thực tế, các thành phần của lớp FPT: Bảo vệ của lớp TSF là cần thiết để cung cấp các yêu cầu mà người ta không thể can thiệp hoặc bỏ qua các SFP trong TOE.

Từ quan điểm của lớp này, ba phần quan trọng sau tạo nên TSF:

a) Thực thi của TSF mà tiến hành và thực hiện các cơ chế bắt buộc các SFR

b) Dữ liệu của TSF: là các cơ sở dữ liệu quản lý hướng dẫn việc thực hiện TSP.

c) Thực thể bên ngoài mà TSF có thể tương tác với để ép buộc các SFR.

Tất cả các họ trong FPT: Bảo vệ của lớp TSF có thể được liên hệ với các lĩnh vực này và thuộc về các cách phân nhóm sau:

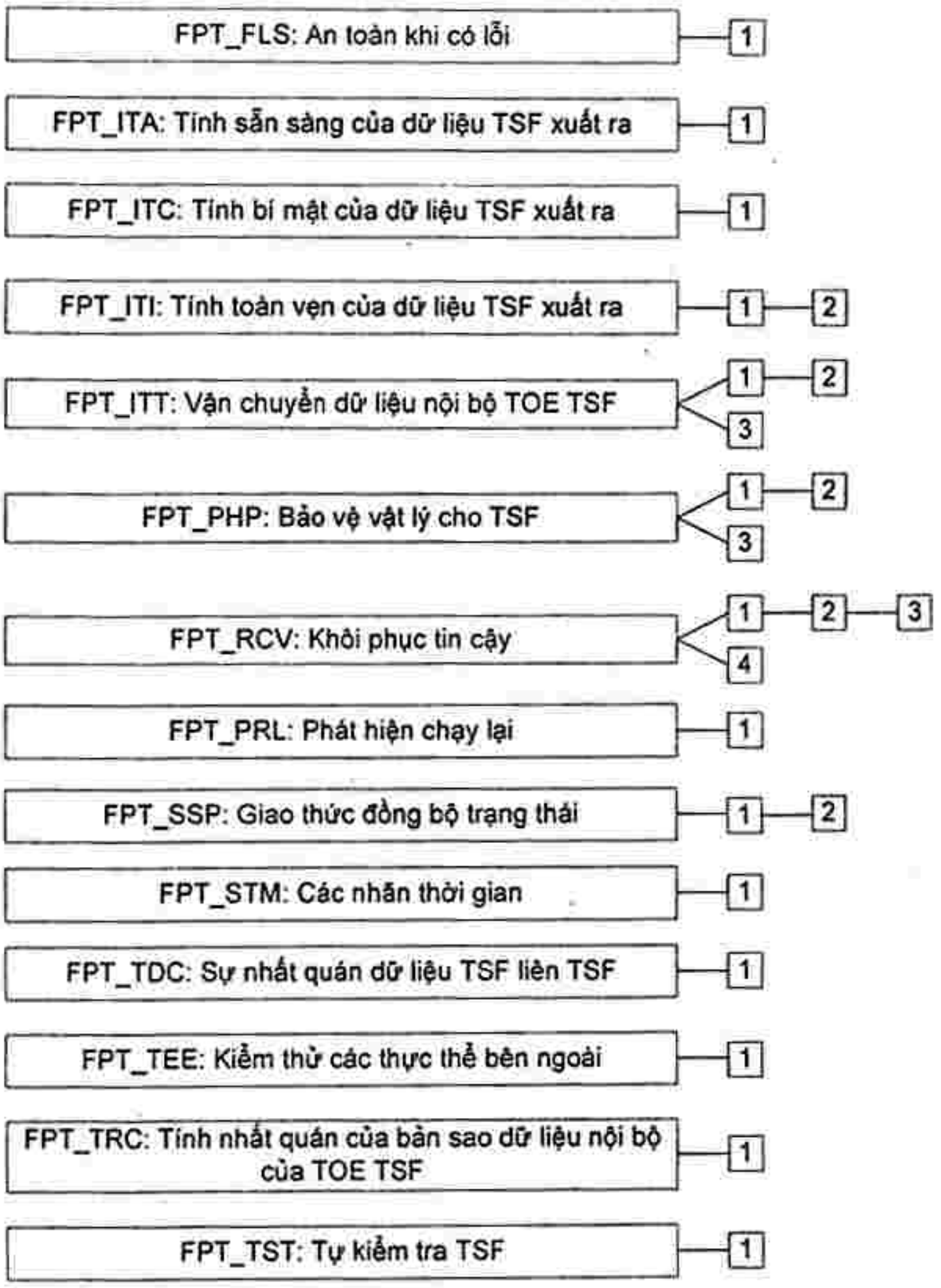
a) Bảo vệ vật lý TSF (FPT_PHP): cung cấp cho người sử dụng được ủy quyền khả năng phát hiện các cuộc tấn công từ bên ngoài vào các phần của TOE tạo nên TSF.

b) Kiểm tra các thực thể bên ngoài (FPT_TEE) và tự kiểm tra TSF (FPT_TST) cung cấp người dùng được cấp quyền với khả năng xác nhận thao tác chính xác của các thực thể bên ngoài tương tác với TSF để ép buộc các SFR, và tính toàn vẹn của dữ liệu TSF và mã thực hiện.

c) Khôi phục được tin cậy (FPT_RCV), An ninh thất bại (FPT_FLS), và tính nhất quán của bản sao dữ liệu TSF bên trong TOE (FPT_TRC): nhắm đến hành vi của TSF khi và ngay sau khi lỗi xảy ra.

d) Tính sẵn sàng của dữ liệu TSF được xuất (FPT_ITA), Tính tin cậy của dữ liệu TSF được xuất (FPT_ITC), Tính toàn vẹn của dữ liệu TSF được xuất (FPT_ITI): nhắm đến việc bảo vệ và tính sẵn sàng của dữ liệu TSF giữa TSF và một sản phẩm IT được tin cậy khác.

e) Truyền dữ liệu TSF trong nội bộ TOE (FPT_ITT): nhắm đến việc bảo vệ dữ liệu TSF khi nó được truyền đi giữa các phần phân tách nhau về mặt vật lý của TOE.



Hình J.1 - Phân cấp lớp FPT: Bảo vệ TSF

f) Phát hiện việc xem lại (FPT_RPL): nhắm đến việc xem lại nhiều loại thông tin và/hoặc thao tác.

g) Giao thức đồng bộ trạng thái (FPT_SSP): nhắm đến sự đồng bộ các trạng thái dựa vào dữ liệu TSF giữa các phần khác nhau của một TSF được phân phối.

h) Dấu thời gian (FPT_STM): nhắm đến việc định thời được tin cậy.

i) Tính nhất quán dữ liệu TSF giữa các TSF (FPT_TDC): nhắm đến sự nhất quán của dữ liệu TSF được chia sẻ giữa TSF và các sản phẩm IT được tin cậy khác.

J.1 An toàn khi có lỗi (FPT_FLS)

J.1.1 Chú thích cho người sử dụng

Các yêu cầu của họ tiêu chuẩn này đảm bảo rằng TOE sẽ không vi phạm các TSP của nó trong trường hợp có một số loại hỏng hóc tại TSF.

J.1.2 FPT_FLS.1 Lỗi với bảo toàn trạng thái an toàn

J.1.2.1 Chú thích cho ứng dụng người sử dụng

Thuật ngữ "trạng thái an toàn" nói tới một trạng thái trong đó dữ liệu TSF là nhất quán và TSF tiếp tục thực hiện đúng TSP. "Trạng thái an toàn" được định nghĩa trong mô hình TSP. Nếu người phát triển được cung cấp một định nghĩa rõ ràng về trạng thái an toàn và lý do vì sao nó nên được giữ an toàn, thì sự phụ thuộc từ FPT_FLS.1 Hỏng hóc có sự duy trì trạng thái an toàn đến ADV_SPM.1 Mô hình chính sách an ninh TOE không chính thống được bỏ qua.

Mặc dù người ta mong muốn kiểm tra các tình huống mà hỏng hóc có sự duy trì trạng thái an toàn xảy ra, điều này là không thể trong tất cả các trường hợp. Tác giả PP/ST nên xác định những tình huống mà việc kiểm tra là bắt buộc và khả thi.

Hỏng hóc trong TSF có thể bao gồm các hỏng hóc "cứng", tức là một thiết bị trục trặc cần bảo dưỡng, phục vụ hoặc sửa chữa của TSF. Hỏng hóc trong TSF cũng có thể bao gồm các hỏng hóc "mềm", chỉ yêu cầu TSF khởi tạo hoặc thiết lập lại.

J.1.2.2 Các hoạt động

J.1.2.2.1 Chỉ định

Trong FPT_FLS.1.1, tác giả PP/ST nên liệt kê các loại hỏng hóc trong TSF mà TSF có thể "mất an toàn", tức là nên duy trì một trạng thái an toàn và tiếp tục thực hiện đúng TSP.

J.2 Tính sẵn sàng xuất dữ liệu TSF (FPT_ITA)

J.2.1 Chú thích cho người sử dụng

Họ tiêu chuẩn này định nghĩa các quy tắc đối với việc ngăn ngừa mất mát tính sẵn sàng của dữ liệu TSF di chuyển giữa TSF và một sản phẩm IT được tin cậy khác. Dữ liệu này có thể là dữ liệu then chốt TSF chẳng hạn như mật khẩu, khóa, dữ liệu kiểm toán hoặc mã thực thi TSF.

Họ tiêu chuẩn này được sử dụng trong ngữ cảnh phân tán trong đó TSF đang cung cấp dữ liệu TSF cho một sản phẩm IT ở xa được tin cậy. TSF chỉ có thể thực hiện các biện pháp tại địa điểm của nó và không thể chịu trách nhiệm về TSF tại một sản phẩm IT được tin cậy nào khác.

Nếu có các đơn vị khác đo lường sự sẵn sàng cho các loại dữ liệu TSF khác nhau thì thành phần này nên được lặp lại cho mỗi cặp duy nhất của đơn vị đo lường và kiểu dữ liệu TSF.

J.2.2 FPT_ITA.1 Tính sẵn sàng liên TSF trong hệ tính sẵn sàng được định nghĩa

J.2.2.1 Các hoạt động

J.2.2.1.1 Chỉ định

Trong FPT_ITA.1.1, tác giả PP/ST nên xác định các loại dữ liệu TSF cụ thể là đối tượng của đơn vị đo lường độ sẵn sàng.

Trong FPT_ITA.1.1, tác giả PP/ST nên xác định đơn vị đo lường độ sẵn sàng đối với dữ liệu TSF khả dụng. Trong FPT_ITA.1.1, tác giả PP/ST nên xác định các điều kiện trong đó sự sẵn sàng phải được đảm bảo. Ví dụ, chúng ta cần phải có một liên kết giữa TOE và sản phẩm IT ở xa được tin cậy.

J.3 Tính bí mật của dữ liệu TSF xuất ra (FPT_ITC)

J.3.1 Chú thích cho người sử dụng

Họ tiêu chuẩn này định nghĩa các quy tắc để bảo vệ hệ thống khỏi hành động cung cấp trái phép dữ liệu di chuyển giữa TSF và một sản phẩm IT ở xa được tin cậy. Ví dụ về dữ liệu này là dữ liệu then chốt như mật khẩu, khóa, dữ liệu kiểm toán hoặc mã thực thi TSF.

Họ tiêu chuẩn này được sử dụng trong ngữ cảnh hệ thống phân tán trong đó TSF đang cung cấp dữ liệu TSF cho một sản phẩm IT được tin cậy khác. TSF chỉ có thể thực hiện các biện pháp tại địa điểm của nó và không thể chịu trách nhiệm về TSF tại một sản phẩm IT được tin cậy nào khác.

J.3.2 FPT_ITC.1 Độ tin cậy liên TSF trong quá trình truyền tải

J.3.2.1 Chú thích cho đánh giá viên

Tính tin cậy của dữ liệu TSF trong thời gian truyền là cần thiết để bảo vệ những thông tin như vậy khỏi bị lộ. Một số thực thi có khả năng cung cấp tính tin cậy bao gồm việc sử dụng các thuật toán mã hóa cũng như các kỹ thuật trải phổ.

J.4 Tính toàn vẹn của dữ liệu TSF xuất ra (FPT_ITI)

J.4.1 Chú thích cho người sử dụng

Họ tiêu chuẩn này định nghĩa các quy tắc cho việc bảo vệ dữ liệu TSF khỏi các thay đổi trái phép trong thời gian truyền giữa TSF và một sản phẩm IT ở xa được tin cậy. Ví dụ của dữ liệu loại này là dữ liệu then chốt TSF như mật khẩu, khóa, dữ liệu kiểm toán hoặc mã thực thi TSF.

Họ tiêu chuẩn này được sử dụng trong ngữ cảnh hệ thống phân tán, trong đó, TSF đang trao đổi dữ liệu TSF với một sản phẩm IT được tin cậy khác. Chú ý rằng một yêu cầu nhắm đến sự thay đổi, phát hiện hoặc khôi phục tại một sản phẩm IT ở xa được tin cậy không thể được xác định, bởi vì các cơ chế mà sản phẩm IT ở xa được tin cậy sẽ sử dụng để bảo vệ dữ liệu của nó không thể được xác định trước. Vì lý do này, những yêu cầu này được diễn tả theo nghĩa của "TSF cung cấp một khả năng" mà sản phẩm IT ở xa được tin cậy có thể sử dụng.

J.4.2 FPT_ITI.1 Phát hiện sự thay đổi liên-TSF

J.4.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này nên được sử dụng trong những tình huống trong đó người ta có khả năng phát hiện khi nào dữ liệu bị thay đổi. Một ví dụ của tình huống như vậy là khi một sản phẩm IT ở xa được tin cậy có thể yêu cầu TSF của TOE truyền lại dữ liệu khi sự thay đổi nội dung được phát hiện, hoặc đáp trả lại những kiểu yêu cầu như vậy.

Sức mạnh được kỳ vọng của việc phát hiện thay đổi nội dung được dựa vào một đơn vị xác định đo lường sự thay đổi, nó là một hàm số của thuật toán được sử dụng, từ đơn giản như sử dụng các cơ chế kiểm tra tổng yếu và kiểm tra chẵn lẻ mà không thể phát hiện được sự thay đổi nhiều bit cho tới các hướng tiếp cận kiểm tra tổng được mã hóa phức tạp hơn.

J.4.2.2 Các hoạt động

J.4.2.2.1 Chỉ định

Trong FPT_ITI.1.1, PP/ST nên xác định đơn vị xác định đo lường sự thay đổi mà cơ chế phát hiện phải thỏa mãn. Đơn vị đo lường sự thay đổi này sẽ xác định sức mạnh kỳ vọng của việc phát hiện thay đổi nội dung.

Trong FPT_ITI.1.2, PP/ST nên xác định những hành động được thực hiện nếu một sự thay đổi dữ liệu TSF được phát hiện ra. Một ví dụ về hành động như vậy là "từ chối dữ liệu TSF, và yêu cầu sản phẩm được tin cậy ban đầu gửi lại dữ liệu TSF".

J.4.3 FPT_ITI.2 Phát hiện và chỉnh sửa thay đổi liên-TSF

J.4.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này nên được sử dụng trong các tình huống trong đó việc phát hiện và khắc phục việc thay đổi dữ liệu then chốt TSF là cần thiết.

Sức mạnh kỳ vọng của việc phát hiện thay đổi nội dung dựa vào một đơn vị đo lường sự thay đổi cụ thể, nó là một hàm số của thuật toán được sử dụng, từ đơn giản như sử dụng các cơ chế kiểm tra tổng yếu và kiểm tra chẵn lẻ mà không thể phát hiện được sự thay đổi nhiều bit cho tới các hướng tiếp cận kiểm tra tổng được mã hóa phức tạp hơn. Đơn vị đo lường cần được định nghĩa có thể hoặc là tham chiếu tới các cuộc tấn công mà nó chống lại (ví dụ chỉ có 1 trong số 1000 bản tin ngẫu nhiên được chấp nhận), hoặc tham chiếu tới các cơ chế phổ biến trong các tài liệu nghiên cứu (ví dụ sức mạnh của thuật toán phải tương đương với sức mạnh của thuật toán SHA)

Hướng tiếp cận được lấy để sửa sự thay đổi thông tin phải được thực hiện thông qua một số dạng kiểm tra tổng sửa sai.

J.4.3.2 Chú thích cho đánh giá viên

Một số cách thức có thể thỏa mãn yêu cầu này liên quan tới việc sử dụng các hàm mật mã hoặc một dạng kiểm tra tổng nào đó.

J.4.3.3 Các hoạt động

J.4.3.3.1 Chỉ định

Trong FPT_ITI.2.1, PP/ST nên xác định đơn vị xác định đo lường sự thay đổi mà cơ chế phát hiện phải thỏa mãn. Đơn vị đo lường sự thay đổi này sẽ xác định sức mạnh kỳ vọng của việc phát hiện thay đổi nội dung.

Trong FPT_ITI.2.2, PP/ST nên xác định những hành động được thực hiện nếu một sự thay đổi dữ liệu TSF được phát hiện ra. Một ví dụ về hành động như vậy là "từ chối dữ liệu TSF, và yêu cầu sản phẩm được tin cậy ban đầu gửi lại dữ liệu TSF".

Trong FPT_ITI.2.3, tác giả PP/ST nên định nghĩa các kiểu thay đổi nội dung mà TSF nên có khả năng khôi phục được từ đó.

J.5 Vận chuyển dữ liệu nội bộ TOE TSF (FPT_ITT)

J.5.1 Chú thích cho người sử dụng

Họ này cung cấp các yêu cầu hướng tới việc bảo vệ dữ liệu TSF khi nó được truyền đi giữa các phần tách biệt nhau của một TOE qua một kênh truyền nội bộ.

Sự quyết định cấp độ tách biệt (vật lý hoặc logic) có thể khiến ứng dụng của họ này trở nên có ích phụ thuộc vào môi trường sử dụng được dự tính. Trong một môi trường thù địch, có thể có nhiều rủi ro từ việc truyền dữ liệu giữa các phần của TOE tách biệt nhau chỉ bởi một kênh hệ thống hoặc một kênh truyền thông giữa các tiến trình. Trong một môi trường hiền hòa hơn, các truyền thông có thể đi qua phương tiện mạng thông thường hơn.

J.5.2 Chú thích cho đánh giá viên

Một cơ chế thiết thực sẵn có cho một TSF để cung cấp việc bảo vệ này là dựa vào mật mã.

J.5.3 FPT_ITT.1 Bảo vệ vận chuyển dữ liệu nội bộ TSF cơ bản

J.5.3.1 Các hoạt động

J.5.3.1.1 Phép chọn

Trong FPT_ITT.1.1, tác giả PP/ST nên xác định kiểu bảo vệ kỳ vọng được cung cấp từ các lựa chọn: lộ thông tin, thay đổi nội dung.

J.5.4 FPT_ITT.2 Phân chia vận chuyển dữ liệu TSF

J.5.4.1 Chú thích cho ứng dụng người sử dụng

Một trong những cách để đạt được sự phân tách dữ liệu TSF dựa vào các thuộc tính có liên quan SFP là thông qua việc sử dụng các kênh truyền logic hoặc vật lý.

J.5.4.2 Các hoạt động

J.5.4.2.1 Phép chọn

Trong FPT_ITT.2.1, tác giả PP/ST nên xác định kiểu bảo vệ kỳ vọng được cung cấp từ các lựa chọn: lộ thông tin, thay đổi nội dung.

J.5.5 FPT_ITT.3 Giám sát tính toàn vẹn dữ liệu TSF

J.5.5.1 Các hoạt động

J.5.5.1.1 Phép chọn

Trong FPT_ITT.3.1, tác giả PP/ST nên xác định kiểu sửa đổi mong muốn mà TSF cần phải có khả năng phát hiện. Tác giả PP/ST nên chọn từ tập sau: sửa đổi dữ liệu, thay thế dữ liệu, sắp xếp lại dữ liệu, xóa dữ liệu, hoặc bất kỹ lỗi toàn vẹn nào.

J.5.5.1.2 Chỉ định

Trong FPT_ITT.3.1, nếu tác giả PP/ST chọn phương án sau trong đoạn trước thì tác giả cũng nên xác định các lỗi toàn vẹn khác mà TSF nên có khả năng phát hiện.

Trong FPT_ITT.3.2, tác giả PP/ST nên xác định hành động được thực hiện khi một lỗi toàn vẹn được xác định.

J.6 Bảo vệ vật lý TSF (FPT_PHP)

J.6.1 Chú thích cho người sử dụng

Các thành phần bảo vệ vật lý TSF tham chiếu tới các giới hạn về truy nhập không được phép tới TSF và tới sự ngăn chặn và chống trả lại thay đổi vật lý không được phép hoặc thay thế của TSF.

Các yêu cầu trong họ này đảm bảo rằng TSF được bảo vệ khỏi sự xáo trộng và can thiệp vật lý. Thỏa mãn các yêu cầu này tạo ra TSF được đóng gói và được sử dụng theo cách thức mà sự xáo trộn được phát hiện, hoặc sự chống trả xáo trộn vật lý được đo lường dựa vào các hệ số làm việc đã được định nghĩa. Nếu không có các thành phần này, các hàm phát hiện của một TSF sẽ đánh mất tính hiệu quả của chúng trong những môi trường mà ở đó hỏng hóc vật lý không thể ngăn chặn được. Thành phần

này cũng cung cấp các yêu cầu liên qua tới cách thức TSF phải đáp trả những nỗ lực làm xáo trộn vật lý.

Ví dụ về các kịch bản xáo trộn vật lý bao gồm tấn công cơ học, bức xạ, thay đổi nhiệt độ.

Có thể chấp nhận để các chức năng sẵn sàng cho người sử dụng được cho phép để phát hiện sự xáo trộn vật lý chỉ sẵn sàng ở chế độ không kết nối hoặc bảo trì. Việc kiểm soát nên ở đúng vị trí để giới hạn truy nhập đối với người sử dụng được cho phép trong những chế độ như vậy. Bởi vì TSF có thể không thao tác trong các chế độ đó, việc cung cấp sự ràng buộc đơn giản đối với truy nhập của người sử dụng được cho phép có thể là không thực hiện được. Thực thi vật lý của TOE có thể bao gồm nhiều cấu trúc: ví dụ một vỏ bọc bên ngoài, thẻ, chip nhớ. Toàn bộ tập hợp các "thành phần" này phải bảo vệ (bảo vệ, nhắc nhở và chống lại) TSF khỏi sự xáo trộn vật lý. Điều này không có nghĩa là tất cả các thiết bị phải cung cấp những đặc trưng này, nhưng toàn bộ cấu trúc vậy lý hoàn chỉnh này nên làm được điều đó.

Mặc dù chỉ có tối thiểu công việc kiểm tra liên quan tới các thành phần này, nó lại là toàn bộ bởi vì một khả năng lớn các cơ chế phát hiện và cảnh báo có thể được thực thi một cách hoàn chỉnh trong phần cứng, bên dưới mức tương tác với một hệ thống con kiểm tra (ví dụ một hệ thống phát hiện bằng phần cứng dựa vào việc làm ngắt mạch và bật sáng một đi-ốt phát quang nếu mạch bị ngắt khi một nút được bấm bởi người sử dụng được cho phép). Tuy nhiên, một tác giả PP/ST có thể các định rằng đối với một môi trường nguy cơ được dự báo cụ thể, việc kiểm tra sự xáo trộn vật lý là cần thiết. Nếu đúng trường hợp này, tác giả PP/ST nên bao gồm các yêu cầu phù hợp trong danh sách các sự kiện cần kiểm tra. Chú ý rằng bao gồm trong các yêu cầu này có thể tiềm ẩn các hệ quả đối với thiết kế phần cứng và giao diện của nó đối với phần mềm.

J.6.2 FPT_PHP.1 Phát hiện thụ động các tấn công vật lý

J.6.2.1 Chú thích cho ứng dụng người sử dụng

FPT_PHP.1 Phát hiện thụ động các tấn công vật lý nên được sử dụng khi các mối đe dọa từ hành động xáo trộn không được phép các thành phần của TOE không được trái với các phương thức mang tính thủ tục. Nó nhắm tới các nguy cơ của các xáo trộn vật lý với TSF không phát hiện được. Điển hình là một người sử dụng được cho phép có thể được cung cấp chức năng xác minh liệu có sự xáo trộn nào đã xảy ra không. Như đã viết, thành phần này đơn giản là cung cấp một khả năng TSF để phát hiện hành động xáo trộn. Đặc tả của các chức năng quản lý trong FMT_MOF.1 Quản lý các chức năng bảo mật nên được cân nhắc để xác định ai có thể sử dụng khả năng đó và bằng cách nào họ có thể sử dụng khả năng đó. Nếu điều này được thực hiện bởi các cơ chế không phải IT (ví dụ kiểm tra vật lý) thì các chức năng quản lý là không bắt buộc.

J.6.3 FPT_PHP.2 Thông báo tấn công vật lý

J.6.3.1 Chú thích cho ứng dụng người sử dụng

FPT_PHP.2 Báo cáo tấn công vật lý nên được sử dụng khi các mối đe dọa từ hành động xáo trộn không được phép các thành phần của TOE không được trái với các phương thức mang tính thủ tục và người ta yêu cầu rằng các cá nhân được Chỉ định được thông báo về hành động xáo trộn vật lý. Nó nhắm tới nguy cơ mà hành động xáo trộn vật lý với các thành phần TSF mặc dù được phát hiện ra nhưng có thể không được chú ý.

J.6.3.2 Các hoạt động

J.6.3.2.1 Chỉ định

Trong FPT_PHP.2.3, tác giả PP/ST nên cung cấp một danh sách các thiết bị / thành phần TSF mà việc phát hiện tích cực các hành động xáo trộn vật lý là bắt buộc.

Trong FPT_PHP.2.3, tác giả PP/ST nên Chỉ định một người sử dụng hoặc một vai trò để nhận báo cáo khi hành động xáo trộn được phát hiện. Kiểu người sử dụng hoặc vai trò có thể đa dạng tùy thuộc vào thành phần quản trị bảo mật cụ thể (từ họ hành vi FMT_MOF.1 Quản lý các chức năng bảo mật) được bao gồm trong PP/ST.

J.6.4 FPT_PHP.3 Chống tấn công vật lý

J.6.4.1 Chú thích cho ứng dụng người sử dụng

Từ một số dạng xáo trộn, việc TSF không chỉ phát hiện ra hành động xáo trộn mà còn thực sự chống lại nó hoặc trì hoãn kẻ tấn công là cần thiết.

Thành phần này nên được sử dụng các thiết bị TSF và các thành phần TSF được kỳ vọng để thao tác trong môi trường mà hành động xáo trộn vật lý (vi dụ quan sát, phân tích hoặc thay đổi) các bộ phận nội tại của một thiết bị TSF hoặc bản thân thành phần đó là một nguy cơ.

J.6.4.2 Các hoạt động

J.6.4.2.1 Chỉ định

Trong FPT_PHP.3.1, tác giả PP/ST nên xác định các kịch bản xáo trộn đối với một danh sách các thiết bị / thành phần TSF mà TSF nên chống trả lại hành động xáo trộn vật lý. Danh sách này có thể được áp dụng cho một tập con đã được định nghĩa các thiết bị và các thành phần vật lý TSF dựa vào các cân nhắc như giới hạn công nghệ và sự phơi bày vật lý tương đối của thiết bị. Tập con như vậy nên được định nghĩa rõ ràng và được hiệu chỉnh. Hơn thế nữa, TSF nên tự động đáp trả lại hành động xáo trộn vật lý. Sự đáp trả tự động nên theo cách mà chính sách của thiết bị được bảo toàn; vi dụ, với một chính sách giữ bí mật, việc vô hiệu hóa về mặt vật lý của thiết bị sao cho thông tin được bảo vệ sẽ không bị lấy đi là chấp nhận được.

Trong FPT_PHP.3.1, tác giả PP/ST nên xác định danh sách các thiết bị / thành phần TSF mà TSF nên bảo vệ chống lại hành động xáo trộn vật lý trong các kịch bản được xác định trước.

J.7 Khôi phục tin cậy (FPT_RCV)

J.7.1 Chú thích cho người sử dụng

Các yêu cầu trong họ này đảm bảo TSF có thể xác định rằng TOE được khởi động mà không bị vô hiệu hóa chức năng bảo vệ và có thể khôi phục mà không bị vô hiệu hóa chức năng bảo vệ sau khi bị gián đoạn thao tác. Họ này là quan trọng bởi vì trạng thái khởi động của TSF xác định việc bảo vệ của các trạng thái sau đó.

Các thành phần khôi phục tạo dựng lại các trạng thái an toàn TSF, hoặc ngăn ngừa sự chuyển sang các trạng thái không an toàn, như là một phản ứng trực tiếp khi gặp các hỏng hóc, gián đoạn thao tác trong dự kiến hoặc khi khởi động. Các hỏng hóc phải được lường trước bao gồm:

a) Tình trạng không thao tác của các hành động không che được mà luôn gây ra đổ vỡ của hệ thống (vi dụ sự thiếu nhất quán của các bảng hệ thống then chốt, các chuyển giao không được kiểm soát

trong nội bộ mã TSF được gây ra bởi các hỏng hóc chớp nhoáng của phần cứng hoặc phần dẻo, hỏng hóc nguồn, hỏng hóc bộ vi xử lý, hỏng hóc về truyền thông).

b) Các hỏng hóc về phương tiện truyền thông gây ra một phần hoặc tất cả các phương tiện truyền thông đại diện cho các đối tượng TSF làm cho chúng trở nên không thể truy nhập được hoặc bị sai lệch (ví dụ: lỗi kiểm tra chẵn lẻ, hỏng đầu đọc ổ đĩa, lỗi đọc/ghi do đầu đọc ổ đĩa bị lệch, lớp phủ từ bị bong, bụi trên bề mặt ổ đĩa)

c) Sự gián đoạn thao tác gây ra bởi hành động quản lý sai lầm hoặc thiếu hành động quản lý đúng lúc (ví dụ: tắt hệ thống không đúng cách bằng việc tắt nguồn, bỏ qua sự khan hiếm các tài nguyên then chốt, cấu hình được cài đặt không phù hợp)

Chú ý rằng việc khôi phục có thể bắt đầu một kịch bản hỏng hóc toàn bộ hoặc một phần. Mặc dù một hỏng hóc toàn bộ có thể xảy ra trong một hệ điều hành đơn nhưng điều này ít có khả năng xảy ra trong một môi trường phân tán. Trong những môi trường như vậy, các hệ thống con có thể bị hỏng nhưng các phần còn lại vẫn thao tác. Hơn nữa, các thành phần then chốt có thể có dự phòng (ổ đĩa, kênh truyền) và có thể có các điểm kiểm tra. Do đó, việc khôi phục được diễn tả theo ý nghĩa là khôi phục về một trạng thái an toàn.

Có các tương tác khác nhau giữa Khôi phục được tin cậy (FPT_RCV) và các thành phần Tự kiểm tra TSF (FPT_TST) được cân nhắc khi lựa chọn Khôi phục được tin cậy (FPT_RCV):

a) Nhu cầu cho việc khôi phục được tin cậy có thể được chỉ ra trong các kết quả của việc tự kiểm tra TSF trong đó các kết quả của các phép tự kiểm tra cho biết rằng TSF đang ở trong một trạng thái không an toàn và trở lại một trạng thái an toàn hoặc yêu cầu vào chế độ bảo dưỡng.

b) Một hỏng hóc, như được trình bày ở trên có thể được xác định bởi nhà quản trị. Hoặc là nhà quản trị thực hiện hành động để đưa TOE trở lại một trạng thái an toàn và sau đó kích hoạt các phép tự kiểm tra để khẳng định rằng đã đạt được trạng thái an toàn. Hoặc, các phép tự kiểm tra có thể được kích hoạt để hoàn chỉnh quá trình khôi phục.

c) Một sự kết hợp của các mục a. và b. ở trên, trong đó nhu cầu đối với việc khôi phục được tin cậy được chỉ ra thông qua kết quả của việc tự kiểm tra TSF, nhà quản trị thực hiện các hành động để đưa TOE trở lại một trạng thái an toàn và sau đó kích hoạt các phép tự kiểm tra để khẳng định rằng đã đạt được trạng thái an toàn.

d) Các phép tự kiểm tra phát hiện một hỏng hóc hoặc sự gián đoạn dịch vụ, sau đó hoặc là khôi phục tự động hoặc đưa vào chế độ bảo dưỡng.

Họ này xác định một chế độ bảo dưỡng. Trong chế độ bảo dưỡng, hành động bình thường có thể không thực hiện được hoặc bị cấm ngặt, bằng không thì các trạng thái không an toàn có thể xảy ra. Trong các tình huống điển hình, chỉ có người sử dụng được cho phép mới nên được cho phép để truy nhập vào chế độ này nhưng các chi tiết thực sự về ai có thể truy nhật vào chế độ này là một chức năng của FMT: Bảo mật và quản lý. Nếu FMT: Bảo mật và quản lý không kiểm soát được ai có thể truy nhập vào chế độ này thì có thể cho phép bất kỳ người sử dụng này khôi phục hệ thống nếu TOE bắt đầu một trạng thái như vậy. Tuy nhiên, trong thực tế, cũng có thể không mong chờ việc người sử dụng khôi phục hệ thống có cơ hội để cấu hình TOE theo cách gây vị phạm các SFR.

Các cơ chế được thiết kế để phát hiện các điều kiện ngoại lệ trong thời gian thao tác đều nằm trong Tự kiểm tra TSF (FPT_TST), Lỗi bảo mật (FPT_FLS), và các lĩnh vực khác mà nhắm tới khái nhiệm

"An toàn phần mềm". Có một khả năng lớn là việc sử dụng các họ này sẽ được yêu cầu để hỗ trợ việc ban hành Khôi phục được tin cậy (FPT_RCV). Điều này là để đảm bảo rằng TOE sẽ không thể phát hiện ra khi nào cần phải khôi phục.

Trong toàn bộ họ này, cụm từ "trạng thái an toàn" được sử dụng. Nó ám chỉ một trạng thái này đó mà TOE có dữ liệu TSF nhất quán và một TSF có thể thi hành chính sách một cách đúng đắn. Trạng thái này có thể là phần "khởi đầu" cho một hệ thống sạch, hoặc nó có thể là một trạng thái được kiểm tra nào đó.

Tiếp theo việc khôi phục, cần khẳng định rằng trạng thái an toàn đã đạt được thông qua việc tự kiểm tra của TSF. Tuy nhiên, nếu việc khôi phục được thực hiện theo cách mà chỉ có một trạng thái an toàn đạt được còn không thi việc khôi phục bị hỏng thi sự phụ thuộc vào thành phần tự kiểm tra TSF FPT_TST.1 Kiểm tra TSF có thể không còn cần thiết.

J.7.2 FPT_RCV.1 Khôi phục thủ công

J.7.2.1 Chú thích cho ứng dụng người sử dụng

Trong phân cấp của họ yêu cầu khôi phục được tin cậy, việc khôi phục chỉ yêu cầu sự can thiệp thủ công là ít được mong đợi nhất, bởi vì nó ngăn việc sử dụng hệ thống theo cách thức tự động. Thành phần này được dự định để sử dụng trong các TOE mà không yêu cầu việc khôi phục tự động về một trạng thái an toàn. Các yêu cầu của thành phần này làm giảm nguy cơ vô hiệu hóa chức năng bảo vệ là kết quả từ việc TOE được thực hiện có giám sát trả về một trạng thái an toàn sau khi khôi phục từ một hỏng hóc hoặc sự gián đoạn nào khác.

J.7.2.2 Chú thích cho đánh giá viên

Các chức năng sẵn có cho người sử dụng được phép đối với việc khôi phục được tin cậy chỉ có trong chế độ bảo dưỡng là chấp nhận được. Việc giám sát nên được đưa vào nhằm giới hạn truy nhập trong khi bảo dưỡng cho người sử dụng được cho phép.

J.7.2.3 Các hoạt động

J.7.2.3.1 Chỉ định

Trong FPT_RCV.1.1, tác giả PP/ST nên xác định danh sách các hỏng hóc hoặc các gián đoạn (ví dụ hỏng nguồn, cạn kiệt lưu trữ kiểm tra, hoặc bất kỳ hỏng hóc hoặc gián đoạn nào) theo sau việc TOE bắt đầu chế độ bảo dưỡng.

J.7.3 FPT_RCV.2 Khôi phục tự động

J.7.3.1 Chú thích cho ứng dụng người sử dụng

Việc khôi phục tự động được cân coi là hữu ích hơn so với khôi phục thủ công bởi vì nó cho phép máy móc thao tác theo cách thức giảm bớt sự chú ý của con người.

Thành phần FPT_RCV.2 Khôi phục tự động mở rộng phạm vi bao quát tính năng của FPT_RCV.1 Khôi phục thủ công bằng cách yêu cầu rằng cần có tối thiểu một cách thức tự động khôi phục từ hỏng hóc hoặc gián đoạn dịch vụ. Nó nhằm tới nguy cơ vô hiệu hóa chức năng bảo vệ bắt nguồn từ một TOE tự động trả về một trạng thái không an toàn sau khi khôi phục từ một hỏng hóc hoặc một sự gián đoạn nào khác.

J.7.3.2 Chú thích cho đánh giá viên

Các chức năng sẵn có cho người sử dụng được phép đối với việc khôi phục được tin cậy chỉ có trong chế độ bảo dưỡng là chấp nhận được. Việc giám sát nên được đưa vào nhằm giới hạn truy nhập trong khi bảo dưỡng cho người sử dụng được cho phép.

Đối với FPT_RCV.2.1, trách nhiệm của nhà phát triển TSF là xác định tập hợp các hỏng hóc có thể khôi phục được và các gián đoạn về dịch vụ. Giả định rằng sức mạnh của các cơ chế khôi phục tự động sẽ được xác minh.

J.7.3.3 Các hoạt động

J.7.3.3.1 Chỉ định

Trong FPT_RCV.2.1, tác giả PP/ST nên xác định danh sách các hỏng hóc hoặc gián đoạn dịch vụ (ví dụ hỏng nguồn, cạn kiệt lưu trữ kiểm tra, hoặc bất kỳ hỏng hóc hoặc gián đoạn nào) theo sau việc TOE bắt đầu chế độ bảo dưỡng.

Trong FPT_RCV.2.2, tác giả PP/ST nên xác định danh sách các hỏng hóc hoặc các gián đoạn khác để buộc thực hiện chức năng khôi phục tự động.

J.7.4 FPT_RCV.3 Khôi phục tự động tránh tổn thất lớn

J.7.4.1 Chú thích cho ứng dụng người sử dụng

Khôi phục tự động được xem là có ích hơn khôi phục thủ công nhưng lại có rủi ro về việc đánh mất một số lượng đáng kể các đối tượng. Việc ngăn ngừa sự mất mát không đáng các đối tượng cung cấp thêm tiện ích cho nỗ lực khôi phục.

Thành phần FPT_RCV.3 Khôi phục tự động mà không bị mất mát không đáng mở rộng phạm vi bao quát tính năng của FPT_RCV.2 Khôi phục tự động bằng cách yêu cầu không có mất mát không đáng của dữ liệu hoặc đối tượng TSF trong TSC. Tại FPT_RCV.2 Khôi phục tự động, các cơ chế khôi phục tự động có thể khôi phục một cách được tin cậy bằng cách xóa bỏ tất cả các đối tượng và trả về cho TSF một trạng thái an toàn. Kiểu khôi phục tự động này được ngăn ngừa trong FPT_RCV.3 Khôi phục tự động mà không bị mất mát không đáng.

Thành phần này nhằm tới nguy cơ vô hiệu hóa chức năng bảo vệ là kết quả từ một TOE tự động trả về một trạng thái không an toàn sau khi khôi phục từ một hỏng hóc hoặc sự gián đoạn khác với sự mất mát lớn về dữ liệu TSF hoặc đối tượng dưới sự kiểm soát của TSF.

J.7.4.2 Chú thích cho đánh giá viên

Các chức năng sẵn có cho người sử dụng được phép đối với việc khôi phục được tin cậy chỉ có trong chế độ bảo dưỡng là chấp nhận được. Việc giám sát nên được đưa vào nhằm giới hạn truy nhập trong khi bảo dưỡng cho người sử dụng được cho phép.

Giả định rằng đánh giá viên sẽ xác minh sức mạnh của các cơ chế khôi phục tự động.

J.7.4.3 Các hoạt động

J.7.4.3.1 Chỉ định

Trong FPT_RCV.3.1, tác giả PP/ST nên xác định danh sách các hỏng hóc hoặc gián đoạn dịch vụ (ví dụ hỏng nguồn, cạn kiệt lưu trữ kiểm tra) theo sau việc TOE bắt đầu chế độ bảo dưỡng.

Trong FPT_RCV.3.2, tác giả PP/ST nên xác định danh sách các hỏng hóc hoặc các gián đoạn khác mà việc khôi phục tự động là phải thực hiện được.

In FPT_RCV.3.3, tác giả PP/ST nên cung cấp một định lượng về mức độ chấp nhận được mất mát dữ liệu hoặc đối tượng TSF.

J.7.5 FPT_RCV.4 Khôi phục chức năng

J.7.5.1 Chú thích cho ứng dụng người sử dụng

Việc khôi phục chức năng yêu cầu rằng nếu như có hỏng hóc trong TSF thì một số SF xác định trong TSF nên hoặc là hoàn thành một cách thành công hoặc là khôi phục về một trạng thái an toàn.

J.7.5.2 Các hoạt động

J.7.5.2.1 Chỉ định

Trong FPT_RCV.4.1, tác giả PP/ST nên xác định danh sách các SF và các kịch bản hỏng hóc. Khi gặp sự kiện một trong các kịch bản đã xác định xảy ra, những SF đã được xác định phải hoặc là hoàn thành một cách thành công hoặc là khôi phục về trạng thái an toàn và chắc chắn.

J.8 Phát hiện chạy lại (FPT_RPL)

J.8.1 Chú thích cho người sử dụng

Họ này nhắm tới việc phát hiện xem lại đối với các loại thực thể khác nhau và các hành động tương ứng để sửa chữa.

J.8.2 FPT_RPL.1 Phát hiện chạy lại

J.8.2.1 Chú thích cho ứng dụng người sử dụng

Các thực thể bao gồm ở đây là, ví dụ, thông điệp, yêu cầu dịch vụ, phản hồi dịch vụ hoặc phiên.

J.8.2.1.1 Chỉ định

Trong FPT_RPL.1.1, tác giả PP/ST nên cung cấp một danh sách các thực thể đã được xác định mà việc phát hiện replay là có thể thực hiện được. Ví dụ về các thực thể như vậy bao gồm: thông điệp, yêu cầu dịch vụ, phản hồi dịch vụ và phiên người sử dụng.

J.8.2.2 Các hoạt động

J.8.2.2.1 Chỉ định

Trong FPT_RPL.1.1, tác giả PP/ST nên cung cấp một danh sách các thực thể đã được xác định mà việc phát hiện replay là có thể thực hiện được. Ví dụ về các thực thể như vậy bao gồm: thông điệp, yêu cầu dịch vụ, phản hồi dịch vụ và phiên người sử dụng.

Trong FPT_RPL.1.2, tác giả PP/ST nên xác định một danh sách các hành động có thể thực hiện bởi TSF khi việc xem lại bị phát hiện. Tập hợp tiềm năng các hành động có thể thực hiện bao gồm: từ chối thực thể được xem lại, yêu cầu khẳng định thực thể từ nguồn được xác định, và ngắt đối tượng mà thực thể được xem lại bắt nguồn từ đó.

J.9 Giao thức đồng bộ trạng thái (FPT_SSP)

J.9.1 Chú thích cho người sử dụng

Các hệ thống phân tán có thể làm tăng độ phức tạp hơn là các hệ thống tập trung thông qua tiềm năng đối với các khác biệt trong trạng thái giữa các thành phần của hệ thống, và thông qua trễ truyền thông. Trong hầu hết các trường hợp, sự đồng bộ trạng thái giữa các chức năng phân tán liên quan tới một giao thức trao đổi, chứ không phải một hành động đơn giản. Khi có ác ý tồn tại trong môi trường phân tán của các giao thức này, cần phải có các giao thức có khả năng tự vệ phức tạp hơn.

Giao thức đồng bộ trạng thái (FPT_SSP) thiết đặt yêu cầu cho các chức năng bảo mật then chốt của TSF để sử dụng một giao thức được tin cậy. Giao thức đồng bộ trạng thái (FPT_SSP) đảm bảo rằng hai phần phân tán của TOE (ví dụ như hai máy tính) có các trạng thái của chúng được đồng bộ nhau sau một hành động liên quan tới bảo mật.

Một số trạng thái có thể không bao giờ được đồng bộ hoặc chi phí giao dịch có thể quá cao trong sử dụng thực tế; việc thu hồi một khóa mật mã là một ví dụ, trong đó việc biết được trạng thái sau hành động thu hồi được khởi phát có thể không bao giờ được biết tới. Hoặc là hành động được thực hiện và sự xác nhận không thể gửi đi được, hoặc là thông điệp bị từ chối bởi đối tác truyền thông thù địch và việc thu hồi không bao giờ xảy ra. Tính không xác định là duy nhất đối với các hệ thống phân tán. Tính không xác định và sự đồng bộ trạng thái là có liên quan, và một giải pháp như nhau có thể áp dụng. Sẽ là vô ích nếu thiết kế cho các trạng thái không xác định; tác giả PP/ST nên diễn tả các yêu cầu khác trong những tình huống như vậy (ví dụ phát báo động, kiểm soát sự kiện).

J.9.2 FPT_SSP.1 Xác nhận tin cậy một chiều (đơn)

J.9.2.1 Chú thích cho ứng dụng người sử dụng

Trong thành phần này, TSF phải cung cấp một xác nhận cho một phần khác của TSF khi được yêu cầu. Việc xác nhận này nên chỉ rõ rằng một phần của TOE phân tán đã nhận thành công một sự chuyển giao không bị thay đổi từ một phần khác của TOE phân tán.

J.9.3 FPT_SSP.2 Xác nhận tin cậy hai chiều

J.9.3.1 Chú thích cho ứng dụng người sử dụng

Trong thành phần này, ngoài TSF có khả năng cung cấp một xác nhận về việc nhận được dữ liệu truyền, TSF phải tuân theo yêu cầu từ một phần khác của TSF về một xác nhận dành cho xác nhận đã nhận được.

Ví dụ, TSF tại chỗ truyền đi một số dữ liệu tới một phần ở xa của TSF. Phần ở xa của TSF xác nhận việc nhận dữ liệu thành công và yêu cầu rằng TSF gửi phải khẳng định là nhận được xác nhận đó. Cơ chế này cung cấp thêm sự tin tưởng rằng cả hai phần của TSF liên quan tới việc truyền dữ liệu biết được rằng việc truyền đã hoàn thành thành công.

J.10 Nhãn thời gian (FPT_STM)

J.10.1 Chú thích cho người sử dụng

Họ này nhắm tới các yêu cầu đối với một chức năng dấu thời gian nằm trong một TOE. Nhiệm vụ của tác giả PP/ST là làm rõ ý nghĩa của cụ từ "dấu thời gian tin cậy được" và xác định trách nhiệm trong việc xác định sự chấp nhận tin cậy.

J.10.2 FPT_STM.1 Thẻ thời gian tin cậy

J.10.2.1 Chú thích cho ứng dụng người sử dụng

Một số khả năng sử dụng của thành phần này bao gồm việc cung cấp dấu thời gian cho các mục đích kiểm soát cũng như cho việc kết thúc thuộc tính bảo mật.

J.11 Tính nhất quán dữ liệu liên-TSF (FPT_TDC)

J.11.1 Chú thích cho người sử dụng

Trong một môi trường phân tán hoặc hệ thống ghép, một TOE có thể cần trao đổi dữ liệu TSF (ví dụ các thuộc tính SFP liên kết với dữ liệu, thông tin kiểm soát, thông tin định danh) với sản phẩm IT được tin cậy khác. Họ này định nghĩa các yêu cầu đối với việc chia sẻ và thông dịch nhất quán các thuộc tính giữa TSF của TOE và các thuộc tính của một sản phẩm IT được tin cậy khác.

Các thành phần trong họ này được dự định để cung cấp các yêu cầu đối với sự hỗ trợ tự động cho sự nhất quán dữ liệu TSF khi dữ liệu như vậy được truyền đi giữa TSF của TOE và sản phẩm IT được tin cậy khác. Cũng có thể các điều kiện hoàn toàn thủ tục có thể được sử dụng để tạo ra tính nhất quán thuộc tính bảo mật, nhưng chúng không được cung cấp ở đây.

Họ này khác với FDP_ETC và FDP_ITC, vì hai họ này chỉ liên quan tới việc giải quyết các thuộc tính bảo mật giữa TSF và các phương tiện xuất/nhập của nó. Nếu tính toàn vẹ của dữ liệu TSF được xét tới, các yêu cầu nên được chọn từ họ Tính toàn vẹn của dữ liệu TSF được xuất (FPT_ITI). Các thành phần này xác định các yêu cầu đối với TSF để có thể phát hiện hoặc phát hiện và sửa các thay đổi đối với dữ liệu TSF khi chuyển qua.

J.11.2 FPT_TDC.1 Tính nhất quán dữ liệu TSF cơ bản liên-TSF

J.11.2.1 Chú thích cho ứng dụng người sử dụng

TSF chịu trách nhiệm duy trì tính nhất quán của dữ liệu TSF được sử dụng bởi hoặc được liên kết với chức năng cụ thể và các chức năng chung cho hai hoặc nhiều hệ thống được tin cậy. Để dữ liệu TSF được sử dụng hợp lý (ví dụ để tạo cho dữ liệu người sử dụng có cùng mức độ bảo vệ như ở bên trong TOE) bằng cách nhận sản phẩm IT được tin cậy, TOE và sản phẩm IT được tin cậy khác phải sử dụng một giao thức được thiết lập trước để trao đổi dữ liệu TSF.

J.11.2.2 Các hoạt động

J.11.2.2.1 Chỉ định

Trong FPT_TDC.1.1, tác giả PP/ST nên định nghĩa danh sách các kiểu dữ liệu TSF mà TSF sẽ cung cấp khả năng thông dịch một cách nhất quán khi được chia sẻ giữa TSF và sản phẩm IT được tin cậy khác.

Trong FPT_TDC.1.2, tác giả PP/ST nên Chỉ định danh sách các quy tắc thông dịch sẽ được áp dụng bởi TSF.

J.12 Kiểm thử các thực thể bên ngoài (FPT_TEE)

J.12.1 Chú thích cho người sử dụng

Họ này định nghĩa các yêu cầu việc kiểm thử một hoặc hơn nữa các thực thể bên ngoài do TSF thực hiện. Các thực thể bên ngoài này không phải là người dùng, và chúng có thể gồm liên hợp của phần mềm và/hoặc phần cứng tương tác với TOE.

Mẫu kiểu kiểm thử có thể là:

a) Các kiểm thử đối với sự xuất hiện của tường lửa, và có thể xem việc cấu hình đã đúng chưa.

b) Các kiểm thử một số tài sản của hệ điều hành mà một TOE chạy trên đó.

c) Kiểm thử một số tài sản của IC mà một OS TOE thẻ thông minh chạy trên đó (có nghĩa máy phát số ngẫu nhiên)

Lưu ý rằng thực thể bên ngoài này có thể "nói dối" về kết quả kiểm thử, hoặc là có mục đích hoặc là do làm việc không đúng.

Các kiểm thử này có thể thực hiện hoặc là chỉ trong một số trạng thái bảo trì, lúc khởi động, đang trực tuyến, hoặc là liên tục. Các thao tác do TOE thực hiện bởi vì kết quả kiểm thử cũng được định nghĩa trong họ này.

J.12.2 Các Chú thích cho đánh giá viên

Các kiểm thử thực thể bên ngoài có thể đủ để kiểm thử tất cả các đặc tính của chúng mà TSF tin cậy.

J.12.3 FPT_TEE.1 Kiểm thử thực thể bên ngoài

J.12.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này không dự định để áp dụng cho người dùng là con người.

Thành phần này hỗ trợ cho việc kiểm thử theo định kỳ các tài sản liên quan các thực thể bên ngoài mà thao tác của TSF dựa vào, bằng việc yêu cầu khả năng gọi chức năng kiểm thử định kỳ.

Tác giả PP/ST có thể lọc các yêu cầu để chỉ rõ chức năng cần sẵn sàng ở chế độ on-line, off-line hay là bảo dưỡng hay không.

J.12.3.2 Các Chú thích cho đánh giá viên

Các chức năng kiểm thử định kỳ sẵn sàng chỉ trong một chế độ off-line hoặc bảo dưỡng là chấp nhận được. Trong khi bảo dưỡng, các kiểm soát cần sẵn sàng để giới hạn người dùng được cấp quyền truy cập vào.

J.12.3.3 Các hoạt động

J12.3.3.1 Phép chọn

Trong FPT_TEE 1.1, tác giả PP/ST cần ghi rõ khi nào TSF sẽ chạy kiểm thử thực thể bên ngoài, trong lúc đầu khởi động, định kỳ trong thao tác thông thường, khi một người dùng được cấp quyền yêu cầu, và trong các điều kiện khác. Nếu các kiểm thử chạy thường xuyên, thì người dùng đầu cuối có thể tin hơn rằng TOE đang vận hành chính xác hơn là nếu các kiểm thử chạy ít thường xuyên. Tuy nhiên, cần tin rằng TOE đang vận hành chính xác phải cân bằng với ảnh hưởng tiềm năng đối với khản năng của TOE, cũng như mọi lần, tự kiểm thử có thể làm chậm thao tác thông thường của TOE.

J.12.3.3.2 Chỉ định

Trong FPT_TEE.1.1, tác giả PP/ST cần ghi rõ các tài sản của các thực thể bên ngoài do các kiểm thử kiểm tra. Các ví dụ về tài sản này có thể gồm cấu hình hoặc tài sản sẵn sàng của máy chủ thư mục hỗ trợ một số phần kiểm soát truy cập của TSF.

Trong FPT_TEE.1.1, tác giả PP/ST cần, nếu chọn các điều kiện khác, chỉ rõ tần số mà tự kiểm thử sẽ chạy. Một ví dụ của điều kiện và tần số khác này có thể sẽ chạy kiểm thử mỗi lần người dùng yêu cầu bắt đầu một phiên với TOE. Ví dụ, có thể là trường hợp kiểm thử một máy chủ thư mục trước khi nó tương tác với TSF trong quá trình xác thực người dùng.

Trong FPT_TEE.1.2, tác giả PP/ST cần chỉ rõ thao tác nào TSF sẽ thực thi khi kiểm thử không thực hiện được. Ví dụ về các thao tác này, được minh họa bởi ví dụ máy chủ thư mục, có thể bao gồm cả việc kết nối tới một máy chủ dự phòng đang sẵn sàng hoặc mặt khác cả việc tìm máy chủ sao lưu.

J.13 Tính nhất quán bản sao dữ liệu bên trong TOE TSF (FPT_TRC)

J.13.1 Chú thích cho người sử dụng

Các yêu cầu của họ này là cần thiết để đảm bảo tính nhất quán của dữ liệu TSF khi dữ liệu này được sao chép ở bên trong TOE. Dữ liệu như vậy có thể trở thành không nhất quán nếu một kênh nội bộ giữa các phần của TOE trở nên không thao tác. Nếu TOE được cấu trúc nội bộ như một mạng của các phần của TOE, điều này có thể xảy ra khi các phần bị vô hiệu hóa, các liên kết mạng bị đứt, v.v.

Cách thức đảm bảo tính nhất quán không được xác định trong thành phần này. Nó có thể đạt được thông qua một dạng của ghi nhớ giao dịch (trong đó các giao dịch thích hợp được truy lục lại cho một trạm khi kết nối lại); nó có thể cập nhật dữ liệu được sao lưu thông qua một giao thức đồng bộ. Nếu một giao thức cụ thể là cần thiết cho một PP/ST, nó có thể được xác định thông qua sự sàng lọc.

Cũng có khả năng không thể đồng bộ được một số trạng thái, hoặc chi phí cho việc đồng bộ như vậy là quá cao. Ví dụ của tình huống như vậy là việc thu hồi kênh truyền thông và khóa mật mã. Các trạng thái trung gian có thể xảy ra, nếu một hành vi cụ thể được mong đợi, nó nên được xác định thông qua sự sàng lọc.

J.13.2 FPT_TRC.1 Tính nhất quán bên trong TSF

J.13.2.1 Các hoạt động

J.13.2.1.1 Chỉ định

Trong FPT_TRC.1.2, tác giả PP/ST nên xác định danh sách các SF phụ thuộc vào tính nhất quán của bản sao dữ liệu TSF.

J.14 Tự kiểm tra TSF (FPT_TST)

J.14.1 Chú thích cho người sử dụng

Họ này định nghĩa các yêu cầu đối với phép tự kiểm tra của TSF tương ứng với một số thao tác chính xác được kỳ vọng. Ví dụ là các giao diện cho các chức năng bắt buộc thực hiện và các thao tác số học mẫu trên các phần then chốt của TOE. Các phép thử này có thể được thực hiện khi khởi động, định kỳ, theo yêu cầu của người sử dụng được cho phép, hoặc khi các điều kiện khác được thỏa mãn. Các hành động được thực hiện bởi TOE là kết quả của phép tự kiểm tra được định nghĩa trong họ khác. Các yêu cầu của họ này cũng là cần thiết để phát hiện sự hư hại của mã thực thi TSF (ví dụ phần mềm TSF) và dữ liệu TSF gây bởi nhiều hỏng hóc khác nhau và không nhất thiết gây ra việc dừng thao tác của TOE (mà có thể được quản lý bởi một họ khác). Các phép kiểm tra này phải được thực hiện bởi vì những hỏng hóc này có thể không được ngăn ngừa một cách cần thiết. Những hỏng hóc như vậy có thể xảy ra hoặc là bởi vì các chế độ hỏng hóc chưa biết trước hoặc sơ suất trong thiết kế

phần cứng, phần dẻo hoặc phần mềm hoặc bởi vì sự hư hại mang tính phá hoại đối với TSF do bảo vệ logic hoặc vật lý không phù hợp.

Thêm vào đó, việc sử dụng thành phần này, với các điều kiện thích hợp, có thể giúp ngăn ngừa các thay đổi TSF không thích hợp hoặc mang tính phá hoại được áp dụng vào TOE thao tác là kết quả của các thao tác bảo dưỡng.

Thuật ngữ "thao tác chính xác của TSF" trước tiên ám chỉ tới thao tác của phần mềm TSF và tính toàn vẹn của dữ liệu TSF. Cỗ máy trừu tượng mà phần mềm TSF được thực thi theo đó được kiểm tra thông qua sự phụ thuộc vào Kiểm tra cỗ máy trừu tượng bên dưới (FPT_AMT).

J.14.2 FPT_TST.1 Kiểm tra TSF

J.14.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cung cấp hỗ trợ cho việc kiểm tra các chức năng then chốt của thao tác TSF bằng cách yêu cầu khả năng kích hoạt các chức năng kiểm tra và kiểm tra tính toàn vẹn của dữ liệu và mã thực thi TSF.

J.14.2.2 Chú thích cho đánh giá viên

Có thể chấp nhận các chức năng dành cho người sử dụng được phép đối với việc kiểm tra định kỳ chỉ dành cho chế độ không kết nối hoặc bảo dưỡng. Các kiểm soát nên ở vị trí để hạn chế truy nhập trong các chế độ này đối với người sử dụng được cho phép.

J.14.2.3 Các hoạt động

J.14.2.3.1 Phép chọn

Trong FPT_TST.1.1, tác giả PP/ST nên xác định khi nào TSF sẽ thực thi phép kiểm tra TSF; trong thời gian khởi động, định kỳ trong thời gian thao tác bình thường, khi nhận được yêu cầu của một người sử dụng được cho phép, khi gặp các điều kiện khác. Đối với trường hợp sau, tác giả PP/ST cũng nên Chỉ định những điều kiện đó là gì thông qua các Chỉ định sau.

Trong FPT_TST.1.1, tác giả PP/ST nên xác định liệu các phép tự kiểm tra có được thực hiện hay không để chứng minh thao tác chính xác của toàn bộ TSF hoặc chỉ một số phần xác định của TSF.

J.14.2.3.2 Chỉ định

Trong FPT_TST.1.1, tác giả PP/ST nên xác định các điều kiện mà phép tự kiểm tra nên xảy ra.

Trong FPT_TST.1.1, tác giả PP/ST nên, nếu được lựa chọn, xác định danh sách các phần của TSF sẽ là chủ thể để tự kiểm tra.

J.14.2.3.3 Phép chọn

Trong FPT_TST.1.2, tác giả PP/ST nên xác định liệu tính toàn vẹn dữ liệu có được xác minh đối với tất cả dữ liệu TSF không hay là chỉ với dữ liệu được lựa chọn.

J.14.2.3.4 Chỉ định

Trong FPT_TST.1.2, tác giả PP/ST nên, nếu được lựa chọn, xác định danh sách dữ liệu TSF sẽ được xác minh tính toàn vẹn.

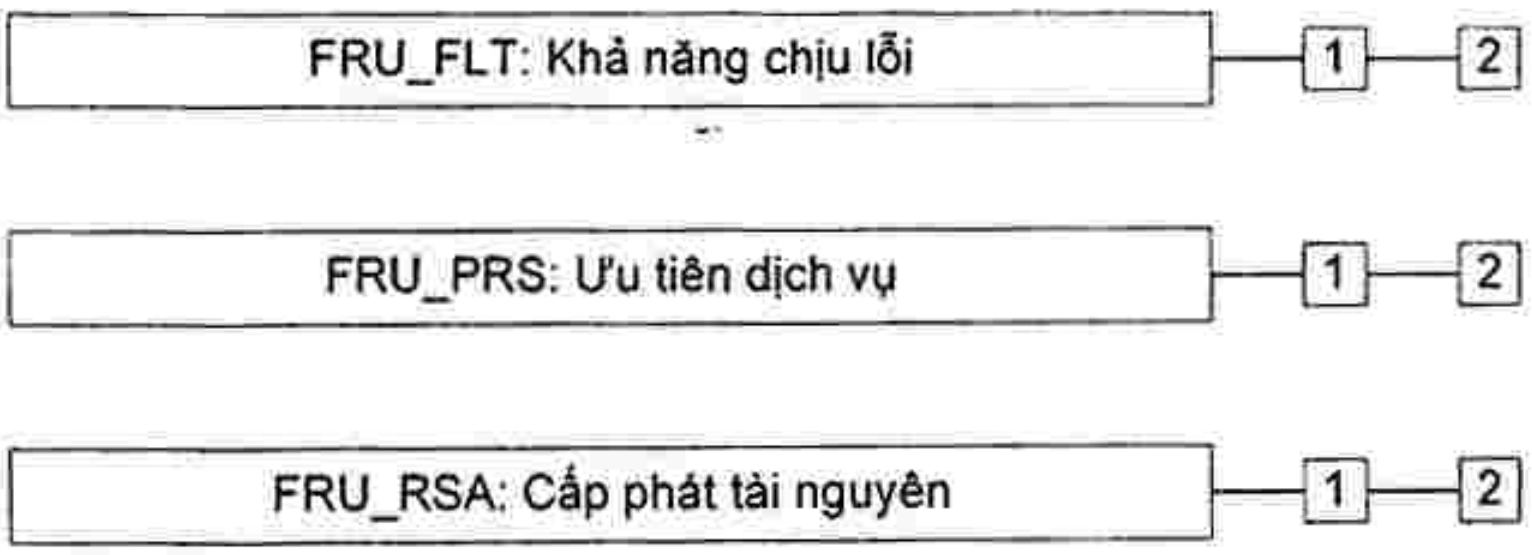
Phụ lục K

(Quy định)

Lớp FRU: Sử dụng tài nguyên

Lớp này cung cấp ba họ yêu cầu chức năng cung cấp sự sẵn sàng được yêu cầu bởi các tài nguyên chẳng hạn như khả năng tính toán và/hoặc không gian lưu trữ. Họ Chịu lỗi cung cấp việc bảo vệ chống lại sự không sẵn sàng của các khả năng gây ra bởi hỏng hóc của TOE. Họ Quyền ưu tiên của dịch vụ đảm bảo rằng các tài nguyên sẽ được cấp phát cho các nhiệm vụ quan trọng hơn hoặc là cấp bách hơn và không thể bị độc chiếm bởi các nhiệm vụ có Quyền ưu tiên thấp hơn. Họ Cấp phát tài nguyên cung cấp các giới hạn trong việc sử dụng các tài nguyên sẵn có, từ đó ngăn chặn người sử dụng khỏi việc độc chiếm tài nguyên.

Hình K.1 cho thấy phân tách của lớp này thành các các thành phần cấu thành của nó.



Hình K.1 – Phân cấp lớp FRU:Sử dụng tài nguyên.

K.1 Khả năng chịu lỗi (FRU_FLT)

K.1.1 Chú thích cho người sử dụng

Họ này cung cấp các yêu cầu đối với tính sẵn có của các khả năng thậm chí trong cả các tình huống trục trặc. Ví dụ về các trục trặc như vậy là trục trặc nguồn, trục trặc phần cứng hoặc lỗi phần mềm. Trong trường hợp xác định được là lỗi như vậy, TOE sẽ duy trì các khả năng đã được xác định. Tác giả PP/ST có thể xác định rằng, ví dụ, một TOE được sử dụng trong nhà máy hạt nhân sẽ có thể tiếp tục thao tác của quy trình tắt hệ thống khi gặp trường hợp trục trặc nguồn hoặc trục trặc truyền thông xảy ra.

Bởi vì TOE chỉ có thể tiếp tục hoặc động chính xác của nó nếu các SFR được bắt buộc thực hiện, yêu cầu là hệ thống này phải giữ nguyên trong một trạng thái an toàn sau khi gặp trục trặc. Khả năng này được cung cấp bởi FPT_FLS.1 Trục trặc với sự duy trì trạng thái an toàn.

Các cơ chế để cung cấp khả năng chịu lỗi có thể là chủ động hoặc bị động. Nếu là cơ chế chủ động, các chức năng xác định được đưa vào thao tác sao cho chúng được kích hoạt trong trường hợp lỗi xảy ra. Ví dụ, báo động lửa là một cơ chế chủ động: TSF sẽ phát hiện lửa và có thể thực hiện hành động như chuyển thao tác sang dự phòng. Trong cơ chế bị động, kiến trúc của TOE có khả năng quản lý lỗi. Ví dụ, việc sử dụng một cách thức bầu đa số nhờ đó với nhiều bộ vi xử lý là một giải pháp bị động; trục trặc của một bộ vi xử lý sẽ không làm gián đoạn hành động của TOE (mặc dù nó cần được phát hiện để cho phép khắc phục).

Đối với họ này, trục trặc được khởi phát một cách vô tình (chẳng hạn như ngập lụt hoặc tháo nhầm thiết bị) hoặc có chủ ý (chẳng hạn như việc độc chiếm) sẽ là không quan trọng.

K.1.2 FRU_FLT.1 Khả năng chịu lỗi suy giảm

K.1.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này được dự định để xác định khả năng nào mà TOE vẫn sẽ cung cấp sau khi xảy ra một trục trặc của hệ thống. Bởi vì thật là khó để mô tả tất cả các trục trặc, phân loại các trục trặc có thể phải xác định. Ví dụ của các trục trặc chung gồm có ngập lụt phòng máy tính, ngắt nguồn điện trong thời gian ngắn, hỏng CPU hoặc máy tính, trục trặc phần mềm hoặc tràn bộ đệm.

K.1.2.2 Các hoạt động

K.1.2.2.1 Chỉ định

Trong FRU_FLT.1.1, tác giả PP/ST nên xác định danh sách các khả năng TOE mà TOE sẽ duy trì trong suốt thời gian và sau khi một lỗi được xác định.

Trong FRU_FLT.1.1, tác giả PP/ST nên xác định danh sách các loại trục trặc mà TOE rõ ràng phải được bảo vệ. Nếu một trục trặc trong danh sách này xảy ra, TOE sẽ có thể tiếp tục thao tác của nó.

K.1.3 FRU_FLT.2 Khả năng chịu đựng lỗi giới hạn

K.1.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này được dự định để xác định loại trục trặc nào mà TOE phải chống chịu được. Bởi vì thật là khó để mô tả tất cả các trục trặc, có thể phải xác định phân loại các trục trặc. Ví dụ của các trục trặc chung gồm có ngập lụt phòng máy tính, ngắt nguồn điện trong thời gian ngắn, hỏng CPU hoặc máy tính, trục trặc phần mềm hoặc tràn bộ đệm.

K.1.3.2 Các hoạt động

K.1.3.2.1 Chỉ định

Trong FRU_FLT.2.1, tác giả PP/ST nên xác định danh sách loại trục trặc mà TOE rõ ràng phải được bảo vệ. Nếu một trục trặc trong danh sách xảy ra, TOE sẽ có khả năng tiếp tục thao tác của nó.

K.2 Ưu tiên dịch vụ (FRU_PRS)

K.2.1 Chú thích cho người sử dụng

Các yêu cầu của họ này cho phép TSF kiểm soát việc sử dụng tài nguyên trong phạm vi TSF bởi người sử dụng và các chủ thể mà các thao tác có quyền ưu tiên cao trong phạm vi TSF sẽ luôn đạt được mà không bị cản trở hoặc bị làm chậm trễ bởi các thao tác có quyền ưu tiên thấp. Nói cách khác, các nhiệm vụ cấp bách sẽ không bị trì hoãn bởi các nhiệm vụ ít cấp bách hơn.

Họ này có thể ứng dụng vào nhiều loại tài nguyên, ví dụ, khả năng xử lý và dung lượng kênh truyền thông.

Cơ chế Quyền ưu tiên của dịch vụ có thể là chủ động hoặc bị động. Trong hệ thống Quyền ưu tiên của dịch vụ bị động, hệ thống sẽ lựa chọn nhiệm vụ có quyền ưu tiên cao nhất khi phải lựa chọn giữa hai ứng dụng đang đợi phục vụ. Trong khi sử dụng các cơ chế Quyền ưu tiên của dịch vụ bị động, khi một nhiệm vụ có quyền ưu tiên thấp đang chạy, nó không thể bị ngắt bởi một nhiệm vụ có quyền ưu tiên cao. Khi sử dụng các cơ chế Quyền ưu tiên của dịch vụ chủ động, các nhiệm vụ có quyền ưu tiên thấp có thể bị ngắt bởi các nhiệm vụ mới có quyền ưu tiên cao.

Yêu cầu kiểm toán nói rằng tất cả các lý do từ chối nên được kiểm toán. Người phát triển được quyết định một thao tác không bị từ chối mà bị trì hoãn.

K.2.2 FRU_PRS.1 Ưu tiên dịch vụ có giới hạn

K.2.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này định nghĩa các quyền ưu tiên cho một chủ thể và các tài nguyên mà quyền ưu tiên này sẽ được sử dụng với. Nếu một chủ thể cố gắng thao tác trên một tài nguyên được kiểm soát bởi các yêu cầu Quyền ưu tiên của Dịch vụ, truy cập và/hoặc thời gian của truy cập sẽ phụ thuộc vào quyền ưu tiên của chủ thể, quyền ưu tiên của chủ thể đang hành động, và quyền ưu tiên của các chủ thể vẫn ở trong hàng đợi.

K.2.2.2 Các hoạt động

K.2.2.2.1 Chỉ định

Trong FRU_PRS.1.2, tác giả PP/ST nên xác định một danh sách các tài nguyên được kiểm soát mà TSF buộc thực hiện quyền ưu tiên của dịch vụ (ví dụ: các tài nguyên như các tiến trình, không gian đĩa, bộ nhớ, băng thông)

K.2.3 FRU_PRS.2 Quyền ưu tiên dịch vụ đầy đủ

K.2.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này định nghĩa các quyền ưu tiên cho một chủ thể. Tất cả các tài nguyên có thể chia sẻ trong TSC sẽ tùy thuộc vào cơ chế Quyền ưu tiên của Dịch vụ. Nếu một chủ thể cố thực hiện trên một tài nguyên TSC chia sẻ được, truy cập và/hoặc thời gian truy cập sẽ phụ thuộc vào quyền ưu tiên của chủ thể, quyền ưu tiên của chủ thể đang hành động, và quyền ưu tiên của các chủ thể vẫn ở trong hàng đợi.

K.3 Cấp phát tài nguyên (FRU_RSA)

K.3.1 Chú thích cho người sử dụng

Các yêu cầu của họ này cho phép TSF kiểm soát việc sử dụng các tài nguyên trong phạm vi TSC bởi người sử dụng và các chủ thể mà việc từ chối dịch vụ không được phép sẽ không xảy ra do việc độc chiếm tài nguyên bởi người sử dụng hoặc chủ thể khác.

Các quy tắc cấp phát tài nguyên cho phép tạo ra hạn ngạch hoặc các cách làm khác để định nghĩa các giới hạn đối với số lượng của không gian tài nguyên hoặc thời gian có thể được cấp phát vì lợi ích của một người sử dụng hoặc một thủ thể xác định. Ví dụ, các quy tắc này có thể là:

Cung cấp cho đối tượng các hạn ngạch mà giới hạn số lượng và/hoặc kích thước của các đối tượng mà một người sử dụng cụ thể có thể cấp phát.

Việc kiểm soát việc cấp phát / giải phóng của các đơn vị tài nguyên đã được Chỉ định trước nằm trong sự kiểm soát của TSF.

Nói chung, những chức năng này sẽ được thực thi thông qua việc sử dụng các thuộc tính được Chỉ định cho người sử dụng và các tài nguyên.

Mục đích của những thành phần này là để đảm bảo một mức độ công bằng cụ thể giữa các người sử dụng và các chủ thể (ví dụ: một người sử dụng đơn lẻ nào đó không nên cấp phát tất cả không gian sẵn có). Bởi vì việc cấp phát tài nguyên thường vượt quá thời gian tồn tại của một chủ thể (tức là tệp

tin thường tồn tại lâu hơn các ứng dụng mà sinh ra nó), và nhiều bản cài đặt của các chủ thể bởi cùng một người sử dụng không nên tác động tiêu cực quá nhiều tới các người sử dụng khác, các thành phần cho phép các giới hạn cấp phát liên quan tới các người sử dụng. Trong một số tình huống các tài nguyên được cấp phát bởi một chủ thể (ví dụ bộ nhớ chính hoặc chu trình CPU). Trong những ví dụ đó, các thành phần cho phép việc cấp phát tài nguyên là dựa trên cấp bậc của chủ thể.

Họ này áp đặt các yêu cầu đối với việc cấp phát tài nguyên, không phải là bản thân việc sử dụng tài nguyên đó. Các yêu cầu kiểm toán do đó, như đã được nói tới, cũng áp dụng cho việc cấp phát tài nguyên, không áp dụng cho việc sử dụng tài nguyên đó.

K.3.2 FRU_RSA.1 Các chỉ tiêu tối đa

K.3.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cung cấp các yêu cầu đối với các cơ chế hạn ngạch mà chỉ áp dụng cho một tập hợp xác định các tài nguyên có thể chia sẻ trong TOE. Các yêu cầu này cho phép các hạn ngạch gắn với một người sử dụng nào đó có thể được Chỉ định cho các nhóm người sử dụng hoặc chủ thể cũng như áp dụng được đối với TOE.

K.3.2.2 Các hoạt động

K.3.2.2.1 Chỉ định

Trong FRU_RSA.1.1, tác giả PP/ST nên xác định danh sách các tài nguyên được kiểm soát mà các giới hạn cấp phát tài nguyên tối đa được yêu cầu với chúng (ví dụ các tiến trình, không gian đĩa, bộ nhớ, băng thông). Nếu tất cả các tài nguyên trong TSF cần được bao bồm, cụm từ "tất cả các tài nguyên TSF" có thể được xác định.

K.3.2.2.2 Phép chọn

Trong FRU_RSA.1.1, tác giả PP/ST nên lựa chọn xem liệu các hạn ngạch tối đa có áp dụng cho những người sử dụng đơn lẻ, cho một nhóm người sử dụng hoặc chủ thể đã được định nghĩa, hoặc bất kỳ kết hợp nào đó của các đối tượng này.

Trong FRU_FSA.1.1, tác giả PP/ST nên lựa chọn xem liệu các hạn ngạch tối đa có thể áp dụng cho bất kỳ thời gian nào (một cách đồng thời), hoặc trong một khoảng thời gian cụ thể.

K.3.3 FRU_RSA.2 Các chỉ tiêu tối đa và tối thiểu

K.3.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cung cấp các yêu cầu đối với các cơ chế hạn ngạch áp dụng cho một tập hợp xác định các tài nguyên chia sẻ được trong TOE. Các yêu cầu này cho phép các hạn ngạch gắn với một người sử dụng nào đó có thể được Chỉ định cho các nhóm người sử dụng hoặc chủ thể cũng như áp dụng được đối với TOE.

K.3.3.2 Các hoạt động

K.3.3.2.1 Chỉ định

Trong FRU_FRS.2.1, tác giả PP/ST nên xác định các tài nguyên mà các giới hạn cấp phát tài nguyên tối đa và tối thiểu được yêu cầu (ví dụ các tiến trình, không gian đĩa, bộ nhớ, băng thông). Nếu tất cả các tài nguyên trong TSF cần được bao gồm, cụm từ "tất cả các tài nguyên TSF" có thể được xác định.

K.3.3.2.2 Phép chọn

Trong FRU_RSA.2.1, tác giả PP/ST nên lựa chọn xem liệu các hạn ngạch tối đa có áp dụng cho những người sử dụng đơn lẻ, cho một nhóm đã được định nghĩa các người sử dụng hoặc các chủ thể hoặc bất kỳ kết hợp nào đó của những đối tượng này.

Trong FRU_RSA.2.1, tác giả PP/ST nên lựa chọn liệu các hạn ngạch nối đa có áp dụng cho thời gian bất kỳ (một cách đồng thời), hoặc trong một khoảng thời gian xác định.

K.3.3.2.3 Chỉ định

Trong FRU_RSA.2.2, tác giả PP/ST nên xác định các tài nguyên được kiểm soát mà các giới hạn cấp phát tối thiểu được thiết đặt (ví dụ các tiến trình, không gian đĩa, bộ nhớ, băng thông). Nếu tất cả các tài nguyên trong TSF cần được bao gồm, cụm từ "tất cả các tài nguyên TSF" có thể được xác định.

K.3.3.2.4 Phép chọn

Trong FRU_RSA.2.2, tác giả PP/ST nên lựa chọn xem liệu các hạn ngạch tối thiểu có áp dụng cho những người sử dụng đơn lẻ, cho một nhóm đã được định nghĩa các người sử dụng hoặc các chủ thể hoặc bất kỳ kết hợp nào đó của những đối tượng này.

Trong FRU_RSA.2.2, tác giả PP/ST nên lựa chọn liệu các hạn ngạch nối thiểu có áp dụng cho thời gian bất kỳ (một cách đồng thời), hoặc trong một khoảng thời gian xác định.

Phụ lục L

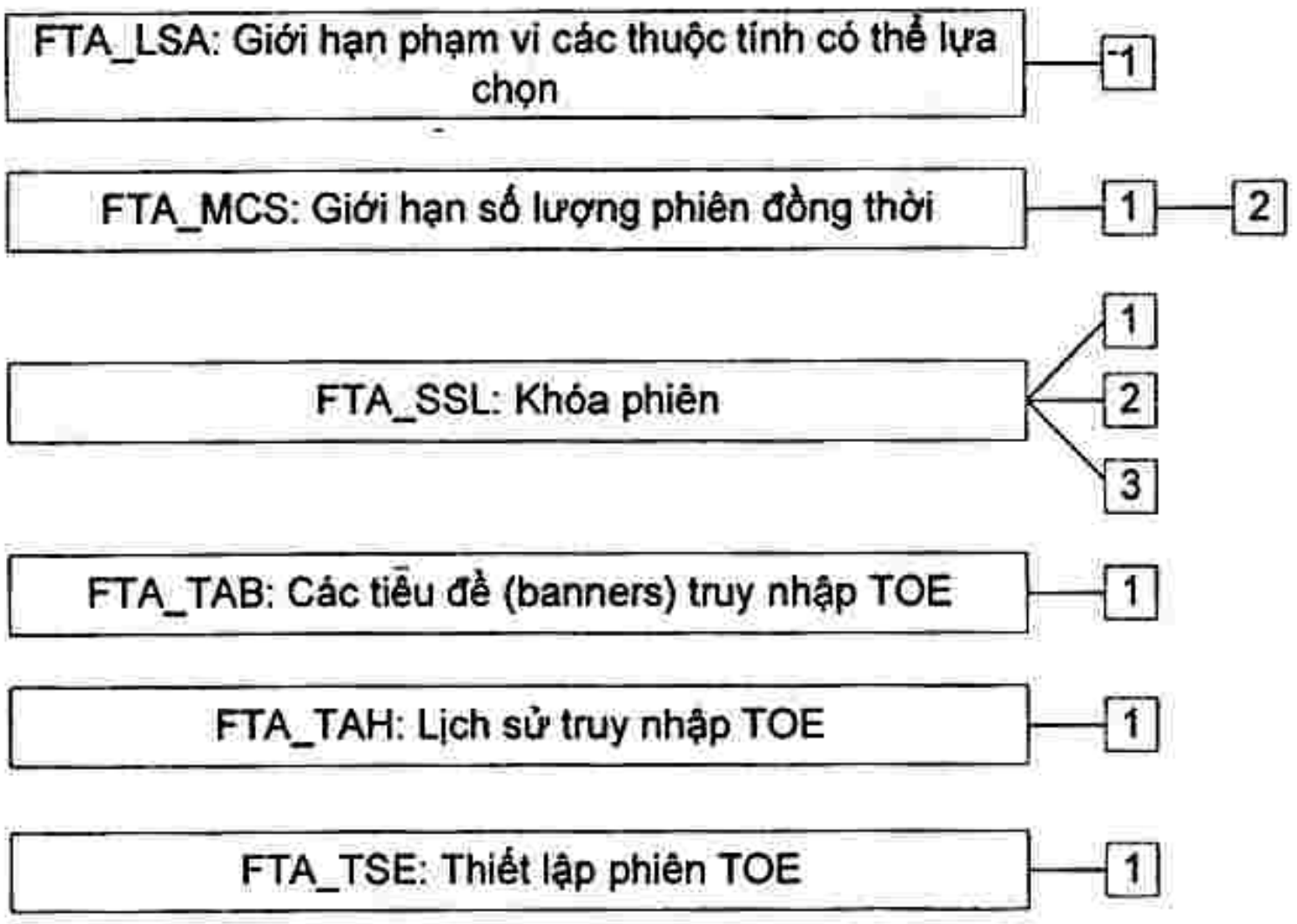
(Quy định)

Lớp FTA: Truy nhập TOE

Việc thiết lập phiên của người sử dụng bao gồm việc tạo ra một hoặc nhiều chủ thể thực hiện các thao tác trong TOE đại diện cho người sử dụng. Vào lúc kết thúc thủ tục thiết lập phiên, với các yêu cầu truy nhập TOE được thỏa mãn, các chủ thể được tạo ra mang các thuộc tính được xác định bởi các chức năng định danh và xác thực. Họ này xác định các yêu cầu chức năng đối với việc kiểm soát sự thiết lập một phiên của người sử dụng.

Một phiên của người sử dụng được định nghĩa là khoảng thời gian bắt đầu vào lúc định danh / xác thực, hoặc nếu phù hợp hơn, lúc bắt đầu của tương tác giữa người sử dụng và hệ thống, cho đến lúc tất cả các chủ thể (các tài nguyên và các thuộc tính) liên quan tới phiên đó được giải phóng.

Hình L.1 minh họa cấu trúc của lớp này thành các thành phần cấu thành của nó.



Hình L.1 – Phân cấp lớp FTA: Truy nhập TOE

L.1 Giới hạn trên phạm vi các thuộc tính có thể lựa chọn (FTA_LSA)

L.1.1 Chú thích cho người sử dụng

Họ này định nghĩa các yêu cầu sẽ giới hạn các thuộc tính an ninh phiên mà một người sử dụng có thể lựa chọn và các chủ thể mà một người sử dụng có thể được gắn với dựa vào: phương thức của truy cập nhập; vị trí hoặc cổng truy nhập; và/hoặc thời gian (ví dụ giờ-trong-ngày, ngày-trong-tuần).

Họ này cung cấp khả năng cho một tác giả PP/ST để xác định các yêu cầu đối với TSF để đặt các giới hạn cho miền của các thuộc tính an ninh của người sử dụng dựa vào một điều kiện môi trường. Ví dụ, một người sử dụng có thể được cho phép để thiết lập một "phiên bí mật" trong suốt nhiều giờ làm việc bình thường nhưng ngoài các giờ đó ra cũng người sử dụng này có thể bị giới hạn chỉ thiết lập được "các phiên không bí mật". Định danh của các ràng buộc có liên quan trên miền của các thuộc tính lựa chọn được có thể đạt được thông qua việc sử dụng thao tác lựa chọn. Các ràng buộc này có thể được

ứng dụng trên cơ sở thuộc tính này kế tiếp thuộc tính kia. Khi tồn tại một nhu cầu xác định các ràng buộc trên nhiều thuộc tính thành phần này sẽ phải được lặp lại cho mỗi thuộc tính. Các ví dụ về các thuộc tính có thể được sử dụng để giới hạn các thuộc tính an ninh phiên là:

a) Phương thức truy nhập có thể được sử dụng để xác định kiểu môi trường mà người sử dụng sẽ thao tác (ví dụ giao thức truyền tệp, đầu cuối, vtam).

b) Vị trí của truy nhập có thể được sử dụng để giới hạn miền của các thuộc tính lựa chọn được của người sử dụng dựa vào một vị trí của người sử dụng hoặc cổng truy nhập. Khả năng này là sử dụng cụ thể trong các môi trường sẵn có các phương tiện quay số hoặc các phương tiện mạng.

c) Thời điểm truy nhập có thể được sử dụng để giới hạn miền của các thuộc tính lựa chọn được của người sử dụng. Ví dụ, các khoảng có thể dựa vào giờ-trong-ngày, ngày-trong-tuần, hoặc các ngày cụ thể. Ràng buộc này cung cấp một số bảo vệ đối với các thao tác của người sử dụng mà có thể xảy ra vào một thời điểm mà việc giám sát phù hợp hoặc các biện pháp thủ tục phù hợp có thể không được sử dụng.

L.1.2 FTA_LSA.1 Giới hạn trên phạm vi các thuộc tính có thể lựa chọn

L.1.2.1 Các hoạt động

L.1.2.1.1 Chỉ định

Trong FTA_LSA.1.1, tác giả PP/ST nên xác định tập hợp các thuộc tính an ninh phiên được ràng buộc. Ví dụ của các thuộc tính an ninh phiên này là mức độ được phép của người sử dụng, mức độ toàn vẹn và các vai trò.

Trong FTA_LSA.1.1, tác giả PP/ST nên xác định tập hợp các thuộc tính có thể được sử dụng để xác định phạm vi của các thuộc tính an ninh phiên. Ví dụ của các thuộc tính như vậy là định danh người sử dụng, vị trí thao tác, thời điểm truy nhập và phương thức truy nhập.

L.2 Giới hạn về nhiều phiên diễn ra đồng thời (FTA_MCS)

L.2.1 Chú thích cho người sử dụng

Họ này định nghĩa số lượng phiên mà một người sử dụng có thể có đồng thời (các phiên đồng thời). Số lượng các phiên đồng thời này có thể hoặc là tập hợp của một nhóm người sử dụng hoặc đối với mỗi người sử dụng đơn lẻ.

L.2.2 FTA_MCS.1 Giới hạn cơ sở trên đa phiên đồng thời

L.2.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cho phép hệ thống giới hạn số lượng phiên để sử dụng hiệu quả các tài nguyên của TOE.

L.2.2.2 Các hoạt động

L.2.2.2.1 Chỉ định

Trong FTA_MCS.1.2, tác giả PP/ST nên xác định một số lượng ngầm định các phiên đồng thời được sử dụng.

L.2.3 FTA_MCS.2 Giới hạn thuộc tính mỗi người dùng cho nhiều phiên đồng thời

L.2.3.1 Chú thích cho ứng dụng người sử dụng

Thành phần này cung cấp các khả năng bổ sung cho FTA_MCS.1 Giới hạn cơ bản về số lượng phiên đồng thời, bằng cách cho phép thực hiện nhiều ràng buộc hơn đối với số lượng phiên đồng thời mà người sử dụng có thể kích hoạt. Các ràng buộc này là dưới dạng các thuộc tính an ninh của người sử dụng, chẳng hạn như định danh người sử dụng hoặc tư cách của một vai trò.

L.2.3.2 Các hoạt động

L.2.3.2.1 Chỉ định

Trong FTA_MCS.2.1, tác giả PP/ST nên xác định các quy tắc xác định số lượng tối đa các phiên đồng thời. Một ví dụ về một quy tắc như vậy là "số lượng tối đa các phiên đồng thời là một nếu người sử dụng có một mức phân loại "bí mật" và bằng năm trong những trường hợp còn lại".

-Trong FTA_MCS.2.2, tác giả PP/ST nên xác định số lượng tối đa ngầm định các phiên đồng thời được sử dụng.

lại người sử dụng, phải xảy ra.

L.3 Khóa và chấm dứt phiên (FTA_SSL)

L.3.1 Chú thích cho người sử dụng

Họ này định nghĩa các yêu cầu đối với TSF để cung cấp khả năng khóa và mở khóa người dùng đầu hoặc TSF đầu và hủy các phiên tương tác.

Khi một người sử dụng đang tương tác trực tiếp với các chủ thể trong TOE (phiên tương tác), thiết bị đầu cuối của người sử dụng là có thể bị tấn công nếu bị bỏ mặc. Họ này cung cấp các yêu cầu đối với TSF để cấm thao tác (khóa) thiết bị đầu cuối hoặc kết thúc phiên sau một khoảng thời gian xác định không thao tác, và đối với người sử dụng để kích hoạt việc cấm thao tác (khóa) thiết bị đầu cuối hoặc hủy phiên. Để kích hoạt lại thiết bị đầu cuối, một sự kiện được xác định bởi tác giả PP/ST, chẳng hạn như xác thực lại người dùng phải xảy ra.

Một người sử dụng được coi là không thao tác nếu người đó không cung cấp bất kỳ kích thích nào với TOE trong một khoảng thời gian cụ thể.

Một tác giả PP/ST nên cân nhắc liệu có nên bao gồm FTP_TRP.1 Đường truyền được tin cậy. Trong trường hợp như vậy, chức năng "khóa phiên" nên được bao gồm trong thao tác tại FTP_TRP.1 Đường truyền được tin cậy.

L.3.2 FTA_SSL.1 Khóa phiên khởi tạo bởi TSF

L.3.2.1 Chú thích cho ứng dụng người sử dụng

FTA_SSL.1 Khóa phiên được khởi phát bởi TSF cung cấp khả năng cho TSF để khóa một phiên người sử dụng đang thao tác sau một khoảng thời gian xác định. Việc khóa một thiết bị đầu cuối có thể ngăn ngừa bất kỳ tương tác nào thêm với một phiên đang thao tác thông qua việc sử dụng đầu cuối đã bị khóa.

Nếu các thiết bị hiển thị được ghi đè, nội dung thay thế không nhất thiết là tĩnh (tức là cho phép "các thao tác tiết kiệm màn hình").

Thành phần này cho phép tác giả PP/ST xác định sự kiện nào sẽ mở khóa cho phiên. Các sự kiện này có thể liên quan tới thiết bị đầu cuối (ví dụ tập hợp cố định các phím để mở khóa cho phiên), người sử dụng (ví dụ xác thực lại) hoặc thời gian.

L.3.2.2 Các hoạt động

L.3.2.2.1 Chỉ định

Trong FTA_SSL.1.1, tác giả PP/ST nên xác định khoảng thời gian không thao tác của người sử dụng từ đó kích hoạt việc khóa một phiên tương tác. Nếu điều này được mong đợi, tác giả PP/ST có thể, thông qua việc Chỉ định, xác định khoảng thời gian còn lại dành cho một nhà quản trị được cho phép hoặc người sử dụng đó. Các chức năng quản lý trong lớp FMT có thể xác định khả năng để thay đổi khoảng thời gian này, đưa chúng trở thành giá trị ngầm định.

Trong FTA_SSL.1.2, tác giả PP/ST nên xác định các sự kiện nên xảy ra trước khi phiên được mở khóa. Các ví dụ về một sự kiện như vậy là: "xác thực lại người sử dụng" hoặc "người sử dụng nhập vào một chuỗi phím để mở khóa".

L.3.3 FTA_SSL.2 Khóa khởi tạo bởi người dùng

L.3.3.1 Chú thích cho ứng dụng người sử dụng

FTA_SSL.2 Việc mở khóa được khởi phát bởi người sử dụng cung cấp khả năng đối với một người sử dụng được cho phép để khóa và mở khóa phiên tương tác riêng của người đó. Điều này cung cấp cho người sử dụng được cho phép khả năng để phong tỏa một cách hiệu quả việc sử dụng thêm các phiên đang thao tác mà không phải ngắt phiên đang thao tác.

Nếu các thiết bị hiển thị được ghi đè, nội dung thay thế không nhất thiết là tĩnh (tức là cho phép "các thao tác tiết kiệm màn hình").

L.3.3.2 Các hoạt động

L.3.3.2.1 Chỉ định

Trong FTA_SSL.2.2, tác giả PP/ST nên xác định các sự kiện nên xảy ra trước khi phiên được mở khóa. Các ví dụ về một sự kiện như vậy là: "xác thực lại người sử dụng" hoặc "người sử dụng nhập vào một chuỗi phím để mở khóa".

L.3.4 FTA_SSL.3 Kết thúc phiên khởi tạo bởi TSF

L.3.4.1 Chú thích cho ứng dụng người sử dụng

FTA_SSL.3 Việc kết thúc được khởi phát bởi TSF yêu cầu TSF kết thúc một phiên người sử dụng không thao tác sau một khoảng thời gian không thao tác.

Tác giả PP/ST nên biết rằng một phiên có thể tiếp tục sau khi người sử dụng kết thúc thao tác của họ, ví dụ, việc xử lý chạy nền. Yêu cầu này có thể ngắt chủ thể chạy nền này sau một khoảng thời gian không thao tác của người sử dụng mà không quan tâm tới trạng thái của chủ thể.

L.3.4.2 Các hoạt động

L.3.4.2.1 Chỉ định

Trong FTA_SSL.3.1, tác giả PP/ST nên xác định khoảng thời gian không thao tác của người sử dụng mà sẽ khởi phát việc kết thúc một phiên không thao tác. Nếu điều này được mong đợi, tác giả PP/ST có thể, thông qua việc Chỉ định, xác định khoảng thời gian còn lại dành cho một nhà quản trị được cho

phép hoặc người sử dụng đó. Các chức năng quản lý trong lớp FMT có thể xác định khả năng để thay đổi khoảng thời gian này, đưa chúng trở thành giá trị ngầm định.

L.3.5 FTA_SSL.4 Kết thúc phiên khởi tạo bởi người dùng

L.3.5.1 Chú thích cho ứng dụng người sử dụng

Việc hủy bỏ người dùng ban đầu FTA_SSL cho phép người dùng được cấp quyền hủy bỏ phiên tương tác của anh ta.

Tác giả PP/ST cần ý thức rằng một phiên có thể tiếp tục sau khi người dùng kết thúc hoạt động của anh ta, ví dụ, xử lý cơ sở. Yêu cầu này có thể cho phép người dùng hủy bỏ đối tượng cơ sở mà không cần quan tâm đến trạng thái của chủ thể.

L.4 Các biểu trưng truy nhập TOE (FTA_TAB)

L.4.1 Chú thích cho người sử dụng

Trước khi định danh và xác thực, các yêu cầu truy nhập TOE cung cấp khả năng cho TOE để hiển thị một thông điệp cảnh báo mang tính chất tư vấn người sử dụng tiềm năng nên gắn với việc sử dụng phù hợp của TOE.

L.4.2 FTA_TAB.1 Các biểu trưng truy nhập TOE mặc định

L.4.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này yêu cầu việc cảnh báo mang tính chất tư vấn liên quan tới việc sử dụng không được phép của TOE. Một tác giả PP/ST có thể sàng lọc yêu cầu để bao gồm một biểu ngữ ngầm định.

L.5 Lịch sử truy nhập TOE (FTA_TAH)

L.5.1 Chú thích cho người sử dụng

Họ này định nghĩa các yêu cầu đối với TSF để hiển thị cho người sử dụng, tiếp theo việc thiết lập thành công phiên làm việc đối với TOE, một lịch sử của các nỗ lực không thành công nhằm truy nhập tài khoản. Lịch sử này có thể bao gồm ngày, giờ, cách thức truy nhập, và cổng của truy nhập thành công cuối cùng vào TOE, cũng như số lượng các nỗ lực không thành công nhằm truy nhập vào TOE tính từ truy nhập thành công cuối cùng bởi một người sử dụng xác định.

L.5.2 FTA_TAH.1 Lịch sử truy nhập TOE

L.5.2.1 Chú thích cho ứng dụng người sử dụng

Họ này có thể cung cấp cho người sử dụng được cho phép thông tin cho chỉ ra sự lạm dụng có thể có đối với tài khoản của người sử dụng.

Thành phần này yêu cầu người sử dụng được cung cấp thông tin. Người sử dụng nên có thể xem lại thông tin, nhưng không bị buộc phải làm như vậy. Nếu một người sử dụng muốn như vậy thì họ có thể, ví dụ, tạo ra các đoạn mã lệnh để từ chối thông tin này và bắt đầu các tiến trình khác.

L.5.2.2 Các hoạt động

L.5.2.2.1 Phép chọn

Trong FTA_TAH.1.1, tác giả PP/ST nên lựa chọn các thuộc tính an ninh của việc thiết lập phiên thành công cuối cùng mà sẽ được hiển thị tại giao diện người sử dụng. Các mục là: ngày, giờ, phương thức truy nhập (chẳng hạn ftp), và/hoặc vị trí (ví dụ thiết bị đầu cuối 50).

Trong FTA_TAH.1.2, tác giả PP/ST nên lựa chọn các thuộc tính an ninh của việc thiết lập phiên thành công cuối cùng mà sẽ được hiển thị tại giao diện người sử dụng. Các mục là: ngày, giờ, phương thức truy nhập (chẳng hạn ftp), và/hoặc vị trí (ví dụ thiết bị đầu cuối 50).

L.6 Thiết lập phiên TOE (FTA_TSE)

L.6.1 Chú thích cho người sử dụng

Họ này định nghĩa các yêu cầu để từ chối chấp nhận một người sử dụng thiết lập một phiên với TOE dựa vào các thuộc tính chẳng hạn như vị trí hoặc cổng truy nhập, thuộc tính an ninh của người sử dụng (ví dụ định danh, mức độ được phép, mức độ toàn vẹn, tư cách thành viên của một vai trò), khoảng thời gian (ví dụ giờ-trong-ngày, ngày-trong-tuần, ngày theo lịch) hoặc kết hợp của các tham số trên.

Họ này cung cấp khả năng cho tác giả PP/ST để xác định các yêu cầu đối với TOE để đặt các ràng buộc lên khả năng của một người sử dụng được cho phép để thiết lập một phiên với TOE. Định danh của các ràng buộc liên quan có thể đạt được thông qua việc sử dụng thao tác lựa chọn. Các ví dụ của các thuộc tính có thể được sử dụng để xác định các ràng buộc thiết lập phiên là:

a) Vị trí của truy nhập có thể được sử dụng để ràng buộc khả năng của một người sử dụng để thiết lập một phiên thao tác với TOE dựa vào vị trí hoặc cổng truy nhập của người sử dụng. Khả năng này là tùy từng sử dụng cụ thể trong các môi trường sẵn có các phương tiện quay số hoặc các phương tiện mạng.

b) Các thuộc tính an ninh của người sử dụng có thể được sử dụng để đặt các ràng buộc lên khả năng của một người sử dụng để thiết lập một phiên thao tác với TOE. Ví dụ, những thuộc tính này có thể cung cấp khả năng từ chối việc thiết lập phiên dựa vào một trong số các thông tin sau:

Định danh của người sử dụng

Mức độ được phép của người sử dụng

Mức độ toàn vẹn của người sử dụng

Tư cách thành viên của một vai trò

Khả năng này là liên quan cụ thể tới các tình huống trong đó việc cho phép hoặc đăng nhập có thể xảy ra tại một vị trí khác so với nơi các kiểm tra truy nhập TOE được thực hiện.

c) Thời gian truy nhập có thể được sử dụng để ràng buộc khả năng của một người sử dụng để thiết lập một phiên thao tác với TOE dựa vào các khoảng thời gian. Ví dụ, các khoảng thời gian có thể dựa vào giờ-trong-ngày, ngày-trong-tuần hoặc các ngày theo lịch. Ràng buộc này cung cấp khả năng bảo vệ mang tính chất hành động chống lại các hành động có thể xảy ra tại một thời điểm mà việc giám sát thích hợp hoặc các biện pháp thủ tục thích hợp có thể không được thực hiện.

L.6.2 FTA_TSE.1 Thiết lập phiên TOE

L.6.2.1 Các hoạt động

L.6.2.1.1 Chỉ định

Trong FTA_TSE.1.1, tác giả PP/ST nên xác định các thuộc tính có thể được sử dụng để hạn chế thiết lập phiên. Ví dụ về các thuộc tính có thể là định danh người sử dụng, vị trí ban đầu (ví dụ không cho

phép thiết bị đầu cuối ở xa), thời gian truy nhập (ví dụ các giờ ở bên ngoài khoảng), hoặc phương thức truy nhập (ví dụ X-windows).

Phụ lục M

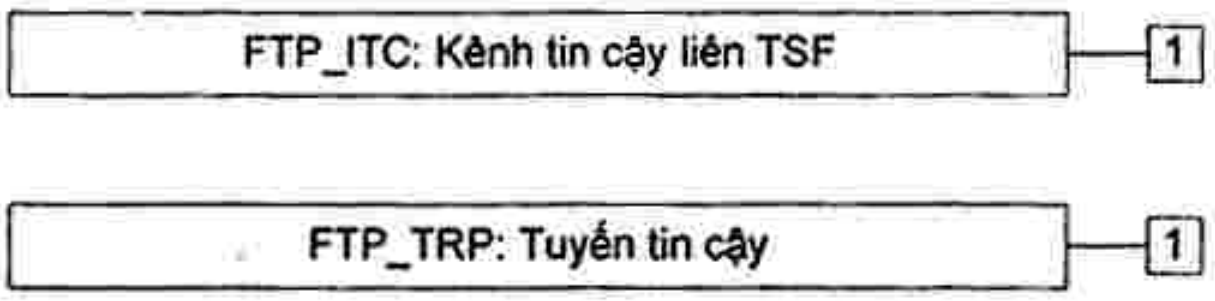
(Quy định)

Lớp FTP: Đường dẫn/Kênh tin cậy

Người sử dụng thường cần thực hiện các chức năng thông qua tương tác trực tiếp với TSF. Một đường truyền được tin cậy cung cấp sự tin tưởng rằng một người sử dụng đang truyền thông trực tiếp với TSF bất cứ khi nào nó được kích hoạt. Một phản hồi của người sử dụng thông qua một đường truyền được tin cậy đảm bảo rằng các ứng dụng không được tin cậy không thể chặn hoặc làm thay đổi phản hồi của người sử dụng. Tương tự như vậy, các kênh được tin cậy là một cách tiếp cận đối với truyền thông an toàn giữa TSF và các sản phẩm IT được tin cậy khác.

Sự thiếu vắng của một đường truyền được tin cậy có thể cho phép các lỗ hổng kiểm soát hoặc kiểm soát truy nhập trong các môi trường mà các ứng dụng không được tin cậy được sử dụng. Những ứng dụng này có thể chặn thông tin riêng tư của người sử dụng, chẳng hạn như mật khẩu, và sử dụng nó để đóng giả những người sử dụng khác. Kết quả là, trách nhiệm đối với bất kỳ hành động hệ thống nào không thể được Chỉ định một cách đáng tin cậy cho một thực thể kiểm soát được. Cũng như vậy, những ứng dụng này có thể đưa ra thông tin sai trên màn hiển thị của người sử dụng không hề nghi ngờ, kết quả là các hành động tiếp theo của người sử dụng có thể bị sai và dẫn đến lỗ hổng an ninh.

Hình M.1 biểu diễn phân tách của lớp này gồm các thành phần cấu thành nó.



Hình M.1 – Phân cấp lớp FTP: Đường dẫn/kênh tin cậy

M.1 Kênh tin cậy liên-TSF (FTP_ITC)

M.1.1 Chú thích cho người sử dụng

Họ này định nghĩa các quy tắc dành cho việc tạo ra một kết nối kênh truyền được tin cậy chạy giữa TSF và một sản phẩm IT được tin cậy khác để đảm bảo hiệu năng của các thao tác an ninh then chốt giữa các sản phẩm. Một ví dụ của một thao tác an ninh then chốt như vậy là việc cập nhật cơ sở dữ liệu xác thực TSF bởi việc chuyển giao dữ liệu từ một sản phẩm được tin cậy mà chức năng của nó là thu thập dữ liệu kiểm toán.

M.1.2 FTP_ITC.1 Kênh tin cậy liên TSF

M.1.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này nên được sử dụng khi yêu cầu một kênh truyền thông được tin cậy giữa TSF và một sản phẩm IT được tin cậy khác.

M:1.2.2 Các hoạt động

M.1.2.2.1 Phép chọn

Trong FTP_ITC.1.2, tác giả PP/ST phải xác định xem liệu TSF cục bộ hay sản phẩm IT được tin cậy ở xa hay cả hai sẽ có khả năng khởi phát kênh truyền được tin cậy.

M.1.2.2.2 Chỉ định

Trong FTP_ITC.1.3, tác giả PP/ST nên xác định các chức năng yêu cầu một kênh truyền được tin cậy. Các ví dụ về các chức năng này có thể bao gồm việc chuyển giao người sử dụng, chủ thể và/hoặc các thuộc tính an ninh đối tượng và đảm bảo tính nhất quán của dữ liệu TSF.

M.2 Đường dẫn tin cậy (FTP_TRP)

M.2.1 Chú thích cho người sử dụng

Họ này định nghĩa các yêu cầu để thiết lập và duy trì việc truyền thông được tin cậy đến và đi khỏi người sử dụng và TSF. Một đường truyền được tin cậy có thể được yêu cầu đối với bất kỳ tương tác liên quan tới an ninh nào. Việc trao đổi đường truyền được tin cậy có thể được khởi phát bởi một người sử dụng trong suốt thời gian tương tác với TSF, hoặc TSF có thể thiết lập truyền thông với người sử dụng thông qua một đường truyền được tin cậy.

M.2.2 FTP_TRP.1 Đường dẫn tin cậy

M.2.2.1 Chú thích cho ứng dụng người sử dụng

Thành phần này nên được sử dụng khi việc truyền thông được tin cậy giữa một người sử dụng và TSF được yêu cầu, hoặc là chỉ dành cho các mục đích xác thực ban đầu hoặc là dành cho các thao tác bổ sung của người sử dụng xác định.

M.2.2.2 Các hoạt động

M.2.2.2.1 Phép chọn

Trong FTP_TRP.1.1, tác giả PP/ST nên xác định liệu đường truyền được tin cậy có phải được mở rộng cho người sử dụng ở xa và/hoặc người sử dụng cục bộ hay không.

Trong FTP_TRP.1.1, tác giả PP/ST nên xác định sẽ bảo vệ dữ liệu không bị sửa đổi, để lộ và/hoặc các kiểu vi phạm tính toàn vẹn và tin cậy khác

M.2.2.2.2 Chỉ định

Trong FTP_TRP.1.1, nếu được lựa chọn, tác giả PP/ST nên xác định bất cứ kiểu bổ sung vi phạm tính toàn vẹn và tin cậy nào trước việc đường dẫn tin cậy sẽ bảo vệ dữ liệu.

M.2.2.2.3 Phép chọn

Trong FTP_TRP.1.2, tác giả PP/ST nên chỉ rõ TSF, người dùng nội bộ, và hoặc người dùng từ xa có thể bắt đầu đường dẫn thế nào.

Trong FTP_TRP.1.3, Tác giả PP/ST nên chỉ rõ đường dẫn tin cậy sẽ được sử dụng cho xác thực người dùng đầu tiên và /hoặc cho các dịch vụ cụ thể khác.

M.2.2.2.4 Chỉ định

Trong FTP_TRP.1.3, nếu được lựa chọn, tác giả PP/ST nên xác định các dịch vụ khác mà nếu cần sẽ yêu cầu đường dẫn tin cậy cho các dịch vụ này.