TCVN

TIÊU CHUẨN QUỐC GIA

TCVN XXX:2026

Xuất bản lần 1

GIAO DỊCH ĐIỆN TỬ - YÊU CẦU VỀ MÔ ĐUN KÝ SỐ CHO MÔ HÌNH KÝ SỐ TỪ XA (REMOTE SIGNING)

Trustworthy Systems Supporting Server Signing - Part 2 : Protection profile for QSCD for Server Signing

HÀ NỘI - 2026

NỘI DUNG

LỜI NÓI ĐẦU 4
1 PHẠM VI ÁP DỤNG 5
2 TÀI LIỆU VIỆN DẪN 5
3 THUẬT NGỮ, ĐỊNH NGHĨA VÀ CHỮ VIẾT TẮT 5
4 GIỚI THIỆU CHUNG 6
4.1 Tổng quan 6
4.2 Tài liệu tham chiếu hồ sơ bảo vệ 6
4.3 Quy định pháp luật 7
4.4 Tổng quan về TOE 7
4.4.1 Chung (General) 7
4.4.2 Loại TOE (TOE type) 9
4.4.3 Vòng đời của TOE (TOE life cycle) 10
4.4.4 Việc sử dụng và tính năng bảo mật chính của TOE 10
4.4.5 Tổng quan chung về môi trường TOE 11
4.4.6 Hardware/software/firmware ngoài TOE 11
4.4.7 Các tùy chọn 11
5 TUYÊN BỐ VỀ SỰ PHÙ HỢP 12
5.1 Tuyên bố sự phù hợp CC 12
5.2 Tuyên bố tuân thủ PP 12
5.4 Tuyên bố mức độ tuân thủ 12
6 XÁC ĐỊNH CÁC VẤN ĐỀ BẢO MẬT 12
6.1 Tài sản 12
6.2 Chủ thể (Subjects) 16
6.3 Các mối đe dọa 17
6.4 Mối quan hệ giữa các mối đe dọa và tài sản (Relation between threats and assets) 21
6.5 Các chính sách bảo mật của tổ chức (Organisational Security Policies - OSP) 22
6.6 Các giả định (Assumptions) 23
7 CÁC MỤC TIÊU BẢO MẬT (SECURITY OBJECTIVES) 24
7.1 Tổng quan 24
7.2 Các mục tiêu bảo mật dành cho TOE (Security objectives for the TOE) 25
7.3 Các mục tiêu bảo mật dành cho Môi trường vận hành (Security Objectives for the Operational Environment) 27
7.4 Định nghĩa vấn đề Bảo mật và Mục tiêu Bảo mật 29
7.5 Cơ sở lý luận cho các mục tiêu bảo mật (Rationale for the security objectives) 34
8 ĐỊNH NGHĨA THÀNH PHẦN MỞ RỘNG 38
8.1 Lớp FCS: Hỗ trợ mật mã (Class FCS: Cryptographic Support) 38
9 CÁC YÊU CẦU AN TOÀN (SECURITY REQUIREMENTS) 40
9.1 Quy ước khi trình bày hồ sơ bảo vệ 40
9.2 Các Chủ thể, Đối tượng và Thao tác vận hành (Subjects, Objects and Operations) 41
9.3 Tổng quan về các SFR (SFRs overview) 42
9.4 Các yêu cầu chức năng bảo mật (Security Functional Requirements) 45
10 CƠ SỞ LÝ LUẬN (RATIONALE) 53
10.1 Cơ sở lý luận về các Yêu cầu An toàn (Security Requirements Rationale) 53
10.2 Sự phụ thuộc giữa các SFR (SFR Dependencies) 54
10.3 Cơ sở lý luận về các Yêu cầu Đảm bảo An toàn (Rationales for SARs) 55

TCVN XXX:2026
LỜI GIỚI THIỆU

Trong bối cảnh hiện nay, đối với lĩnh vực cung cấp dịch vụ tin cậy nói chung và dịch vụ chứng thực chữ ký số công cộng nói chung Bộ Khoa học và Công nghệ đã xây dựng hành lang pháp lý, cụ thể như:

- Nghị định số 23/2025/NĐ-CP ngày 21 tháng 02 năm 2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ tin cậy;

- Thông tư số 50/TT-BKHCN ngày 31 tháng 12 năm 2025 của Bộ trưởng Bộ Khoa học và Công nghệ ban hành QCVN 137:2025/BKHCN quy định các yêu cầu kỹ thuật đối với dịch vụ chứng thực chữ ký số công cộng.

Do đó các Tổ chức chứng thực công cộng khi triển khai hệ thống cung cấp dịch vụ chứng thực chữ ký số cần tuân thủ các quy chuẩn Việt Nam được quy định tại QCVN 137:2025/BKHCN.

Đối với dịch vụ chứng thực chữ ký số theo mô hình ký số từ xa nói riêng là mô hình mà khóa bí mật của thuê bao được tạo và lưu trữ tại hệ thống của Tổ chức chứng thực công cộng, việc tạo chữ ký số được thực hiện từ xa theo lệnh của thuê bao thông qua cơ chế xác thực và ủy quyền nghiêm ngặt. Vì vậy, yêu cầu về mô đun ký số cho mô hình ký số từ xa cần tuân thủ theo EN 419241-2:2019 và được chuẩn hóa phù hợp với điều kiện thực tế tại Việt Nam.

Tài liệu này quy định các yêu cầu về mô đun ký số cho mô hình ký số từ xa dựa trên tham chiếu các tiêu chuẩn quốc tế cũng giúp các tổ chức đánh giá có phương tiện để chuẩn hóa, đánh giá hệ thống của các Tổ chức chứng thực theo mô hình ký số từ xa.

Lời nói đầu

TCVN xxx:2026 được xây dựng trên cơ sở tham khảo Tiêu chuẩn quốc tế EN 419 241-2 được xây dựng và phát triển bởi CEN (Comité Européen de Normalisation / European Committee for Standardization - Ủy ban Tiêu chuẩn Châu Âu), có điều chỉnh, sửa đổi, bổ sung để phù hợp với điều kiện của Việt Nam.

TCVN xxx:2026 do Trung tâm Chứng thực điện tử quốc gia biên soạn, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

T I Ê U C H U Ẩ N Q U Ố C G I A **TCVN XXX:2026**

GIAO DỊCH ĐIỆN TỬ - YÊU CẦU VỀ MÔ ĐUN KÝ SỐ CHO MÔ HÌNH KÝ SỐ TỪ XA (REMOTE SIGNING)

Trustworthy Systems Supporting Server Signing - Part 2 : Protection profile for QSCD for Server Signing

1 Phạm vi áp dụng

Tài liệu này quy định các tiêu chuẩn cho hồ sơ bảo vệ của Thiết bị tạo chữ ký số ký trên máy chủ ký số (Protection Profile for QSCD for Server Signing)

2 Tài liệu viện dẫn

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

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

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

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

EN 419241-1, Trustworthy Systems Supporting Server Signing - Part 1 : General System Security Requirements (Hệ thống tin cậy hỗ trợ ký số trên máy chủ - Phần 1: Các yêu cầu chung về bảo mật hệ thống).

EN 419221-5, Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services (Hồ sơ bảo vệ cho mô-đun mật mã TSP - Phần 5: Mô-đun mật mã cho các dịch vụ tin cậy).

3 Thuật ngữ, định nghĩa và chữ viết tắt

3.1. Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong TCVN 8709-1:2011, EN 419241-1, EN 419221-5 và các thuật ngữ sau:

3.1.1

Chứng thư chữ ký số (certificate)

Chứng thư chữ ký điện tử là thông điệp dữ liệu nhằm xác nhận cơ quan, tổ chức, cá nhân được chứng thực là người ký chữ ký điện tử. Chứng thư chữ ký điện tử đối với chữ ký số được gọi là chứng thư chữ ký số

CHÚ THÍCH: Nguồn: Khoản 13 Điều 3 Luật Giao dịch điện tử số 20/2023/QH15 ngày 22/6/2023.

3.1.2

Delegated party (Bên được ủy quyền)

Tổ chức thầu phụ hoặc bên được ủy quyền của tổ chức cung cấp dịch vụ tin cậy (TSP)

3.1.3

Giá trị chữ ký số (digital signature value) kết quả của một thao tác mật mã có sử dụng khóa ký

Chú thích 1: Trong tài liệu này, Con dấu, Chữ ký, Chữ ký số hoặc Con dấu số đều biểu thị cho Giá trị Chữ ký số.

3.1.4

Khóa ký một lần (one-time signing key) khóa ký được tạo ra, sử dụng và hủy bỏ dựa trên một lệnh ủy quyền duy nhất, thường được liên kết với một phiên duy nhất để ký DTBS/R (Dữ liệu cần ký/Đại diện của dữ liệu cần ký)

Chú thích 1: Trái ngược với các khóa ký thông thường, có thể được sử dụng trong nhiều phiên ký khác nhau.

3.2. Chữ viết tắt

CA	Certification Authority	Tổ chức chứng thực
CM	Cryptographic Module certified according to [EN 419 221–5]	Mô-đun mật mã được chứng nhận theo [EN 419 221–5]
CSR	Certification Signing Request	Yêu cầu cấp chứng thư chữ ký số
DTBS/R	Data To Be Signed Representation	Bản biểu diễn của dữ liệu cần được ký/ Giá trị băm của dữ liệu cần được ký
PP	Protection Profile	Hồ sơ bảo vệ
QSCD	Qualified Electronic Signature (or Electronic Seal)	Thiết bị tạo chữ ký số
SSA	Server Signning Application	Ứng dụng ký trên máy chủ ký số

4 Quy định chung

4.1 Tổng quan

Phần này cung cấp thông tin tổng quan và thông tin quản lý tài liệu cần thiết để tiến hành đăng ký hồ sơ bảo vệ. Phần 4.2 "Tài liệu tham chiếu Hồ sơ bảo vệ" cung cấp các thông tin mô tả và dán nhãn cần thiết cho việc đăng ký Hồ sơ bảo vệ (PP). Phần 4.3 Quy định pháp luật. Phần 4.4 "Tổng quan về TOE" tóm tắt TOE (Đối tượng đánh giá) dưới dạng văn bản tường thuật. Theo đó, nội dung này cung cấp cái nhìn tổng quan cho người dùng tiềm năng để quyết định xem PP này có phù hợp với nhu cầu của họ hay không. Nội dung này có thể được sử dụng như một bản tóm tắt độc lập trong các danh mục và sổ đăng ký PP.

4.2 Tài liệu tham chiếu hồ sơ bảo vệ

- **Tiêu đề:** Hồ sơ bảo vệ theo Tiêu chí chung (Common Criteria) – Hồ sơ bảo vệ cho QSCD dành cho Ký số trên máy chủ

- **Phiên bản CC (Tiêu chí chung):** v3.1 bản phát hành 4
- **Phiên bản PP:** 1.0
- **Tác giả:** WG17 (Nhóm công tác 17)
- **Từ khóa:** Ký số trên máy chủ (Server Signing)

4.3 Quy định pháp luật

Theo quy định tại Thông tư số 50/2025/TT-BKHCN ban hành "Quy chuẩn kỹ thuật quốc gia về yêu cầu đối với dịch vụ chứng thực chữ ký số công cộng" đã định nghĩa:

Mô hình ký số từ xa: Mô hình mà khóa bí mật của thuê bao được tạo và lưu trữ tại hệ thống của Tổ chức chứng thực công cộng, việc tạo chữ ký số được thực hiện từ xa theo lệnh của thuê bao thông qua cơ chế xác thực và ủy quyền nghiêm ngặt.

Do đó các Tổ chức chứng thực công cộng nên áp dụng các quy trình bảo mật quản trị và quản lý cụ thể để đảm bảo rằng môi trường tạo chữ ký điện tử là tin cậy và được sử dụng dưới sự kiểm soát duy nhất của người ký. Quy định này yêu cầu, đối với mô hình ký số từ xa phải sử dụng các thiết bị tạo chữ ký số (gọi tắt là QSCD) đáp ứng quy định tại mục 2.3 QCVN 137:2025/BKHCN quy chuẩn kỹ thuật quốc gia về yêu cầu đối với dịch vụ chứng thực chữ ký số công cộng.

4.4 Tổng quan về TOE

4.4.1 Chung (General)

Hệ thống tin cậy hỗ trợ ký máy chủ (TW4S) là một hệ thống cung cấp dich vụ chữ ký số theo mô hình ký số từ xa. Nó đảm bảo rằng khóa ký của người ký hoặc các khóa ký chỉ được sử dụng dưới sự kiểm soát duy nhất của người ký cho mục đích đã định.

Trong tài liệu này, TW4S sử dụng Mô-đun mật mã để tạo khóa ký và tạo giá trị chữ ký số.

Hệ thống bao gồm môi trường cục bộ và từ xa. Người ký ở trong môi trường cục bộ và tương tác bằng thiết bị (ví dụ: máy tính xách tay, máy tính bảng hoặc điện thoại thông minh) với Ứng dụng ký trên máy chủ ký số (SSA) trong môi trường từ xa.

Mục đích của sự tương tác giữa thiết bị và SSA là để người ký sử dụng dịch vụ ký SSA. Thao tác chữ ký được thực hiện bằng giao thức kích hoạt chữ ký (SAP), yêu cầu dữ liệu kích hoạt chữ ký (SAD) được cung cấp tại môi trường cục bộ. SAD liên kết với nhau bởi ba yếu tố: xác thực người ký bằng khóa ký và Giá trị băm của dữ liệu cần được ký (DTBS / R (s)).

Để đảm bảo người ký có quyền kiểm soát duy nhất các khóa ký của mình, thao tác ký cần được ủy quyền. Điều này được thực hiện bởi Mô-đun kích hoạt chữ ký (SAM), có thể xử lý một điểm cuối của SAP, xác minh SAD và kích hoạt khóa ký trong Mô-đun mật mã được chứng nhận theo [EN 419 221–5] (CM). Cả CM và SAM phải được đặt trong một môi trường được được bảo vệ chống tấn công và can thiệp vật lý. Xác thực SAD có

nghĩa là SAM kiểm tra ràng buộc giữa ba yếu tố của SAD cũng như kiểm tra xem người ký có được xác thực hay không.

Một trong ba yếu tố SAD là xác thực người ký. Việc xác thực người ký được giả định sẽ được tiến hành theo EN 419241-1 SCAL.2 đối với các chữ ký đủ điều kiện. Điều này có nghĩa là xác thực người ký có thể được thực hiện theo một trong những cách sau:

- Trực tiếp bởi SAM. Trong trường hợp này, SAM xác minh (các) yếu tố xác thực của người ký.
- Gián tiếp bởi SAM (thông qua cơ chế liên kết định danh Federated Identity / SSO). Trong trường hợp này, một dịch vụ xác thực bên ngoài thuộc hệ thống TW4S hoặc do một bên được ủy quyền sẽ thực hiện việc xác minh (các) yếu tố xác thực của người ký và phát hành một khẳng định (assertion) chứng minh rằng người ký đã được xác thực thành công. Sau đó, SAM sẽ tiến hành kiểm tra và xác thực khẳng định này.
- Sự kết hợp của hai phương pháp trực tiếp hoặc gián tiếp, trong đó một phần của xác thực người ký được thực hiện trực tiếp bởi SAM và phần khác được thực hiện gián tiếp bởi SAM.

Lưu ý: SAD chỉ được sử dụng 1 lần, có quy định về thời gian hiệu lực của SAD (thời gian ngắn, 3 phút, hoặc 5 phút) sau thời gian đó SAD tự hết hiệu lực, SAD bị vô hiệu hóa ngay lập tức khi ký số thành công. Trước khi tạo SAD, người ký phải biết được mình đang xác thực ký cái gì, ký đơn lẻ 1 tài liệu hay ký số cho nhiều tài liệu/giao dịch.

Trong thực tế triển khai hệ thống chữ ký số từ xa (TW4S), để đạt được cấp độ bảo mật cao nhất thường yêu cầu xác thực hai hoặc nhiều yếu tố (Multi-Factor Authentication - MFA). Mô hình kết hợp này hoạt động dựa trên việc chia sẻ trách nhiệm xác thực:

- **Phần trực tiếp bởi SAM (Direct):** Người dùng gửi một yếu tố xác thực trực tiếp vào SAM thông qua giao thức an toàn (SAP). SAM sẽ tự mình đối chiếu và xác minh yếu tố này.

  Ví dụ: Người dùng nhập mã PIN bí mật được lưu trữ hoặc quản lý trực tiếp trong phân hệ bảo mật của lõi SAM.

- **Phần gián tiếp bởi SAM (Indirect):** Một yếu tố xác thực khác của người dùng sẽ được xử lý thông qua một dịch vụ hoặc nền tảng định danh bên ngoài, sau đó dịch vụ này gửi một phiếu xác nhận (assertion/token) để SAM kiểm tra lại.

  Ví dụ: Người dùng quét khuôn mặt/vân tay (sinh trắc học) hoặc nhận mã OTP được xác thực qua một hệ thống Định danh điện tử độc lập (như hệ thống quản lý danh tính tập trung, ứng dụng định danh chuyên dụng trên di động). Hệ thống này xác nhận "Hợp lệ" và gửi thông điệp được ký số sang cho SAM.

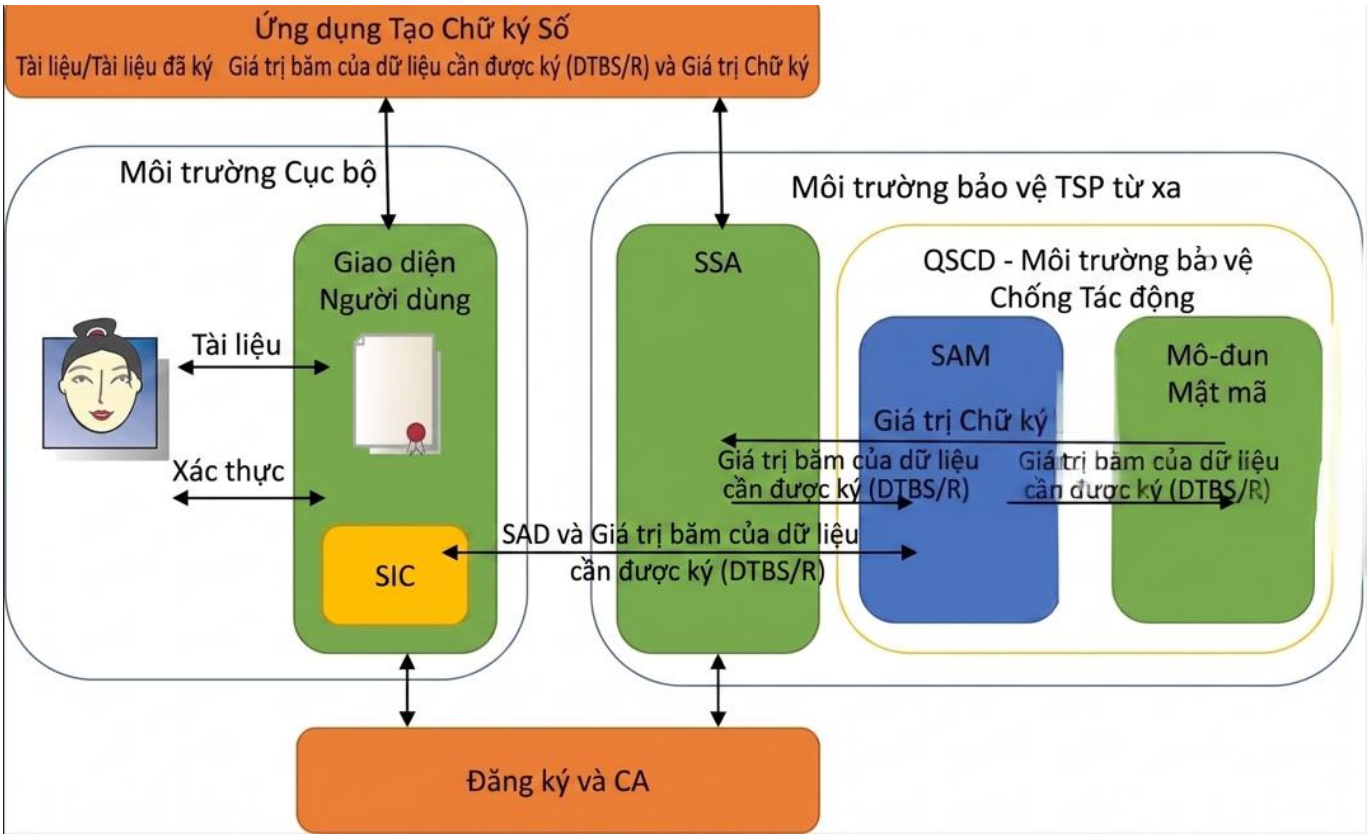
Trong trường hợp việc xác thực người ký không được thực hiện trực tiếp bởi SAM, SAM phải giả định (dựa trên môi trường vận hành) rằng một phần hoặc toàn bộ quy trình xác thực đã diễn ra và tin cậy vào một khẳng định (assertion). Trong phạm vi Hồ sơ bảo vệ (PP) này, 'xác thực người ký' có nghĩa là người ký đã được xác thực theo một trong ba phương thức được đề cập ở trên.

Mô-đun SAM (Mô-đun kích hoạt chữ ký) chính là TOE (Đối tượng đánh giá) của Hồ sơ bảo vệ (PP) này. Để đạt được chứng nhận là một thiết bị QSCD (Thiết bị tạo chữ ký điện tử đủ điều kiện), bắt buộc phải có sự kết hợp

giữa TOE này và một Mô-đun mật mã đã được cấp chứng nhận tuân thủ tiêu chuẩn EN 419221-5. *Hình minh họa dưới đây cung cấp một cái nhìn tổng quan về môi trường mà TOE được đặt trên đó.*

Người ký được đặt trong môi trường cục bộ với giao diện người dùng trên thiết bị (ví dụ: máy tính xách tay, máy tính bảng, điện thoại thông minh). Giao diện người dùng có chức năng hiển thị tài liệu cho người ký. Thiết bị sử dụng thành phần tương tác người ký (SIC) để giao tiếp với SSA. SSA chuyển tiếp thông tin liên lạc từ SIC hoặc từ SSA tới QSCD. Bên trong QSCD, SAM nhận các thông báo và tùy chọn giao tiếp với SSA để lấy dữ liệu liên quan. Khi mô-đun SAM đã xác minh SAD, nó có thể cho phép kích hoạt khóa ký trong CM và tạo ra giá trị chữ ký số. Giá trị được trả lại cho SSA và có thể được chuyển đến SCA hoặc SIC. Theo quan điểm của TOE, SSA và giao diện Người dùng hoạt động như các mô-đun hỗ trợ hiển thị tài liệu và chuyển tiếp các thông điệp giao tiếp.

TOE tạo hồ sơ đánh giá cho tất cả các sự kiện liên quan đến bảo mật và dựa vào SSA để lưu trữ và cung cấp kiểm soát truy cập cho các hồ sơ.



TW4S dựa trên các dịch vụ khác:

- Người ký sẽ được xác định và đăng ký. Nó có thể liên quan đến việc thiết lập cơ chế xác thực cho người ký.

- Khóa ký được cấp bởi Tổ chức chứng thực công cộng.

- Ứng dụng tạo chữ ký số có trách nhiệm tạo ra văn bản đã ký bằng cách sử dụng các giá trị chữ ký do hệ thống TW4S cung cấp.

4.4.2 Loại TOE (TOE type)

TOE (Đối tượng đánh giá) là một thành phần phần mềm thực hiện Giao thức Kích hoạt Chữ ký (SAP). Thành phần này có thể được triển khai theo một trong hai cách: hoặc nằm bên trong phần bảo vệ chống tác động vật lý (tamper protected) của Mô-đun Mật mã, hoặc nằm trong một môi trường bảo vệ chống tác động chuyên dụng độc lập được kết nối với Mô-đun Mật mã thông qua một kênh truyền đáng tin cậy (trusted channel).

TOE sử dụng Dữ liệu Kích hoạt Chữ ký (SAD) do người ký cung cấp để kích hoạt khóa ký tương ứng nhằm sử dụng trong Mô-đun Mật mã.

Sự kết hợp giữa TOE và Mô-đun Mật mã cấu thành một thiết bị QSCD (Thiết bị tạo chữ ký số).

4.4.3 Vòng đời của TOE (TOE life cycle)

Vòng đời của TOE bao gồm các giai đoạn liên tiếp nhau: phát triển, sản xuất, chuẩn bị và đưa vào vận hành sử dụng.

Phát triển (Development): Nhà phát triển TOE tiến hành xây dựng ứng dụng TOE và biên soạn tài liệu hướng dẫn đi kèm. Quá trình này có sử dụng bất kỳ tài liệu hướng dẫn phù hợp nào dành cho các thành phần hoạt động kết hợp với TOE, bao gồm cả Mô-đun Mật mã (HSM).

Bàn giao (Delivery): TOE được bàn giao một cách an toàn từ nhà phát triển TOE đến Nhà cung cấp dịch vụ tin cậy (TSP).

Cài đặt và cấu hình (Installation and configuration): TSP tiến hành cài đặt và cấu hình TOE với các dữ liệu cấu hình và dữ liệu khởi tạo thích hợp. Quá trình cài đặt có thể cho phép khởi tạo các Người dùng có đặc quyền (Privileged Users).

Lưu ý: Người dùng có đặc quyền (Privileged Users) tương ứng nhân sự vận hành hệ thống (Operator) hoặc quản trị hệ thống (Administrator). Trong tài liệu này, để không làm xung đột trách nhiệm và lợi ích của nhân sự nên sử dụng Người dùng có đặc quyền (Privileged Users).

Giai đoạn vận hành (Operational phase): Trong quá trình vận hành, TOE có thể được Người dùng có đặc quyền để tạo ra các nhân sự vận hành mới hoặc tạo Người ký (Signers). Người dùng có đặc quyền có thể duy trì và bảo dưỡng cấu hình của TOE. Cả Người dùng có đặc quyền và Người ký đều có thể tạo các khóa ký cho một Người ký. Người dùng có đặc quyền và Người ký có thể cung cấp dữ liệu cần ký cho TOE, nhưng chỉ duy nhất Người ký mới có quyền ủy quyền (cho phép) tạo chữ ký số.

Giai đoạn kết thúc vòng đời (hủy bỏ/thải loại) của TOE nằm ngoài phạm vi của tài liệu này.

4.4.4 Việc sử dụng và tính năng bảo mật chính của TOE

Các tính năng bảo mật chính của TOE là:

- Quản lý nhà điều hành: Người dùng có đặc quyền có thể tạo Người dùng có đặc quyền khác.
- Quản lý hệ thống: Người dùng có đặc quyền có thể xử lý cấu hình hệ thống.
- Quản lý người ký bao gồm:
  - Người dùng có đặc quyền có thể tạo Người ký.
  - Người dùng có đặc quyền có thể gán một trong ba mô hình xác thực (trực tiếp, gián tiếp hoặc hỗn hợp) cho một Người ký.
  - Người dùng có đặc quyền hoặc Người ký có thể khởi tạo các khóa ký và Dữ liệu xác thực chữ ký (SVD - cụ thể là Khóa công khai / Public Key) bằng cách sử dụng Mô-đun Mật mã (HSM), sau đó gán định danh khóa ký (signing key identifier) và SVD đó cho một Người ký.
  - Người dùng có đặc quyền hoặc Người ký có thể vô hiệu hóa một định danh khóa ký để Người ký

không thể tiếp tục sử dụng khóa đó.

- Vận hành hoạt động ký số
  - Người dùng có đặc quyền hoặc Người ký có thể cung cấp Giá trị băm của dữ liệu cần được ký (DTBS/R) để tiến hành ký.
  - Mối liên kết giữa quy trình xác thực người ký, giá trị băm DTBS/R và định danh khóa ký sẽ do **Dữ liệu Kích hoạt Chữ ký (SAD)** xử lý. SAD này được trao đổi một cách an toàn với TOE thông qua **Giao thức Kích hoạt Chữ ký (SAP)**. Bên trong lõi TOE, các hành động sau sẽ được thực hiện:
    - SAD được xác minh tính toàn vẹn.
    - SAD được xác minh rằng nó liên kết với xác thực Người ký, (các) DTBS / R và mã định danh khóa ký.
    - Người ký xác định trong SAD được xác thực bằng một trong ba sơ đồ xác thực.
    - (Các) DTBS / R được sử dụng cho các hoạt động chữ ký được liên kết với SAD.
    - Mã định danh khóa ký được chỉ định cho Người ký.
    - TOE sử dụng Dữ liệu Ủy quyền để kích hoạt khóa ký trong Mô-đun Mật mã.
    - TOE sử dụng Mô-đun mật mã để tạo chữ ký.
- TOE tạo hồ sơ đánh giá cho tất cả các sự kiện liên quan đến bảo mật và dựa vào SSA để lưu trữ và cung cấp kiểm soát truy cập cho các hồ sơ.

TOE xử lý các tài sản dữ liệu như được chỉ định trong 6.1.

4.4.5 Tổng quan chung về môi trường TOE

- Hồ sơ bảo vệ (PP) này được xây dựng nhằm hỗ trợ các Nhà cung cấp dịch vụ tin cậy (TSP) có nhu cầu sử dụng một thiết bị QSCD cho mô hình ký trên máy chủ (server signing).

- TOE được kỳ vọng sẽ:

1. Vận hành như một phần của hệ thống ký trên máy chủ theo quy định trong tiêu chuẩn **EN 419241-1**.
2. Được sử dụng bởi một TSP đang áp dụng các chính sách bảo mật theo yêu cầu đối với các TSP cung cấp dịch vụ tạo chữ ký số.
3. Được sử dụng kết hợp với các TSP có chức năng cung cấp dịch vụ chứng thực chữ ký số (CA).

4.4.6 Hardware/software/firmware ngoài TOE

- Để có thể vận hành, TOE cần tối thiểu các thành phần phần cứng, phần mềm hoặc firmware bên ngoài sau đây:

- **Ứng dụng Tạo Chữ ký Số (SCA - Signature Creation Application):** Có nhiệm vụ quản lý văn bản cần ký và chuyển văn bản đó tới ứng dụng SSA, có thể chuyển trực tiếp hoặc chuyển thông qua SIC.
- **Cấu phần SSA (Ứng dụng ký trên máy chủ ký số):** Chịu trách nhiệm xử lý thông tin liên lạc giữa mô-đun SAM nằm bên trong thiết bị QSCD và thành phần SIC nằm trên thiết bị của người ký.
- **Thành phần SIC (Thành phần Tương tác Người ký):** Được người ký sử dụng cục bộ (trên thiết bị cá nhân) để giao tiếp và kết nối với các hệ thống từ xa.
- **Mô-đun Mật mã (HSM):** Đã được cấp chứng nhận tuân thủ tiêu chuẩn **EN 419221-5**, đóng vai trò hỗ trợ và nền tảng cho hoạt động của TOE.

4.4.7 Các tùy chọn

Hồ sơ bảo vệ (PP) này bao gồm các tùy chọn mà người viết Tài liệu mục tiêu bảo mật (ST writer - Security Target writer) phải chỉ rõ. Để hỗ trợ người viết ST trong việc xác định các tùy chọn này, nội dung tổng hợp của chúng được trình bày chi tiết trong Bảng 1.

Bảng 1

Lựa chọn	Sự miêu tả
Triển khai	TOE có thể được triển khai trong một Mô-đun mật mã hoặc trong một mô-đun phần cứng chuyên dụng. Người viết ST sẽ đặc biệt chú ý đến các SFR FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FCS_RNG.1, FPT_PHP.1, FPT_PHP.3 và FTP_ITC.1 / CM vì các SFR này có thể được đáp ứng khác nhau tùy thuộc vào việc triển khai.

5 Tuyên bố về sự phù hợp

5.1 Tuyên bố sự phù hợp CC

- Hồ sơ bảo vệ (PP) này tuyên bố **mở rộng Phần 2 (Part 2 extended)** và **tuân thủ Phần 3 (Part 3 conformant)** của Tiêu chí Chung (Common Criteria), đồng thời được biên soạn dựa trên Tiêu chí Chung phiên bản 3.1 R4 [CC1], [CC2] và [CC3].

- Yêu cầu đảm bảo an toàn (assurance requirement) của Hồ sơ bảo vệ này là **EAL4+ (EAL4 augmented)**. Thành phần tăng cường được lựa chọn từ:

AVA_VAN.5 Phân tích lỗ hổng có phương pháp ở mức nâng cao (Advanced methodical vulnerability analysis)

5.2 Tuyên bố tuân thủ PP

Hồ sơ bảo vệ (PP) này không tuyên bố tuân thủ bất kỳ Hồ sơ bảo vệ nào khác.

5.3 Cơ sở lý luận về tính tuân thủ

Vì Hồ sơ bảo vệ (PP) này không tuyên bố tuân thủ bất kỳ hồ sơ bảo vệ nào khác, nên không cần thiết phải đưa ra cơ sở lý luận ở mục này.

5.4 Tuyên bố mức độ tuân thủ

Hồ sơ bảo vệ (PP) này yêu cầu sự tuân thủ nghiêm ngặt (strict conformance) đối với bất kỳ Tài liệu mục tiêu bảo mật (ST) hoặc Hồ sơ bảo vệ (PP) nào khác tuyên bố tuân thủ theo Hồ sơ bảo vệ (PP) này.

6 Xác định các vấn đề bảo mật

6.1 Tài sản

- TOE sở hữu các tài sản sau đây, những tài sản này cần được bảo vệ tính toàn vẹn (integrity) và tính bí mật (confidentiality) như mô tả dưới đây. TOE phải đảm bảo rằng bất cứ khi nào một tài sản được lưu trữ kiên cố (lưu dữ liệu lâu dài) bên ngoài TOE, TOE phải thực hiện các hoạt động mật mã cần thiết để thực thi tính bí mật

và phát hiện xem tài sản đó có bị sửa đổi hay không. Việc kiểm soát truy cập đối với các tài sản của TOE khi nằm ngoài phạm vi TOE sẽ do môi trường vận hành thực thi.

- R.Signing_Key_Id (Định danh Khóa ký): Khóa ký là khóa bí mật (private key) của một cặp khóa bất đối xứng được sử dụng để tạo ra một chữ ký số dưới quyền kiểm soát duy nhất của người ký. Khóa ký chỉ có thể được sử dụng bởi Mô-đun Mật mã (HSM). TOE sử dụng tài sản R.Signing_Key_Id để định danh một khóa ký cụ thể nằm trong Mô-đun Mật mã. Mối ràng buộc liên kết giữa R.Signing_Key_Id và R.Signer (Người ký) phải được bảo vệ tính toàn vẹn.

- Lưu ý ứng dụng 1 (Application Note 1)

Tính toàn vẹn, tính bí mật của khóa ký và mối liên kết giữa R.Signing_Key_Id với chính khóa ký đó thuộc về trách nhiệm của Mô-đun Mật mã. TOE sẽ chịu trách nhiệm đảm bảo rằng chỉ có duy nhất người ký mới có thể sử dụng khóa ký đó dưới sự kiểm soát duy nhất của mình.

R.Authorisation_Data (Dữ liệu Ủy quyền): Là dữ liệu được TOE sử dụng để kích hoạt một khóa ký trong Mô-đun Mật mã. Khóa ký này được định danh bởi R.Signing_Key_Id. Tài sản này phải được bảo vệ tính toàn vẹn và tính bí mật tuyệt đối.

- Lưu ý ứng dụng 2 (Application Note 2)

R.Authorisation_Data (Dữ liệu Ủy quyền) được Mô-đun Mật mã sử dụng để kích hoạt một khóa ký. Dữ liệu này có thể là một tài sản sẵn có của TOE hoặc do TOE tạo ra (phái sinh) từ gói dữ liệu SAD. Trong cả hai trường hợp, TOE bắt buộc phải xác thực gói dữ liệu SAD trước khi R.Authorisation_Data được sử dụng để kích hoạt khóa ký bên trong Mô-đun Mật mã.

Nếu TOE tạo ra R.Authorisation_Data từ gói dữ liệu SAD, thì dữ liệu này có thể không cần phải lưu giữ lại trong TOE.

R.SVD (Dữ liệu xác thực chữ ký): Là phần khóa công khai (public key) liên kết với khóa ký, được sử dụng để thực hiện việc kiểm tra và xác thực chữ ký số. Tài sản R.SVD phải được bảo vệ tính toàn vẹn.

TOE sử dụng một Mô-đun Mật mã để thực hiện việc khởi tạo cặp khóa ký. Là một phần của quy trình khởi tạo cặp khóa ký này, Mô-đun Mật mã sẽ cung cấp cho TOE mã định danh R.Signing_Key_Id và khóa công khai R.SVD. Sau đó, TOE sẽ cung cấp khóa công khai R.SVD này cho ứng dụng SSA để xử lý các bước tiếp theo phục vụ cho việc cấp phát chứng thư số cho cặp khóa đó.

R.DTBS/R (Giá trị băm của dữ liệu cần được ký): Tập hợp dữ liệu được truyền tới TOE để phục vụ việc tạo chữ ký số thay mặt cho người ký. Giá trị băm DTBS/R phải được bảo vệ tính toàn vẹn. Việc truyền dữ liệu DTBS/R tới TOE bắt buộc phải yêu cầu bên gửi - có thể là Người ký hoặc Người dùng có đặc quyền - phải được xác thực danh tính thành công.

- Lưu ý ứng dụng (Application Note) về mặt logic kỹ thuật, thường thiết lập quy tắc kiểm tra tính toàn vẹn của mã băm tài liệu từ lúc bắt đầu gửi cho đến khi đưa vào HSM.

- Lưu ý ứng dụng 3 (Application Note 3)

Tính bí mật (confidentiality) của tài sản R.DTBS/R (Giá trị băm của dữ liệu cần được ký) không phải là yêu cầu bắt buộc theo quy định tại Luật Giao dịch điện tử năm 2023.

R.SAD (Dữ liệu kích hoạt chữ ký): Là tập hợp các dữ liệu tham gia vào giao thức kích hoạt chữ ký (SAP), có nhiệm vụ kích hoạt dữ liệu tạo chữ ký số (khóa ký) để tạo ra một chữ ký số dưới sự kiểm soát duy nhất của người ký. Tài sản R.SAD bắt buộc phải kết hợp đồng thời các yếu tố sau:

Quy trình xác thực mạnh (strong authentication) của người ký theo quy định trong tiêu chuẩn EN 419241-1.

Một tham chiếu duy nhất dẫn đến R.Signing_Key_Id (trừ trường hợp một khóa cụ thể đã được ngầm định sẵn, ví dụ: khóa mặc định hoặc khóa dùng một lần - one-time key).

Một giá trị băm R.DTBS/R cụ thể được chỉ định.

Tài sản R.SAD phải được bảo vệ tính toàn vẹn và tính bí mật tuyệt đối.

- Lưu ý ứng dụng 4 (Application Note 4)

Nếu gói dữ liệu SAD không yêu cầu các dữ liệu mã hóa, thì yêu cầu về tính bí mật được coi là đã được đáp ứng. Người viết Tài liệu mục tiêu bảo mật (ST writer) phải mô tả rõ phần nào của gói dữ liệu SAD bắt buộc phải được bảo vệ tính bí mật.

- Lưu ý ứng dụng 5 (Application Note 5)

Gói dữ liệu R.SAD có thể bao gồm một số hoặc tất cả các yếu tố xác thực, hoặc bao gồm các bằng chứng từ các hệ thống khác minh chứng rằng một số hoặc tất cả các yếu tố xác thực đã được xác minh thành công.

- Lưu ý ứng dụng 6 (Application Note 6)

Tham chiếu duy nhất dẫn đến R.Signing_Key_Id bên trong R.SAD có thể là một chứng thư số, một định danh khóa hoặc thông tin phái sinh thu được từ quá trình xác thực của người ký.

Một số giải pháp có thể sử dụng các khóa ký dùng một lần (one-time signing keys) - loại khóa được khởi tạo, cấp chứng thư số và sử dụng trong phạm vi một phiên ký giới hạn. Thông tin phái sinh từ quá trình xác thực người ký có thể được sử dụng để phân tách các phiên ký (nếu một người ký có nhiều phiên ký đồng thời với TOE), hoặc để suy ra R.Signing_Key_Id nếu đó là khóa dùng một lần. Khi kết thúc phiên ký, khóa ký phải được hủy kích hoạt một cách tin cậy.

Đối với các giải pháp chỉ xử lý duy nhất một khóa ký cho mỗi người ký, tham chiếu đến R.Signing_Key_Id có thể được hiểu ngầm và lược bỏ khỏi gói dữ liệu SAD.

Người viết Tài liệu mục tiêu bảo mật (ST writer) phải mô tả rõ R.Signing_Key_Id là gì đối với một TOE cụ thể.

R.Signature (Chữ ký số / Giá trị chữ ký): Là kết quả của hoạt động ký và là một giá trị chữ ký số. R.Signature được tạo ra trên giá trị băm R.DTBS/R bằng cách sử dụng R.Signing_Key_Id bởi Mô-đun Mật mã (HSM) dưới sự kiểm soát của người ký như một phần của giao thức SAP. Tài sản R.Signature phải được bảo vệ tính toàn vẹn. R.Signature có thể được kiểm tra và xác thực ở bên ngoài TOE bằng cách sử dụng khóa công khai R.SVD.

R.Audit (Dữ liệu kiểm toán / Nhật ký hệ thống): Là các bản ghi kiểm toán chứa nhật ký của các sự kiện bắt buộc phải kiểm toán. Các nhật ký này do TOE tạo ra và được lưu trữ ở môi trường bên ngoài. Tài sản R.Audit phải được bảo vệ tính toàn vẹn.

R.Signer (Thông tin Người ký): Là một đối tượng trong TOE chứa tập hợp dữ liệu giúp định danh người ký duy nhất trong phạm vi TOE. Tài sản R.Signer phải được bảo vệ tính toàn vẹn và tính bí mật.

- Lưu ý ứng dụng 7 (Application Note 7)

Đối tượng R.Signer chỉ cần đảm bảo tính duy nhất trong phạm vi nội bộ của TOE. TOE không có trách nhiệm thiết lập mối liên hệ giữa đối tượng R.Signer này với danh tính thực tế ngoài đời thực của người ký. Người ký được coi là chủ sở hữu của đối tượng R.Signer định danh duy nhất trong TOE.

- Lưu ý ứng dụng 8 (Application Note 8)

Đối tượng R.Signer có thể bao gồm các tham chiếu đến 0, 1 hoặc có nhiều mã định danh R.Signing_Key_Id và khóa công khai R.SVD khác nhau.

- Lưu ý ứng dụng 9 (Application Note 9)

Nếu đối tượng R.Signer không yêu cầu dữ liệu phải mã hóa, thì yêu cầu về tính bí mật được coi là đã được đáp ứng. Người viết ST phải mô tả rõ phần nào của đối tượng R.Signer bắt buộc phải được bảo vệ tính bí mật.

R.Reference_Signer_Authentication_Data (Dữ liệu xác thực người ký tham chiếu): Là tập hợp dữ liệu được TOE sử dụng để xác thực người ký. Nó chứa toàn bộ dữ liệu (ví dụ: số sê-ri của thiết bị OTP, số điện thoại, cấu hình giao thức...) và các khóa (ví dụ: khóa thiết bị, khóa xác thực...) được TOE sử dụng để kiểm tra danh tính người ký. Thành phần này có thể bao gồm một khóa công khai SVD hoặc chứng thư số để xác thực một khẳng định (assertion) được cung cấp từ kết quả của quy trình xác thực ủy quyền (xác thực gián tiếp).

Tài sản R.Reference_Signer_Authentication_Data phải được bảo vệ tính toàn vẹn và tính bí mật tuyệt đối.

- Lưu ý ứng dụng 10 (Application Note 10)

R.Reference_Signer_Authentication_Data được TOE sử dụng để xác thực người ký, còn R.Authorisation_Data được TOE sử dụng để kích hoạt khóa ký trong Mô-đun Mật mã (HSM).

- Lưu ý ứng dụng 11 (Application Note 11)

Nếu R.Reference_Signer_Authentication_Data không yêu cầu dữ liệu phải mã hóa thì yêu cầu về tính bí mật được coi là đã được đáp ứng. Người viết ST phải mô tả rõ phần nào của tài sản này bắt buộc phải được bảo vệ tính bí mật.

R.TSF_DATA (Dữ liệu cấu hình chức năng an toàn của TOE): Là tập hợp các dữ liệu cấu hình hệ thống được sử dụng để vận hành TOE. Tài sản này phải được bảo vệ tính toàn vẹn.

- Lưu ý ứng dụng 12 (Application Note 12)

Dữ liệu cấu hình TOE có thể bao gồm: thuật toán mã hóa, độ dài khóa, các luồng quy trình cho giao thức SAP...

R.Privileged_User (Thông tin Người dùng có đặc quyền): Là một đối tượng trong TOE chứa tập hợp dữ liệu định danh duy nhất một Người dùng có đặc quyền (nhân sự quản trị/vận hành) trong phạm vi TOE. Tài sản này phải được bảo vệ tính toàn vẹn.

R.Reference_Privileged_User_Authentication_Data (Dữ liệu xác thực người dùng có đặc quyền tham chiếu): Là tập hợp dữ liệu được TOE sử dụng để xác thực Người dùng có đặc quyền. Tài sản này phải được bảo vệ tính toàn vẹn và tính bí mật.

- Lưu ý ứng dụng 13 (Application Note 13)

Nếu tài sản này không yêu cầu dữ liệu phải mã hóa thì yêu cầu về tính bí mật được coi là đã được đáp ứng. Người viết ST phải mô tả rõ phần nào của tài sản bắt buộc phải được bảo vệ tính bí mật.

R.Random (Dữ liệu ngẫu nhiên bí mật): Là các bí mật ngẫu nhiên (ví dụ: các khóa mật mã ngẫu nhiên) được TOE sử dụng để vận hành hệ thống và thiết lập giao tiếp an toàn với các bên bên ngoài. Tài sản này phải được bảo vệ tính toàn vẹn và tính bí mật tuyệt đối.

6.2 Chủ thể (Subjects)

Danh sách các chủ thể sau đây thực hiện tương tác với TOE:

Người ký (Signer): Là cá nhân (natural person) hoặc pháp nhân (legal person) sử dụng TOE thông qua giao thức SAP - nơi họ cung cấp dữ liệu SAD và có thể ký vào (các) giá trị băm DTBS/R bằng cách sử dụng khóa ký của mình nằm bên trong Mô-đun Mật mã (HSM).

Người dùng có đặc quyền (Privileged User): Là nhân sự thực hiện các chức năng quản trị của TOE và có khả năng cung cấp giá trị băm DTBS/R cho TOE như một phần của hoạt động vận hành ký số.

- Lưu ý ứng dụng 14 (Application Note 14)

Danh sách các chủ thể được mô tả trong tiêu chuẩn EN 419241-1:2018, mục 6.2.1.2 SRG M.1.2 chứa nhiều vai trò hơn vì danh sách đó bao quát toàn bộ hệ thống TW4S hoàn chỉnh.

Người viết Tài liệu mục tiêu bảo mật (ST writer) phải mô tả rõ các vai trò cụ thể mà sản phẩm thực tế triển khai và cách các vai trò này liên kết với các quy tắc ủy quyền trong các Yêu cầu chức năng bảo mật (SFR).

- Lưu ý ứng dụng 15 (Application Note 15)

Ứng dụng SSA (Ứng dụng ký trên máy chủ ký số) đóng một vai trò đặc biệt vì nó tương tác trực tiếp với TOE. Người dùng có đặc quyền có thể tương tác với TOE theo cách trực tiếp hoặc thông qua ứng dụng SSA. Nếu bản thân ứng dụng SSA (dưới dạng một dịch vụ tự động) có thể thực hiện được các chức năng quản trị - ví dụ như khởi tạo tài khoản người ký - thì trong phạm vi Hồ sơ bảo vệ (PP) này, hành động đó được coi là vai trò của Người dùng có đặc quyền.

- Lưu ý ứng dụng 16 (Application Note 16)

Việc khởi tạo tài khoản người ký, quản lý dữ liệu xác thực người ký tham chiếu và quy trình khởi tạo khóa ký sẽ được thực hiện kết hợp với một đại lý (RA - Registration Authority) – tổ chức cung cấp dịch vụ đăng ký sử dụng ứng dụng SSA, như được quy định cụ thể trong tiêu chuẩn (ví dụ: [ETSI EN 319 411-1]).

6.3 Các mối đe dọa

6.3.1 Tổng quan

Các mối đe dọa sau đây được định nghĩa đối với TOE. Kẻ tấn công (attacker) được mô tả trong mỗi mối đe dọa là một chủ thể không được cấp quyền thực hiện hoạt động liên quan, nhưng kẻ đó có thể xuất hiện dưới danh nghĩa là một người dùng vô danh hoặc là một trong các chủ thể đã được định nghĩa khác.

6.3.2 Giai đoạn đăng ký (Enrolment)

Các mối đe dọa trong giai đoạn đăng ký bao gồm:

- T.ENROLMENT_SIGNER_IMPERSONATION (Giả mạo người ký trong giai đoạn đăng ký)

Kẻ tấn công giả mạo danh tính của người ký trong quá trình đăng ký tài khoản hệ thống. Ví dụ, việc giả mạo có thể thực hiện bằng cách:

Truyền thông tin Người ký (R.Signer) sai lệch từ Cơ quan đăng ký (RA) vào TOE.

Truyền dữ liệu xác thực người ký tham chiếu (R.Reference_Signer_Authentication_Data) sai lệch từ RA vào TOE.

Các tài sản bị đe dọa bao gồm: R.Signer và R.Reference_Signer_Authentication_Data.

Sự giả mạo này có thể dẫn đến việc hệ thống xác thực sai người ký trong tương lai, từ đó dẫn đến các hoạt động ký số trái phép thay mặt cho người ký hợp pháp.

- T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED (Lộ lọt dữ liệu xác thực của người ký trong giai đoạn đăng ký)

Kẻ tấn công có thể thu thập được một phần hoặc toàn bộ Dữ liệu xác thực người ký tham chiếu (R.Reference_Signer_Authentication_Data) trong giai đoạn đăng ký. Nguy cơ này có thể xảy ra trong quá trình khởi tạo, lưu trữ hoặc truyền dữ liệu vào TOE, hoặc trong quá trình truyền tải giữa người ký và TOE. Ví dụ như:

- Thông qua việc đọc trộm dữ liệu (xâm phạm tính bí mật).
- Thông qua việc thay đổi dữ liệu, ví dụ: thay đổi dữ liệu về một giá trị mà kẻ tấn công đã biết trước (xâm phạm tính toàn vẹn).

Tài sản bị đe dọa: R.Reference_Signer_Authentication_Data.

Hậu quả: Việc lộ lọt dữ liệu này có thể dẫn đến việc hệ thống xác thực sai người ký, từ đó dẫn đến các hoạt động ký số trái phép thay mặt cho người ký hợp pháp.

Lưu ý: Các mối đe dọa trong giai đoạn đăng ký sẽ trở thành các mối đe dọa đối với môi trường vận hành bên ngoài trong trường hợp TOE hỗ trợ cơ chế xác thực gián tiếp (xác thực từ một dịch vụ bên ngoài).

- Lưu ý ứng dụng 17 (Application Note 17)

Phải có một kênh truyền tải an toàn để chuyển tài sản R.SVD (Khóa công khai) từ TOE đến Đại lý (RA) hoặc Tổ chức chứng thực (CA). Mô-đun SAM được kỳ vọng sẽ tạo ra một Yêu cầu cấp chứng thư chữ ký số (CSR - Certificate Signing Request).

Nếu dịch vụ đăng ký của TSP cấp phát chứng thư chữ ký số yêu cầu một bản "bằng chứng về quyền sở hữu hoặc quyền kiểm soát khóa bí mật" (proof of possession or control of the private key) liên kết với khóa công khai SVD đó, như được quy định tại tiêu chuẩn [ETSI EN 319 411-1] Điều 6.3.1 a), thì mối đe dọa này (T.SVD_FORGERY) có thể được ngăn chặn mà không cần áp dụng bất kỳ biện pháp đặc biệt tại TOE.

6.3.3 Quản lý người ký

Các mối đe dọa trong quá trình quản lý người ký bao gồm:

- **T.ADMIN_IMPERSONATION (Giả mạo Quản trị viên / Người dùng có đặc quyền)** Kẻ tấn công giả mạo thành một Người dùng có đặc quyền (Privileged User) để cập nhật, thay đổi các tài sản như: Dữ liệu xác thực người ký tham chiếu (R.Reference_Signer_Authentication_Data), Định danh khóa ký (R.Signing_Key_Id) hoặc Khóa công khai (R.SVD).

Tài sản bị đe dọa: R.Reference_Signer_Authentication_Data, R.SVD và R.Signing_Key_Id. **Hậu quả:** Việc sửa đổi dữ liệu trái phép này có thể tạo điều kiện cho một quy trình xác thực người ký sai lệch có thể xảy ra trong tương lai, dẫn đến các hoạt động ký số trái phép thay mặt cho người ký hợp pháp.

- **T.MAINTENANCE_AUTHENTICATION_DISCLOSE (Lộ lọt dữ liệu xác thực trong quá trình bảo trì/cập nhật)** Kẻ tấn công làm lộ lọt hoặc thay đổi (ví dụ: chuyển đổi về một giá trị mà kẻ tấn công đã biết trước) Dữ liệu xác thực người ký tham chiếu (R.Reference_Signer_Authentication_Data) trong quá trình hệ thống thực hiện cập nhật/bảo trì, từ đó kẻ tấn công có khả năng tự tạo ra chữ ký số.

Tài sản bị đe dọa: R.Reference_Signer_Authentication_Data và R.Signing_Key_Id. **Hậu quả:** Việc lộ lọt dữ liệu này có thể dẫn đến việc hệ thống xác thực sai người ký, từ đó dẫn đến các hoạt động ký số trái phép thay mặt cho người ký hợp pháp.

6.3.4 Vận hành

Mục này mô tả các mối đe dọa đối với hoạt động vận hành ký số, bao gồm cả quy trình xác thực.

- T.AUTHENTICATION_SIGNER_IMPERSONATION (Giả mạo người ký trong quá trình xác thực)

Kẻ tấn công giả mạo danh tính của người ký bằng cách sử dụng Dữ liệu xác thực người ký tham chiếu (R.Reference_Signer_Authentication_Data) bị làm giả, sau đó truyền dữ liệu này tới TOE trong suốt giao thức SAP và sử dụng nó để ký vào chính giá trị băm DTBS/R đó hoặc một giá trị băm DTBS/R đã bị sửa đổi.

Tài sản bị đe dọa: R.Reference_Signer_Authentication_Data, R.SAD và R.Signing_Key_Id.

- T.SIGNER_AUTHENTICATION_DATA_MODIFIED (Sửa đổi dữ liệu xác thực của người ký) Kẻ tấn công có thể sửa đổi Dữ liệu xác thực người ký tham chiếu (R.Reference_Signer_Authentication_Data) ngay bên trong TOE hoặc trong quá trình hệ thống thực hiện bảo trì.

Tài sản bị đe dọa: R.Reference_Signer_Authentication_Data.

Hậu quả: Việc sửa đổi dữ liệu trái phép này có thể dẫn đến việc hệ thống xác thực sai người ký, từ đó dẫn đến các hoạt động ký số trái phép thay mặt cho người ký hợp pháp.

- T.SAP_BYPASS (Bỏ qua giao thức kích hoạt chữ ký - SAP)

Kẻ tấn công bỏ qua một hoặc nhiều bước trong giao thức SAP và có khả năng tự tạo ra chữ ký số mà không cần người ký phải thực hiện ủy quyền (cho phép) cho hoạt động đó.

Tài sản bị đe dọa: R.SAD.

- T.SAP_REPLAY (Tấn công lặp lại giao thức kích hoạt chữ ký - SAP Replay)

Kẻ tấn công thực hiện gửi lặp lại (replay) một hoặc nhiều bước của giao thức SAP và có khả năng tự tạo ra chữ ký số mà không cần người ký thực hiện ủy quyền cho hoạt động đó.

Tài sản bị đe dọa: R.SAD.

- T.SAD_FORGERY (Giả mạo dữ liệu kích hoạt chữ ký): Kẻ tấn công giả mạo hoặc can thiệp vào R.SAD trong quá trình truyền tải qua SAP và có khả năng tạo ra chữ ký mà không cần sự ủy quyền thực hiện từ người ký. Tài sản R.SAD đang bị đe dọa.

- Kẻ tấn công làm giả hoặc thao túng cấu trúc gói dữ liệu R.SAD (Dữ liệu kích hoạt chữ ký) trong quá trình truyền tải thuộc giao thức SAP, từ đó có khả năng tự tạo ra chữ ký số mà không cần người ký phải thực hiện ủy quyền cho hoạt động đó.

Tài sản bị đe dọa: R.SAD.

- T.SIGNATURE_REQUEST_DISCLOSURE (Lộ lọt yêu cầu ký số)

Kẻ tấn công thu thập và biết được thông tin của tài sản R.DTBS/R (Giá trị băm của dữ liệu cần được ký) hoặc R.SAD (Dữ liệu kích hoạt chữ ký) trong quá trình các dữ liệu này được truyền tải tới TOE.

Tài sản bị đe dọa: R.DTBS/R và R.SAD.

Biện pháp giảm thiểu: Nếu hệ thống quy định cấu phần R.DTBS/R hoặc R.SAD không bắt buộc phải mã hóa dữ liệu thì mối đe dọa này được coi là đã được giảm thiểu (hoặc không gây rủi ro an toàn cốt lõi).

- T.DTBSR_FORGERY (Giả mạo giá trị băm của dữ liệu cần được ký)

Kẻ tấn công sửa đổi tài sản R.DTBS/R trong quá trình truyền tải tới TOE, từ đó có khả năng tạo ra một chữ ký số trên chính giá trị băm đã bị sửa đổi này mà không cần người ký thực hiện ủy quyền vận hành cho giá trị băm R.DTBS/R đó.

Tài sản bị đe dọa: R.DTBS/R.

- T.SIGNATURE_FORGERY (Giả mạo giá trị chữ ký số đầu ra)

Kẻ tấn công sửa đổi giá trị chữ ký số R.Signature trong hoặc sau quá trình khởi tạo, hoặc trong quá trình truyền tải chữ ký đó ra bên ngoài phạm vi TOE.

Tài sản bị đe dọa: R.Signature.

- Lưu ý ứng dụng 18 (Application Note 18)

Việc sửa đổi chữ ký số hoàn toàn có thể bị phát hiện bởi ứng dụng SSA hoặc bất kỳ bên sử dụng dịch vụ (relying party) nào khác thông qua quy trình kiểm tra và kiểm thử (validation) hiệu lực của chữ ký số đó.

6.3.5 Hệ thống

Các mối đe dọa đối với hệ thống bao gồm:

- T.PRIVILEGED_USER_INSERTION (Cài cắm trái phép Người dùng có đặc quyền)

Kẻ tấn công có khả năng tự khởi tạo đối tượng R.Privileged_User bao gồm cả R.Reference_Privileged_User_Authentication_Data (Dữ liệu xác thực người dùng có đặc quyền tham chiếu) giả mạo, từ đó có thể đăng nhập vào TOE dưới danh nghĩa là một Người dùng có đặc quyền (nhân sự quản trị/vận hành).

Tài sản bị đe dọa: R.Privileged_User và R.Reference_Privileged_User_Authentication_Data.

- T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION (Sửa đổi dữ liệu xác thực của Người dùng có đặc quyền)

Kẻ tấn công sửa đổi tài sản R.Reference_Privileged_User_Authentication_Data của một tài khoản quản trị hợp pháp, từ đó có thể đăng nhập vào TOE dưới danh nghĩa của Người dùng có đặc quyền đó.

Tài sản bị đe dọa: R.Reference_Privileged_User_Authentication_Data.

- T.AUTHORISATION_DATA_UPDATE (Cập nhật trái phép dữ liệu ủy quyền)

Kẻ tấn công giả mạo thành một Người dùng có đặc quyền để tiến hành cập nhật, thay đổi tài sản R.Authorisation_Data (Dữ liệu ủy quyền gửi vào HSM), từ đó có khả năng kích hoạt trái phép một khóa ký nằm trong Mô-đun Mật mã (HSM).

Tài sản bị đe dọa: R.Authorisation_Data và R.Signing_Key_Id.

- Lưu ý ứng dụng 19 (Application Note 19)

Trong một số ứng dụng, kẻ tấn công chỉ cần có quyền truy cập vào hai tài sản R.Authorisation_Data và R.Signing_Key_Id là đã đủ để tự kích hoạt khóa ký bên trong Mô-đun Mật mã (HSM). Do mã định danh R.Signing_Key_Id là tài sản chỉ yêu cầu bảo vệ tính toàn vẹn chứ không bắt buộc bảo vệ tính bí mật, nên việc quyền truy cập vào tài sản R.Authorisation_Data bắt buộc chỉ được phép cấp cho các nhân sự vận hành đã được ủy quyền (authorized operators).

- T.AUTHORISATION_DATA_DISCLOSE (Lộ lọt dữ liệu ủy quyền)

Kẻ tấn công làm lộ lọt tài sản R.Authorisation_Data trong quá trình hệ thống thực hiện cập nhật/bảo trì, từ đó có khả năng tự kích hoạt một khóa ký bên trong HSM.

Tài sản bị đe dọa: R.Authorisation_Data và R.Signing_Key_Id.

- T.CONTEXT_ALTERATION (Thay đổi bối cảnh / Cấu hình hệ thống)

Kẻ tấn công sửa đổi dữ liệu cấu hình hệ thống R.TSF_DATA để thực hiện một hoạt động vận hành trái phép.

Tài sản bị đe dọa: R.Signing_Key_Id, R.SVD, R.SAD, R.Reference_Signer_Authentication_Data và R.TSF_DATA.

- T.AUDIT_ALTERATION (Sửa đổi dữ liệu kiểm toán / Nhật ký hệ thống)

Kẻ tấn công sửa đổi hệ thống nhật ký kiểm toán nhằm xóa sạch hoặc che giấu dấu vết của việc thay đổi cấu hình hoặc sử dụng TOE trái phép.

Tài sản bị đe dọa: R.SVD, R.SAD, R.Signer, R.Reference_Signer_Authentication_Data, R.DTBS/R, R.Signature, R.AUDIT và R.TSF_DATA.

- T.RANDOM (Tấn công suy đoán dữ liệu ngẫu nhiên bí mật)

Kẻ tấn công có khả năng dự đoán được các bí mật ngẫu nhiên của hệ thống (R.Random), từ đó có thể tự khởi tạo, sửa đổi các đối tượng trong TOE hoặc can thiệp trái phép vào quá trình truyền thông kết nối với các hệ thống bên ngoài.

Tài sản bị đe dọa: R.Random.

6.4 Mối quan hệ giữa các mối đe dọa và tài sản (Relation between threats and assets)

Bảng dưới đây cung cấp một cái nhìn tổng quan về mối quan hệ giữa tài sản, các thuộc tính bảo mật liên quan và các mối đe dọa. Để biết thêm thông tin chi tiết, vui lòng tham khảo nội dung của từng mối đe dọa cụ thể trong các mục trước đó.

Bảng 2

Tài sản	Kích thước bảo mật	Các mối đe dọa
R.Sign_Key_Id	Tính toàn vẹn	T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION
R.Authorisation_Data	Tính toàn vẹn	T.AUTHORISATION_DATA_UPDATE
	Tính bí mật	T.AUTHORISATION_DATA_UPDAT E T.AUTHORISATION_DATA _DISCLOSE
R.SVD	Tính toàn vẹn	T.SVD_FORGERY T.ADMIN_IMPERSONATION T.CONTEXT_ALTERATION T.AUDIT_ALTERATION
R.DTBS / R	Tính toàn vẹn	T.SIGNATURE_REQUEST_DISCLOSE T.DTBSR_FORGERY
	Xác thực nguồn gốc	T.DTBSR_FORGERY

R.SAD	Tính toàn vẹn	T.AUTHENTICATION_SIGNER_IMPERSONATIO N T.CONTEXT_ALTERATION T.AUDIT_ALTERATION T.SAP_BYPASS T.SAP_REPLAY T.SAD_FORGERY
	Tính bí mật	T.AUTHENTICATION_SIGNER_IMPERSONATION T.DTBSR_FORGERY T.CONTEXT_ALTERATION
R.Signature	Tính toàn vẹn	T.SIGNATURE_FORGERY
R.Audit	Tính toàn vẹn	T.AUDIT_ALTERATION
R.Signer	Tính toàn vẹn	T.ENROLMENT_SIGNER_IMPERSONATION
R.Reference_Signer_Authenti cation_Data	Tính toàn vẹn	T.ENROLMENT_SIGNER_IMPERSONATION T.ENROLMENT_SIGNER_AUTHENTICATION_DAT A_D PHÁT HÀNH T. SIGNER_AUTHENTICATION_DATA_MODIFIED T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION T.AUDIT_ALTERATION
	Tính bí mật	T.ENROLMENT_SIGNER_IMPERSONATION T.ENROLMENT_SIGNER_AUTHENTICATION_DAT A_D PHÁT HÀNH T.SIGNER_AUTHENTICATION_DATA_MODIFIED T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION
R.Privileged_User	Tính toàn vẹn	T.PRIVILEGED_USER_INSERTION T.REFERENCE_PRIVILEGED_USER_AUTHENTICA TIO N_DATA_MODIFICATION
R.Reference_Privileged_User _Authentication_Data	Tính toàn vẹn	T.PRIVILEGED_USER_INSERTION T.REFERENCE_PRIVILEGED_USER_AUTHENTICA TIO N_DATA_MODIFICATION
	Tính bảo mật cao	T.PRIVILEGED_USER_INSERTION T.REFERENCE_PRIVILEGED_USER_AUTHENTICA TIO N_DATA_MODIFICATION
R.RANDOM	Tính toàn vẹn	T.RANDOM
	Tính bảo mật	T.RANDOM
R.TSF_DATA	Tính toàn vẹn	T.CONTEXT_ALTERATION T.AUDIT_ALTERATION

6.5 Các chính sách bảo mật của tổ chức (Organisational Security Policies - OSP)

- TOE phải tuân thủ các Chính sách bảo mật của tổ chức (OSP) dưới đây. Các chính sách này đóng vai trò là những quy tắc bảo mật, quy trình, thực hành hoặc hướng dẫn bắt buộc mà một tổ chức áp đặt lên các hoạt động vận hành của mình.

- OSP.RANDOM (Chính sách về dữ liệu ngẫu nhiên)

- TOE bắt buộc phải khởi tạo các số ngẫu nhiên đáp ứng một thước đo chất lượng cụ thể (quality metric). Các số ngẫu nhiên này phải đảm bảo tính phù hợp để sử dụng làm khóa mật mã, dữ liệu xác thực/ủy quyền, hoặc làm dữ liệu hạt giống (seed data) cho một bộ sinh số ngẫu nhiên khác được sử dụng cho các mục đích nêu trên.

- OSP.CRYPTO (Chính sách về mã hóa mật mã)

- TOE chỉ được phép sử dụng các thuật toán, tham số thuật toán và độ dài khóa mật mã đã được phê duyệt, khuyến nghị bởi các cơ quan quản lý có thẩm quyền (recognized authorities) và được các TSP đánh giá là phù hợp. Chính sách này áp dụng bao gồm cả quy trình khởi tạo số ngẫu nhiên, khởi tạo cặp khóa ký, tạo chữ ký số cũng như việc bảo vệ tính toàn vẹn và tính bí mật của các tài sản thuộc TOE.

6.6 Các giả định (Assumptions)

Môi trường vận hành của TOE phải đáp ứng các giả định an toàn dưới đây:

- A.PRIVILEGED_USER (Giả định về Người dùng có đặc quyền / Nhân sự quản trị)

Hệ thống mặc định giả định rằng toàn bộ nhân sự tham gia vào quá trình quản trị, vận hành TOE đều là những người đáng tin cậy, có đủ năng lực chuyên môn, sở hữu đầy đủ các nguồn lực và kỹ năng cần thiết để thực hiện công việc của mình, đồng thời đã được đào tạo bài bản để triển khai các hoạt động mà họ chịu trách nhiệm.

- A.SIGNER_ENROLMENT (Giả định về Quy trình đăng ký người ký)

Quy trình đăng ký thông tin người ký và quản lý chứng thư số bắt buộc phải được thực hiện một cách nghiêm ngặt, tuân thủ theo các quy định được quy định tại Nghị định số 23/2025/NĐ-CP. Các hướng dẫn chi tiết về cách thức triển khai một hệ thống đăng ký và quản lý chứng thư số và quản lý vòng đời chứng thư số theo quy định tại Thông tư số 50/2025/TT-BKHCN.

- A.SIGNER_AUTHENTICATION_DATA_PROTECTION (Giả định về việc bảo vệ dữ liệu xác thực của người ký)

Hệ thống mặc định giả định rằng người ký sẽ tự có ý thức bảo mật, không tiết lộ hoặc làm lộ lọt các yếu tố xác thực (như mã PIN, mật khẩu, khóa thiết bị) của chính mình cho bất kỳ ai khác.

- A.SIGNER_DEVICE (Giả định về thiết bị của người ký)

Hệ thống giả định rằng thiết bị đầu cuối và cấu phần giao tiếp thông minh (SIC - Signer Interaction Component / ví dụ: ứng dụng Smart CA cài trên điện thoại) được người ký sử dụng để tương tác với ứng dụng SSA và lõi TOE hoàn toàn nằm dưới quyền kiểm soát duy nhất của người ký trong suốt quá trình vận hành tạo chữ ký số; nghĩa là thiết bị đó được bảo vệ an toàn, chống lại các loại mã độc (malicious code/malware).

- A.CA (Giả định về Tổ chức chứng thực công cộng)

Hệ thống giả định rằng tổ chức cung cấp dịch vụ tin cậy (TSP) được cấp phép cung cấp dịch vụ chứng thực chữ ký số công cộng phải luôn tuân thủ đầy đủ các yêu cầu tương ứng dành cho TSP đủ điều kiện đã được quy định rõ trong Nghị định số 23/2025/NĐ-CP.

- A.ACCESS_PROTECTED (Giả định về môi trường tiếp cận được bảo vệ)

Hệ thống giả định rằng TOE được vận hành trong một môi trường được bảo vệ nghiêm ngặt, có cơ chế giới hạn và kiểm soát truy cập vật lý (physical access) vào thiết bị phần cứng chứa TOE, chỉ cho phép những Người dùng có đặc quyền (Privileged Users) đã được ủy quyền tiếp cận. Môi trường phần cứng và phần mềm của TOE (bao gồm cả các ứng dụng phía máy khách/client applications) phải được cài đặt, bảo trì bởi các Người dùng có đặc quyền trong một trạng thái an toàn cao, nhằm giảm thiểu các rủi ro đặc thù áp dụng cho môi trường triển khai thực tế đó.

Hệ thống giả định rằng bất kỳ dữ liệu nhật ký kiểm toán do TOE sinh ra đều chỉ được xử lý và quản lý bởi nhân sự đã được ủy quyền trong một môi trường được bảo vệ an toàn về mặt vật lý. Nhân sự thực hiện các hoạt động này phải hành động tuân thủ nghiêm ngặt theo các quy trình thực hành đã được thiết lập sẵn.

Hệ thống giả định rằng trong trường hợp các bản sao của dữ liệu được bảo vệ bởi TOE được quản lý hoặc lưu trữ ở bên ngoài phạm vi của TOE, thì các ứng dụng phía máy khách (client applications) và các thực thể liên quan khác phải cung cấp các biện pháp bảo vệ phù hợp cho khối dữ liệu đó, đạt cấp độ bảo mật tương ứng theo yêu cầu bối cảnh của ứng dụng và các rủi ro trong môi trường triển khai thực tế.

- Lưu ý ứng dụng 21 (Application Note 21)

Người viết Tài liệu mục tiêu bảo mật (ST writer) bắt buộc phải mô tả chi tiết những loại dữ liệu nào sẽ được quản lý và lưu trữ ở bên ngoài phạm vi của TOE.

- A.AUTH_DATA (Giả định về kiểm soát dữ liệu kích hoạt)

Hệ thống mặc định giả định rằng giao thức kích hoạt chữ ký (SAP) được thiết kế theo cách đảm bảo việc kích hoạt khóa ký hoàn toàn nằm dưới quyền kiểm soát duy nhất (sole control) của người ký với mức độ tin cậy cao. Khi gói dữ liệu kích hoạt chữ ký (SAD) được gửi tới và tiếp nhận bởi TOE, hệ thống sẽ mặc định giả định rằng gói dữ liệu SAD đó đã được nộp dưới quyền kiểm soát toàn diện của người ký thông qua các phương thức/thiết bị do chính người ký sở hữu và nắm giữ.

- A.TSP_AUDITED (Giả định về việc kiểm toán nhà cung cấp dịch vụ tin cậy)

Hệ thống giả định rằng Tổ chức cung cấp dịch vụ tin cậy (TSP) triển khai ứng dụng SSA và cấu phần TOE là một TSP đã được cấp phép theo quy định tại Nghị định số 23/2025/NĐ-CP, đồng thời đã được kiểm toán và chứng nhận tuân thủ đầy đủ các yêu cầu nghiêm ngặt dành cho TSP theo quy định.

- A.SEC_REQ (Giả định về yêu cầu an toàn hệ thống) Hệ thống mặc định giả định rằng Tổ chức cung cấp dịch vụ tin cậy (TSP) thiết lập và duy trì một môi trường vận hành tuân thủ nghiêm ngặt theo các yêu cầu bảo mật dành cho mức độ đảm bảo kích hoạt chữ ký **SCAL2 (Signature Activation Level 2)** được định nghĩa trong tiêu chuẩn EN 419241-1.

7 Các mục tiêu bảo mật (Security Objectives)

7.1 Tổng quan

Phần này xác định và định nghĩa các mục tiêu bảo mật dành cho TOE (Mục tiêu bảo mật cho phần mềm lõi) và môi trường vận hành của nó (Mục tiêu bảo mật cho môi trường).

Các mục tiêu bảo mật này phản ánh mục đích cốt lõi đã được tuyên bố, nhằm ngăn chặn/vô hiệu hóa các mối đe dọa đã được chỉ ra (tại Mục 6.3), đồng thời cân nhắc đến các giả định nền tảng (tại Mục 6.6).

7.2 Các mục tiêu bảo mật dành cho TOE (Security objectives for the TOE)

Các mục tiêu bảo mật dưới đây mô tả các chức năng an toàn thông tin bắt buộc phải được cung cấp bởi chính bản thân TOE.

7.2.1 Giai đoạn đăng ký (Enrolment)

- OT.SIGNER_PROTECTION (Bảo vệ thông tin Người ký)

TOE phải đảm bảo rằng các dữ liệu liên kết với đối tượng Người ký (R.Signer) bắt buộc phải được bảo vệ tính toàn vẹn và bảo vệ tính bí mật nếu có yêu cầu cấu hình cụ thể.

- OT.REFERENCE_SIGNER_AUTHENTICATION_DATA (Bảo vệ dữ liệu xác thực người ký tham chiếu)

TOE phải có khả năng xử lý một cách an toàn dữ liệu xác thực chữ ký — Dữ liệu xác thực người ký tham chiếu (R.Reference_Signer_Authentication_Data) — như một thành phần cấu thành bên trong đối tượng Người ký (R.Signer).

- OT.SIGNER_KEY_PAIR_GENERATION (An toàn quy trình khởi tạo cặp khóa ký của người ký)

TOE phải có khả năng sử dụng Mô-đun Mật mã (HSM) một cách an toàn để khởi tạo các cặp khóa ký cho người ký, đồng thời thực hiện gán mã định danh khóa ký (R.Signing_Key_Id) và khóa công khai (R.SVD) tương ứng vào đối tượng Người ký (R.Signer).

- OT.SVD (Bảo vệ tính toàn vẹn của Dữ liệu xác thực chữ ký / Khóa công khai) TOE phải đảm bảo rằng tài sản R.SVD (Khóa công khai) liên kết với đối tượng Người ký (R.Signer) tuyệt đối không bị sửa đổi hay tráo đổi trước khi nó được cơ quan CA cấp chứng thư số (certified).

7.2.2 Quản lý người dùng

- OT.PRIVILEGED_USER_MANAGEMENT (Quản lý Người dùng có đặc quyền)

TOE phải đảm bảo rằng bất kỳ hành vi sửa đổi, cập nhật nào đối với đối tượng R.Privileged_User (Thông tin Người dùng có đặc quyền) và R.Reference_Privileged_User_Authentication_Data (Dữ liệu xác thực Admin tham chiếu) đều phải được thực hiện dưới sự kiểm soát chặt chẽ của một Người dùng có đặc quyền hợp pháp.

- OT.PRIVILEGED_USER_AUTHENTICATION (Xác thực Người dùng có đặc quyền)

TOE phải đảm bảo rằng bất kỳ nhân sự quản trị nào mang vai trò Người dùng có đặc quyền đều bắt buộc phải được xác thực danh tính thành công trước khi được phép thực hiện bất kỳ hành động nào tác động lên TOE.

Lưu ý ứng dụng 22 (Application Note 22)

Ngoại lệ duy nhất đối với mục tiêu bảo mật này là khi (tập hợp) Người dùng có đặc quyền ban đầu được khởi tạo như một phần của quy trình khởi tạo/cài đặt hệ thống (system initialisation).

- OT.PRIVILEGED_USER_PROTECTION (Bảo vệ Người dùng có đặc quyền)

TOE phải đảm bảo rằng các dữ liệu liên kết với đối tượng R.Privileged_User bắt buộc phải được bảo vệ tính toàn vẹn và bảo vệ tính bí mật nếu có yêu cầu cấu hình cụ thể.

- OT.SIGNER_MANAGEMENT (Quản lý cấu phần Người ký)

TOE phải đảm bảo rằng bất kỳ hành vi sửa đổi nào đối với đối tượng R.Signer, Dữ liệu xác thực người ký tham chiếu (R.Reference_Signer_Authentication_Data), Định danh khóa ký (R.Signing_Key_Id) và Khóa công khai (R.SVD) đều phải được thực hiện dưới sự kiểm soát của Người ký hoặc Người dùng có đặc quyền.

7.2.3 Vận hành sử dụng (Usage)

- OT.SAD_VERIFICATION (Xác minh dữ liệu kích hoạt chữ ký)

TOE phải thực hiện việc xác minh gói dữ liệu R.SAD. Nghĩa là, hệ thống phải kiểm tra và đối chiếu để đảm bảo tồn tại một mối liên kết chặt chẽ giữa các thành phần cấu thành bên trong gói dữ liệu SAD, đồng thời đảm bảo rằng người ký đã được xác thực mạnh (strongly authenticated).

- Lưu ý ứng dụng 23 (Application Note 23)

Trong trường hợp TOE tạo ra (phái sinh) dữ liệu ủy quyền từ dữ liệu xác thực nằm trong gói SAD và sử dụng dữ liệu này để kích hoạt khóa ký bên trong mô-đun mật mã, thì hàm chức năng này có thể phụ thuộc vào các cơ chế kiểm soát do chính mô-đun mật mã (HSM) cung cấp.

- Lưu ý ứng dụng 24 (Application Note 24)

Các yêu cầu đối với quy trình xác thực được mô tả chi tiết trong tiêu chuẩn EN 419241-1, mục SRA_SAP.1.1.

- OT.SAP (Thực thi giao thức kích hoạt chữ ký)

TOE phải triển khai điểm cuối phía máy chủ (server-side end point) của một Giao thức kích hoạt chữ ký (SAP), nhằm cung cấp các tính năng sau:

- Xác thực người ký (Signer authentication).

Bảo vệ tính toàn vẹn của gói dữ liệu SAD được truyền tải.

Bảo vệ tính bí mật của ít nhất là các thành phần chứa thông tin nhạy cảm nằm trong gói dữ liệu SAD.

Bảo vệ hệ thống chống lại các cuộc tấn công lặp lại (replay), tấn công bỏ qua (bypass) một hoặc nhiều bước của quy trình, và tấn công làm giả (forgery).

- Lưu ý ứng dụng 25 (Application Note 25)

Quy trình xác thực người ký được mặc định giả định là sẽ được tiến hành tuân thủ theo tiêu chuẩn EN 419241-1, cấp độ SCAL2 đối với chữ ký số đủ điều kiện (qualified signatures). Điều này có nghĩa là việc xác thực người ký có thể được thực hiện theo một trong các cách sau: (Đoạn này trong văn bản gốc của bạn bị ngắt quãng nửa chừng, nhưng theo tiêu chuẩn EN 419241-1, các cách này thường bao gồm: xác thực trực tiếp bởi TOE, xác thực ủy quyền qua một bên thứ ba được tin cậy, hoặc xác thực đa yếu tố MFA kết hợp giữa thiết bị vật lý và mã PIN/sinh trắc học).

- Xác thực trực tiếp bởi SAM: Trong trường hợp này, SAM sẽ trực tiếp thực hiện việc kiểm tra và xác minh (verify) các yếu tố xác thực của người ký.
- Xác thực gián tiếp bởi SAM: Trong trường hợp này, một dịch vụ xác thực bên ngoài (nằm trong hệ thống TW4S tổng thể) hoặc một bên được ủy quyền sẽ thực hiện việc xác minh các yếu tố xác thực của người ký, sau đó phát hành một khẳng định/chứng thực danh tính (assertion) rằng người ký đã được xác thực thành công. SAM sẽ chịu trách nhiệm kiểm tra và xác minh tính hợp lệ của khẳng định/chứng thực này.
- - Sự kết hợp của cả hai mô hình: Áp dụng đồng thời hoặc linh hoạt cả hai cơ chế xác thực trực tiếp và

gián tiếp nêu trên.

- OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION (Bảo vệ dữ liệu xác thực chữ ký)

TOE phải đảm bảo rằng các dữ liệu xác thực chữ ký (như thông tin trong gói SAD) bắt buộc phải được bảo vệ chống lại các cuộc tấn công đánh cắp, lộ lọt trong quá trình truyền tải tới TOE — những cuộc tấn công có thể làm tổn hại đến hiệu lực và tính an toàn của chính các dữ liệu này khi dùng cho mục đích xác thực.

- OT.DTBSR_INTEGRITY (Bảo vệ tính toàn vẹn của giá trị băm tài liệu cần ký)

TOE phải đảm bảo rằng tài sản R.DTBS/R (Giá trị băm của dữ liệu cần được ký) bắt buộc phải được bảo vệ tính toàn vẹn một cách tuyệt đối trong suốt quá trình truyền tải tới TOE.

- OT.SIGNATURE_INTEGRITY (Bảo vệ tính toàn vẹn của giá trị chữ ký số)

TOE phải đảm bảo rằng giá trị chữ ký số (R.Signature) đầu ra tuyệt đối không thể bị sửa đổi, thao túng hoặc làm giả khi đang nằm bên trong phạm vi xử lý nội bộ của TOE.

- OT.CRYPTO (Tuân thủ các tiêu chuẩn mã hóa mật mã) TOE chỉ được phép sử dụng các thuật toán, tham số thuật toán và độ dài khóa mật mã đã được quy định tại QCVN 137:2025/BKHCN. Yêu cầu này áp dụng bắt buộc đối với tất cả các hoạt động bao gồm: khởi tạo số ngẫu nhiên, khởi tạo các cặp khóa ký, tạo chữ ký số, cũng như quy trình bảo vệ tính toàn vẹn (integrity) và tính bí mật (confidentiality) của các tài sản thuộc TOE.

7.2.4 Hệ thống (System)

- OT.RANDOM (Đảm bảo chất lượng dữ liệu ngẫu nhiên)

Các số ngẫu nhiên do TOE khởi tạo để sử dụng làm khóa mật mã, sử dụng trong các giao thức bảo mật hoặc làm dữ liệu hạt giống (seed data) cho một bộ sinh số ngẫu nhiên khác cho các mục đích trên, bắt buộc phải đáp ứng một thước đo chất lượng cụ thể (defined quality metric) nhằm đảm bảo rằng các số ngẫu nhiên này không thể bị suy đoán (not predictable) và có độ hỗn loạn (entropy) đầy đủ.

- OT.SYSTEM_PROTECTION (Bảo vệ cấu hình hệ thống)

TOE phải đảm bảo rằng mọi hành vi sửa đổi đối với tài sản R.TSF_DATA (Dữ liệu cấu hình chức năng an toàn) đều phải được ủy quyền bởi Người dùng có đặc quyền (Privileged User), đồng thời hệ thống phải có khả năng phát hiện ra mọi hành vi sửa đổi trái phép.

- OT.AUDIT_PROTECTION (Bảo vệ dữ liệu kiểm toán / Nhật ký hệ thống)

TOE phải đảm bảo rằng mọi hành vi sửa đổi, can thiệp trái phép vào tài sản R.AUDIT (Dữ liệu nhật ký kiểm toán) đều phải bị hệ thống phát hiện ra ngay lập tức.

7.3 Các mục tiêu bảo mật dành cho Môi trường vận hành (Security Objectives for the Operational Environment)

Môi trường vận hành của TOE phải đáp ứng các mục tiêu bảo mật sau đây nhằm đảm bảo an toàn cho toàn bộ hệ thống:

- OE.SVD_AUTHENTICITY (Đảm bảo tính xác thực của Khóa công khai)

Môi trường vận hành phải đảm bảo tính toàn vẹn (integrity) của tài sản SVD (Khóa công khai) trong quá trình truyền tải ra bên ngoài phạm vi TOE để gửi tới CA.

- OE.CA_REQUEST_CERTIFICATE (Yêu cầu cấp chứng thư số từ CA)

Môi trường vận hành phải đảm bảo rằng tổ chức cung cấp dịch vụ tin cậy (TSP) đủ điều kiện thực hiện cung cấp dịch vụ chứng thực chữ ký số công cộng phải luôn tuân thủ theo quy định tại Nghị định số 23/2025/NĐ-CP.

Môi trường vận hành phải sử dụng một quy trình yêu cầu cấp chứng thư chữ ký số - bao gồm cả khóa SVD, thông tin người ký và chữ ký của CA - theo cách thức chứng minh được rằng người ký thực sự nắm quyền kiểm soát khóa ký (khóa bí mật) liên kết với khóa công khai SVD được gửi đi để chứng thực đó. Tính toàn vẹn của yêu cầu cấp chứng thư này phải được bảo vệ tuyệt đối.

- OE.CERTIFICATE_VERFICATION (Xác duyệt chứng thư số)

Môi trường vận hành phải thực hiện việc kiểm tra, xác minh để đảm bảo chứng thư số được cấp cho tài sản R.SVD có chứa chính xác khóa R.SVD đó.

- OE.SIGNER_AUTHENTICATION_DATA (Bảo vệ dữ liệu xác thực của người ký ở vòng ngoài)

Quy trình quản lý các dữ liệu thuộc về yếu tố xác thực của người ký ở bên ngoài phạm vi TOE (phía khách hàng) phải được thực hiện một cách an toàn tuyệt đối.

- OE.DELEGATED_AUTHENTICATION (Ủy quyền xác thực danh tính)

Nếu TOE có hỗ trợ và được cấu hình để sử dụng cơ chế ủy quyền xác thực (xác thực gián tiếp qua bên thứ ba), thì TSP triển khai ứng dụng SSA và TOE phải đảm bảo rằng tất cả các yêu cầu quy định trong tiêu chuẩn EN 419241-1 mục SRA_SAP.1.1 đều được đáp ứng đầy đủ.

Ngoài ra, TSP phải đảm bảo rằng:

Bên được ủy quyền xác thực phải đáp ứng tất cả các yêu cầu liên quan của tiêu chuẩn này cũng như các yêu cầu về định danh xác thực điện tử theo quy định hiện hành.

Nếu người ký chỉ được xác thực duy nhất thông qua một bên được ủy quyền, TSP phải đảm bảo rằng các thành phần khóa bí mật (secret key material) dùng để xác thực bên được ủy quyền đó với TOE phải được lưu trữ bên trong một mô-đun mật mã đã được chứng nhận, tuân thủ theo yêu cầu được định nghĩa trong tiêu chuẩn EN 419241-1 mục SRG_KM.1.1.

Hoạt động kiểm toán định kỳ đối với TSP đủ điều kiện theo tiêu chuẩn EN 419241-1 phải cung cấp đầy đủ bằng chứng chứng minh rằng bất kỳ bên được ủy quyền nào cũng đều đáp ứng các yêu cầu từ mục EN 419241-1 SRA_SAP.1.1, và tùy chọn thêm mục SRG_KM.1.1 trong trường hợp người ký chỉ xác thực duy nhất qua bên được ủy quyền đó.

- OE.DEVICE (An toàn thiết bị đầu cuối của người ký)

Thiết bị đầu cuối (máy tính, máy tính bảng hoặc điện thoại thông minh) chứa cấu phần giao tiếp SIC và được người ký sử dụng để tương tác với TOE phải được bảo vệ an toàn, chống lại các loại mã độc (malicious code). Thiết bị này phải tham gia kết nối bằng cách sử dụng cấu phần SIC như một phần cục bộ (phía khách hàng) của giao thức SAP và có thể thực hiện tính toán gói dữ liệu SAD như mô tả trong tiêu chuẩn EN 419241-1. Thiết bị cũng có thể được sử dụng để hiển thị nội dung văn bản/tài liệu cần ký cho người dùng xem.

- OE.ENV (An toàn môi trường vận hành vật lý và quy trình của TSP)

TSP triển khai ứng dụng SSA và TOE phải là một TSP đủ điều kiện đã được cấp phép và phải được kiểm toán kỹ thuật theo quy định tại Nghị định số 23/2025/NĐ-CP. Hoạt động kiểm toán đối với TSP

đủ điều kiện phải bao quát toàn bộ các mục tiêu bảo mật dành cho môi trường vận hành được chỉ định trong điều khoản này.

TOE phải được vận hành bên trong một môi trường được bảo vệ nghiêm ngặt, có cơ chế giới hạn quyền tiếp cận vật lý (physical access) vào TOE, chỉ cho phép những người dùng có đặc quyền (privileged users) đã được ủy quyền. Môi trường phần cứng và phần mềm của TOE (bao gồm cả các ứng dụng phía máy khách/client applications) phải được cài đặt và bảo trì bởi các Quản trị viên trong một trạng thái an toàn cao, nhằm giảm thiểu các rủi ro cụ thể áp dụng cho môi trường triển khai đó, bao gồm (khi áp dụng):

Bảo vệ chống lại nguy cơ mất mát hoặc mất trộm thiết bị TOE hoặc bất kỳ tài sản nào của TOE được lưu trữ ở môi trường bên ngoài.

Thực hiện hoạt động kiểm tra định kỳ nhằm ngăn chặn và phát hiện các hành vi can thiệp, phá hoại vật lý (bao gồm các nỗ lực tấn công kênh kề - side-channel attacks, hoặc cố tình tiếp cận các đường cáp kết nối giữa các phần tách biệt về mặt vật lý của TOE, hoặc các phần của thiết bị phần cứng).

Bảo vệ chống lại nguy cơ bị tấn công khai thác dựa trên sự bức xạ phát tán từ TOE (ví dụ: bức xạ điện từ - electromagnetic emanations) dựa theo kết quả đánh giá rủi ro đối với môi trường vận hành.

Bảo vệ chống lại các hành vi thay đổi cấu hình và cài đặt phần mềm trái phép trên TOE cũng như trên thiết bị phần cứng (appliance).

Bảo vệ ở cấp độ an toàn tương đương đối với tất cả các phiên bản (instances) của TOE đang nắm giữ cùng một loại tài sản (ví dụ: trường hợp một khóa ký được lưu dưới dạng sao lưu dự phòng - backup ở nhiều hơn một thiết bị TOE).

- OE.CRYPTOMODULE_CERTIFIED (Chứng nhận an toàn cho Mô-đun Mật mã / HSM)

Nếu TOE được triển khai dưới dạng một ứng dụng nội bộ nằm trong cùng một ranh giới vật lý (physical boundary) với mô-đun mật mã được định nghĩa trong tiêu chuẩn EN 419221-5, thì TOE sẽ tin tưởng và dựa vào mô-đun mật mã đó để cung cấp một môi trường chống can thiệp vật lý (tamper-protected environment), cung cấp các chức năng mật mã và khởi tạo số ngẫu nhiên.

Nếu TOE được triển khai trong một ranh giới vật lý độc lập tách biệt, thì TOE sẽ tin tưởng và dựa vào mô-đun mật mã để thực hiện các chức năng mật mã và khởi tạo số ngẫu nhiên. Lúc này, ranh giới vật lý riêng biệt phải bảo vệ TOE một cách cơ học, tuân thủ theo các tiêu chuẩn FPT_PHP.1 và FPT_PHP.3 quy định trong EN 419221-5.

- Lưu ý ứng dụng 26 (Application Note 26)

Trong trường hợp tài liệu Mục tiêu Bảo mật (ST) tuyên bố tuân thủ Hồ sơ Bảo vệ (PP) này và tuân thủ tiêu chuẩn EN 419221-5 như đã ghi trong phần Tuyên bố tuân thủ PP (PP Claim), thì việc chứng nhận cho tài liệu ST đó đã bao hàm đầy đủ yêu cầu này đối với Môi trường vận hành.

- OE.TW4S_CONFORMANT (Tuân thủ khung kiến trúc hệ thống ký số từ xa)

TOE phải được vận hành bởi một Tổ chức cung cấp dịch vụ tin cậy (TSP) đủ điều kiện trong một môi trường đáp ứng đầy đủ các tiêu chuẩn kỹ thuật của hệ thống tổng thể quy định trong tiêu chuẩn EN 419241-1.

7.4 Định nghĩa vấn đề Bảo mật và Mục tiêu Bảo mật

Các bảng sau đây ánh xạ các mục tiêu bảo mật với định nghĩa vấn đề bảo mật.

Bảng 3 - Các Mục tiêu An toàn TOE và các mối đe dọa.

	Ghi danh	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTIC	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD
Ghi danh					
T.ENROLMENT_SIGNER_IMPERSONATION		X	X		
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED		X	X		
T.SVD_FORGERY				X	X
Quản lý người ký					
T.ADMIN_IMPERSONATION					
T.MAINTENANCE_AUTHENTICATION_DISCLOSE			X		
Sử dụng					
T.AUTHENTICATION_SIGNER_IMPERSONATION					
T.SIGNER_AUTHENTICATION_DATA_MODIFIED			X		
T.SAP_BYPASS					
T.SAP_REPLAY					
T.SAD_FORGERY					
T.DTBSR_FORGERY					
T.SIGNATURE_FORGERY					
Hệ thống					
T.AUTHORISATION_DATA_UPDATE					
T.AUTHORISATION_DATA_DISCLOSE					
T.CONTEXT_ALTERATION					
T.AUDIT_ALTERATION					
T.RANDOM					

Bảng 4 - Các mục tiêu và mối đe dọa bảo mật TOE

	Quản lý người dùng	OT.PRIVILEGED_USER_MANAGEMENT	OT.PRIVILEGED_USER_AUTHENTICATION	OT.PRIVILEGED_USER_PROTECTION	OT.SIGNER_MANAGEMENT	Hệ thống	OT.RANDOM	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION
Ghi danh									

T.ENROLMENT_SIGNER_IMPERSONATION					X				
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED									
T.SVD_FORGERY									
Quản lý người ký									
T.ADMIN_IMPERSONATION			X		X				
T.MAINTENANCE_AUTHENTICATION_DISCLOSE									
Sử dụng									
T.AUTHENTICATION_SIGNER_IMPERSONATION									
T.SIGNER_AUTHENTICATION_DATA_MODIFIED									
T.SAP_BYPASS									
T.SAP_REPLAY									
T.SAD_FORGERY									
T.DTBSR_FORGERY									
T.SIGNATURE_FORGERY									
Hệ thống									
T.PRIVILEGED_USER_INSERTION		X	X						
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_ MODIFICATION		X	X	X					
T.AUTHORISATION_DATA_UPDATE								X	
T.AUTHORISATION_DATA_DISCLOSE								X	
T.CONTEXT_ALTERATION								X	
T.AUDIT_ALTERATION									X
T.RANDOM							X		

Bảng 5 - Các mục tiêu và mối đe dọa bảo mật TOE

	Sử dụng	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PR	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO
Ghi danh							
T.ENROLMENT_SIGNER_IMPERSONATION							
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA _DISC ĐÃ THAM GIA							
T.SVD_FORGERY							X
Quản lý người ký							
T.ADMIN_IMPERSONATION							
T.MAINTENANCE_AUTHENTICATION_DISCLOSE							
Sử dụng							
T.AUTHENTICATION_SIGNER_IMPERSONATION		X					
T.SIGNER_AUTHENTICATION_DATA_MODIFIED			X	X			
T.SAP_BYPASS			X				
T.SAP_REPLAY			X				
T.SAD_FORGERY			X	X			
T.SIGNATURE_REQUEST_DISCLOSURE			X				
T.DTBSR_FORGERY					X		
T.SIGNATURE_FORGERY						X	X
Hệ thống							
T.PRIVILEGED_USER_INSERTION							
T.REFERENCE_PRIVILEGED_USER_AUTHENTICAT ION_ DATA_MODIFICATION							
T.AUTHORISATION_DATA_UPDATE							
T.AUTHORISATION_DATA_DISCLOSE							
T.CONTEXT_ALTERATION							
T.AUDIT_ALTERATION							

Bảng 6 - Các Mục tiêu An toàn TOE và Chính sách Bảo mật Tổ chức

	Ghi danh	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTIC	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD	OT.RANDOM	OT.CRYPTO
OSP.RANDOM						X	
OSP.CRYPTO							X

Bảng 7 - Các Đe doạ và Mục tiêu An ninh đối với Môi trường

	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTICATION_	OE.DEVICE	OE.ENV	OE.CRYPTOMODULE_CERTIFIED	OE.TW4S_CONFORMANT
Ghi danh							
T.ENROLMENT_SIGNER_IMPERSONATION							X
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA _DISC ĐÃ THAM GIA			X	X			
T.SVD_FORGERY	X	X					
Quản lý người ký							
T.ADMIN_IMPERSONATION							
T.MAINTENANCE_AUTHENTICATION_DISCLOSE							
Sử dụng							
T.AUTHENTICATION_SIGNER_IMPERSONATION							
T.SIGNER_AUTHENTICATION_DATA_MODIFIED							
T.SAP_BYPASS				X			
T.SAP_REPLAY				X			
T.SAD_FORGERY			X	X			
T.DTBSR_FORGERY				X			
T.SIGNATURE_FORGERY							
Hệ thống							

T.PRIVILEGED_USER_INSERTION							
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_ DATA_MODIFICATION							
T.AUTHORISATION_DATA_UPDATE							
T.AUTHORISATION_DATA_DISCLOSE							
T.CONTEXT_ALTERATION							
T.AUDIT_ALTERATION							

Bảng 8 - Mục tiêu an ninh đối với môi trường và Các giả định và Mục tiêu an ninh đối với môi trường

	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTICATION_DA	OE.DEVICE	OE.ENV	OE.CRYPTOMODULE_CERTIFIED	OE.TW4S_CONFORMANT
Chính sách bảo mật của tổ chức							
OSP.TSP_AUDITED							X
OSP.RANDOM							
OSP.CRYPTO						X	
Giả định							
A.PRIVILEGED_USER							X
A.SIGNER_ENROLMENT					X		
A.SIGNER_AUTHENTICATION_DATA_PROTECTION			X				
A.SIGNATURE_REQUEST_DISCLOSURE				X			
A.SIGNER_DEVICE				X			
A.CA		X					
A.ACCESS_PROTECTED					X		
A.AUTH_DATA				X			
A.TSP_AUDITED					X		
A.SEC_REQ							X

7.5 Cơ sở lý luận cho các mục tiêu bảo mật (Rationale for the security objectives)

7.5.1 Tổng quan

Phần này cung cấp các lập luận chứng minh rằng các mục tiêu bảo mật được thiết lập đã bao quát, xử lý triệt để từng mối đe dọa (Threat), chính sách bảo mật của tổ chức (OSP) và giả định (Assumption).

7.5.2 Mối đe dọa và Mục tiêu bảo mật (Threats and objectives)

- T.ENROLMENT_SIGNER_IMPERSONATION (Giả mạo người ký khi đăng ký) được giải quyết bởi:

OT.SIGNER_PROTECTION: Đòi hỏi thông tin R.Signer phải được bảo vệ tính toàn vẹn và các phần nhạy cảm phải được bảo vệ tính bí mật.

OT.SIGNER_MANAGEMENT: Đòi hỏi quy trình khởi tạo thông tin người ký phải được thực hiện một cách an toàn.

OT.REFERENCE_SIGNER_AUTHENTICATION_DATA: Đòi hỏi TOE phải có khả năng gán dữ liệu xác thực người ký vào đúng đối tượng người ký tương ứng.

OE.TW4S_CONFORMANT: Đòi hỏi quy trình đăng ký người ký phải được xử lý tuân thủ theo mức độ đảm bảo (Assurance level) tối thiểu từ mức "Đáng kể" (Substantial) trở lên.

- T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED (Lộ dữ liệu xác thực khi đăng ký) được giải quyết bởi:

OT.REFERENCE_SIGNER_AUTHENTICATION_DATA: Đòi hỏi dữ liệu xác thực phải được xử lý một cách an toàn.

OT.SIGNER_PROTECTION: Đòi hỏi các thuộc tính (bao gồm cả dữ liệu xác thực người ký) phải được bảo vệ tính toàn vẹn và tính bí mật nếu cần.

OE.SIGNER_AUTHENTICATION_DATA: Đòi hỏi bản thân người ký phải tự giữ bí mật dữ liệu xác thực của mình.

OE.DEVICE: Đòi hỏi thiết bị do người ký sử dụng không được làm lộ lọt dữ liệu xác thực.

T.SVD_FORGERY (Giả mạo Khóa công khai SVD) được giải quyết bởi:

OT.SIGNER_KEY_PAIR_GENERATION: Đòi hỏi phải sử dụng một Mô-đun Mật mã (HSM) để khởi tạo cặp khóa cho người ký.

OT.SVD: Đòi hỏi khóa công khai SVD phải được bảo vệ nghiêm ngặt khi còn nằm bên trong TOE.

OT.CRYPTO: Đòi hỏi phải sử dụng các thuật toán mật mã đã được phê duyệt/khuyến nghị.

OE.SVD_AUTHENTICITY: Đòi hỏi môi trường vận hành phải bảo vệ tính toàn vẹn của khóa SVD trong quá trình truyền tải từ TOE đến CA.

OE.CA_REQUEST_CERTIFICATE: Đòi hỏi yêu cầu cấp chứng thư số phải được bảo vệ tính toàn vẹn.

- T.ADMIN_IMPERSONATION (Giả mạo Quản trị viên) được giải quyết bởi:

OT.SIGNER_MANAGEMENT và OT.PRIVILEGED_USER_AUTHENTICATION: Đòi hỏi mọi thay đổi đối với thông tin đại diện và thuộc tính của người ký phải được thực hiện theo một phương thức đã được ủy quyền hợp pháp.

T.MAINTENANCE_AUTHENTICATION_DISCLOSE (Lộ dữ liệu xác thực khi bảo trì) được giải quyết bởi:

OT.REFERENCE_SIGNER_AUTHENTICATION_DATA: Đòi hỏi dữ liệu xác thực hệ thống phải được xử lý một cách an toàn tuyệt đối.

- T.AUTHENTICATION_SIGNER_IMPERSONATION (Giả mạo người ký khi xác thực) được giải quyết bởi:

OT.SAD_VERIFICATION: Đòi hỏi TOE phải thực hiện kiểm tra và xác duyệt gói dữ liệu SAD nhận được trong giao thức SAP.

- T.SIGNER_AUTHENTICATION_DATA_MODIFIED (Sửa đổi dữ liệu xác thực người ký) được giải quyết bởi:

OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION: Đòi hỏi gói dữ liệu SAD khi truyền tải trong giao thức SAP phải được bảo vệ chống lại các cuộc tấn công.

OT.REFERENCE_SIGNER_AUTHENTICATION_DATA: Đòi hỏi dữ liệu xác thực phải được lưu trữ, xử lý an toàn.

OT.SAP: Đòi hỏi tính toàn vẹn của gói SAD phải được bảo vệ xuyên suốt quá trình truyền tải trong giao thức SAP.

T.SAP_BYPASS (Bỏ qua giao thức SAP) được giải quyết bởi:

OT.SAP: Đòi hỏi tất cả các bước của giao thức SAP (bao gồm cả khâu xác minh gói SAD) bắt buộc phải được hoàn thành đầy đủ một cách tuần tự.

OE.DEVICE: Đòi hỏi cấu phần giao tiếp người ký (SIC) phải tham gia bắt buộc vào giao thức SAP.

T.SAP_REPLAY (Tấn công lặp lại phiên SAP) được giải quyết bởi:

OT.SAP: Đòi hỏi giao thức kích hoạt chữ ký phải có cơ chế chống lại việc bị gửi lặp lại một phần hoặc toàn bộ gói tin cũ.

OE.DEVICE: Đòi hỏi cấu phần SIC phải tham gia trực tiếp vào giao thức SAP để tạo các yếu tố động chống lặp lại.

- T.SIGNATURE_REQUEST_DISCLOSURE (Lộ lọt thông tin yêu cầu ký số) được giải quyết bởi:

OT.SAP: Đòi hỏi giao thức bảo mật phải có khả năng truyền tải dữ liệu một cách an toàn (mã hóa đường truyền).

- T.SAD_FORGERY (Giả mạo gói dữ liệu kích hoạt SAD) được giải quyết bởi:

OT.SAP: Đòi hỏi TOE phải có khả năng phát hiện nếu gói dữ liệu SAD bị sửa đổi trong quá trình truyền tải tới TOE.

OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION: Đòi hỏi dữ liệu xác thực chữ ký phải được bảo vệ trong suốt quá trình truyền tới TOE.

OE.SIGNER_AUTHENTICATION_DATA: Đòi hỏi người ký phải có trách nhiệm bảo vệ dữ liệu xác thực của mình.

OE.DEVICE: Đòi hỏi thiết bị của người ký phải tham gia chính xác vào giao thức SAP; đặc biệt, thiết bị không được làm lộ dữ liệu xác thực.

T.DTBSR_FORGERY (Giả mạo mã băm tài liệu cần ký) được giải quyết bởi:

OT.DTBSR_INTEGRITY: Đòi hỏi tài sản R.DTBS/R phải được bảo vệ tính toàn vẹn tuyệt đối trong quá trình truyền tải tới TOE.

OE.DEVICE: Đòi hỏi cấu phần SIC trên thiết bị đầu cuối phải tham gia kiểm soát chặt chẽ trong giao thức SAP.

- T.SIGNATURE_FORGERY (Giả mạo giá trị chữ ký số đầu ra) được giải quyết bởi:

OT.SIGNATURE_INTEGRITY: Đòi hỏi chuỗi chữ ký số phải được bảo vệ tính toàn vẹn tuyệt đối ngay bên trong nội bộ TOE.

OT.CRYPTO: Đòi hỏi phải sử dụng các thuật toán mật mã mạnh được phê duyệt để chống phá mã chữ ký.

- T.PRIVILEGED_USER_INSERTION (Cài cắm trái phép Admin) được giải quyết bởi:

OT.PRIVILEGED_USER_MANAGEMENT: Quy định chỉ có Người dùng có đặc quyền hiện tại mới có quyền tạo mới một tài khoản R.Privileged_User.

OT.PRIVILEGED_USER_AUTHENTICATION: Đòi hỏi mọi Người dùng có đặc quyền bắt buộc phải được xác thực danh tính trước khi vận hành.

T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION (Sửa đổi dữ liệu xác thực của Admin) được giải quyết bởi:

OT.PRIVILEGED_USER_MANAGEMENT: Quy định chỉ có Người dùng có đặc quyền mới có quyền sửa đổi tài khoản R.Privileged_User.

OT.PRIVILEGED_USER_AUTHENTICATION: Yêu cầu bắt buộc phải xác thực danh tính Admin.

OT.PRIVILEGED_USER_PROTECTION: Đòi hỏi thông tin của Người dùng có đặc quyền phải được bảo vệ tính toàn vẹn.

- T.AUTHORISATION_DATA_UPDATE (Cập nhật trái phép dữ liệu ủy quyền) được giải quyết bởi:

OT.SYSTEM_PROTECTION: Đòi hỏi mọi hành vi thay đổi, sửa đổi trái phép đối với cấu hình hệ thống của TOE đều phải bị phát hiện ra ngay lập tức.

- T.AUTHORISATION_DATA_DISCLOSE (Lộ lọt dữ liệu ủy quyền) được giải quyết bởi:

OT.SYSTEM_PROTECTION: Đòi hỏi mọi hành vi tiếp cận hoặc thay đổi trái phép đối với cấu hình hệ thống của TOE phải bị phát hiện.

- T.CONTEXT_ALTERATION (Thay đổi cấu hình hệ thống) được giải quyết bởi:

OT.SYSTEM_PROTECTION: Đòi hỏi bất kỳ hành vi sửa đổi trái phép nào đối với cấu hình chức năng an toàn của TOE phải bị phát hiện.

- T.AUDIT_ALTERATION (Sửa đổi nhật ký kiểm toán) được giải quyết bởi:

OT.AUDIT_PROTECTION: Đòi hỏi mọi hành vi can thiệp, sửa đổi dữ liệu nhật ký kiểm toán (R.AUDIT) đều phải bị hệ thống phát hiện.

- T.RANDOM (Tấn công suy đoán số ngẫu nhiên) được giải quyết bởi:

OT.RANDOM: Đòi hỏi các số ngẫu nhiên được sinh ra phải không thể dự đoán trước và đạt độ hỗn loạn (entropy) đầy đủ.

7.5.3 Chính sách bảo mật của tổ chức và Mục tiêu bảo mật (Organizational security policies and objectives)

OSP.RANDOM được giải quyết bởi:

OT.RANDOM: Đòi hỏi các số ngẫu nhiên hệ thống sử dụng phải không thể dự đoán và có độ hỗn loạn (entropy) cao, đáp ứng các tiêu chí đo lường chất lượng cụ thể.

OSP.CRYPTO được giải quyết bởi:

OT.CRYPTO: Đòi hỏi bắt buộc phải sử dụng các thuật toán, tham số thuật toán và độ dài khóa mật mã đã được các cơ quan quản lý có thẩm quyền phê duyệt.

OE.CRYPTOMODULE_CERTIFIED: Đòi hỏi hệ thống phải sử dụng một mô-đun mật mã (HSM) đã được chứng nhận để cung cấp môi trường chống can thiệp vật lý, thực thi các chức năng mật mã và sinh số ngẫu nhiên.

7.5.4 Giả định và Mục tiêu bảo mật (Assumptions and objectives)

A.PRIVILEGED_USER được giải quyết bởi:

OE.TW4S_CONFORMANT: Đòi hỏi môi trường vận hành nơi TOE chạy phải tuân thủ tiêu chuẩn [EN 419 241-1], trong đó Điều khoản SRG_M.1.8 quy định bắt buộc các quản trị viên hệ thống phải được đào tạo bài bản và chuyên nghiệp.

A.SIGNER_ENROLMENT được giải quyết bởi:

OE.ENV: Đòi hỏi Tổ chức cung cấp dịch vụ tin cậy (TSP) phải trải qua các kỳ kiểm toán chứng nhận định kỳ để đảm bảo khâu đăng ký hồ sơ tuân thủ nghiêm ngặt theo luật định.

A.SIGNER_AUTHENTICATION_DATA_PROTECTION được giải quyết bởi:

OE.SIGNER_AUTHENTICATION_DATA: Đòi hỏi người ký phải có nghĩa vụ tự bảo vệ và giữ bí mật tuyệt đối các yếu tố xác thực cá nhân của mình.

A.SIGNER_DEVICE được giải quyết bởi:

OE.DEVICE: Đòi hỏi thiết bị đầu cuối của người ký (điện thoại/máy tính) phải có các biện pháp tự bảo vệ để chống lại mã độc và phần mềm gián điệp.

A.CA được giải quyết bởi:

OE.CA_REQUEST_CERTIFICATE: Đòi hỏi hệ thống CA bên ngoài phải thực hiện đúng quy trình nghiệp vụ để cấp các chứng thư số có chứa chính xác khóa công khai SVD được gửi sang.

A.ACCESS_PROTECTED được giải quyết bởi:

OE.ENV: Đòi hỏi TOE phải được đặt và vận hành trong một môi trường được bảo vệ nghiêm ngặt bằng các cơ chế kiểm soát tiếp cận vật lý (Trung tâm dữ liệu đạt chuẩn).

A.AUTH_DATA được giải quyết bởi:

OE.DEVICE: Đòi hỏi thiết bị đầu cuối cá nhân của người ký phải tham gia thực thi một cách chính xác các bước quy định trong giao thức kích hoạt chữ ký SAP.

A.TSP_AUDITED được giải quyết bởi:

OE.ENV: Đòi hỏi hệ thống phải được triển khai và vận hành bởi một tổ chức cung cấp dịch vụ tin cậy đã được cấp phép và đã được kiểm toán đạt chuẩn.

A.SEC_REQ được giải quyết bởi:

OE.TW4S_CONFORMANT: Đòi hỏi toàn bộ hệ thống tổng thể nơi TOE vận hành phải đạt chứng nhận tuân thủ đầy đủ khung tiêu chuẩn bảo mật hệ thống từ xa EN 419241-1.

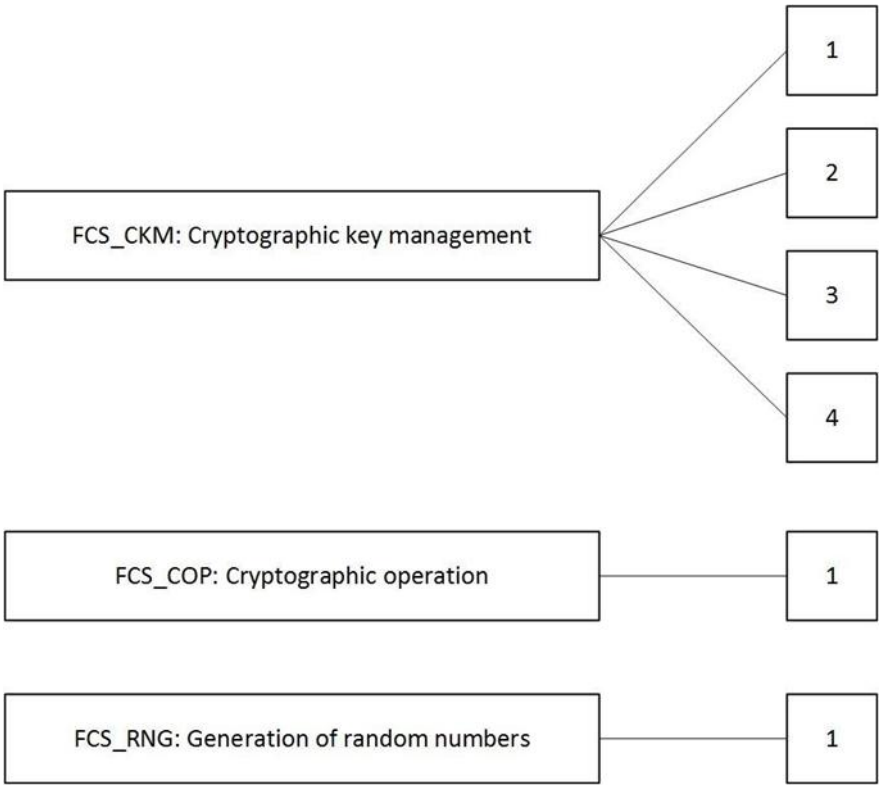
8 Định nghĩa thành phần mở rộng

8.1 Lớp FCS: Hỗ trợ mật mã (Class FCS: Cryptographic Support)

8.1.1 Tổng quan

Lớp FCS: Hỗ trợ mật mã (Cryptographic Support) như được định nghĩa trong [CC2] được mở rộng thêm một họ (family) mới, đó là: Khởi tạo số ngẫu nhiên (FCS_RNG). Họ này liên quan trực tiếp đến các chức năng sinh số ngẫu nhiên an toàn trong mật mã.

Sơ đồ phân rã cấu trúc dưới đây minh họa các thành phần cốt lõi của Lớp FCS: Hỗ trợ mật mã sau khi đã được bổ sung thêm họ mới FCS_RNG:



Hình 2

8.1.2 Khởi tạo số ngẫu nhiên (FCS_RNG)

Họ (family) này mô tả các yêu cầu chức năng đối với quy trình khởi tạo số ngẫu nhiên được sử dụng cho các mục đích mật mã.

Hành vi của họ (Family behaviour):

Họ này định nghĩa các yêu cầu về mặt chất lượng đối với quy trình khởi tạo số ngẫu nhiên, các số ngẫu nhiên này được thiết kế để sử dụng cho các mục đích mã hóa mật mã và an toàn hệ thống.

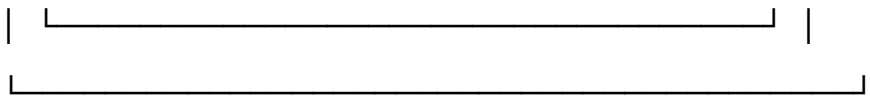
Phân cấp cấu phần (Component levelling):

┌──┐

│ FCS_RNG: Khởi tạo số ngẫu nhiên │

│ ┌──────────────────────────────────────┐ │

│ │ FCS_RNG.1 Khởi tạo số ngẫu nhiên │ │



FCS_RNG.1 (Khởi tạo số ngẫu nhiên): Yêu cầu việc khởi tạo các số ngẫu nhiên phải đáp ứng một tiêu chuẩn chất lượng định trước, đảm bảo tính không thể dự đoán và có độ hỗn loạn (entropy) đầy đủ.

FCS_RNG.1.1 TSF (Chức năng an toàn của TOE) phải cung cấp một bộ sinh số ngẫu nhiên [lựa chọn: vật lý (physical), thực tế phi vật lý (non-physical true), tiền định (deterministic), vật lý lai (hybrid physical), tiền định lai (hybrid deterministic)] để thực thi: [gán: danh sách các khả năng/tính năng an toàn].

FCS_RNG.1.2 TSF phải cung cấp các [lựa chọn: bit, octet của bit, các số [gán: định dạng của các số]] đáp ứng [gán: một thước đo chất lượng định nghĩa trước].

- Lưu ý ứng dụng 27 (Application Note 27)

Bộ sinh số ngẫu nhiên vật lý (Physical RNG): Tạo ra số ngẫu nhiên thông qua một nguồn nhiễu dựa trên các quy trình vật lý ngẫu nhiên (ví dụ: nhiễu nhiệt, nhiễu bán dẫn).

Bộ sinh số ngẫu nhiên thực tế phi vật lý (Non-physical true RNG): Sử dụng nguồn nhiễu dựa trên các quy trình ngẫu nhiên phi vật lý như sự tương tác của con người (tốc độ gõ phím, chuyển động của chuột).

Bộ sinh số ngẫu nhiên tiền định (Deterministic RNG): Sử dụng một dữ liệu hạt giống ngẫu nhiên (random seed) để tạo ra kết quả đầu ra giả ngẫu nhiên (pseudorandom).

Bộ sinh số ngẫu nhiên lai (Hybrid RNG): Kết hợp các nguyên lý của bộ sinh số ngẫu nhiên vật lý và tiền định. Trong đó:

Bộ sinh số ngẫu nhiên vật lý lai (Hybrid physical RNG): Tạo ra một lượng độ hỗn loạn (entropy) tối thiểu bằng hoặc lớn hơn lượng entropy mà kết quả đầu ra của RNG có thể chứa.

Bộ sinh số ngẫu nhiên tiền định lai (Hybrid deterministic RNG): Có trạng thái nội bộ chứa entropy tươi mới (fresh entropy), nhưng lượng entropy này thấp hơn lượng entropy mà kết quả đầu ra của RNG có thể chứa.

9 Các yêu cầu bảo mật (Security Requirements)

9.1 Quy ước khi trình bày hồ sơ bảo vệ

Các quy ước dưới đây được sử dụng thống nhất trong việc định nghĩa các Yêu cầu chức năng an toàn (SFRs):

- **Tinh chỉnh (Refinements):** Các nội dung tinh chỉnh được thực hiện trực tiếp trong tài liệu Hồ sơ bảo vệ (PP) này luôn luôn là các phần cập nhật, sửa đổi của văn bản gốc thuộc SFR. Chúng được đánh dấu bằng định dạng **chữ in đậm** và văn bản gốc ban đầu sẽ được ghi chú ở phần chân trang (footnote).
- **Lựa chọn (Selections):** Các nội dung lựa chọn đã được thực hiện sẵn trong tài liệu PP này được viết bằng định dạng *chữ in nghiêng*, và văn bản gốc ban đầu sẽ được ghi chú ở phần chân trang. Đối với các nội dung lựa chọn được để trống nhằm mục đích cho tác giả tài liệu Mục tiêu bảo mật (Security Target - ST) tự điền vào, chúng sẽ xuất hiện trong dấu ngoặc vuông kèm theo chỉ dẫn cần thực hiện lựa chọn, [lựa chọn:], và mô tả của các phương án lựa chọn sẽ được viết bằng *chữ in nghiêng*.

- **Gán giá trị (Assignments):** Các nội dung gán giá trị đã được thực hiện sẵn trong tài liệu PP này được viết bằng định dạng *chữ in nghiêng*, và văn bản gốc ban đầu sẽ được ghi chú ở phần chân trang. Đối với các nội dung gán giá trị được để trống nhằm mục đích cho tác giả tài liệu ST tự điền vào, chúng sẽ xuất hiện trong dấu ngoặc vuông kèm theo chỉ dẫn cần thực hiện gán giá trị, [gán:], và phần mô tả nội dung gán giá trị sẽ được viết bằng *chữ in nghiêng*.
- **Lặp lại (Iterations):** Các thao tác lặp lại đối với một thành phần SFR (khi áp dụng cho các mục tiêu khác nhau) được ký hiệu bằng một dấu gạch chéo / kèm theo mã định danh phân biệt phép lặp đặt ngay sau mã hiệu của cấu phần đó (ví dụ: FCS_COP.1/Signing).

9.2 Các Chủ thể, Đối tượng và Thao tác vận hành (Subjects, Objects and Operations)

Mục này mô tả chi tiết danh mục các chủ thể (chủ thể kích hoạt hành động), đối tượng (tài sản chịu tác động) và các thao tác vận hành được hỗ trợ và kiểm soát bởi TOE.

Bảng 9

Subject	Mô tả chi tiết
R.Signer	Đại diện trong TOE, người dùng cuối muốn tạo chữ ký điện tử
R.Privileged_User	Đại diện cho bên trong TOE, một người dùng đặc quyền có thể quản trị TOE và một số hoạt động liên quan đến R.Signer

Bảng 10

Object	Mô tả chi tiết
R.Reference_Privileged_User _Authentication_Data	Dữ liệu được TOE sử dụng để xác thực Người dùng đặc quyền
R.Reference_Signer_Authentication_Data	Dữ liệu được TOE sử dụng để xác thực Người ký
R.SVD	Phần công khai của cặp khóa chữ ký R.Signer
R.Sign_Key_Id	Số nhận dạng đại diện cho phần riêng tư của cặp khóa chữ ký R.Signer
R.DTBS / R	Dữ liệu được ký kết đại diện
R.Authorisation_Data	Dữ liệu được Mô-đun mật mã sử dụng để kích hoạt phần riêng tư của cặp khóa chữ ký R.Signer
R.Signature	Kết quả của một hoạt động chữ ký
R.TSF_DATA	Dữ liệu cấu hình TOE

Bảng 11

Subject	Operation	Object	Mô tả chi tiết
R.Privileged_User	Create_New_Privileged_User	R.Privileged_User R.Reference_Privileged_User _Authentication_Data	Một người dùng đặc quyền mới có thể được tạo bao gồm đối tượng đại diện cho người dùng đặc quyền mới cũng như đối tượng được sử dụng để xác thực người dùng đặc quyền mới được tạo.
R.Privileged_User	Create_New_Signer	R.Signer R.Reference_Signer_Authentication_Data	Có thể tạo người ký mới bao gồm đối tượng đại diện cho người ký mới cũng như đối tượng được sử dụng để xác thực người ký mới được tạo.
R.Privileged_User R.Signer	Generate_Signer_Key_Pair	R.Signer R.SVD R.Sign_Key_Id	Một cặp khóa có thể được tạo và gán cho người ký.
R. Người dùng đặc quyền R.Signer	Signer_Maintenance	R.Signer R.SVD R.Sign_Key_Id	Một cặp khóa có thể bị xóa khỏi người ký.
R. Người dùng đặc quyền	Supply_DTBS / R	R.Signer R.DTBS / R	Dữ liệu được ký bởi một người ký có thể được cung cấp bởi một người dùng có đặc quyền.
R.Signer	Đang ký	R.Authorisation_Data R.Signer R.Signs_Key_Id R.DTBS / R R.Signature	Người ký có thể ký dữ liệu để được ký dẫn đến một chữ ký.
R. Người dùng đặc quyền	TOE_Maintenance	R.TSF_DATA	Cấu hình TOE có thể được duy trì bởi một người dùng đặc quyền.

9.3 Tổng quan về các SFR (SFRs overview)

Mục này cung cấp một cái nhìn tổng quan về cách thức các Yêu cầu chức năng an toàn (SFRs) liên kết chặt chẽ với nhau nhằm xử lý các kịch bản sử dụng TOE và bảo vệ đối tượng Người ký (R.Signer).

- Đối tượng Người ký (Signer object)

FIA_ATD.1 và FIA_USB.1 đòi hỏi đối tượng R.Signer bắt buộc phải được thiết lập và duy trì trạng thái an toàn bởi TOE.

FDP_ITC.2/Signer mô tả chi tiết các yêu cầu bảo mật đối với quá trình nhập khẩu (import) đối tượng R.Signer từ môi trường ngoài vào hệ thống.

FDP_ETC.2/Signer mô tả các yêu cầu bảo mật đối với quá trình xuất khẩu (export) đối tượng R.Signer ra ngoài phạm vi TOE.

FDP_UIT.1 đòi hỏi đối tượng R.Signer phải được bảo vệ toàn vẹn tuyệt đối dữ liệu khi thực hiện các thao tác nhập khẩu và xuất khẩu này.

FPT_TDC.1 yêu cầu TOE phải có khả năng diễn giải chính xác các dữ liệu liên quan đến đối tượng R.Signer khi được chia sẻ hoặc truyền nhận với ứng dụng máy chủ ký số (SSA).

FMT_MSA.1, FMT_MSA.2 và FMT_MSA.3 mô tả các quy tắc phân quyền cho việc khởi tạo, duy trì và sử dụng đối tượng R.Signer cũng như đặt ra các yêu cầu ràng buộc kỹ thuật đối với giá trị thuộc tính của đối tượng này.

- Xác thực danh tính (Authentication)

FIA_AFL.1 thiết lập cơ chế giới hạn số lần thử xác thực sai liên tiếp (ngăn chặn các cuộc tấn công dò quét/brute-force mật mã).

FDP_UCT.1 đảm bảo rằng toàn bộ dữ liệu kiểm soát truy cập và dữ liệu dòng thông tin nhạy cảm bắt buộc phải được truyền tải dưới dạng mã hóa bí mật (confidential).

FIA_UID.2 và FIA_UAU.1 yêu cầu mọi người dùng bắt buộc phải được định danh (identified) và xác thực (authenticated) thành công trước khi hệ thống cho phép thực thi bất kỳ hành động nào đại diện cho người dùng đó.

FIA_UAU.5/Signer và FIA_UAU.5/Privileged User đặc tả danh mục cụ thể các cơ chế xác thực được hệ thống chấp nhận đối với từng nhóm đối tượng tương ứng.

- Khởi tạo cấu phần Người ký (Create Signer)

FDP_ACC.1/Signer Creation kết hợp với FDP_ACF.1/Signer Creation mô tả chi tiết các quy tắc và chính sách kiểm soát truy cập bắt buộc phải áp dụng khi khởi tạo mới một đối tượng R.Signer trong hệ thống.

FIA_USB.1 định nghĩa các quy tắc ủy quyền liên kết thuộc tính an toàn phục vụ khâu tạo tài khoản người ký mới.

- Khởi tạo cặp khóa ký (Signer Key Pair Generation)

FDP_ACC.1/Signer Key Pair Generation và FDP_ACF.1/Signer Key Pair Generation mô tả chính sách kiểm soát truy cập nghiêm ngặt đối với tác vụ sinh cặp khóa ký.

FCS_CKM.1 quy định các tiêu chuẩn và thuật toán áp dụng cho quá trình sinh các cặp khóa ký an toàn của khách hàng.

- Xóa khóa ký của người dùng (Signer Key Pair Deletion)

FDP_ACC.1/Signer Key Pair Deletion và FDP_ACF.1/Signer Key Pair Deletion mô tả quyền hạn kiểm soát truy cập đối với hành vi xóa bỏ cặp khóa ký.

FCS_CKM.4 bắt buộc các khóa bí mật khi xóa phải được hủy bỏ một cách an toàn tuyệt đối (Zeroization/phá hủy dấu vết bộ nhớ), không thể khôi phục lại.

- Bảo trì thông tin người ký (Signer Maintenance)

FDP_ACC.1/Signer Maintenance và FDP_ACF.1/Signer Maintenance mô tả các yêu cầu kiểm soát truy cập đối với tác vụ cập nhật, thay đổi dữ liệu xác thực người ký tham chiếu (R.Reference_Signer_Authentication_Data) thuộc đối tượng R.Signer.

- Cung cấp giá trị băm tài liệu cần ký (Supply DTBS/R)

FDP_ACC.1/Supply DTBS/R và FDP_ACF.1/Supply DTBS/R mô tả các yêu cầu kiểm soát quyền truy cập, quy định chỉ những Người dùng có đặc quyền (Privileged User) được ủy quyền mới có quyền nạp/cung cấp giá trị băm của tài liệu cần ký (R.DTBS/R) vào lõi hệ thống.

- Thực thi tạo chữ ký số (Signing)

FDP_IFF.1/Signer và FDP_IFC.1/Signer mô tả chính sách kiểm soát luồng thông tin và các điều kiện tiên quyết bắt buộc phải thỏa mãn trước khi một lệnh tạo chữ ký số có thể được triển khai thực tế.

FDP_UIT.1 yêu cầu đối tượng dữ liệu kích hoạt chữ ký R.SAD phải được bảo vệ toàn vẹn, chống lại mọi hành vi sửa đổi trái phép và bẻ gãy các cuộc tấn công lặp lại (replay attacks).

FDP_ACC.1/Signing và FDP_ACF.1/Signing đặc tả ma trận kiểm soát truy cập trực tiếp cho phiên ký số.

FCS_COP.1 yêu cầu TOE phải thực hiện tác vụ tính toán mật mã để tạo ra chữ ký số (R.Signature) tuân thủ chính xác theo danh mục các giải thuật an toàn được chỉ định cụ thể trong tài liệu ST.

- Đối tượng Người dùng có đặc quyền (Privileged User object)

FIA_ATD.1 và FIA_USB.1 yêu cầu đối tượng dữ liệu quản trị R.Privileged_User phải được TOE bảo vệ và quản lý thuộc tính an toàn ổn định.

FDP_ITC.2/Privileged User quy định các yêu cầu kỹ thuật an toàn khi nhập khẩu dữ liệu tài khoản Admin.

FDP_ETC.2/Privileged User quy định các yêu cầu kỹ thuật khi xuất khẩu dữ liệu tài khoản Admin.

FDP_UIT.1 bảo vệ tính toàn vẹn dữ liệu của tài khoản R.Privileged_User khi thực hiện luồng nạp/xuất thông tin.

FPT_TDC.1 yêu cầu TOE có năng lực đồng bộ và diễn giải đúng cấu trúc dữ liệu của tài khoản Admin khi chia sẻ thông tin với hệ thống SSA ngoài.

FMT_MSA.1, FMT_MSA.2, FMT_MSA.3 mô tả các quy tắc quản lý, sửa đổi thuộc tính và thiết lập giá trị an toàn mặc định cho nhóm tài khoản quản trị.

- Khởi tạo tài khoản quản trị (Privileged User Creation)

FDP_ACC.1/Privileged User Creation và FDP_ACF.1/Privileged User Creation thiết lập chính sách kiểm soát truy cập nghiêm ngặt để tạo mới một tài khoản Admin (ngăn chặn hành vi cài cắm tài khoản quản trị ma).

FIA_USB.1 quy định các ràng buộc về quyền hạn khi gán thuộc tính an toàn cho Admin mới.

- Bảo trì hệ thống TOE (TOE Maintenance)

FDP_ACC.1/TOE Maintenance và FDP_ACF.1/TOE Maintenance kiểm soát các lệnh can thiệp sâu vào nhân cấu hình cốt lõi của TOE.

FMT_SMF.1 và FMT_SMF.2 yêu cầu TOE phải cung cấp đầy đủ các giao diện/hàm chức năng quản trị để thực thi việc quản lý hệ thống, phân vai trò (Roles) và quản lý người dùng (Users).

- Nhật ký kiểm toán (Audit)

FAU_GEN.1 và FAU_GEN.2 định nghĩa chi tiết danh mục cấu trúc các sự kiện bảo mật hệ thống bắt buộc phải ghi log (như tạo khóa, xóa khóa, phiên đăng nhập, thay đổi cấu hình) và tự động gắn vết sự kiện đó với định danh tài khoản chính xác của người thực hiện.

- Kênh truyền thông bảo mật (Communication)

FPT_ITC.2 yêu cầu toàn bộ các kênh truyền kết nối và dữ liệu đi vào TOE bắt buộc phải có nguồn gốc định danh tin cậy phát ra từ ứng dụng SSA.

FTP_TRP.1/SSA và FTP_TRP.1/SIC thiết lập cơ chế thiết lập đường truyền bảo mật an toàn cao (Trusted Path) do chính Người dùng có đặc quyền hoặc Người ký chủ động khởi tạo, bảo vệ luồng dữ liệu chống nghe trộm và can thiệp giữa đường.

9.4 Các yêu cầu chức năng bảo mật (Security Functional Requirements)

Các yêu cầu chức năng bảo mật (SFR) riêng biệt được đặc tả cụ thể trong các phân đoạn dưới đây.

9.4.1 Kiểm toán bảo mật (Security Audit - FAU)

FAU_GEN.1 Sinh nhật ký kiểm toán (Audit data generation)

- **FAU_GEN.1.1:** TSF (Chức năng bảo mật của TOE) phải có khả năng tạo ra một bản ghi kiểm toán đối với các sự kiện có thể kiểm toán (auditable events) sau đây:
    - a) Khởi động (Start-up) và tắt (Shutdown) các chức năng kiểm toán;
    - b) Tất cả các sự kiện có thể kiểm toán đối với mức độ kiểm toán [lựa chọn: tối thiểu (minimum), cơ bản (basic), chi tiết (detailed), không quy định]; và
    - c) Quản lý Người dùng có đặc quyền (Privileged User management);
    - d) Xác thực Người dùng có đặc quyền (Privileged User authentication);
    - e) Quản lý Người ký (Signer management);
    - f) Xác thực Người ký (Signer authentication);
    - g) Sinh cặp khóa ký (Signing key generation);
    - h) Hủy bỏ khóa ký (Signing key destruction);
    - i) Kích hoạt và sử dụng khóa ký (Signing key activation and usage), bao gồm cả mã băm (hash) của dữ liệu cần ký R.DTBS/R và chữ ký số đầu ra R.Signature;
    - j) Thay đổi cấu hình của TOE (Change of TOE configuration);
    - k) [gán: các sự kiện có thể kiểm toán cụ thể khác].

Lưu ý ứng dụng 28 (Application Note 28): Tác vụ quản lý các đối tượng R.Privileged_User (Người dùng có đặc quyền) và R.Signer (Người ký) phải bao gồm tất cả các sự kiện liên quan đến việc khởi tạo, sửa đổi hoặc xóa bỏ các đối tượng này. Tác vụ xác thực Người ký phải bao gồm cả các sự kiện xác thực thất bại đối với một khẳng định danh tính (assertion) được cung cấp bởi một bên được ủy quyền (delegated party). Việc thay đổi cấu hình TOE phải bao gồm tất cả các sự kiện khởi tạo, sửa đổi và xóa bỏ đối tượng cấu hình.

Lưu ý ứng dụng 29 (Application Note 29): Việc tạo ra một yêu cầu chứng nhận (certification request) chính là một hành vi sử dụng khóa ký và bắt buộc phải được lưu vết trong nhật ký kiểm toán.

Lưu ý ứng dụng 30 (Application Note 30): Một số giải pháp triển khai thực tế có thể không ghi nhận trực tiếp giá trị mã băm R.DTBS/R vào nhật ký kiểm toán vì lý do bảo vệ quyền riêng tư của người dùng. Đối với các hệ thống như vậy, tác giả tài liệu ST (Mục tiêu bảo mật) phải mô tả rõ phương pháp sử dụng nhật ký kiểm toán để chứng minh một giá trị R.DTBS/R cụ thể đã được ký số thành công.

- **FAU_GEN.1.2:** TSF phải ghi lại trong mỗi bản ghi kiểm toán tối thiểu các thông tin sau đây:
    - a) Ngày giờ diễn ra sự kiện, loại sự kiện, định danh chủ thể (nếu có), và kết quả (thành công hoặc thất bại) của sự kiện;

- b) Đối với mỗi loại sự kiện kiểm toán, dựa trên định nghĩa về các sự kiện có thể kiểm toán của các thành phần chức năng có trong tài liệu PP/ST: [gán: Loại hành động được thực hiện (thành công hoặc thất bại), định danh của vai trò thực hiện thao tác, và [gán: các thông tin liên quan đến kiểm toán khác]].

Lưu ý ứng dụng 31 (Application Note 31): Nhật ký kiểm toán (Audit trail) tuyệt đối không được chứa bất kỳ dữ liệu nào cho phép khôi phục lại các thông tin nhạy cảm của người dùng, bao gồm: Dữ liệu kích hoạt chữ ký (R.SAD), Dữ liệu xác thực người ký tham chiếu (R.Reference_Signer_Authentication_Data) và Dữ liệu ủy quyền (R.Authorization_Data).

FAU_GEN.2 Gắn vết định danh kiểm toán (User identity association)

- **FAU_GEN.2.1:** Đối với các sự kiện kiểm toán phát sinh từ hành động của những người dùng đã được định danh, TSF phải có khả năng liên kết từng sự kiện có thể kiểm toán đó với định danh chính xác của người dùng đã gây ra sự kiện.

9.4.2 Hỗ trợ mật mã (Cryptographic Support - FCS)

FCS_CKM.1 Sinh khóa mật mã (Cryptographic key generation)

- **FCS_CKM.1.1:** TSF phải tạo ra các khóa mật mã tuân thủ chính xác theo thuật toán sinh khóa mật mã được chỉ định [gán: thuật toán sinh khóa mật mã] và kích thước khóa mật mã được chỉ định [gán: kích thước khóa mật mã] đáp ứng các tiêu chuẩn sau: [gán: danh sách các tiêu chuẩn].

Lưu ý ứng dụng 32 (Application Note 32): TOE được kỳ vọng sẽ sử dụng một mô-đun mật mã (Cryptographic Module) đã được chứng nhận tuân thủ tiêu chuẩn [EN 419 221-5] để thực hiện khâu sinh khóa (xem thêm mục *OE.CRYPTOMODULE_CERTIFIED*). Mặc dù bản thân lõi TSF của phần mềm có thể không tự sinh khóa, SFR này thể hiện yêu cầu bắt buộc TSF phải gọi/kích hoạt mô-đun mật mã phần cứng (HSM) với các tham số thích hợp bất cứ khi nào có yêu cầu sinh khóa hệ thống. Hướng dẫn về các thuật toán mật mã bảo mật có thể tham khảo tại tiêu chuẩn [ETSI TS 119 312] và tài liệu của nhóm [SOGIS].

Lưu ý ứng dụng 33 (Application Note 33): Tài liệu ST dự kiến sẽ sử dụng các khóa mật mã cho nhiều mục đích khác nhau (ví dụ: khóa ứng dụng, khóa hạ tầng, khóa phiên,...). Tác giả tài liệu ST nên thực hiện lặp lại (iteration) SFR này cho từng loại khóa (ví dụ: FCS_CKM.1/RSA và FCS_CKM.1/AES) mà hệ thống tự tạo ra.

FCS_CKM.4 Hủy khóa mật mã (Cryptographic key destruction)

- **FCS_CKM.4.1:** TSF phải hủy bỏ các khóa mật mã tuân thủ chính xác theo phương pháp hủy khóa mật mã được chỉ định [gán: phương pháp hủy khóa mật mã] đáp ứng các tiêu chuẩn sau: [gán: danh sách các tiêu chuẩn].

Lưu ý ứng dụng 34 (Application Note 34): TOE được kỳ vọng sẽ sử dụng mô-đun mật mã đạt chuẩn [EN 419 221-5] để thực hiện tác vụ hủy khóa. Mặc dù lõi TSF có thể không trực tiếp xóa hạt vật lý của khóa, SFR này yêu cầu TSF phải gọi hàm hủy của mô-đun mật mã với các tham số chuẩn xác. Tài liệu ST phải chỉ rõ phương pháp phá hủy bảo mật (Zeroization) đối với tất cả các khóa bí mật và khóa hỗ trợ để đảm bảo không để lại dấu vết trong bộ nhớ. Tác giả ST có thể dùng mô tả hành động kỹ thuật thực tế thay vì viện dẫn một tiêu chuẩn bên ngoài tại ô gán cuối cùng.

FCS_COP.1 Vận hành mật mã (Cryptographic operation)

- **FCS_COP.1.1:** TSF phải thực hiện [gán: danh sách các tác vụ vận hành mật mã] tuân thủ chính xác theo thuật toán mật mã được chỉ định [gán: thuật toán mật mã] và kích thước khóa mật mã được chỉ định [gán: kích thước khóa mật mã] đáp ứng các tiêu chuẩn sau: [gán: danh sách các tiêu chuẩn].

Lưu ý ứng dụng 37 (Application Note 37): Đối với dịch vụ chữ ký số trong khối Liên minh Châu Âu (EU), việc hoàn thiện cấu phần này phải tuân theo Định chế (EU) No 910/2014 [eIDAS]. *Tại Việt Nam, khâu này sẽ được ST writer gán các thuật toán quy định bởi Bộ Khoa học và Công nghệ như SHA-256, RSA từ 2048-bit trở lên hoặc ECC.*

FCS_RNG.1 Khởi tạo số ngẫu nhiên (Generation of Random Numbers)

- **FCS_RNG.1.1:** TSF phải cung cấp một bộ sinh số ngẫu nhiên [lựa chọn: vật lý, thực tế phi vật lý, tiền định, vật lý lai, tiền định lai] để thực thi: [gán: danh sách các tính năng bảo mật].
- **FCS_RNG.1.2:** TSF phải cung cấp các [lựa chọn: bit, octet của bit, các số [gán: định dạng của các số]] đáp ứng [gán: một thước đo chất lượng định nghĩa trước].

Lưu ý ứng dụng 39 (Application Note 39): SFR FCS_RNG.1 này chỉ áp dụng nếu phần mềm TOE được triển khai độc lập và nằm ngoài ranh giới vật lý của mô-đun mật mã HSM. Nếu TOE nằm hoàn toàn trong cùng một ranh giới vật lý với HSM, các yêu cầu về sinh số ngẫu nhiên đã được kiểm soát bởi tiêu chuẩn [EN 419 221-5].

9.4.3 Bảo vệ dữ liệu người dùng (User Data Protection - FDP)

FDP_ACC.1 Kiểm soát truy cập dựa trên cấu phần (Subset access control)

Do tính chất phân tách quyền hạn trong hệ thống chữ ký số từ xa, yêu cầu kiểm soát truy cập FDP_ACC.1 được lặp lại thành nhiều phân hệ độc lập:

1. FDP_ACC.1/Privileged User Creation (Khởi tạo Người dùng có đặc quyền)

- **FDP_ACC.1.1/Privileged User Creation:** TSF phải thực thi Chính sách kiểm soát truy cập khởi tạo Người dùng có đặc quyền (Privileged User Creation SFP) đối với:
    - **Chủ thể (Subjects):** Người dùng có đặc quyền (Privileged User).
    - **Đối tượng (Objects):** Các thuộc tính bảo mật mới của Người dùng có đặc quyền chuẩn bị được tạo ra.
    - **Thao tác (Operations):** Create_New_Privileged_User: TOE khởi tạo đối tượng dữ liệu R.Privileged_User và dữ liệu xác thực tham chiếu tương ứng R.Reference_Privileged_User_Authentication_Data dựa trên thông tin được truyền tới từ một Người dùng có đặc quyền hiện tại.

2. FDP_ACC.1/Signer Creation (Khởi tạo Người ký)

- **FDP_ACC.1.1/Signer Creation:** TSF phải thực thi Chính sách kiểm soát truy cập khởi tạo Người ký (Signer Creation SFP) đối với:
    - **Chủ thể:** Người dùng có đặc quyền (Privileged User).
    - **Đối tượng:** Các thuộc tính bảo mật mới của đối tượng Người ký chuẩn bị được tạo ra.
    - **Thao tác:** Create_New_Signer: TOE khởi tạo thực thể R.Signer và dữ liệu xác thực người ký tham chiếu R.Reference_Signer_Authentication_Data.

3. FDP_ACC.1/Signer Key Pair Generation (Sinh cặp khóa ký)

- **FDP_ACC.1.1/Signer Key Pair Generation:** TSF phải thực thi Chính sách kiểm soát truy cập sinh cặp khóa ký đối với:
    - **Chủ thể:** Người dùng có đặc quyền, Người ký (Signer).
    - **Đối tượng:** Cặp khóa ký số của khách hàng.
    - **Thao tác:** Generate_Signer_Key_Pair.

4. FDP_ACC.1/Signer Key Pair Deletion (Xóa cặp khóa ký)

- **FDP_ACC.1.1/Signer Key Pair Deletion:** TSF phải thực thi Chính sách kiểm soát truy cập xóa cặp khóa ký đối với:
    - **Chủ thể:** Người dùng có đặc quyền, Người ký.
    - **Đối tượng:** Khóa ký số của khách hàng (R.Signing_Key).
    - **Thao tác:** Delete_Signer_Key_Pair.

5. FDP_ACC.1/Signer Maintenance (Bảo trì Người ký)

- **FDP_ACC.1.1/Signer Maintenance:** TSF phải thực thi Chính sách kiểm soát bảo trì Người ký đối với:
    - **Chủ thể:** Người dùng có đặc quyền, hoặc Người ký sở hữu tài khoản.
    - **Đối tượng:** Dữ liệu thuộc tính của cấu phần R.Signer.
    - **Thao tác:** Maint_Signer_Attributes (Cập nhật dữ liệu xác thực tham chiếu).

6. FDP_ACC.1/Supply DTBS/R (Cung cấp giá trị băm tài liệu)

- **FDP_ACC.1.1/Supply DTBS/R:** TSF phải thực thi Chính sách kiểm soát nạp dữ liệu cần ký đối với:
    - **Chủ thể:** Người dùng có đặc quyền (Hệ thống SSA ứng dụng máy chủ).
    - **Đối tượng:** Cấu phần dữ liệu R.DTBS/R.
    - **Thao tác:** Supply_DTBS/R_To_TOE.

7. FDP_ACC.1/Signing (Thực thi ký số)

- **FDP_ACC.1.1/Signing:** TSF phải thực thi Chính sách kiểm soát truy cập phiên ký số đối với:
    - **Chủ thể:** Người ký (hoặc Chủ thể đại diện được ủy quyền hợp pháp).
    - **Đối tượng:** Khóa ký bí mật R.Signing_Key, Dữ liệu cần ký R.DTBS/R và Dữ liệu kích hoạt chữ ký R.SAD.
    - **Thao tác:** Sign_DTBS/R.

8. FDP_ACC.1/TOE Maintenance (Bảo trì hệ thống TOE)

- **FDP_ACC.1.1/TOE Maintenance:** TSF phải thực thi Chính sách kiểm soát truy cập bảo trì TOE đối với nhóm Người dùng có đặc quyền quản trị cao cấp khi thay đổi các cấu hình lõi của phần mềm SAM.

FDP_ACF.1 Kiểm soát truy cập dựa trên thuộc tính (Security attribute based access control)

Mỗi phân hệ thuộc tính sẽ đi kèm một quy tắc phê duyệt hành động nghiêm ngặt tại mục FDP_ACF.1. Dưới đây là đặc tả tiêu biểu cho hai phân hệ cốt lõi nhất của hệ thống ký số từ xa:

Phân hệ Khởi tạo Người dùng có đặc quyền (Privileged User Creation)

- **FDP_ACF.1.1/Privileged User Creation:** TSF phải thực thi Chính sách để kiểm soát quyền truy cập của các đối tượng dựa trên thuộc tính bảo mật sau:
    - *(1) Liệu chủ thể kích hoạt có phải là một Người dùng có đặc quyền được cấp quyền khởi tạo tài khoản quản trị mới hay không.*
- **FDP_ACF.1.2/Privileged User Creation:** TSF phải áp dụng quy tắc sau để quyết định thao tác:

- *(1) Chỉ có Người dùng có đặc quyền đã được phân vai trò/quyền hạn rõ ràng mới được phép thực thi lệnh Create_New_Privileged_User.*

- **FDP_ACF.1.3 & .4:** Cho phép thiết lập các quy tắc phê duyệt hoặc từ chối đặc biệt [gán: các quy tắc bổ sung hoặc Không có].

Phân hệ Thực thi ký số (Signing) - Lõi vận hành Smart CA

- **FDP_ACF.1.1/Signing:** TSF phải thực thi Chính sách kiểm soát truy cập phiên ký số dựa trên các thuộc tính bảo mật của đối tượng:
  - Khóa ký sở hữu bởi Người ký (R.Signing_Key).
  - Trạng thái hợp lệ và tính toàn vẹn của Dữ liệu kích hoạt chữ ký số (R.SAD).
- **FDP_ACF.1.2/Signing:** TSF chỉ cho phép thực thi thao tác ký số (Sign_DTBS/R) khi đáp ứng đầy đủ các quy tắc điều kiện tiên quyết sau:
  - *(1) Dữ liệu kích hoạt chữ ký số R.SAD gửi lên hệ thống phải được xác thực thành công.*
  - *(2) Mã định danh của Người ký (Signer ID) được liên kết trong gói dữ liệu R.SAD phải trùng khớp hoàn toàn với mã định danh của chủ sở hữu Khóa ký bí mật R.Signing_Key.*
  - *(3) Toàn bộ các điều kiện sử dụng khóa ký quy định trong thuộc tính bảo mật của Người ký phải được thỏa mãn (ví dụ: chứng thư số còn hiệu lực, trạng thái không bị tạm dừng).*

FDP_UIT.1 Bảo vệ tính toàn vẹn dữ liệu truyền nhận (Data exchange integrity)

- **FDP_UIT.1.1:** TSF phải thực thi chính sách kiểm soát để có khả năng **phát hiện ra các hành vi sửa đổi dữ liệu (modification), xóa bỏ (deletion), chèn thêm (insertion) và phát lại gói tin (replay)** đối với các dữ liệu người dùng được truyền nhận giữa TOE và các hệ thống bên ngoài.
- **FDP_UIT.1.2:** TSF phải có hành động cấu hình sẵn [gán: hành động từ chối lệnh, khóa phiên hoặc ghi log cảnh báo] khi phát hiện ra bất kỳ lỗi toàn vẹn hoặc hành vi tấn công phát lại nào đối với gói dữ liệu R.SAD và R.DTBS/R.

9.4.4 Định danh và Xác thực (Identification and Authentication - FIA)

FIA_AFL.1 Giới hạn số lần xác thực sai (Authentication failure handling)

- **FIA_AFL.1.1:** TSF phải phát hiện khi số lần thử xác thực không thành công liên tiếp vượt quá ngưỡng cấu hình [gán: số lần thử sai, thường từ 3 đến 5 lần] liên quan đến các tác vụ đăng nhập của Người ký hoặc Quản trị viên.
- **FIA_AFL.1.2:** Khi số lần thử sai vượt quá ngưỡng quy định, TSF phải thực hiện hành động: **khóa tạm thời hoặc vô hiệu hóa tài khoản** [gán: thời gian khóa hoặc yêu cầu quy trình mở khóa thủ công từ Admin].

FIA_UAU.5 Cơ chế xác thực linh hoạt (Multiple authentication mechanisms)

- **FIA_UAU.5.1:** TSF phải cung cấp các cơ chế xác thực bao gồm: [gán: danh sách các cơ chế xác thực như mật mã, OTP, SMS, Chữ ký số, Xác thực sinh trắc học thông qua SAML/OIDC hoặc định danh gián tiếp] để thực hiện việc xác thực người dùng.
- **FIA_UAU.5.2:** TSF phải áp dụng các cơ chế này theo quy tắc: Dữ liệu kích hoạt R.SAD chỉ được coi là hợp lệ khi được ký hoặc xác nhận bởi chính các yếu tố xác thực mạnh được cấu hình riêng cho tài khoản Người ký đó.

9.4.5 Quản lý bảo mật (Security Management - FMT)

- **FMT_SMF.1 Đặc tả các chức năng quản lý:** TSF phải có khả năng thực thi các hàm quản trị hệ thống bao gồm: cấu hình chính sách bảo mật, quản lý vòng đời tài khoản người dùng, thay đổi khóa hệ thống.
- **FMT_SMR.1 Vai trò bảo mật:** TSF phải phân tách rõ ràng các vai trò trong hệ thống, tối thiểu bao gồm: Vai trò Người ký (Signer) và Vai trò Người dùng có đặc quyền (Privileged User - bao gồm Admin hệ thống và Kỹ thuật viên).

9.4.6 Bảo vệ các chức năng bảo mật (Protection of the TSF - FPT / FTP)

- **FPT_TDC.1 Tin cậy dữ liệu giữa các hệ thống:** TSF phải có khả năng diễn giải đồng bộ và chính xác các thuộc tính bảo mật của đối tượng khi trao đổi dữ liệu với ứng dụng máy chủ SSA, đảm bảo không có sự sai lệch thông tin định danh người ký khi đi vào lõi phần mềm.
- **FTP_TRP.1 Kênh truyền tin cậy (Trusted Path):** TSF phải thiết lập một kênh truyền thông tin cậy được bảo vệ bằng các giao thức mật mã mạnh (như TLS 1.3 với cơ chế xác thực hai chiều mTLS), ngăn chặn hoàn toàn nguy cơ bị nghe trộm (disclosure) hoặc can thiệp chỉnh sửa dữ liệu trên đường truyền từ thiết bị đầu cuối của người dùng tới hệ thống Smart CA.

9.4.7 Các Kênh truyền/Đường truyền tin cậy (Trusted Paths/Channels - FTP)

1. Cấu phần FTP_TRP.1/SSA: Đường truyền tin cậy kết nối với Hệ thống máy chủ ký số (SSA)

- **FTP_TRP.1.1/SSA:** TSF phải cung cấp một đường truyền thông tin kết nối giữa chính nó và những người dùng thuộc nhóm [lựa chọn: từ xa (remote), cục bộ (local)] mang vai trò Người dùng có đặc quyền thông qua ứng dụng SSA. Đường truyền này phải tách biệt về mặt logic (logically distinct) với các đường truyền thông tin khác, đồng thời phải đảm bảo xác thực chắc chắn các điểm cuối (endpoints) và bảo vệ dữ liệu truyền tải chống lại hành vi [lựa chọn: sửa đổi (modification), lộ lọt (disclosure), [gán: các loại vi phạm tính toàn vẹn hoặc tính bí mật khác]].
- **FTP_TRP.1.2/SSA:** TSF phải cho phép [lựa chọn: TSF, người dùng cục bộ, người dùng từ xa] mang vai trò Người dùng có đặc quyền thông qua SSA chủ động khởi tạo giao tiếp truyền thông qua đường truyền tin cậy này.
- **FTP_TRP.1.3/SSA:** TSF phải bắt buộc sử dụng đường truyền tin cậy đối với các tác vụ sau:
    - (1) FDP_ACC.1.1/Privileged User Creation (Khởi tạo Người dùng có đặc quyền)
    - (2) FDP_ACC.1/Signer Creation (Khởi tạo Người ký)
    - (3) FDP_ACC.1/Signer Maintenance (Bảo trì Người ký)
    - (4) FDP_ACC.1/Signer Key Pair Generation (Sinh cặp khóa ký cho người ký)
    - (5) FDP_ACC.1/Signer Key Pair Deletion (Xóa cặp khóa ký của người ký)
    - (6) FDP_ACC.1/Supply DTBS/R (Cung cấp giá trị băm tài liệu cần ký)
    - (7) FDP_ACC.1/TOE Maintenance (Bảo trì hệ thống TOE)
    - (8) [lựa chọn: xác thực người dùng ban đầu, [gán: các dịch vụ khác bắt buộc yêu cầu đường truyền tin cậy]

Lưu ý ứng dụng 73 (Application Note 73):

Vì không phải tất cả dữ liệu truyền tới TOE đều cần được bảo vệ tính bí mật, tiêu chuẩn FTP_TRP.1/SSA chỉ đưa ra yêu cầu bắt buộc là bảo vệ dữ liệu chống lại hành vi sửa đổi/thao túng trái phép (bảo vệ tính toàn vẹn).

2. Cấu phần FTP_TRP.1/SIC: Đường truyền tin cậy kết nối với Cấu phần giao tiếp người ký (SIC)

- **FTP_TRP.1.1/SIC:** TSF phải cung cấp một đường truyền thông tin kết nối giữa chính nó và những người dùng thuộc nhóm [lựa chọn: từ xa, cục bộ] mang vai trò Người ký từ xa thông qua cấu phần SIC. Đường truyền này phải tách biệt về mặt logic với các đường truyền thông tin khác, đồng thời phải đảm bảo xác thực chắc chắn các điểm cuối và bảo vệ dữ liệu truyền tải chống lại hành vi [lựa chọn: sửa đổi, lộ lọt, [gán: các loại vi phạm tính toàn vẹn hoặc tính bí mật khác].
- **FTP_TRP.1.2/SIC:** TSF phải cho phép [lựa chọn: TSF, người dùng cục bộ, người dùng từ xa] ^{158} mang vai trò Người ký từ xa thông qua cấu phần SIC chủ động khởi tạo giao tiếp truyền thông qua đường truyền tin cậy này.
- **FTP_TRP.1.3/SIC:** TSF phải bắt buộc sử dụng đường truyền tin cậy đối với các tác vụ sau:
    - (1) FDP_ACC.1/Signer Maintenance (Bảo trì Người ký)
    - (2) FDP_ACC.1/Signer Key Pair Generation (Sinh cặp khóa ký cho người ký)
    - (3) FDP_ACC.1/Signer Key Pair Deletion (Xóa cặp khóa ký của người ký)
    - (4) FDP_ACC.1/Signing (Thực thi ký số)
    - (5) [gán: các dịch vụ khác bắt buộc yêu cầu đường truyền tin cậy]

Lưu ý ứng dụng 74 (Application Note 74):

Tương tự như trên, do không phải mọi dữ liệu truyền tải đều cần mã hóa bí mật, cấu phần FTP_TRP.1.1/SIC chỉ bắt buộc yêu cầu bảo vệ chống sửa đổi dữ liệu. Người viết tài liệu ST (Mục tiêu bảo mật) phải mô tả chi tiết nếu Giao thức kích hoạt chữ ký (SAP) được sử dụng để truyền tải thông tin nhạy cảm và nêu rõ phương thức bảo vệ tính bí mật cho khối thông tin này.

Hệ thống TOE không bắt buộc phải xác duyệt trực tiếp cấu phần SIC với vai trò là một điểm cuối truyền thông độc lập, mà nó có thể tin tưởng hoàn toàn dựa vào kết quả của quy trình xác thực người ký (Signer Authentication).

3. Cấu phần FTP_ITC.1/CM: Kênh truyền tin cậy kết nối với Mô-đun Mật mã (HSM)

- **FTP_ITC.1.1/CM:** TSF phải cung cấp một kênh truyền thông tin kết nối giữa chính nó và [tinh chỉnh: một mô-đun mật mã được chứng nhận tuân thủ theo tiêu chuẩn EN 419 221–5].
- Kênh truyền này phải tách biệt về mặt logic với các kênh truyền thông tin khác, đồng thời phải đảm bảo xác thực chắc chắn các điểm cuối và bảo vệ dữ liệu truyền tải chống lại hành vi sửa đổi (modification) hoặc lộ lọt (disclosure).
- **FTP_ITC.1.2/CM:** TSF phải cho phép TSF và [tinh chỉnh: một mô-đun mật mã được chứng nhận tuân thủ theo tiêu chuẩn EN 419 221–5] chủ động khởi tạo giao tiếp truyền thông qua kênh truyền tin cậy này.
- **FTP_ITC.1.3/CM:** TSF phải chủ động khởi tạo kết nối giao tiếp thông qua kênh truyền tin cậy này để thực hiện tác vụ: [gán: danh sách các hàm chức năng bắt buộc yêu cầu kênh truyền tin cậy].

Lưu ý ứng dụng 75 (Application Note 75):

Yêu cầu FTP_ITC.1/CM bắt buộc phải được hoàn thiện chi tiết trong tài liệu ST nhằm phản ánh chính xác phương thức kết nối vật lý và logic giữa phần mềm TOE và mô-đun mật mã HSM, đồng thời lập luận tính an toàn của phương thức đó.

Trong trường hợp phần mềm TOE và mô-đun mật mã HSM cùng nằm trong một thiết bị phần cứng vật lý duy nhất (ví dụ: phần mềm TOE là một ứng dụng cục bộ chạy trên máy chủ server và giao tiếp trực tiếp với card HSM cắm qua cổng PCI nội bộ), mối quan hệ bảo mật này phải được làm rõ để chứng minh tính miễn nhiễm trước các cuộc tấn công đánh cắp dữ liệu trên bo mạch.

9.5 Các yêu cầu đảm bảo an toàn (Security Assurance Requirements)

Cấp độ yêu cầu đảm bảo an toàn (Assurance level) được thiết lập cho hệ thống là **EAL4+** và được gia cường (augmented) thêm thành phần **AVA_VAN.5** (Đánh giá mức độ tổn hại: Khả năng chống tấn công nâng cao / Advanced vulnerability analysis). Các cấu phần đảm bảo an toàn cụ thể được xác định chi tiết trong bảng dưới đây, với thành phần gia cường được đánh dấu bằng định dạng **chữ in đậm**.

Vì TOE được vận hành bên trong một môi trường được bảo vệ nghiêm ngặt về mặt vật lý như đã mô tả trong mục mục tiêu môi trường *OE.ENV*, quy trình đánh giá và kiểm định tuân thủ theo Hồ sơ bảo vệ (PP) này thông thường sẽ không bao gồm các kịch bản tấn công phá hoại vật lý (physical attacks) trực tiếp lên thiết bị.

Lớp đảm bảo	**Các thành phần đảm bảo**
Phát triển (ADV)	Mô tả kiến trúc bảo mật (ADV_ARC.1)
Lớp đảm bảo	Các thành phần đảm bảo
	Đặc tả chức năng hoàn chỉnh (ADV_FSP.4)
	Trình diễn triển khai TSF (ADV_IMP.1)
	Thiết kế mô-đun cơ bản (ADV_TDS.3)
Tài liệu hướng dẫn (AGD)	Hướng dẫn sử dụng hoạt động (AGD_OPE.1)
	Quy trình chuẩn bị (AGD_PRE.1)
Hỗ trợ vòng đời (ALC)	Hỗ trợ sản xuất, quy trình chấp nhận và tự động hóa (ALC_CMC.4)
	Sự cố theo dõi phạm vi CM (ALC_CMS.4)
	Thủ tục giao hàng (ALC_DEL.1)
	Xác định các biện pháp bảo mật (ALC_DVS.1)
	Mô hình vòng đời do nhà phát triển xác định (ALC_LCD.1)
	Các công cụ phát triển được xác định rõ ràng (ALC_TAT.1)
Bảo vệ Mục tiêu đánh giá (ASE)	Tuyên bố về sự phù hợp (ASE_CCL.1)
	Định nghĩa thành phần mở rộng (ASE_ECD.1)
	Giới thiệu ST (ASE_INT.1)
	Mục tiêu bảo mật (ASE_OBJ.2)
	Yêu cầu bảo mật bắt nguồn (ASE_REQ.2)
	Định nghĩa vấn đề bảo mật (ASE_SPD.1)
	Đặc tả tóm tắt TOE (ASE_TSS.1)
Kiểm tra (ATE)	Phân tích vùng phủ sóng (ATE_COV.2)
	Thử nghiệm: thiết kế cơ bản (ATE_DPT.1)
	Kiểm tra chức năng (ATE_FUN.1)
	Thử nghiệm độc lập - mẫu (ATE_IND.2)
Tính dễ bị tổn thương thẩm định, lượng định, đánh giá (AVA)	Nâng cao có phương pháp sự dễ bị tổn thương phân tích (AVA_VAN.5)

10 Cơ sở lý luận (Rationale)

10.1 Cơ sở lý luận về các Yêu cầu An toàn (Security Requirements Rationale)

Bảng đối chiếu dưới đây được sử dụng để chứng minh rằng mọi Yêu cầu chức năng an toàn (SFR) đều được thiết lập nhằm đáp ứng một mục tiêu bảo mật cụ thể, và ngược lại, mọi mục tiêu bảo mật đề ra đều được bao quát đầy đủ bởi ít nhất một SFR. Bảng này không mang tính chất khép kín theo nghĩa cấu thành tất cả các điểm giao chéo có thể xảy ra giữa hai tập hợp.

- **OT.SIGNER_PROTECTION (Bảo vệ Người ký):** Mục tiêu này được xử lý bằng các yêu cầu xuất khẩu và nhập khẩu đối tượng Người ký (R.Signer) một cách an toàn thông qua các SFR: FDP_ETC.2/Signer, FDP_IFC.1/Signer, FDP_IFF.1/Signer, FDP_ITC.2/Signer, FDP_UCT.1, FDP_UIT.1 và FPT_TDC.1. Các đặc tả thực tế về dữ liệu cấu thành đối tượng được mô tả trong FIA_ATD.1 và FIA_USB.1.
- **OT.REFERENCE_SIGNER_AUTHENTICATION_DATA (Bảo vệ Dữ liệu xác thực người ký tham chiếu):** Mục tiêu này được xử lý bởi FDP_ACC.1/Signer Creation, FDP_ACF.1/Signer Creation, FDP_ACC.1/Signer Maintenance và FDP_ACF.1/Signer Maintenance. Các SFR này mô tả quy tắc kiểm soát truy cập đối với hành vi khởi tạo và cập nhật đối tượng Người ký (R.Signer) cũng như Dữ liệu xác thực người ký tham chiếu (R.Reference_Signer_Authentication_Data).
- **OT.SIGNER_KEY_PAIR_GENERATION (Sinh cặp khóa ký của Người ký):** Mục tiêu này được đáp ứng bởi các yêu cầu về sinh khóa và thuật toán mật mã quy định tại FCS_CKM.1 và FCS_COP.1. Cấu phần FCS_RNG.1 cung cấp một nguồn cấp số ngẫu nhiên tin cậy phục vụ khâu sinh khóa. FCS_CKM.4 mô tả các yêu cầu đối với việc hủy bỏ/xóa khóa an toàn. Các SFR FDP_ACC.1/Signer Key Pair Generation và FDP_ACF.1/Signer Key Pair Generation mô tả chính sách kiểm soát truy cập đối với tác vụ sinh cặp khóa. FIA_USB.1 quy định rằng định danh khóa ký của người ký (R.Signing_Key_Id) phải được liên kết chặt chẽ với đối tượng Người ký. Cấu phần FTP_ITC.1/CM được sử dụng để thiết lập kênh truyền thông an toàn với Mô-đun Mật mã (HSM).
- **OT.SVD (Bảo vệ Dữ liệu xác thực chữ ký số - Khóa công khai):** Mục tiêu này được xử lý bởi các yêu cầu trong FDP_ACC.1/Signer Key Pair Generation và FDP_ACF.1/Signer Key Pair Generation để bảo vệ tính toàn vẹn của khóa công khai khi xuất xưởng.
- **OT.PRIVILEGED_USER_MANAGEMENT (Quản lý Người dùng có đặc quyền):** Mục tiêu này được đáp ứng bởi các yêu cầu xuất khẩu và nhập khẩu đối tượng Người dùng có đặc quyền (R.Privileged_User) một cách an toàn thông qua các SFR: FDP_ETC.2/Privileged User, FDP_IFC.1/Privileged User, FDP_IFF.1/Privileged User, FDP_ITC.2/Privileged User và FPT_TDC.1. Các thuộc tính dữ liệu thực tế được đặc tả trong FIA_ATD.1 và FIA_USB.1. Khâu xác thực danh tính của Người dùng có đặc quyền được xử lý bởi FIA_UID.2, FMT_MSA.1/Privileged User, FMT_MSA.2 và FMT_MSA.3/Privileged User. Các SFR FDP_ACC.1/Privileged User Creation và FDP_ACF.1/Privileged User Creation mô tả quy tắc kiểm soát truy cập để tạo mới một tài khoản Người dùng có đặc quyền.
- **OT.PRIVILEGED_USER_AUTHENTICATION (Xác thực Người dùng có đặc quyền):** Mục tiêu này được đảm bảo xử lý bởi hệ thống các SFR: FIA_AFL.1 (xử lý đăng nhập sai), FIA_UAU.1 (bắt buộc xác thực) và FIA_UAU.5/Privileged User (cơ chế xác thực linh hoạt cho quản trị viên).
- **OT.PRIVILEGED_USER_PROTECTION (Bảo vệ tài khoản Người dùng có đặc quyền):** Mục tiêu này được xử lý bằng các yêu cầu xuất khẩu và nhập khẩu đối tượng Người dùng có đặc quyền một cách an toàn (FDP_ETC.2/Privileged User, FDP_IFC.1/Privileged User, FDP_IFF.1/Privileged User, FDP_ITC.2/Privileged User và FPT_TDC.1). Cấu trúc dữ liệu cụ thể được mô tả trong FIA_ATD.1 và FIA_USB.1. SFR FIA_UID.2 đảm bảo rằng Người dùng có đặc quyền bắt buộc phải được xác thực thành công trước khi hệ thống cho phép họ thực hiện bất kỳ thao tác quản trị nào.

- **OT.SIGNER_MANAGEMENT (Quản lý Người ký):** Mục tiêu này được xử lý bởi các yêu cầu kiểm soát truy cập trong FDP_ACC.1/Signer Creation, FDP_ACF.1/Signer Creation, FDP_ACC.1/Signer Maintenance và FDP_ACF.1/Signer Maintenance. Việc xác thực danh tính của Người ký và Người dùng có đặc quyền được quản lý chặt chẽ bởi FIA_UID.2, FMT_MSA.1/Signer, FMT_MSA.1/Privileged User, FMT_MSA.2, FMT_MSA.3/Signer và FMT_MSA.3/Privileged User.
- **OT.SYSTEM_PROTECTION (Bảo vệ toàn vẹn hệ thống TOE):** Mục tiêu này được đảm bảo bởi FMT_MTD.1 (quản lý dữ liệu TSF), FMT_SMF.1 (giao diện chức năng quản lý) và FMT_SMR.2 (phân định vai trò an toàn). Các SFR FDP_ACC.1/TOE Maintenance và FDP_ACF.1/TOE Maintenance mô tả các quy tắc kiểm soát truy cập để quản lý dữ liệu cấu hình TSF. Hai cấu phần FPT_PHP.1 và FPT_PHP.3 mô tả các yêu cầu bảo vệ vật lý và logic cho TSF. FTP_TRP.1/SSA quy định rằng chỉ có Người dùng có đặc quyền được ủy quyền mới có quyền can thiệp bảo trì hệ thống TOE.
- **OT.AUDIT_PROTECTION (Bảo vệ nhật ký kiểm toán):** Mục tiêu này được xử lý bằng các yêu cầu tạo bản ghi nhật ký kiểm toán trong FAU_GEN.1 và FAU_GEN.2, kết hợp với việc sử dụng nguồn nhãn thời gian tin cậy (reliable timestamps) quy định tại FPT_STM.1.
- **OT.SAD_VERIFICATION (Xác minh Dữ liệu kích hoạt chữ ký số):** Mục tiêu này được xử lý bởi các cấu phần FIA_AFL.1, FIA_UAU.1 và FIA_UAU.5/Signer. Các cấu phần FDP_ACC.1/Signing và FDP_ACF.1/Signing mô tả các quy tắc kiểm soát truy cập đối với thao tác tạo chữ ký số cũng như quy trình xác minh Giao thức kích hoạt chữ ký (SAP).
- **OT.SAP (Bảo vệ giao thức kích hoạt chữ ký):** Mục tiêu này được bao quát bởi các yêu cầu an toàn của FTP_TRP.1/SIC (đường truyền tin cậy) và FPT_RPL.1 (chống tấn công phát lại) áp dụng cho giao thức kết nối giữa Cấu phần giao tiếp người ký (SIC) và TSF.
- **OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION (Bảo vệ dữ liệu xác thực chữ ký):** Mục tiêu này được bao quát bởi FTP_TRP.1/SIC, quy định yêu cầu bảo vệ tính toàn vẹn tuyệt đối cho mọi dữ liệu được truyền tải từ phía người dùng đến hệ thống TOE.
- **OT.DTBSR_INTEGRITY (Bảo vệ tính toàn vẹn của giá trị băm tài liệu cần ký):** Mục tiêu này được bao quát bởi FTP_TRP.1/SSA và FTP_TRP.1/SIC, đòi hỏi toàn bộ quá trình truyền nhận dữ liệu băm của tài liệu phải được bảo vệ tính toàn vẹn, chống sửa đổi trái phép.
- **OT.SIGNATURE_INTEGRITY (Bảo vệ tính toàn vẹn của chữ ký số đầu ra):** Mục tiêu này được xử lý bởi FCS_COP.1, quy định các yêu cầu kỹ thuật đối với các thuật toán mật mã an toàn. Cấu phần FTP_ITC.1/CM có thể được sử dụng để truyền tải dữ liệu một cách an toàn và bí mật giữa phần mềm TOE và Mô-đun mật mã phần cứng (HSM). Quyền kiểm soát truy cập đối với bản thân thao tác ký số được đảm bảo bởi FDP_ACC.1/Signing và FDP_ACF.1/Signing.
- **OT.CRYPTO (Vận hành mật mã an toàn):** Mục tiêu này được bao quát bởi FCS_CKM.1 (sinh khóa) và FCS_COP.1 (vận hành mật mã), đặc tả chi tiết các yêu cầu đối với quy trình tạo khóa và các giải thuật mã hóa áp dụng.
- **OT.RANDOM (Khởi tạo số ngẫu nhiên chất lượng cao):** Mục tiêu này được đảm bảo hoàn toàn bởi FCS_RNG.1, quy định các tiêu chuẩn kỹ thuật nghiêm ngặt đối với bộ sinh số ngẫu nhiên.

10.2 Sự phụ thuộc giữa các SFR (SFR Dependencies)

10.2.1 Tổng quan

Sự phụ thuộc và các mối quan hệ ràng buộc logic chéo giữa các yêu cầu chức năng an toàn (SFR) được giải quyết đầy đủ như trình bày cụ thể trong **Bảng 14** *(Chú thích: Trong tài liệu gốc, Bảng 14 là ma*

trận liệt kê chi tiết các điều kiện phụ thuộc của từng mã hiệu SFR theo đúng quy chuẩn Common Criteria Phần 2).

10.3 Cơ sở lý luận về các Yêu cầu Đảm bảo An toàn (Rationales for SARs)

Cấp độ đảm bảo an toàn **EAL4+** cho phép nhà phát triển đạt được mức độ tin tưởng tối đa từ quy trình thiết kế kỹ thuật an toàn chủ động, dựa trên các thực hành phát triển thương mại tốt (good commercial development practices). Các thực hành này mặc dù rất nghiêm ngặt, chặt chẽ nhưng không đòi hỏi nhà phát triển phải sở hữu những kiến thức chuyên môn quá sâu biệt lệ, kỹ năng toán học chính thức (formal methods) hay các nguồn lực đặc biệt khác. EAL4+ là cấp độ đánh giá cao nhất mà một doanh nghiệp có khả năng khả thi về mặt kinh tế để áp dụng nâng cấp, áp dụng bổ sung (retro-fit) cho một dòng sản phẩm sẵn có của mình.

Do hệ thống TOE chịu trách nhiệm quản lý trực tiếp dữ liệu tạo chữ ký số (khóa bí mật), sinh khóa và cấp quyền sử dụng khóa, nên nó phải tự quản lý các thuộc tính bảo mật mà không thể phó thác cho cấu phần nào khác ngoài TOE. Mặc dù hệ thống TOE được giả định là luôn vận hành trong một môi trường được bảo vệ nghiêm ngặt về mặt vật lý (trung tâm dữ liệu phòng Server đạt chuẩn), hệ thống này trên thực tế vẫn phải đối mặt với nguy cơ từ các cuộc tấn công logic từ xa (remote logical attacks) thông qua mạng Internet. Do đó, hệ thống lõi SAM bắt buộc phải được đánh giá kiểm định năng lực nhằm đối phó với những cuộc tấn công có **Tiềm lực tấn công mức độ Cao (High attack potential)**.

Vì lý do đó, cấp độ đánh giá **EAL4+** đã được gia cường (augmented) thêm thành phần **AVA_VAN.5** (Đánh giá lỗ hổng hệ thống: Mức độ cao).
