1. **Introduction**

GlobalPlatform là một tổ chức được thành lập bởi các công ty hàng đầu trong ngành thanh toán và truyền thông, khu vực chính phủ và cộng đồng nhà cung cấp, và là tổ chức đầu tiên thúc đẩy cơ sở hạ tầng toàn cầu để triển khai thẻ thông minh trên nhiều ngành.

Mục tiêu:

Thông số kỹ thuật thẻ GlobalPlatform nhằm mục tiêu cho phép người dùng sử dụng thẻ thông minh cho nhiều chức năng khác nhau một cách an toàn, hiệu quả và tiết kiệm chi phí.

Lịch sử:

Từ giữa những năm 1990, ngành công nghiệp thẻ chip đã chứng kiến ​​sự ra đời của các thông số kỹ thuật hệ thống mở như Java Card™ và MULTOS™, tạo nền tảng cho thẻ chip đa ứng dụng.

Năm 2001, NICSS đã định nghĩa một khuôn khổ quản lý nội dung thẻ dựa trên PKI dành riêng cho thị trường chính phủ.

GlobalPlatform, dựa trên sáng kiến ​​Nền tảng mở của Visa International, đã hợp tác với ngành công nghiệp thẻ chip để phát triển một tiêu chuẩn quản lý thẻ trung lập với phần cứng, nhà cung cấp và ứng dụng.

Kiến trúc và Chức năng

Thông số kỹ thuật GlobalPlatform cung cấp:

Kiến trúc quản lý thẻ và bảo mật chung: Bảo vệ cơ sở hạ tầng thẻ chip.

Khả năng di chuyển công nghệ: Cho phép chuyển đổi sang công nghệ thẻ khác trong tương lai mà không ảnh hưởng đến cơ sở hạ tầng.

Hỗ trợ mật mã: Cung cấp chức năng mã hóa tối thiểu cho việc tạo chữ ký và sử dụng bởi các ứng dụng trên thẻ.

Quản lý vòng đời ứng dụng: Bao gồm các quy trình tải, cài đặt, kích hoạt, khóa, xóa và chấm dứt ứng dụng.

Hệ thống quản lý thẻ: Giúp quản lý an toàn nội dung thẻ.

Cơ chế bảo mật: Sử dụng các kỹ thuật như mã hóa, xác thực và quản lý khóa.

Giao thức kênh bảo mật: Đảm bảo an toàn cho việc giao tiếp giữa thẻ và các thiết bị bên ngoài.

1. **Kiến trúc hệ thống**

(mô tả chi tiết về cấu trúc và cách thức hoạt động của thẻ chip, đặc biệt tập trung vào vai trò then chốt của Miền bảo mật.)

Việc triển khai thẻ chip đa ứng dụng, công nghệ động cũng giống như triển khai một lượng lớn máy trạm trong mạng lưới bán kết nối. Điểm tương đồng này cho thấy thẻ chip có khả năng lưu trữ và xử lý nhiều ứng dụng cùng lúc, đồng thời cho phép cập nhật, xóa và cài đặt ứng dụng mới.

Kiến trúc GlobalPlatform được thiết kế để cung cấp cho Ngân hàng Phát hành Thẻ một hệ thống quản lý thẻ thông minh hiệu quả.

Mặc dù GlobalPlatform dựa trên mô hình chỉ có một Ngân hàng Phát hành Thẻ duy nhất cho mỗi thẻ, nhưng nó cũng mang lại sự linh hoạt cho Ngân hàng Phát hành Thẻ trong việc quản lý một loạt đối tác kinh doanh luôn thay đổi, những người có thể muốn chạy ứng dụng trên thẻ của Ngân hàng Phát hành Thẻ.

GlobalPlatform trao cho Ngân hàng Phát hành Thẻ quyền kiểm soát tối cao đối với thẻ của họ bằng cách cho phép họ chia sẻ quyền kiểm soát một phần thẻ với các đối tác kinh doanh. Tuy nhiên, quyền kiểm soát cuối cùng vẫn luôn thuộc về Ngân hàng Phát hành Thẻ.

Thông qua GlobalPlatform, các đối tác kinh doanh của Ngân hàng Phát hành Thẻ có thể được phép quản lý các ứng dụng của riêng họ trên thẻ của Ngân hàng Phát hành Thẻ một cách phù hợp.

1. **Kiến trúc thẻ**

Kiến trúc thẻ GlobalPlatform bao gồm nhiều thành phần đảm bảo giao diện trung lập với phần cứng và nhà cung cấp cho các ứng dụng và hệ thống quản lý ngoài thẻ.

Mọi ứng dụng đều được triển khai trong môi trường thời gian chạy an toàn, bao gồm API trung lập với phần cứng để hỗ trợ tính di động của ứng dụng. GlobalPlatform không yêu cầu công nghệ môi trường thời gian chạy cụ thể.

Trình quản lý thẻ (Card Manager) là thành phần thẻ GlobalPlatform chính, hoạt động như người quản trị trung tâm cho thẻ GlobalPlatform. Các ứng dụng quản lý khóa và bảo mật đặc biệt được gọi là Miền bảo mật được tạo ra để đảm bảo sự tách biệt hoàn toàn các khóa giữa Bên phát hành thẻ và nhiều nhà cung cấp Miền bảo mật khác.

Cấu hình mẫu của thẻ bao gồm:

•Một hoặc nhiều ứng dụng từ Bên phát hành thẻ.

•Một hoặc nhiều ứng dụng từ một trong các đối tác kinh doanh của Bên phát hành thẻ, được gọi là Nhà cung cấp ứng dụng.

•Một hoặc nhiều ứng dụng cung cấp dịch vụ chung (ví dụ: dịch vụ CVM) cho các ứng dụng khác**.**

**3.1**

Miền bảo mật: Trái tim của hệ thống bảo mật

Miền bảo mật là yếu tố cốt lõi trong kiến trúc hệ thống của thẻ chip. Nó được ví như một "người gác cổng" đáng tin cậy, chịu trách nhiệm quản lý mọi hoạt động liên quan đến bảo mật và ủy quyền trên thẻ. Mỗi Miền bảo mật được thiết lập riêng cho từng thực thể, đảm bảo sự tách biệt và độc lập giữa các ứng dụng và dữ liệu

Mỗi Miền bảo mật được thiết lập thay mặt cho một trong các thực thể sau:

•Tổ chức phát hành thẻ

•Nhà cung cấp ứng dụng

•Cơ quan kiểm soát

Chức năng chính của Miền bảo mật

•Quản lý khóa: Mỗi Miền bảo mật tự quản lý khóa riêng, bao gồm tạo, lưu trữ, sử dụng khóa cho mã hóa, giải mã, và xác minh chữ ký số.

•Cung cấp dịch vụ bảo mật: Miền bảo mật cung cấp các dịch vụ bảo mật cho ứng dụng, như xử lý khóa, mã hóa, giải mã, tạo và xác minh chữ ký số.

•Xác minh DAP: Miền bảo mật sử dụng cơ chế Xác minh Mẫu Xác thực Dữ liệu (DAP) để đảm bảo tính xác thực của Khối dữ liệu tệp tải

3.2:

3.3 : Runtime Environment

Môi trường Thời chạy (RTE) của GlobalPlatform được thiết kế để hoạt động trên bất kỳ môi trường thời chạy thẻ an toàn, đa ứng dụng nào. RTE có các trách nhiệm chính sau:

* Cung cấp một API trung lập phần cứng cho các ứng dụng. Điều này cho phép các ứng dụng được chuyển đổi giữa các loại thẻ khác nhau mà không cần sửa đổi code.
* Cung cấp không gian lưu trữ và thực thi an toàn cho các ứng dụng. Điều này đảm bảo rằng code và dữ liệu của mỗi ứng dụng được bảo vệ và cách ly khỏi các ứng dụng khác trên thẻ.
* Cung cấp dịch vụ giao tiếp giữa thẻ và các thực thể bên ngoài. Điều này bao gồm việc truyền tải các lệnh và phản hồi một cách an toàn và đáng tin cậy.

Tóm lại, RTE đóng vai trò quan trọng trong việc cung cấp một môi trường hoạt động an toàn và hiệu quả cho các ứng dụng trên thẻ GlobalPlatform.

3.4: Trusted Framework

Thẻ GlobalPlatform có thể chứa một hoặc nhiều Khung Tin cậy (Trusted Frameworks) để cung cấp dịch vụ giao tiếp giữa các Ứng dụng. Khung Tin cậy không phải là Ứng dụng hay Miền Bảo mật, mà là một phần mở rộng đặc biệt của môi trường thời chạy của thẻ (card’s run-time environment).

3.5 : GlobalPlatform Environment (OPEN)

**Môi trường GlobalPlatform (OPEN) đóng vai trò quản lý trung tâm trên thẻ**, cung cấp nhiều chức năng quan trọng nếu môi trường thời chạy (RTE) không hỗ trợ hoặc không tuân thủ theo tiêu chuẩn GlobalPlatform.

* **OPEN cung cấp API cho ứng dụng, phân phối lệnh, lựa chọn ứng dụng, quản lý kênh logic (tùy chọn) và quản lý nội dung thẻ (Card Content management)**.
* OPEN chịu trách nhiệm tải code ứng dụng, quản lý nội dung thẻ, và quản lý bộ nhớ.
* OPEN quản lý việc cài đặt ứng dụng được tải lên thẻ và đảm bảo việc thực thi các nguyên tắc bảo mật được xác định cho quản lý nội dung thẻ.

**Một chức năng quan trọng khác của OPEN là phân phối lệnh APDU và lựa chọn ứng dụng:**

* Khi lệnh SELECT được xử lý thành công, OPEN sẽ đặt ứng dụng được tham chiếu trong lệnh SELECT thành ứng dụng được chọn, và các lệnh tiếp theo sẽ được chuyển đến ứng dụng đã chọn.

**Kênh logic (logical channels) cung cấp khả năng chọn nhiều ứng dụng đồng thời.**

* OPEN dựa vào RTE để kiểm soát việc một ứng dụng có thể được chọn đồng thời với chính nó hoặc ứng dụng khác hay không.
* Khi hỗ trợ kênh logic, OPEN cho phép cả ứng dụng không có khái niệm về kênh logic và ứng dụng hỗ trợ đa lựa chọn (multi-selectable).
* Việc hỗ trợ kênh logic là tùy chọn, và thẻ có thể hỗ trợ một hoặc nhiều kênh logic bổ sung (Supplementary Logical Channels) (tối đa 19 kênh theo tiêu chuẩn ISO 7816-4).

**OPEN sở hữu và sử dụng GlobalPlatform Registry - một cơ sở dữ liệu nội bộ dùng để quản lý nội dung thẻ.** GlobalPlatform Registry chứa thông tin để quản lý thẻ, tệp tải thực thi (Executable Load Files), ứng dụng, liên kết miền bảo mật và đặc quyền.

3.6 GlobalPlatform API

API GlobalPlatform cung cấp các dịch vụ cho Ứng dụng (ví dụ: xác minh Chủ thẻ, cá nhân hóa hoặc dịch vụ bảo mật). API này cũng cung cấp các dịch vụ quản lý Nội dung thẻ (ví dụ: khóa thẻ hoặc cập nhật Trạng thái vòng đời ứng dụng) cho Ứng dụng.

3.7 Card Content

**Nội dung Thẻ (Card Content)** trong thẻ GlobalPlatform được định nghĩa trong phần 3.7 của tài liệu. **Tất cả Nội dung Thẻ ban đầu đều được lưu trữ dưới dạng Tệp Tải Thực thi (Executable Load File)**.

* Tệp Tải Thực thi có thể tồn tại ở **Bộ nhớ Khó thay đổi (Immutable Persistent Memory)** hoặc **Bộ nhớ Dễ thay đổi (Mutable Persistent Memory)**.
  + Nếu nằm trong Bộ nhớ Khó thay đổi, tệp được tải trong quá trình sản xuất và không thể thay đổi (ngoại trừ việc bị vô hiệu hóa).
  + Nếu nằm trong Bộ nhớ Dễ thay đổi, tệp có thể được tải lên hoặc xóa bỏ trong giai đoạn **Tiền Phát hành (Pre-Issuance)** hoặc **Hậu Phát hành (Post-Issuance)**.
* Mỗi Tệp Tải Thực thi có thể chứa **một hoặc nhiều Mô-đun Thực thi (Executable Modules)**, là mã ứng dụng.

**Quá trình cài đặt và quản lý nội dung thẻ được thực hiện bởi Môi trường GlobalPlatform (OPEN)**, như đã thảo luận trong phần 3.5 của tài liệu và trong lịch sử hội thoại của chúng ta. OPEN đảm bảo các nguyên tắc bảo mật được thực thi trong quá trình quản lý nội dung thẻ.

3.8 Card Manager

Card Manager là một thuật ngữ chung cho các thực thể quản lý thẻ của thẻ GlobalPlatform. Card Manager được chia thành ba thực thể riêng biệt:

* The GlobalPlatform Environment (OPEN)
* The Issuer Security Domain
* Cardholder Verification Method Services

1. **Security Architecture**

**4.1 Goals**

Mục tiêu chính của kiến trúc bảo mật GlobalPlatform là đảm bảo tính bảo mật và toàn vẹn của các thành phần thẻ trong suốt vòng đời của thẻ. Điều này có nghĩa là các thành phần thẻ phải được bảo vệ khỏi các cuộc tấn công, sửa đổi trái phép và đảm bảo hoạt động đáng tin cậy.

Các thành phần thẻ bao gồm:

•Môi trường thời chạy (Runtime Environment): Đảm bảo môi trường thực thi an toàn cho tất cả các ứng dụng trên thẻ.

•Môi trường GlobalPlatform (OPEN): Cung cấp các dịch vụ quản lý ứng dụng và thẻ an toàn.

•Miền bảo mật của nhà phát hành (Issuer Security Domain): Quản lý khóa và đảm bảo an ninh cho toàn bộ thẻ.

•Các Miền bảo mật bổ sung (Supplementary Security Domains): Cung cấp các dịch vụ bảo mật bổ sung cho các ứng dụng.

•Các ứng dụng (Applications): Thực hiện các chức năng cụ thể của thẻ.

Để đạt được mục tiêu bảo mật, GlobalPlatform hỗ trợ nhiều cơ chế bảo mật, bao gồm:

•Toàn vẹn dữ liệu (Data Integrity): Đảm bảo dữ liệu không bị sửa đổi trái phép.

•Khả dụng tài nguyên (Resource Availability): Đảm bảo các tài nguyên thẻ luôn sẵn sàng cho các ứng dụng được ủy quyền.

•Bảo mật (Confidentiality): Bảo vệ dữ liệu bí mật khỏi bị truy cập trái phép.

•Xác thực (Authentication): Xác minh danh tính của các thực thể tham gia vào hệ thống.

**4.2 Security Responsibilities and Requirements**

**Trách nhiệm và yêu cầu bảo mật**

Phần 4.2 đi sâu vào phân tích trách nhiệm bảo mật của các bên tham gia trong hệ thống GlobalPlatform, bao gồm Nhà phát hành thẻ, Nhà cung cấp ứng dụng, Cơ quan Kiểm soát, cũng như các yêu cầu bảo mật cho các thành phần trên thẻ và hệ thống Back-end.

### **4.2.1 Trách nhiệm Bảo mật của Nhà phát hành Thẻ (Card Issuer)**

Nhà phát hành thẻ, với vai trò chủ sở hữu thẻ, chịu trách nhiệm chính trong việc đảm bảo tính bảo mật của thẻ. Các trách nhiệm chính của Nhà phát hành thẻ bao gồm:

* **Tạo và tải khóa Miền bảo mật của Nhà phát hành (Issuer Security Domain keys).**
* **Thiết lập và thực thi các tiêu chuẩn và chính sách bảo mật cho Nhà cung cấp ứng dụng**, bao gồm tất cả các khía cạnh của ứng dụng được cung cấp cho Nhà phát hành thẻ hoặc hoạt động trên thẻ.
* **Phối hợp với Nhà cung cấp ứng dụng để tạo và khởi tạo các Miền bảo mật bổ sung.**
* **Xác định chính sách quản lý vòng đời thẻ và ứng dụng**, kiểm tra tốc độ giao dịch, mức độ bảo mật, đặc quyền và các thông số bảo mật khác.
* **Quản lý việc tải và cài đặt mã ứng dụng** trong cả giai đoạn Tiền phát hành và Hậu phát hành.
* **Cấp phép mã hóa cho các hoạt động tải, cài đặt và trích xuất dữ liệu** do Nhà cung cấp ứng dụng thực hiện.

### **4.2.2 Trách nhiệm Bảo mật của Nhà cung cấp Ứng dụng (Application Provider)**

Nhà cung cấp ứng dụng chịu trách nhiệm về tính bảo mật của ứng dụng. Các trách nhiệm chính bao gồm:

* **Tạo khóa cho Miền bảo mật của mình** hoặc lấy khóa từ một bên thứ ba đáng tin cậy.
* **Phối hợp với Nhà phát hành thẻ để tải khóa đã tạo vào Miền bảo mật của Nhà cung cấp ứng dụng.**
* **Cung cấp ứng dụng đáp ứng các tiêu chuẩn và chính sách bảo mật của Nhà phát hành thẻ.**
* **Cung cấp chữ ký khối dữ liệu tệp tải (Load File Data Block)** theo chính sách bảo mật riêng để đảm bảo tính toàn vẹn và xác thực nguồn gốc.
* **Xin phép trước từ Nhà phát hành thẻ** cho các hoạt động tải, cài đặt và trích xuất dữ liệu.
* **Cung cấp biên nhận cho các hoạt động tải, cài đặt, xóa và trích xuất dữ liệu** theo chính sách của Nhà phát hành thẻ.

### **4.2.3 Trách nhiệm Bảo mật của Cơ quan Kiểm soát (Controlling Authority)**

Cơ quan Kiểm soát có trách nhiệm thực thi các chính sách bảo mật off-card và on-card. Các trách nhiệm chính bao gồm:

* **Tạo khóa cho Miền bảo mật của mình** hoặc lấy khóa từ một bên thứ ba đáng tin cậy.
* **Phối hợp với Nhà phát hành thẻ để tải khóa đã tạo vào Miền bảo mật của Cơ quan Kiểm soát.**
* **Đảm bảo rằng các ứng dụng tuân thủ các chính sách bảo mật đã được thiết lập.**
* **Cung cấp chữ ký cho Khối dữ liệu ứng dụng (DAP - Delegated Application Package)** để đảm bảo tính toàn vẹn và xác thực nguồn gốc.

### **4.2.4 Yêu cầu Bảo mật cho các Thành phần trên Thẻ (On-Card Components)**

Phần này nêu chi tiết các yêu cầu bảo mật cho từng thành phần trên thẻ, nhằm đảm bảo an ninh cho toàn bộ hệ thống thẻ. Các thành phần bao gồm:

* **Môi trường thời chạy (Runtime Environment):** Yêu cầu bảo vệ **tính toàn vẹn và tính bảo mật** của môi trường thời chạy, **quản lý bộ nhớ an toàn**, **cung cấp giao tiếp an toàn** với các thực thể off-card và **hỗ trợ cho việc kết thúc phiên giao tiếp** an toàn.
* **Khung tin cậy (Trusted Framework):** Yêu cầu **kiểm tra các quy tắc truy cập ứng dụng**, **thực thi các quy tắc bảo mật** cho giao tiếp giữa các ứng dụng và **đảm bảo định tuyến tin nhắn an toàn**.
* **Môi trường GlobalPlatform (OPEN):** Yêu cầu bảo vệ **tính toàn vẹn** của OPEN, **kiểm tra các quy tắc truy cập ứng dụng**, **quản lý vòng đời thẻ và ứng dụng**, **đảm bảo ủy quyền** cho các thay đổi nội dung thẻ và **xác minh chữ ký mã ứng dụng**.
* **Miền bảo mật (Security Domain):** Yêu cầu **giao tiếp an toàn** với các thực thể off-card, **quản lý dữ liệu an toàn**, **cung cấp dịch vụ bảo mật** cho ứng dụng trong quá trình cá nhân hóa, **yêu cầu OPEN thực hiện các hoạt động quản lý nội dung thẻ** và **xác minh ủy quyền** cho các thay đổi nội dung thẻ.
* **Ứng dụng dịch vụ toàn cầu (Global Services Application):** Yêu cầu **cung cấp dịch vụ cho các ứng dụng khác** một cách an toàn, **lưu trữ dữ liệu an toàn** và **thực hiện các biện pháp bảo mật nội bộ**.
* **Ứng dụng (Application):** Khuyến nghị **giới hạn quyền truy cập dữ liệu và tài nguyên** cho các chức năng cần thiết và **thực hiện các biện pháp bảo mật nội bộ** theo yêu cầu của Nhà cung cấp ứng dụng.

### **4.2.5 Yêu cầu Bảo mật cho Hệ thống Back-end (Back-End System)**

Hệ thống Back-end cũng đóng vai trò quan trọng trong việc đảm bảo tính bảo mật của toàn bộ hệ thống. Mặc dù thẻ và quy trình tải đã được thiết kế để cung cấp một môi trường ổn định và an toàn, nhưng **bảo mật hoàn toàn không thể được đảm bảo nếu không có hệ thống Back-end đáng tin cậy.**

**Tóm lại, phần 4.2 nhấn mạnh tầm quan trọng của việc phân chia trách nhiệm bảo mật rõ ràng giữa các bên tham gia trong hệ thống GlobalPlatform.** Việc tuân thủ các yêu cầu bảo mật cho cả thành phần trên thẻ và hệ thống Back-end là điều kiện tiên quyết để đảm bảo an ninh cho toàn bộ hệ thống.

**4.3 Cryptographic Support**

Phần 4.3 tập trung vào khả năng hỗ trợ mã hóa, một yêu cầu quan trọng đối với thẻ GlobalPlatform. Khả năng này được sử dụng cho nhiều mục đích, bao gồm tạo chữ ký và được cung cấp cho các ứng dụng trên thẻ.

Miền bảo mật của nhà phát hành (Issuer Security Domain) phải triển khai ít nhất một Giao thức Kênh Bảo mật (Secure Channel Protocol), trong khi các Miền bảo mật bổ sung (Supplementary Security Domains) phải triển khai ít nhất một giao thức.

Thẻ GlobalPlatform nên hỗ trợ mã hóa đối xứng, chẳng hạn như thuật toán DES hoặc AES. Thẻ có thể hỗ trợ thêm mã hóa bất đối xứng, như thuật toán RSA hoặc mã hóa đường cong elliptic (ECC).

### Các dịch vụ mã hóa được mô tả trong phần này bao gồm:

* Toàn vẹn và xác thực (Integrity and authentication): Đảm bảo dữ liệu không bị thay đổi trái phép và xác minh nguồn gốc.
* Nhắn tin an toàn (Secure messaging): Bảo vệ tính bảo mật và toàn vẹn của các tin nhắn được trao đổi.

Nếu được cung cấp, các dịch vụ mã hóa và giải mã cho bất kỳ dữ liệu nào bằng các thuật toán này phải khả dụng cho các ứng dụng.

Nhà phát hành thẻ và/hoặc Cơ quan kiểm soát có trách nhiệm thiết lập các quy trình off-card phù hợp để tuân thủ các hạn chế của chính phủ về mã hóa. Đặc tả kỹ thuật này không đề cập đến các tính năng để vô hiệu hóa hoặc hạn chế việc sử dụng mã hóa bởi các ứng dụng trên thẻ.

### 4.3.1 Quản lý Nội dung Thẻ An toàn (Secure Card Content Management)

Khái niệm về toàn vẹn và xác thực (integrity and authentication) đại diện cho một giá trị bổ sung được liên kết với một tin nhắn hoặc một khối dữ liệu.

Mục đích của giá trị bổ sung này là cung cấp phương pháp xác minh nguồn gốc và/hoặc tính toàn vẹn của thông điệp.

### 1. Load File Data Block Hash (LFDBH)

* Mục đích: Xác minh tính toàn vẹn của toàn bộ Khối dữ liệu tệp tải (Load File Data Block) khi được tải lên thẻ GlobalPlatform.
* Cách thức: Bằng cách tạo ra một giá trị băm (hash) duy nhất từ khối dữ liệu. Bất kỳ thay đổi nào đối với dữ liệu sẽ dẫn đến thay đổi giá trị băm, cho phép phát hiện các sửa đổi trái phép.
* Sử dụng trong:
  + Tính toán Chữ ký Khối dữ liệu tệp tải (Load File Data Block Signature - DAP)
  + Tính toán Mã thông báo tải (Load Token)
* Bắt buộc khi:
  + Có Mã thông báo (Token) hoặc Khối DAP trong tệp tải
  + Khối dữ liệu tệp tải được mã hóa
* Tùy chọn khi: Không có Token, DAP Block, hoặc mã hóa.
* Kiểm tra tính hợp lệ: Nếu LFDBH có trong tệp tải, nó phải được kiểm tra.

### 2. Load File Data Block Signature (DAP)

* Mục đích: Xác thực Khối dữ liệu tệp tải trước khi xử lý nội dung thực tế của nó.
* Cách thức: Là chữ ký của LFDBH, được tạo bởi một thực thể off-card (Nhà cung cấp ứng dụng hoặc Cơ quan xác minh). Chữ ký này được bao gồm trong Khối DAP của tệp tải.
* Yêu cầu: Miền bảo mật phải có đặc quyền Xác minh DAP (DAP Verification) và được cá nhân hóa với khóa thích hợp.
* Kiểm tra tính hợp lệ: Mỗi chữ ký trong Khối DAP phải được xác minh bởi Miền bảo mật thích hợp khi được trình bày trong quá trình tải tệp lên thẻ.

### 3. Delegated Management Tokens

* Mục đích: Ủy quyền cho Nhà cung cấp ứng dụng thực hiện các hoạt động quản lý nội dung thẻ.
* Cách thức: Chữ ký của một hoặc nhiều chức năng quản lý được ủy quyền (tải, cài đặt, trích xuất và xóa). Được tạo bởi Nhà phát hành thẻ và được sử dụng để cung cấp cho Nhà phát hành thẻ khả năng kiểm soát việc thay đổi nội dung thẻ.
* Kiểm tra tính hợp lệ: Được xác minh trên thẻ bởi Miền bảo mật thích hợp (Token Verification).

### 4. Receipts

* Mục đích: Cung cấp xác nhận rằng một hoạt động quản lý được ủy quyền đã được thực hiện thành công.
* Cách thức: Một giá trị mã hóa do thẻ cung cấp (nếu được yêu cầu bởi Nhà phát hành thẻ).

### 4.3.2 Giao tiếp An toàn (Secure Communication)

Giao tiếp an toàn được thiết lập bằng cách sử dụng Kênh Bảo mật (Secure Channel). Giao thức Kênh Bảo mật xác định các cơ chế bảo mật sẽ được sử dụng giữa một thực thể off-card và một miền bảo mật trên thẻ.

Giao thức cung cấp các dịch vụ sau:

* Xác thực lẫn nhau (Mutual authentication)
* Bảo vệ tính bảo mật (Confidentiality protection)
* Bảo vệ tính toàn vẹn (Integrity protection)

cho các tin nhắn APDU (Application Protocol Data Unit) được trao đổi trên Kênh Logic cơ bản hoặc bổ sung. Việc xử lý lệnh bởi ứng dụng nằm ngoài phạm vi của đặc tả kỹ thuật này.

1. **Mô hình Vòng đời (Life Cycle Models)**

Phần 5 của tài liệu giới thiệu về các mô hình vòng đời được sử dụng để kiểm soát chức năng và bảo mật của các thành phần GlobalPlatform, bao gồm:

* Thẻ (Card)
* Tệp Tải Thực thi (Executable Load Files)
* Mô-đun Thực thi (Executable Modules)
* Miền Bảo mật (Security Domains)
* Ứng dụng (Applications)

OPEN chịu trách nhiệm duy trì thông tin vòng đời trong Sổ đăng ký GlobalPlatform (GlobalPlatform Registry) và quản lý các yêu cầu chuyển đổi trạng thái.

Mỗi thành phần có một mô hình vòng đời riêng biệt, thể hiện các trạng thái và quá trình chuyển đổi giữa chúng.

### 5.1 Vòng đời Thẻ (Card Life Cycle)

OPEN chịu trách nhiệm duy trì bảo mật và quản trị tổng thể của thẻ và nội dung của nó. Vòng đời thẻ bắt đầu với trạng thái OP\_READY (sẵn sàng hoạt động) và kết thúc ở trạng thái TERMINATED (đã chấm dứt).

#### Các trạng thái chính của thẻ:

* OP\_READY: Môi trường runtime sẵn sàng, Miền bảo mật của Nhà phát hành sẵn sàng nhận, thực thi và phản hồi các lệnh APDU.
* INITIALIZED: Thẻ đã được khởi tạo nhưng chưa được cá nhân hóa với các khóa bảo mật.
* SECURED: Thẻ đã được cá nhân hóa với các khóa bảo mật và sẵn sàng để sử dụng.
* CARD\_LOCKED: Tất cả chức năng của thẻ bị vô hiệu hóa, ngoại trừ Ứng dụng Cuối cùng (Final Application) nếu có.
* TERMINATED: Thẻ bị vô hiệu hóa vĩnh viễn và không thể sử dụng được nữa.

Các trạng thái chuyển đổi được thể hiện trong Hình 5-1.

### 5.2 Vòng đời Tệp Tải Thực thi / Mô-đun Thực thi (Executable Load File/ Executable Module Life Cycle)

Tệp Tải Thực thi chứa mã thực thi của một hoặc nhiều ứng dụng (Mô-đun Thực thi). OPEN sở hữu và duy trì thông tin vòng đời của Tệp Tải Thực thi trong Sổ đăng ký GlobalPlatform.

* Tệp Tải Thực thi chỉ có một trạng thái là LOADED (đã tải), cho biết tệp đã được tải lên thẻ và thông tin của nó có trong Sổ đăng ký.
* Mô-đun Thực thi có vòng đời gắn liền với Tệp Tải Thực thi. Nó chuyển sang trạng thái INSTANTIATED (đã khởi tạo) khi được tạo ra từ Mô-đun Thực thi trong Tệp Tải Thực thi.

### 5.3 Vòng đời Ứng dụng và Miền Bảo mật (Application and Security Domain Life Cycle)

Vòng đời của Ứng dụng hoặc Miền Bảo mật bắt đầu khi ứng dụng được khởi tạo từ Mô-đun Thực thi.

OPEN kiểm soát trạng thái ban đầu của Ứng dụng và Miền Bảo mật (INSTALLED, SELECTABLE) và có thể khóa hoặc xóa chúng. Ứng dụng tự quản lý các trạng thái tiếp theo của nó.

#### Các trạng thái chính của Ứng dụng:

* INSTALLED: Ứng dụng đã được cài đặt nhưng chưa sẵn sàng để lựa chọn.
* SELECTABLE: Ứng dụng sẵn sàng để lựa chọn và sử dụng.
* LOCKED: Ứng dụng bị khóa và không thể lựa chọn hoặc sử dụng được.

Ứng dụng cũng có thể có các trạng thái riêng, không do OPEN kiểm soát.

#### Các trạng thái chính của Miền Bảo mật:

* INSTALLED: Miền Bảo mật đã được cài đặt nhưng chưa sẵn sàng để lựa chọn.
* SELECTABLE: Miền Bảo mật sẵn sàng để lựa chọn.
* PERSONALIZED: Miền Bảo mật đã được cá nhân hóa với các khóa bảo mật.
* LOCKED: Miền Bảo mật bị khóa và không thể lựa chọn hoặc sử dụng được.

Hình 5-2 và 5-3 minh họa các trạng thái chuyển đổi của Ứng dụng và Miền Bảo mật.

### 5.4 Minh họa Vòng đời (Sample Life Cycle Illustration)

Phần này cung cấp một ví dụ về vòng đời của một thẻ GlobalPlatform từ khi tạo đến khi kết thúc, cùng với trạng thái của các Tệp Tải Thực thi, Mô-đun Thực thi và Ứng dụng. Hình 5-4 minh họa ví dụ này.

### Tóm tắt:

Phần 5 trình bày chi tiết về các mô hình vòng đời của các thành phần GlobalPlatform, bao gồm Thẻ, Tệp Tải Thực thi, Mô-đun Thực thi, Miền Bảo mật và Ứng dụng. Mỗi mô hình vòng đời bao gồm các trạng thái và quá trình chuyển đổi giữa chúng, giúp đảm bảo tính bảo mật và kiểm soát chặt chẽ đối với nội dung và hoạt động của thẻ.

1. **GlobalPlatform Environment (OPEN)**

**Môi trường GlobalPlatform (OPEN)** là một thành phần quan trọng trên thẻ GlobalPlatform, đóng vai trò là **quản trị trung tâm**, chịu trách nhiệm quản lý và điều phối các hoạt động trên thẻ. Phần 6 của tài liệu tập trung mô tả chi tiết về kiến trúc, chức năng và cách thức hoạt động của OPEN.

### **6.1 Tổng quan**

Môi trường GlobalPlatform (OPEN) hoạt động như một hệ thống quản lý trung tâm trên thẻ, chịu trách nhiệm quản lý và điều phối các hoạt động trên thẻ GlobalPlatform. OPEN cung cấp một loạt các chức năng quan trọng, đặc biệt là khi môi trường runtime bên dưới không hỗ trợ đầy đủ các chức năng này.

OPEN thực hiện ba chức năng chính:

* Điều phối Lệnh (Command Dispatch): OPEN nhận và xử lý các lệnh APDU đến từ đầu đọc thẻ. OPEN quyết định ứng dụng hoặc miền bảo mật nào sẽ được chọn để xử lý lệnh. Ngoài ra, OPEN quản lý việc lựa chọn và kích hoạt ứng dụng, cũng như quản lý các kênh logic (tùy chọn).
* Quản lý Nội dung Thẻ (Card Content Management): OPEN xử lý việc tải, cài đặt, cập nhật và xóa bỏ nội dung trên thẻ. Điều này bao gồm quản lý các tệp tải thực thi (Executable Load Files) và các mô-đun thực thi (Executable Modules), đồng thời thực thi các quy tắc kiểm soát truy cập cho việc quản lý nội dung.
* Quản lý Bảo mật (Security Management): OPEN chịu trách nhiệm quản lý trạng thái khóa/mở khóa của miền bảo mật và ứng dụng. OPEN cũng quản lý việc khóa/mở khóa thẻ, chấm dứt hoạt động thẻ và theo dõi việc sử dụng đặc quyền của ứng dụng và miền bảo mật. OPEN cung cấp khả năng kiểm tra trạng thái của nội dung thẻ bằng cách truy xuất thông tin trạng thái liên quan đến bất kỳ ứng dụng nào có trên thẻ. OPEN cũng đảm bảo rằng các hạn chế về tài nguyên được tôn trọng trong quá trình tải và cài đặt nội dung mới cũng như trong quá trình thực thi ứng dụng.

Kiến trúc của OPEN được xây dựng dựa trên Sổ đăng ký GlobalPlatform (GlobalPlatform Registry). Sổ đăng ký này là một kho dữ liệu trung tâm, lưu trữ tất cả thông tin cần thiết cho OPEN để thực hiện các chức năng của mình.

### **6.2 Các dịch vụ OPEN (OPEN Services)**

OPEN cung cấp các dịch vụ cho các ứng dụng trên thẻ, bao gồm:

* Truy vấn trạng thái vòng đời của ứng dụng và thẻ.
* Truy cập vào các dịch vụ của miền bảo mật được liên kết với ứng dụng.
* Chuyển đổi trạng thái vòng đời của thẻ sang CARD\_LOCKED hoặc TERMINATED.
* Cài đặt nội dung của các byte lịch sử (historical bytes) cho thẻ tiếp xúc và thẻ không tiếp xúc Loại A.
* Chuyển đổi trạng thái vòng đời của ứng dụng.
* Truy cập vào thông tin trong Sổ đăng ký GlobalPlatform.
* Truy cập vào các ứng dụng dịch vụ toàn cầu.

### **6.3 Điều phối lệnh (Command Dispatch)**

## **6.3 Điều phối Lệnh (Command Dispatch)**

OPEN đóng vai trò như một **"người điều phối giao thông"** cho các lệnh APDU được gửi đến thẻ.

**Quy trình điều phối lệnh:**

1. **OPEN nhận lệnh:** Tất cả các lệnh được gửi đến thẻ GlobalPlatform sẽ được OPEN xử lý hoặc chuyển tiếp đến ứng dụng đã chọn để xử lý.
2. **Xử lý lệnh SELECT [by name]:** Lệnh SELECT [by name] được OPEN xử lý trực tiếp. Lệnh này được sử dụng để chọn một ứng dụng hoặc miền bảo mật cụ thể trên thẻ.
3. **Chuyển tiếp lệnh:**
   * Lệnh SELECT [by AID] được chuyển tiếp đến ứng dụng được chỉ định bởi AID trong lệnh.
   * Bất kỳ loại lệnh nào khác sẽ được chuyển tiếp đến ứng dụng hiện đang được chọn.

**OPEN xử lý các kênh logic:**

* Lệnh có thể được nhận trên Kênh Logic Cơ bản (số kênh logic 0) hoặc trên Kênh Logic Bổ sung (số kênh logic khác 0).
* Nếu thẻ chỉ hỗ trợ Kênh Logic Cơ bản, lệnh MANAGE CHANNEL sẽ được chuyển tiếp đến ứng dụng hiện đang được chọn.
* Nếu thẻ hỗ trợ kênh logic, OPEN sẽ xử lý lệnh MANAGE CHANNEL để mở hoặc đóng Kênh Logic Bổ sung.

**Ví dụ về hoạt động của OPEN trong việc điều phối lệnh:**

* **Chọn Miền Bảo mật Nhà phát hành:**
  + Một cách để chọn Miền Bảo mật Nhà phát hành là chỉ định AID của nó trong lệnh SELECT với tùy chọn [first or only occurrence].
  + Hoặc, lệnh SELECT có thể không chứa dữ liệu, trong trường hợp này, AID của Miền Bảo mật Nhà phát hành sẽ được sử dụng.
* **Kênh Logic Bổ sung không hợp lệ:**
  + Nếu một lệnh đến trên Kênh Logic Bổ sung chưa được mở, OPEN sẽ trả về lỗi.
* **Tìm kiếm ứng dụng:**
  + Lệnh SELECT [by name] [first or only occurrence] sẽ bắt đầu tìm kiếm từ đầu Sổ đăng ký GlobalPlatform.
  + Lệnh SELECT [by name] [next occurrence] sẽ bắt đầu tìm kiếm từ mục tiếp theo sau ứng dụng hiện đang được chọn trên Kênh Logic Cơ bản trong Sổ đăng ký GlobalPlatform.

**Tóm lại,** OPEN đóng vai trò then chốt trong việc điều phối các lệnh APDU đến thẻ GlobalPlatform bằng cách chuyển tiếp chúng đến đúng ứng dụng hoặc miền bảo mật. OPEN cũng quản lý các kênh logic để hỗ trợ nhiều phiên giao tiếp đồng thời.

### 

### **6.4 Kênh logic và lựa chọn ứng dụng (Logical Channels and Application Selection)**

**6.4.1 Gán Lựa chọn Ngầm:**

* **Miền Bảo mật Nhà phát hành** là ứng dụng có thể chọn ngầm theo mặc định trên tất cả các kênh logic của tất cả các giao diện I/O thẻ được hỗ trợ bởi thẻ.
* **Lựa chọn ngầm trên một kênh logic cụ thể của một giao diện I/O thẻ cụ thể chỉ có thể được gán nếu Miền Bảo mật Nhà phát hành là ứng dụng có thể chọn ngầm trên kênh logic đó của giao diện I/O thẻ đó** và không có Ứng dụng Bị khóa nào khác được đăng ký là có thể chọn ngầm cho cùng một kênh logic và giao diện I/O thẻ.
* **Một Ứng dụng được cài đặt hoặc được chọn với một tham số Lựa chọn Ngầm cụ thể được đăng ký trong Sổ đăng ký GlobalPlatform là ứng dụng có thể chọn ngầm trên (các) kênh logic của (các) giao diện I/O thẻ được chỉ định trong tham số** nếu không có Ứng dụng nào khác (ngoài Miền Bảo mật Nhà phát hành) đã được đăng ký là có thể chọn ngầm trên (các) kênh logic đó của (các) giao diện I/O thẻ đó.
* **Một Ứng dụng được cài đặt và được chọn với đặc quyền Đặt lại Thẻ và không có tham số Lựa chọn Ngầm được đăng ký trong Sổ đăng ký GlobalPlatform là ứng dụng có thể chọn ngầm trên Kênh Logic Cơ bản cho tất cả các giao diện I/O thẻ được hỗ trợ bởi thẻ** nếu không có Ứng dụng nào khác (ngoài Miền Bảo mật Nhà phát hành) đã được đăng ký là có thể chọn ngầm trên Kênh Logic Cơ bản của bất kỳ giao diện I/O thẻ nào.
* **Nếu một Ứng dụng có thể chọn ngầm trên (các) kênh logic cụ thể của (các) giao diện I/O thẻ cụ thể bị xóa, Miền Bảo mật Nhà phát hành sẽ trở thành ứng dụng có thể chọn ngầm trên (các) kênh logic đó của (các) giao diện I/O thẻ đó.**

OPEN sẽ sử dụng đăng ký lựa chọn ngầm của mỗi Ứng dụng để kiểm soát các yêu cầu hành vi thời gian chạy sau:

* **Xác định Ứng dụng có thể chọn ngầm trên Kênh Logic Cơ bản của giao diện I/O thẻ hiện tại trong chuỗi đặt lại hoặc kích hoạt thẻ**
* **Xác định Ứng dụng có thể chọn ngầm khi mở trên giao diện I/O thẻ hiện tại một Kênh Logic Bổ sung mới từ Kênh Logic Cơ bản**

**6.4.2 Kênh Logic Cơ bản:**

Kênh Logic Cơ bản là giao diện khả dụng vĩnh viễn cho thẻ GlobalPlatform. OPEN phải hỗ trợ Kênh Logic Cơ bản này.

**6.4.2.1 Lựa chọn Ứng dụng trên Kênh Logic Cơ bản:**

OPEN phải hỗ trợ lựa chọn Ứng dụng trên Kênh Logic Cơ bản thông qua hai quy trình:

* **Lựa chọn Ngầm sau khi đặt lại thẻ (xem [ISO 7816-3] cho thẻ tiếp xúc) hoặc chuỗi kích hoạt (xem [ISO 14443-3] cho thẻ không tiếp xúc)**
* **Lựa chọn Rõ ràng thông qua lệnh SELECT [theo tên]**

OPEN cũng có thể hỗ trợ các quy trình lựa chọn bổ sung.

**Lựa chọn AID một phần như được định nghĩa trong phần 6.4.2.1.2, Lựa chọn Rõ ràng trên Kênh Logic Cơ bản, phải được hỗ trợ.** (Lựa chọn AID một phần không yêu cầu Thực thể ngoài thẻ phải biết AID đầy đủ.) Vì nhiều Ứng dụng trên thẻ có thể có cùng AID một phần, nên yêu cầu phải có một phương pháp để chọn tất cả các Ứng dụng khớp với AID một phần.

**6.4.2.1.1 Lựa chọn Ngầm trên Kênh Logic Cơ bản:**

Sau khi phiên thẻ được thiết lập (đối với thẻ tiếp xúc theo [ISO 7816-4] sau khi Trả lời Đặt lại hoặc sau chuỗi kích hoạt cho thẻ không tiếp xúc theo [ISO 14443-3]) và trước khi lệnh đầu tiên được phát hành cho thẻ, **Ứng dụng được định nghĩa là có thể chọn ngầm trên Kênh Logic Cơ bản và cho giao diện I/O thẻ đó sẽ trở thành Ứng dụng được chọn trên Kênh Logic Cơ bản cho giao diện I/O thẻ đó.**

Hành vi thời gian chạy:

Các yêu cầu sau đây áp dụng cho OPEN cho quy trình lựa chọn Ứng dụng ngầm:

* Nếu thẻ ở Trạng thái Vòng đời Thẻ CARD\_LOCKED hoặc TERMINATED, Ứng dụng có đặc quyền Ứng dụng Cuối cùng là Ứng dụng được chọn trên Kênh Logic Cơ bản và OPEN sẽ không cố gắng xác định Ứng dụng có thể chọn ngầm.
* Trong mọi trường hợp khác, **OPEN sẽ tìm kiếm trong Sổ đăng ký GlobalPlatform một Ứng dụng được đánh dấu là có thể chọn ngầm trên Kênh Logic Cơ bản cho giao diện I/O thẻ hiện tại (ví dụ: tiếp xúc hoặc không tiếp xúc) và nếu Ứng dụng này không ở Trạng thái Vòng đời Ứng dụng LOCKED, nó sẽ trở thành Ứng dụng được chọn trên Kênh Logic Cơ bản.** Nếu đây là Ứng dụng ở Trạng thái Vòng đời Ứng dụng LOCKED, Ứng dụng có đặc quyền Ứng dụng Cuối cùng sẽ trở thành Ứng dụng được chọn trên Kênh Logic Cơ bản.

**6.4.2.1.2 Lựa chọn Rõ ràng trên Kênh Logic Cơ bản:**

Bất cứ lúc nào trong Phiên Thẻ, OPEN có thể nhận được yêu cầu chọn Ứng dụng trên Kênh Logic Cơ bản (lệnh SELECT [theo tên] [lần xuất hiện đầu tiên hoặc duy nhất]). **OPEN sẽ xác định xem AID được yêu cầu có khớp hoặc khớp một phần với một mục nhập trong Sổ đăng ký GlobalPlatform hay không và liệu mục nhập này có thể chọn được hay không.**

Bất cứ lúc nào trong Phiên Thẻ đã chứa lệnh SELECT [theo tên] [lần xuất hiện đầu tiên hoặc duy nhất], OPEN có thể nhận được yêu cầu chọn Ứng dụng tiếp theo (lệnh SELECT [theo tên] [lần xuất hiện tiếp theo]) trên Kênh Logic Cơ bản. **OPEN sẽ xác định xem AID được yêu cầu có khớp hoặc khớp một phần với một mục nhập khác trong Sổ đăng ký GlobalPlatform hay không và liệu mục nhập này có thể chọn được hay không.**

Đối với cả lệnh SELECT [theo tên] [lần xuất hiện đầu tiên hoặc duy nhất] và lệnh SELECT [theo tên] [lần xuất hiện tiếp theo], **một Ứng dụng sẽ trở thành Ứng dụng được chọn trên Kênh Logic Cơ bản nếu tất cả những điều sau đây đều đúng:**

* AID được yêu cầu khớp (hoàn toàn hoặc một phần) với AID của Ứng dụng.
* Ứng dụng đang được chọn ở Trạng thái Vòng đời Ứng dụng chính xác.
* Ứng dụng không có hạn chế do lựa chọn nhiều và hỗ trợ giao diện thẻ hiện tại.

Hành vi thời gian chạy:

Các yêu cầu sau đây áp dụng cho OPEN trong quy trình lựa chọn Ứng dụng rõ ràng (SELECT [theo tên]) trên Kênh Logic Cơ bản (Hành vi này không áp dụng nếu Trạng thái Vòng đời Thẻ là TERMINATED):

* Trong Trạng thái Vòng đời Thẻ CARD\_LOCKED:
  + Nếu Ứng dụng đang được chọn có đặc quyền Ứng dụng Cuối cùng, Ứng dụng này sẽ được chọn lại và một cảnh báo được trả về cho Thực thể ngoài thẻ.
  + Nếu bất kỳ Ứng dụng nào khác đang được chọn, Ứng dụng có đặc quyền Ứng dụng Cuối cùng vẫn được chọn và một lỗi được trả về cho Thực thể ngoài thẻ.
* Nếu nhận được SELECT [theo tên] [lần xuất hiện đầu tiên hoặc duy nhất] hoặc SELECT [theo tên] [lần xuất hiện tiếp theo] và trường dữ liệu của tin nhắn lệnh không có, **Miền Bảo mật Nhà phát hành sẽ trở thành Ứng dụng được chọn hiện tại và lệnh SELECT được gửi đến Miền Bảo mật Nhà phát hành.**
* Nếu nhận được SELECT [theo tên] [lần xuất hiện đầu tiên hoặc duy nhất], quá trình tìm kiếm luôn bắt đầu từ đầu Sổ đăng ký GlobalPlatform.
* Nếu nhận được SELECT [theo tên] [lần xuất hiện tiếp theo], quá trình tìm kiếm luôn bắt đầu từ mục nhập sau Ứng dụng được chọn hiện tại trên Kênh Logic Cơ bản trong Sổ đăng ký GlobalPlatform.
* Nếu tìm thấy khớp hoàn toàn hoặc một phần và Ứng dụng này ở Trạng thái Vòng đời Ứng dụng INSTALLED, hãy tiếp tục tìm kiếm thông qua Sổ đăng ký GlobalPlatform để tìm kiếm khớp hoàn toàn hoặc một phần tiếp theo. Nếu không tìm thấy khớp hoàn toàn hoặc một phần tiếp theo, OPEN sẽ trả về lỗi thích hợp cho Thực thể ngoài thẻ.
* Nếu tìm thấy khớp hoàn toàn hoặc một phần và Ứng dụng này ở Trạng thái Vòng đời Ứng dụng LOCKED, hãy tiếp tục tìm kiếm thông qua Sổ đăng ký GlobalPlatform để tìm kiếm khớp hoàn toàn hoặc một phần tiếp theo. Trong trường hợp Ứng dụng bị khóa này đã được chọn hiện tại trên Kênh Logic Cơ bản, OPEN sẽ chấm dứt Phiên Ứng dụng này. Nếu không tìm thấy khớp hoàn toàn hoặc một phần tiếp theo, OPEN sẽ trả về lỗi thích hợp cho Thực thể ngoài thẻ.
* Nếu tìm thấy khớp hoàn toàn hoặc một phần và Ứng dụng này không thể được chọn do hạn chế lựa chọn nhiều hoặc vì Ứng dụng từ chối lựa chọn (ví dụ: vì nó không hỗ trợ giao diện thẻ hiện tại), hãy tiếp tục tìm kiếm thông qua Sổ đăng ký GlobalPlatform để tìm kiếm khớp hoàn toàn hoặc một phần tiếp theo. Nếu không tìm thấy khớp hoàn toàn hoặc một phần tiếp theo, OPEN sẽ trả về lỗi thích hợp cho Thực thể ngoài thẻ.
* Nếu tìm thấy khớp hoàn toàn hoặc một phần và Ứng dụng này có thể chọn được (ví dụ: ở Trạng thái Vòng đời Ứng dụng chính xác và không có hạn chế lựa chọn nhiều), thì nó sẽ trở thành Ứng dụng được chọn hiện tại trên Kênh Logic Cơ bản và lệnh SELECT [theo tên], cho dù là [lần xuất hiện đầu tiên hoặc duy nhất] hoặc [lần xuất hiện tiếp theo], sẽ được xử lý theo các yêu cầu của môi trường thời gian chạy (ví dụ: được gửi đến Ứng dụng).
* Nếu hoàn toàn không tìm thấy khớp hoàn toàn hoặc một phần, Ứng dụng được chọn hiện tại trên Kênh Logic Cơ bản sẽ vẫn là Ứng dụng được chọn và:
  + Nếu lệnh SELECT [theo tên] có tham số [lần xuất hiện đầu tiên hoặc duy nhất] được đặt, lệnh SELECT được gửi đến Ứng dụng.
  + Nếu lệnh SELECT [theo tên] có tham số [lần xuất hiện tiếp theo] được đặt, OPEN sẽ trả về lỗi thích hợp cho Thực thể ngoài thẻ.
* Trong trường hợp Phiên Ứng dụng hiện tại đã bị chấm dứt và không tìm thấy khớp hoàn toàn hoặc một phần tiếp theo, OPEN sẽ cố gắng chọn Ứng dụng được đánh dấu là có thể chọn ngầm trên Kênh Logic Cơ bản cho giao diện thẻ hiện tại.

**6.4.2.2 Quản lý Kênh Logic trên Kênh Logic Cơ bản:**

Bất cứ lúc nào trong Phiên Thẻ, OPEN có thể nhận được yêu cầu trên Kênh Logic Cơ bản để mở hoặc đóng Kênh Logic Bổ sung.

Nếu thẻ chỉ hỗ trợ Kênh Logic Cơ bản và không có khái niệm về hỗ trợ kênh logic, lệnh MANAGE CHANNEL được gửi đến Ứng dụng được chọn hiện tại. Trong trường hợp này, khi Miền Bảo mật là Ứng dụng được chọn hiện tại, lệnh sẽ bị từ chối.

Trên các thẻ hỗ trợ kênh logic, nếu nhận được MANAGE CHANNEL [mở]:

* Nếu một Ứng dụng được chỉ định là có thể chọn ngầm trên Kênh Logic Bổ sung mới cho giao diện thẻ hiện tại, Ứng dụng đó được chọn ngầm trên Kênh Logic Bổ sung mới được mở và các yêu cầu hành vi thời gian chạy được áp dụng.
* Nếu không, Ứng dụng được chỉ định là có thể chọn ngầm trên Kênh Logic Cơ bản cho giao diện thẻ này được chọn ngầm trên Kênh Logic Bổ sung mới được mở và các yêu cầu hành vi thời gian chạy được áp dụng.

Trên các thẻ hỗ trợ kênh logic, nếu nhận được MANAGE CHANNEL [đóng], hãy chấm dứt Phiên Ứng dụng được chọn hiện tại trên Kênh Logic Bổ sung được chỉ định bởi lệnh và sau đó đóng kênh logic đó. **Kênh Logic Cơ bản không bao giờ có thể bị đóng.**

Hành vi thời gian chạy:

Khi nhận được lệnh MANAGE CHANNEL [mở], các yêu cầu sau đây được áp dụng:

* Nếu thẻ ở Trạng thái Vòng đời Thẻ CARD\_LOCKED hoặc TERMINATED, hãy trả về lỗi thích hợp.
* Nếu số lượng kênh logic được hỗ trợ bởi OPEN không đủ để mở Kênh Logic Bổ sung mới, hãy trả về lỗi thích hợp.
* **OPEN sẽ tìm kiếm trong Sổ đăng ký GlobalPlatform Ứng dụng hỗ trợ giao diện thẻ hiện tại và được đánh dấu là có thể chọn ngầm trên Kênh Logic Bổ sung mới (hoặc nếu không, trên Kênh Logic Cơ bản) và:**
  + Nếu đây là Ứng dụng ở Trạng thái Vòng đời Ứng dụng LOCKED, Ứng dụng có đặc quyền Ứng dụng Cuối cùng sẽ trở thành Ứng dụng được chọn trên Kênh Logic Bổ sung.
  + Nếu Ứng dụng này không thể được chọn do hạn chế lựa chọn nhiều, kênh logic mới sẽ không được mở và OPEN sẽ trả về lỗi thích hợp.
  + Nếu không, Kênh Logic Bổ sung được mở và Ứng dụng này sẽ trở thành Ứng dụng được chọn trên Kênh Logic Bổ sung.

**6.4.2.3 Gửi Lệnh Ứng dụng trên Kênh Logic Cơ bản:**

Sau khi Ứng dụng trở thành Ứng dụng được chọn trên Kênh Logic Cơ bản, trách nhiệm gửi lệnh tiếp theo vẫn thuộc về OPEN.

Việc xử lý các lệnh SELECT [theo tên] và các yêu cầu hành vi thời gian chạy cho OPEN được mô tả trong phần 6.4.2.1.2, Lựa chọn Rõ ràng trên Kênh Logic Cơ bản.

Trên các thẻ nhận biết kênh logic, các lệnh MANAGE CHANNEL chỉ được OPEN xử lý và không được gửi đến Ứng dụng.

**6.4.3 Kênh Logic Bổ sung:**

Kênh Logic Bổ sung, nếu được hỗ trợ, cho phép Ứng dụng được chọn đồng thời với các Ứng dụng được chọn trên các kênh logic khác.

**6.4.3.1.2 Lựa chọn Rõ ràng trên Kênh Logic Bổ sung:**

Bất cứ lúc nào trên Kênh Logic Bổ sung đang mở, OPEN có thể nhận được yêu cầu chọn Ứng dụng trên Kênh Logic Bổ sung này (lệnh SELECT [theo tên] [lần xuất hiện đầu tiên hoặc duy nhất]). **OPEN sẽ xác định xem AID được yêu cầu có khớp hoặc khớp một phần với một mục nhập trong Sổ đăng ký GlobalPlatform hay không và liệu mục nhập này có thể chọn được hay không.**

Bất cứ lúc nào trên Kênh Logic Bổ sung đang mở đã chứa lệnh SELECT [theo tên] [lần xuất hiện đầu tiên hoặc duy nhất] kể từ khi Kênh Logic Bổ sung được mở lần cuối, OPEN có thể nhận được yêu cầu chọn Ứng dụng tiếp theo (lệnh SELECT [theo tên] [lần xuất hiện tiếp theo]) trên Kênh Logic Bổ sung này. OPEN sẽ xác định xem AID được yêu cầu có khớp hoặc khớp một phần với một mục nhập khác trong Sổ đăng ký GlobalPlatform hay không và liệu mục nhập này có thể chọn được hay không.

**Đối với cả lệnh SELECT [theo tên] [lần xuất hiện đầu tiên hoặc duy nhất] và lệnh SELECT [theo tên] [lần xuất hiện tiếp theo], một Ứng dụng sẽ trở thành Ứng dụng được chọn trên Kênh Logic Bổ sung nếu tất cả những điều sau đây đều đúng:**

* AID được yêu cầu khớp (hoàn toàn hoặc một phần) với AID của Ứng dụng.
* Ứng dụng đang được chọn ở Trạng thái Vòng đời Ứng dụng chính xác.
* Ứng dụng không có hạn chế do lựa chọn nhiều và hỗ trợ giao diện thẻ hiện tại.

Hành vi thời gian chạy:

Các yêu cầu sau đây áp dụng cho OPEN trong quy trình lựa chọn Ứng dụng rõ ràng (SELECT [theo tên]) trên Kênh Logic Bổ sung:

* Nếu thẻ ở Trạng thái Vòng đời Thẻ CARD\_LOCKED hoặc TERMINATED:
  + Đóng Kênh Logic Bổ sung, nếu hiện đang mở.
  + Trả về lỗi thích hợp cho Thực thể ngoài thẻ.
* Nếu nhận được SELECT [theo tên] [lần xuất hiện đầu tiên hoặc duy nhất], quá trình tìm kiếm luôn bắt đầu từ đầu Sổ đăng ký GlobalPlatform.
* Nếu nhận được SELECT [theo tên] [lần xuất hiện tiếp theo], quá trình tìm kiếm luôn bắt đầu từ mục nhập sau Ứng dụng được chọn hiện tại trên Kênh Logic Bổ sung này trong Sổ đăng ký GlobalPlatform.
* Nếu tìm thấy khớp hoàn toàn hoặc một phần và Ứng dụng này ở Trạng thái Vòng đời Ứng dụng INSTALLED, hãy tiếp tục tìm kiếm thông qua Sổ đăng ký GlobalPlatform để tìm kiếm khớp hoàn toàn hoặc một phần tiếp theo. Nếu không tìm thấy khớp hoàn toàn hoặc một phần tiếp theo, OPEN sẽ trả về lỗi thích hợp cho Thực thể ngoài thẻ.
* Nếu tìm thấy khớp hoàn toàn hoặc một phần và Ứng dụng này ở Trạng thái Vòng đời Ứng dụng LOCKED, hãy tiếp tục tìm kiếm thông qua Sổ đăng ký GlobalPlatform để tìm kiếm khớp hoàn toàn hoặc một phần tiếp theo. Trong trường hợp Ứng dụng bị khóa này đã được chọn hiện tại trên cùng Kênh Logic Bổ sung, OPEN sẽ chấm dứt Phiên Ứng dụng này. Nếu không tìm thấy khớp hoàn toàn hoặc một phần tiếp theo, OPEN sẽ trả về lỗi thích hợp cho Thực thể ngoài thẻ.
* Nếu tìm thấy khớp hoàn toàn hoặc một phần và Ứng dụng này không thể được chọn do hạn chế lựa chọn nhiều hoặc vì Ứng dụng từ chối lựa chọn (ví dụ: vì nó không hỗ trợ giao diện thẻ hiện tại), hãy tiếp tục tìm kiếm thông qua Sổ đăng ký GlobalPlatform để tìm kiếm khớp hoàn toàn hoặc một phần tiếp theo. Nếu không tìm thấy khớp hoàn toàn hoặc một phần tiếp theo, OPEN sẽ trả về lỗi thích hợp cho Thực thể ngoài thẻ.
* Nếu tìm thấy khớp hoàn toàn hoặc một phần và Ứng dụng này có thể chọn được (ví dụ: ở Trạng thái Vòng đời Ứng dụng chính xác và không có hạn chế lựa chọn nhiều), thì nó sẽ trở thành Ứng dụng được chọn hiện tại trên Kênh Logic Bổ sung và lệnh SELECT [theo tên], cho dù là [lần xuất hiện đầu tiên hoặc duy nhất] hoặc [lần xuất hiện tiếp theo], sẽ được xử lý theo các yêu cầu của môi trường thời gian chạy (ví dụ: được gửi đến Ứng dụng).
* Nếu hoàn toàn không tìm thấy khớp hoàn toàn hoặc một phần, Ứng dụng được chọn hiện tại trên Kênh Logic Bổ sung sẽ vẫn là Ứng dụng được chọn và:
  + Nếu lệnh SELECT [theo tên] có tham số [lần xuất hiện đầu tiên hoặc duy nhất] được đặt, lệnh SELECT được gửi đến Ứng dụng.
  + Nếu lệnh SELECT [theo tên] có tham số [lần xuất hiện tiếp theo] được đặt, OPEN sẽ trả về lỗi thích hợp cho Thực thể ngoài thẻ.

**6.4.3.2 Quản lý Kênh Logic trên Kênh Logic Bổ sung:**

Bất cứ lúc nào trên Kênh Logic Bổ sung đang mở, OPEN có thể nhận được yêu cầu để mở hoặc đóng Kênh Logic Bổ sung.

**Nếu nhận được MANAGE CHANNEL [mở] và Ứng dụng được chọn trên Kênh Logic Bổ sung ban đầu không có hạn chế lựa chọn nhiều, Ứng dụng này sẽ trở thành Ứng dụng được chọn trên Kênh Logic Bổ sung mới được mở.**

Nếu nhận được MANAGE CHANNEL [đóng], hãy chấm dứt Phiên Ứng dụng được chọn hiện tại trên Kênh Logic Bổ sung được chỉ định bởi lệnh và sau đó đóng kênh logic đó. **Kênh Logic Cơ bản không bao giờ có thể bị đóng.**

Hành vi thời gian chạy:

Khi nhận được lệnh MANAGE CHANNEL [mở], các yêu cầu sau đây được áp dụng:

* Nếu thẻ ở Trạng thái Vòng đời Thẻ CARD\_LOCKED hoặc TERMINATED, hãy trả về lỗi thích hợp.
* Nếu số lượng kênh logic được hỗ trợ bởi OPEN không đủ để mở Kênh Logic Bổ sung mới, hãy trả về lỗi thích hợp.
* Nếu Ứng dụng được chọn hiện tại trên Kênh Logic Bổ sung ban đầu không thể được chọn trên Kênh Logic Bổ sung mới do hạn chế lựa chọn nhiều, kênh logic mới sẽ không được mở và OPEN sẽ trả về lỗi thích hợp.
* Nếu không, Kênh Logic Bổ sung được chỉ định bởi lệnh được mở và **Ứng dụng được chọn hiện tại trên Kênh Logic Bổ sung ban đầu sẽ trở thành Ứng dụng được chọn trên Kênh Logic Bổ sung mới được mở.**

**6.4.3.3 Gửi Lệnh Ứng dụng trên Kênh Logic Bổ sung:**

Sau khi Ứng dụng trở thành Ứng dụng được chọn trên Kênh Logic Bổ sung, trách nhiệm gửi lệnh tiếp theo vẫn thuộc về OPEN.

Việc xử lý các lệnh SELECT [theo tên] và các yêu cầu hành vi thời gian chạy cho OPEN được mô tả trong phần 6.4.3.1.2, Lựa chọn Rõ ràng trên Kênh Logic Bổ sung.

Các lệnh MANAGE CHANNEL chỉ được OPEN xử lý và không được gửi đến Ứng dụng.

### 

### **6.5 Sổ đăng ký GlobalPlatform (GlobalPlatform Registry)**

* **Mục đích**: GlobalPlatform Registry được sử dụng để:
  + Lưu trữ thông tin quản lý thẻ.
  + Lưu trữ thông tin quản lý ứng dụng (ví dụ: AID, Security Domain được liên kết và các đặc quyền).
  + Hỗ trợ dữ liệu quản lý tài nguyên thẻ.
  + Lưu trữ thông tin về vòng đời ứng dụng.
  + Lưu trữ thông tin về vòng đời thẻ.
  + Theo dõi bất kỳ bộ đếm nào được liên kết với nhật ký.
* **Nội dung**:
  + **Tất cả các ứng dụng**, bao gồm **tất cả các Security Domain và tất cả các Executable Load Files, đều phải có một mục trong GlobalPlatform Registry.**
  + Không có định dạng bắt buộc nào cho việc lưu trữ các phần tử dữ liệu này.
* **Cập nhật**: Nội dung của GlobalPlatform Registry có thể được cập nhật để đáp ứng với:
  + Hành động được OPEN gọi nội bộ.
  + Hành động được gọi bởi một ứng dụng được ủy quyền.
* **Phần tử dữ liệu ứng dụng/Executable Load File/Executable Module**:
  + **AID**: Mỗi Executable Load File hoặc Executable Module được liên kết với một AID duy nhất trên thẻ. AID của ứng dụng có thể giống với AID của Executable Module nhưng không được giống với AID của Executable Load File hoặc AID của ứng dụng khác đã có trong GlobalPlatform Registry.
  + **Vòng đời**: Phần tử dữ liệu Vòng đời ứng dụng chứa Vòng đời hiện tại của ứng dụng, Executable Load File hoặc Executable Module.
  + **Tham số quản lý tài nguyên bộ nhớ**: Các tham số này chỉ định các giới hạn về mức tiêu thụ bộ nhớ của ứng dụng (ví dụ: giới hạn tĩnh, giới hạn động).
  + **Tham số lựa chọn ngầm**: Tham số này cho biết liệu một ứng dụng có thể được chọn ngầm định trên một kênh logic cụ thể hay không.
  + **ID nhà cung cấp ứng dụng**: Registry lưu trữ mã định danh của Nhà cung cấp ứng dụng, là chủ sở hữu của ứng dụng hoặc Executable Load File khi được cung cấp rõ ràng trong quá trình tải hoặc cài đặt.
  + **Tham số dịch vụ**: Tham số dịch vụ xác định dịch vụ do ứng dụng dịch vụ toàn cầu cung cấp.
* **Dữ liệu toàn thẻ**:
  + Trạng thái vòng đời thẻ.
  + Bất kỳ hạn chế nào đối với chức năng Quản lý nội dung thẻ của OPEN.

GlobalPlatform Registry đóng vai trò là **cơ sở dữ liệu trung tâm cho tất cả thông tin quản lý thẻ và ứng dụng**. OPEN sử dụng Registry này để thực hiện các chức năng khác nhau, chẳng hạn như **điều phối lệnh** và **quản lý nội dung thẻ.**

### **6.6 Đặc quyền (Privileges)**

Đặc quyền xác định quyền truy cập và khả năng của ứng dụng và miền bảo mật.

**Các đặc quyền chính bao gồm:**

* **Security Domain:** Xác định một ứng dụng là miền bảo mật.
* **Card Reset:** Cho phép ứng dụng nhận biết sự kiện thẻ được khởi động lại.
* **Card Lock:** Cho phép ứng dụng khóa thẻ.
* **DAP Verification:** Cho phép miền bảo mật xác minh chữ ký DAP của tệp tải thực thi.
* **Delegated Management:** Cho phép ứng dụng thực hiện các hoạt động quản lý nội dung thẻ.
* **Authorized Management:** Cho phép miền bảo mật thực hiện các hoạt động quản lý nội dung thẻ.
* **Token Verification:** Cho phép miền bảo mật xác minh mã thông báo quản lý.
* **Global Lock:** Cho phép ứng dụng khóa hoặc mở khóa bất kỳ ứng dụng nào trên thẻ.
* **CVM Management:** Cho phép ứng dụng quản lý các cơ chế xác minh người dùng (Cardholder Verification Methods - CVM).
* **Final Application:** Xác định ứng dụng là ứng dụng cuối cùng được chọn khi thẻ bị khóa.
* **Global Platform Protectable:** Cho phép ứng dụng sử dụng cơ chế bảo vệ dữ liệu của GlobalPlatform.
* **Trusted Path:** Cho phép miền bảo mật chuyển tiếp lệnh đến ứng dụng được liên kết.
* **Mandated DAP Verification:** Bắt buộc phải xác minh chữ ký DAP cho tất cả các tệp tải thực thi.

### **6.7 Khung tin cậy GlobalPlatform (The GlobalPlatform Trusted Framework)**

GlobalPlatform Trusted Framework mô tả một cơ chế cho phép các lệnh APDU nhận được bởi Security Domain có thể được chuyển tiếp an toàn đến một trong các ứng dụng được liên kết với nó, thông qua Trusted Framework.

Dưới đây là tóm tắt những điểm chính của phần này:

* Mục đích:
  + Trusted Framework cung cấp dịch vụ giao tiếp giữa các ứng dụng trên thẻ GlobalPlatform.
  + Cơ chế này cho phép Security Domain chuyển tiếp các lệnh APDU một cách an toàn đến ứng dụng đích.
* Hoạt động:
  + Security Domain (có thể là Issuer Security Domain hoặc Supplementary Security Domain) nhận được một lệnh APDU.
  + Security Domain giải mã lệnh APDU trước khi chuyển nó cho GlobalPlatform Trusted Framework.
  + GlobalPlatform Trusted Framework chuyển tiếp lệnh đã được giải mã đến ứng dụng đích được chỉ định bởi Security Domain nhận lệnh.
* Kiểm tra bảo mật:
  + GlobalPlatform Trusted Framework thực hiện các kiểm tra sau trước khi chuyển tiếp lệnh:
    - Security Domain nhận lệnh phải có đặc quyền Trusted Path.
    - Ứng dụng đích phải tồn tại trong GlobalPlatform Registry và đã kích hoạt điểm nhập 'Process Data'.
    - Ứng dụng đích không bị hạn chế lựa chọn đa năng nếu nó đã được chọn trên một kênh logic khác.
    - Ứng dụng đích phải được liên kết với Security Domain hiện đang được chọn.

Tóm lại, GlobalPlatform Trusted Framework cung cấp một cơ chế an toàn và linh hoạt để giao tiếp giữa các ứng dụng trên thẻ GlobalPlatform. Cơ chế này đảm bảo rằng các lệnh APDU được chuyển tiếp an toàn đến ứng dụng đích và chỉ những Security Domain được ủy quyền mới có thể tương tác với các ứng dụng được liên kết.

**7. Security Domains**

Là một thành phần quan trọng trong kiến trúc thẻ thông minh GlobalPlatform. Security Domain hoạt động như những đại diện trên thẻ của các cơ quan bên ngoài thẻ, chịu trách nhiệm quản lý khóa, mã hóa, giải mã, tạo và xác minh chữ ký số cho các ứng dụng của nhà cung cấp (bên phát hành thẻ, nhà cung cấp ứng dụng hoặc cơ quan kiểm soát).

### **7.1 General Description**

Phần này giới thiệu tổng quan về Security Domain:

* **Security Domain** hoạt động như những ứng dụng đặc quyền, giữ **khóa mật mã** để hỗ trợ **Secure Channel Protocol** và/hoặc **ủy quyền các chức năng quản lý nội dung thẻ.** [7.1]
* Mỗi **ứng dụng** và **Executable Load File** đều được liên kết với một **Security Domain** duy nhất. Ứng dụng có thể sử dụng các dịch vụ mật mã từ Security Domain mà nó được liên kết. [7.1]

Có ba loại Security Domain:

* **Issuer Security Domain**: Là Security Domain **bắt buộc** và **quan trọng nhất**, đại diện cho quản trị viên thẻ, thường là bên phát hành thẻ.
* **Supplementary Security Domain**: Là các Security Domain bổ sung, **tùy chọn**, đại diện cho nhà cung cấp ứng dụng, bên phát hành thẻ hoặc đại diện của họ.
* **Controlling Authority Security Domain**: Là loại Security Domain **đặc biệt**, thuộc **Supplementary Security Domain**, đại diện cho Cơ quan kiểm soát (nếu có).

Mỗi Security Domain được thiết lập thay mặt cho bên phát hành thẻ, nhà cung cấp ứng dụng hoặc cơ quan kiểm soát, và cung cấp các dịch vụ bảo mật cho các ứng dụng của nhà cung cấp đó.

Các Miền bảo mật chịu trách nhiệm quản lý khóa riêng của mình. Điều này đảm bảo rằng các Ứng dụng và dữ liệu từ các Nhà cung cấp ứng dụng khác nhau có thể cùng tồn tại trên cùng một thẻ mà không vi phạm quyền riêng tư và tính toàn vẹn của từng Nhà cung cấp ứng dụng

### **7.1.1 Issuer Security Domain**

Phần này đi sâu vào **Issuer Security Domain**, nhấn mạnh các đặc điểm riêng biệt:

* **Issuer Security Domain** hoạt động tương tự như bất kỳ Security Domain nào, nhưng có một số đặc điểm đặc biệt.
* Nó **luôn tồn tại** trên thẻ GlobalPlatform và **không thể bị xóa**.
* Issuer Security Domain **sở hữu đặc quyền Authorized Management**, cho phép nó **quản lý tất cả ứng dụng và dữ liệu** trên thẻ, bao gồm cả việc **xác minh các hoạt động quản lý nội dung thẻ** được thực hiện bởi các Security Domain khác.
* Khóa của **Issuer Security Domain** có thể được sử dụng để xác minh **bất kỳ hoạt động Quản lý nội dung thẻ** nào được thực hiện bởi **bất kỳ Security Domain nào khác**.
* Issuer Security Domain có thể được **liên kết với chính nó**, nghĩa là khi sử dụng dịch vụ của Security Domain được liên kết, nó sẽ sử dụng chính dịch vụ của nó.

7.2 Security Domain Association

Phần **7.2 Security Domain Association** tập trung vào cách các Security Domain được liên kết với nhau trong thẻ thông minh GlobalPlatform, tạo thành một hệ thống phân cấp kiểm soát an ninh.

Ứng dụng, bao gồm cả Security Domain, có thể sử dụng các dịch vụ của Security Domain được liên kết để cung cấp các Secure Channel Session và các dịch vụ mật mã khác.

Ứng dụng không cần biết trước AID của Security Domain được liên kết vì thông tin này được lưu trữ trong GlobalPlatform Registry.

OPEN sẽ cung cấp cho ứng dụng một tham chiếu đến Security Domain được liên kết.

Tuy nhiên, ứng dụng không nên lưu trữ tham chiếu này để sử dụng trong tương lai vì Security Domain được liên kết có thể thay đổi do quá trình trao quyền (extradition).

* **Liên kết (Association):**
  + Các ứng dụng (bao gồm Security Domain) có thể sử dụng dịch vụ của Security Domain mà nó được liên kết.
  + Security Domain có thể được liên kết với một Security Domain khác, hoặc liên kết với chính nó.
  + Khi một Security Domain được liên kết với chính nó, nó trở thành **gốc (root)** của một hệ thống phân cấp liên kết.
  + Mối quan hệ liên kết Security Domain được thể hiện bằng cụm từ "**được liên kết với (is associated with)**".
* **Hệ thống phân cấp (Hierarchy):**
  + Do khả năng liên kết linh hoạt, các Security Domain trên thẻ tạo thành một hoặc nhiều hệ thống phân cấp liên kết.
  + Hình 7-1 minh họa hai hệ thống phân cấp: một bắt đầu từ **Issuer Security Domain**, một bắt đầu từ **Supplementary Security Domain** đã được **trao quyền (extradit)** cho chính nó.
  + **Liên kết trực tiếp (Directly Associated):** Khi một Security Domain được liên kết với một ứng dụng khác, ta nói Security Domain đó được liên kết trực tiếp với ứng dụng đó.
  + **Liên kết gián tiếp (Indirectly Associated):** Các Security Domain ở cấp cao hơn trong hệ thống phân cấp được xem là liên kết gián tiếp với các ứng dụng ở cấp thấp hơn.
  + **Phân cấp con (Sub-hierarchy):** Bao gồm một Security Domain và tất cả các Security Domain và ứng dụng được liên kết trực tiếp hoặc gián tiếp với nó.

7.3 Security Domain Services

### **7.3.1 Security Domain Support for Secure Messaging**

Mục này mô tả cách ứng dụng có thể tận dụng **dịch vụ Secure Messaging của Security Domain được liên kết**, thay vì tự triển khai giao thức Secure Messaging riêng. Điều này giúp đơn giản hóa việc tích hợp bảo mật cho ứng dụng. Các dịch vụ Secure Messaging bao gồm:

* **Khởi tạo Secure Channel Session** sau khi xác minh thành công một thực thể ngoài thẻ.
* **Mở gói (unwrap) lệnh** nhận được trong Secure Channel Session bằng cách xác minh tính toàn vẹn và/hoặc giải mã dữ liệu gốc (trong trường hợp cần bảo mật).
* **Kiểm soát trình tự các lệnh APDU**.
* **Giải mã khối dữ liệu bí mật**.
* **Thiết lập mức bảo mật** (toàn vẹn và/hoặc bảo mật) để áp dụng cho lệnh tiếp theo và/hoặc phản hồi tiếp theo.
* **Đóng Secure Channel Session** theo yêu cầu và hủy mọi bí mật liên quan đến Secure Channel Session đó.

Tùy thuộc vào giao thức Secure Channel được hỗ trợ, dịch vụ Security Domain cũng có thể bao gồm:

* **Đóng gói (wrap) phản hồi** được gửi trong Secure Channel Session bằng cách thêm tính toàn vẹn và/hoặc mã hóa dữ liệu gốc (trong trường hợp cần bảo mật).
* **Mã hóa khối dữ liệu bí mật**.
* **Kiểm soát trình tự các phản hồi APDU**.

Ngoài ra, **Security Domain có thể hỗ trợ quản lý nhiều Secure Channel Session đồng thời**, hoặc chỉ giới hạn ở một Secure Channel Session. Trong trường hợp hỗ trợ nhiều Secure Channel Session đồng thời, Security Domain phải có khả năng phân biệt giữa các phiên và dữ liệu liên quan.

**Hình 7-2 minh họa luồng nhắn tin** khi một ứng dụng sử dụng dịch vụ Secure Messaging từ Security Domain được liên kết.

### **7.3.2 Security Domain Support for Application Personalization**

Mục này trình bày **cách ứng dụng sử dụng dịch vụ liên lạc an toàn và giải mã khóa của Security Domain được liên kết** để quản lý việc tải dữ liệu cá nhân hóa một cách an toàn. Có hai cách để thực hiện điều này:

1. **Sử dụng dịch vụ nhắn tin thời gian chạy (runtime messaging support)** được mô tả trong phần 7.3.1.
2. **Sử dụng khả năng truy cập ứng dụng của Security Domain**, được mô tả trong phần này.

Phương pháp thứ hai dựa trên khả năng của Security Domain **truy cập trực tiếp vào ứng dụng được liên kết** để xử lý dữ liệu cá nhân hóa. **Hình 7-3 minh họa luồng dữ liệu** trong quá trình cá nhân hóa ứng dụng thông qua Security Domain được liên kết

7.4 Security Domain Data

### **7.4.1 Issuer Security Domain**

**Issuer Security Domain phải có khả năng xử lý các dữ liệu sau:**

* **Issuer Identification Number (IIN):** Số nhận dạng nhà phát hành.
* **Card Image Number (CIN):** Số hình ảnh thẻ.
* **Card Recognition Data:** Dữ liệu nhận dạng thẻ.
* **Dữ liệu sở hữu của nhà phát hành thẻ.**

Ngoài ra, **Issuer Security Domain cũng có thể xử lý dữ liệu tùy chọn sau:**

* **Card Capability Information:** Thông tin khả năng của thẻ.

Tất cả dữ liệu này có thể được truy xuất từ ​​thẻ bằng lệnh **GET DATA**.

### **7.4.2 Supplementary Security Domain**

**Supplementary Security Domain có thể xử lý các dữ liệu nhận dạng riêng:**

* **Security Domain Provider Identification Number (SIN):** Số nhận dạng nhà cung cấp Security Domain.
* **Security Domain Image Number:** Số hình ảnh Security Domain.
* **Security Domain Management Data:** Dữ liệu quản lý Security Domain.
* **Security Domain Manager URL:** URL của trình quản lý Security Domain.
* **Dữ liệu sở hữu của nhà cung cấp ứng dụng.**

Khi có mặt, những dữ liệu này có thể được truy xuất từ ​​Security Domain bằng lệnh **GET DATA**.

7.5 Security Domain Keys

Phần **7.5 Security Domain Keys** tập trung vào cách Security Domain quản lý khóa, bao gồm thông tin khóa, điều kiện truy cập khóa và cách thức quản lý dữ liệu và khóa.

### **7.5.1 Key Information**

Phần này mô tả thông tin chi tiết về các khóa được sử dụng bởi mỗi giao thức Secure Channel Protocol, được định nghĩa trong Phụ lục D, E và F. Thông tin chi tiết về Token, Receipt, và DAP key có thể được tìm thấy trong phần C.1.

Mỗi khóa có các thuộc tính sau:

* Key Version Number và Key Identifier.
  + Không có giới hạn hay thứ tự nào được xác định trước trong việc gán Key Version Number và Key Identifier, bao gồm cả việc sử dụng các giá trị không tuần tự trong cùng một Security Domain.
* Key Type.
  + Key Type xác định thuật toán mã hóa và thành phần khóa.

**Sự kết hợp của Key Identifier và Key Version Number xác định duy nhất một khóa trong Security Domain.** Key Type cho biết thuật toán mã hóa và thành phần khóa được sử dụng. Việc xác định rõ ràng khóa và thuật toán giúp ngăn chặn việc sử dụng sai chức năng mã hóa.

Thực thể ngoài thẻ có thể lấy thông tin về khóa Security Domain bằng lệnh GET DATA với Key Information Template (tag 'E0').

**Security Domain quản lý khóa như sau:**

* Key Identifier và Key Version Number được sử dụng để tham chiếu duy nhất từng khóa trong Security Domain.
* Security Domain lưu trữ tất cả thông tin khóa được cung cấp trong lệnh PUT KEY, liên kết với mỗi khóa.
* Các cơ chế kiểm soát tốc độ liên quan đến việc sử dụng khóa cụ thể (ví dụ: bộ đếm và giới hạn số lần thử khóa) phụ thuộc vào chính sách bảo mật của nhà cung cấp Security Domain.

### **7.5.2 Key Access Conditions**

**Điều kiện truy cập được gán cho khóa Security Domain có thể là:**

* **"Owner only":** Chỉ Security Domain sở hữu khóa mới có quyền truy cập.
* **"Authorized users other than the owner":** Các ứng dụng được liên kết với Security Domain có quyền truy cập, nhưng Security Domain không có quyền truy cập.
* **"Any authorized user, including the owner":** Cả Security Domain và các ứng dụng được liên kết đều có quyền truy cập.

Phiên bản hiện tại của Specification định nghĩa các điều kiện truy cập sau cho khóa Security Domain, được mã hóa trên một byte như sau:

* '00': Bất kỳ người dùng nào được ủy quyền, bao gồm cả chủ sở hữu; đây là điều kiện truy cập mặc định cho Secure Channel Protocol Keys, khi không được cung cấp rõ ràng trong lệnh PUT KEY.
* '01': Chỉ chủ sở hữu; đây là điều kiện truy cập mặc định cho Token và DAP Keys, khi không được cung cấp rõ ràng trong lệnh PUT KEY.
* '02': Người dùng được ủy quyền khác với chủ sở hữu.
* '03' đến '7F': Được dành riêng cho GlobalPlatform sử dụng trong tương lai.
* '80' đến 'FE': Được dành riêng cho mục đích sử dụng độc quyền.
* 'FF': Không khả dụng.

**Các quy tắc kiểm soát truy cập áp dụng cho bất kỳ khóa Security Domain nào được thực thi như sau:**

* Để sử dụng bất kỳ dịch vụ mã hóa nào của Security Domain, ứng dụng sẽ yêu cầu OPEN cung cấp dịch vụ đó.
* OPEN sẽ kiểm tra các điều kiện truy cập của khóa được yêu cầu và chỉ cấp quyền truy cập cho ứng dụng nếu nó được ủy quyền.
* Security Domain sẽ thực thi các quy tắc kiểm soát truy cập của riêng nó khi xử lý các yêu cầu từ OPEN (ví dụ: từ chối yêu cầu truy cập khóa với điều kiện truy cập được đặt thành '01').

### **7.6 Data and Key Management**

Các dịch vụ này liên quan đến việc lưu trữ khóa mã hóa và dữ liệu trên thẻ.

**Hành vi Runtime** Khi nhận được yêu cầu quản lý dữ liệu/khóa, Security Domain tương ứng sẽ quản lý dữ liệu/khóa theo các quy tắc kiểm soát truy cập của riêng nó.

Trạng thái vòng đời của thẻ không được là CARD\_LOCKED hoặc TERMINATED.

Khi nhận được lệnh DELETE [key], PUT KEY, hoặc STORE DATA, Security Domain thực hiện quản lý dữ liệu hoặc khóa sẽ áp dụng chính sách truyền thông an toàn của riêng nó. (Lưu ý: Mức độ bảo mật tối thiểu được định nghĩa trong Bảng 11-2). Nhà cung cấp Security Domain có thể áp dụng chính sách quản lý khóa của riêng mình liên quan đến việc xóa khóa.

**8 Global Platform Services**

8.1 Global Services Applications

Phần **8.1 Global Services Applications** tập trung vào cách các ứng dụng đặc biệt, được gọi là **Global Services Applications**, cung cấp dịch vụ cho các ứng dụng khác trên thẻ GlobalPlatform.

**Đặc điểm nổi bật của Global Services Applications:**

* **Quyền Global Service:** Các ứng dụng này được phân biệt bằng **quyền Global Service**, cho phép chúng cung cấp dịch vụ cho các ứng dụng khác.
* **Đăng ký dịch vụ:** Global Services Applications **đăng ký các dịch vụ duy nhất** mà chúng cung cấp với **OPEN**, một thành phần hệ thống quản lý truy cập ứng dụng và dịch vụ.
* **Global Service Parameters:** Các thông số này, bao gồm tên dịch vụ, được sử dụng để **xác định và phân biệt các dịch vụ** khác nhau được cung cấp.

**Cơ chế đăng ký và truy cập Global Services:**

1. **Đăng ký Global Services:**
   * **Trong quá trình cài đặt (INSTALL),** ứng dụng được gán quyền "Global Service" và cung cấp Global Service Parameters (tùy chọn), bao gồm tên dịch vụ.
     + Ví dụ, tag 'CB' trong trường Install Parameters có thể chứa một hoặc nhiều thông số dịch vụ hai byte, đại diện cho Global Service Parameters.
   * **Global Service Parameters** được ghi lại trong **GlobalPlatform Registry**, một cơ sở dữ liệu trung tâm chứa thông tin về các ứng dụng và dịch vụ trên thẻ.
   * Ngoài ra, ứng dụng Global Services Application có thể **đăng ký trực tiếp** một hoặc nhiều dịch vụ với OPEN thông qua **GlobalPlatform API**.
   * **OPEN chịu trách nhiệm đảm bảo tính duy nhất** của mỗi tên dịch vụ được đăng ký, ngăn ngừa xung đột và nhầm lẫn.
2. **Truy cập Global Services:**
   * Các ứng dụng khác sử dụng **GlobalPlatform API** để **truy cập Global Services** đã được đăng ký.
   * Ứng dụng có thể **truy cập dịch vụ** bằng cách sử dụng:
     + **Tên dịch vụ duy nhất**: Truy cập bất kỳ ứng dụng Global Services Application nào cung cấp dịch vụ đó.
     + **Tên dịch vụ và AID**: Truy cập một ứng dụng Global Services Application cụ thể.
3. **Cấu trúc Global Service Parameters:**
   * Mỗi **service name** được mã hóa trên **hai byte**.
     + Byte đầu tiên xác định **họ dịch vụ**. Ví dụ:
       - 'C0': GlobalPlatform Secure Channel
       - 'C1': GlobalPlatform CVM
     + Byte thứ hai xác định **mã định danh dịch vụ cụ thể** trong họ dịch vụ đó.

**Tóm lại,** Global Services Applications đóng vai trò quan trọng trong việc mở rộng chức năng và cung cấp tính linh hoạt cho các ứng dụng trên thẻ GlobalPlatform. Bằng cách đăng ký và truy cập các dịch vụ được cung cấp bởi các ứng dụng Global Services Applications, các ứng dụng khác có thể tận dụng các chức năng chuyên biệt và tăng cường khả năng của mình.

8.2 CVM Application

Phần **8.2 CVM Application** tập trung vào cách quản lý **Cardholder Verification Methods (CVM)**, được sử dụng để xác thực chủ thẻ trên thẻ GlobalPlatform. Các ứng dụng CVM là các ứng dụng đặc biệt chịu trách nhiệm cung cấp và quản lý các dịch vụ xác minh chủ thẻ.

**Các ứng dụng CVM được phân biệt với các ứng dụng khác bằng quyền CVM**. Quyền này cho phép chúng thực hiện các chức năng liên quan đến CVM, chẳng hạn như xác minh mã PIN và quản lý trạng thái CVM. Quyền CVM có thể được gán cho ứng dụng trong quá trình cài đặt.

**Ví dụ về CVM được tiêu chuẩn hóa bởi GlobalPlatform là global PIN**, được gán mã định danh CVM '11'. GlobalPlatform dành riêng dải mã định danh CVM từ '01' đến '7F' cho các CVM được tiêu chuẩn hóa. Các dải mã định danh khác được dành cho các scheme riêng lẻ do GlobalPlatform đăng ký ('80' đến 'EF') hoặc sử dụng độc quyền ('F0' đến 'FF').

**Một CVM Application có thể hỗ trợ nhiều CVM khác nhau**, và **trên một thẻ có thể có nhiều CVM Application**.

**Các dịch vụ CVM được cung cấp bởi CVM Application:**

**Dành cho các ứng dụng khác trên thẻ:**

* Truy xuất trạng thái CVM (ví dụ: đã được nhập, xác minh hay bị khóa).
* Truy xuất số lần thử CVM còn lại trước khi bị khóa.
* Xác minh giá trị CVM được cung cấp.

**Dành cho các ứng dụng có quyền CVM Management:**

* Đặt giá trị CVM mới.
* Đặt giới hạn số lần thử CVM.

**Để cung cấp dịch vụ CVM duy nhất cho các ứng dụng khác**, CVM Application phải đăng ký với OPEN mã định danh CVM mà nó hỗ trợ. OPEN đảm bảo tính duy nhất của mã định danh CVM trên toàn bộ thẻ. Việc tái sử dụng mã định danh chỉ có thể xảy ra khi mã định danh CVM bị hủy đăng ký hoặc ứng dụng CVM tương ứng bị xóa.