QUY CHẾ CHỨNG THỰC HỆ THỐNG CẤP PHÁT DẤU THỜI GIAN

*****

TimeStamp Practices Statement (CPS)

MỤC LỤC

I. KHÁI QUÁT CHUNG

I.1.Giới thiệu

FPT TSA là một cơ sở hạ tầng cấp phát dấu thời gian trực thuộc Tổ chức cung cấp dịch vụ chứng thư chữ ký số quốc gia (ROOTCA) của Bộ thông tin và Truyền thông nước Cộng Hòa Xã hội Chủ Nghĩa Việt Nam. Việc lựa chọn xây dựng hệ thống dấu thời gian có sự chứng nhận của ROOT CA giúp FPT có đủ thẩm quyền cấp dấu thời gian cho các cơ quan nhà nước, tổ chức, doanh nghiệp, cá nhân có yêu cầu xin cấp và sử dụng dấu thời gian của FPT TSA. FPT TSA là tên gọi của dịch vụ cấp dấu thời gian do công ty FPT cung cấp.

Hệ thống cấp dấu thời gian FPT TSA (FPT TSA) là hệ thống dấu thời gian tuân thủ đầy đủ các tiêu chuẩn của thông tư 06/2015/TT-BTTTT do Bộ TT & TT ban hành.

Các quy định về quy chế chứng thực (CPS) của dịch vụ FPT TSA được trình bày trong tài liệu này, gồm có: phát hành, quản lý, thu hồi dịch vụ cấp phát dấu thời gian.

Bản CPS này là một chính sách quan trọng trong quá trình cung cấp dịch vụ cung cấp dấu thời gian. CPS cung cấp nội dung các yêu cầu về kinh doanh, luật pháp, kỹ thuật cho quá trình chấp nhận, cấp phát, quản lý, thu hồi dịch vụ cho hệ thống dấu thời gian. Các yêu cầu của CPS được gọi là các "*chuẩn FPT TSA*", có nhiệm vụ cung cấp tính bảo mật và toàn vẹn cho dịch vụ FPT TSA, được áp dụng cho tất cả các thành phần tham gia dịch vụ dấu thời gian FPT TSA. Các thành phần tham gia dịch vụ FPT TSA phải tuân thủ các yêu cầu được đề ra trong CPS này.

FPT TSA là một hệ thống thực thuộc RootCA của Bộ Thông tin Truyền Thông nước Cộng Hòa Xã hội Chủ Nghĩa Việt Nam do vậy bản CPS này sẽ phải chịu sự quản lý của luật pháp Việt Nam cũng như tuân theo các chính sách, quy chế, văn bản và thủ tục ban hành bởi RootCA Việt Nam và các đơn vị chức năng có liên quan khác.

Bản CPS của dịch vụ FPT TSA được xây dựng tuân theo khuyến nghị RFC 3161 (Internet X.509 Public Key Infrastructure Time-Stamp Protocol).

Với thế mạnh về hạ tầng công nghệ thông tin của mình, đề án xây dựng hệ thống chứng thực chữ ký số của công ty TNHH Hệ thống Thông tin FPT sẽ hướng tới mục tiêu sau:

- Xây dựng dịch vụ dấu thời gian tin cậy trên toàn lãnh thổ Việt Nam
- Các dịch vụ thương mại điện tử, giao dịch trực tuyến cũng như chính phủ điện tử.

I.2.Các loại dấu thời gian của dịch vụ FPT TSA

Mô hình ứng dụng PKI của hệ thống FPT TSA sẽ đóng vai trò:

- Giải pháp giúp doanh nghiệp thực hiện các giao dịch điện tử với đối tác, mà không phải đầu tư một mạng riêng, một cổng giao dịch web, hoặc các dịch vụ riêng mới. Giải pháp cung cấp các kênh an toàn giữa các đối tác trên mạng công cộng. Giải pháp có khả năng hỗ trợ đa ứng dụng, ứng dụng Internet, web hoặc phi web, Unix hay Windows.
- Giải pháp cho phép các đối tác khai thác nguồn sức mạnh của Internet để tự truy cập và phục vụ các dịch vụ như CRM (Customer Relationship Management) hay B2B (Business to Business). Tất cả sẽ được thực hiện đơn giản với mức xác thực và bảo mật cao tới tận hai đầu.
- Giải pháp kết hợp các khả năng an toàn và bảo mật tiên tiến của PKI, quản lý chứng thực, một cổng an ninh web với khả năng nhận thực, xác thực, bảo mật, quản lý và kiểm soát an toàn cho các ứng dụng web.
- Giải pháp cho các ứng dụng trực tuyến. Các ứng dụng dữ liệu thông tin nhậy cảm, có giá trị cao với chữ ký điện tử cho xác thực và thừa nhận.

Hệ thống cung cấp dịch vụ chứng thực chữ ký số FPT TSA cung cấp các sản phẩm sau:

1. Dịch vụ dấu thời gian dành cho khách hàng cá nhân.
2. Dịch vụ dấu thời gian cho khách hàng doanh nghiệp, tổ chức.

I.3.Quy trình hoạt động FPT TSA

I.3.1. Thuật ngữ và viết tắt

CA Certification Authority

IT Information Technology

OID Object Identifier

TSA Time Stamping Authority

TSP Trust Service Provider

TSPS Timestamping Policy and Practice Statement

TST Times tamp Token

TSU Timestamping Unit

UTC Coordinated Universal Time

I.3.2. Định nghĩa.

1.1.1.1. Coordinated Universal Time (UTC)

UTC là viết tắt của từ tiếng Anh "Coordinated Universal Time" và một từ tiếng Pháp "Temps Universel Coordonné".

Giờ UTC có nghĩa là thời gian phối hợp quốc tế, được cơ quan Đo lường Quốc tế (BIPM) chọn làm cơ sở pháp lý để định vị thời gian.

UTC ra đời dựa theo tiêu chuẩn múi giờ cũ là giờ GMT - giờ quốc tế.

2.1.1.1. Network Time Protocol (NTP)

Network Time Protocol (NTP) là một thuật toán phần mềm giữ cho các máy tính và các thiết bị công nghệ khác nhau có thể đồng bộ hóa thời gian với nhau. NTP đã đạt được thành công trong việc giữ các thiết bị đồng bộ hóa hiệu quả trong chỉ trong vài milliseconds (1/1000s), nhưng để có thể làm được điều này nó cần phải có một hệ thống thời gian đáng tin cậy để sử dụng làm điểm thời gian chính cho việc đồng bộ.

3.1.1.1. Relying party

Các đối tượng sử dụng trong hệ thống FPT CA là tất cả các tổ chức hay cá nhân sử dụng hệ thống FPT TSA để sử dụng dấu thời gian. Những đối tượng này dựa trên các chức năng của hệ thống FPT TSA để nhận được dấu thời gian để phục vụ vi của mình và xác thực các đối tượng khác trong quá trình trao đổi thông tin.

4.1.1.1. Time Stamping Authority (TSA)

Đó là TSP cung cấp dịch vụ ghi dấu dấu thời gian bằng cách sử dụng một hoặc nhiều đơn vị dấu thời gian.

5.1.1.1. Registration Authority – RA

RA là một đối tượng được CA tin cậy uỷ quyền có trách nhiệm đăng ký và đảm bảo tính đúng đắn nội dung thông tin trong dấu thời gian của những thuê bao sử dụng hệ thống dấu thời gian. RA sẽ thu thập thông tin trên và cung cấp cho CA trực thuộc. RA bao gồm một tập hợp phần cứng máy tính, phần mềm, và những người vận hành trực tiếp thuộc trung tâm FPT-CA. Mỗi RA sẽ thường xuyên vận

hành bởi một người, và mỗi CA sẽ quản lý một nhóm RA tin cậy. Do đó điều kiện hoạt động của RA do CA cấp phép và quy định.

Các nhiệm vụ của RA bao gồm:

- Xác thực nhận dạng đối tượng.
- Xác nhận liên kết giữa thông tin truy cập và đặc điểm nhận dạng của đối tượng yêu cầu gồm phương thức chứng minh sở hữu phù hợp

I.3.3. Quy trình hoạt động

Để đảm bảo hoạt động của hệ thống FPT TSA sẽ sử dụng các chức năng của hệ thống như sau:

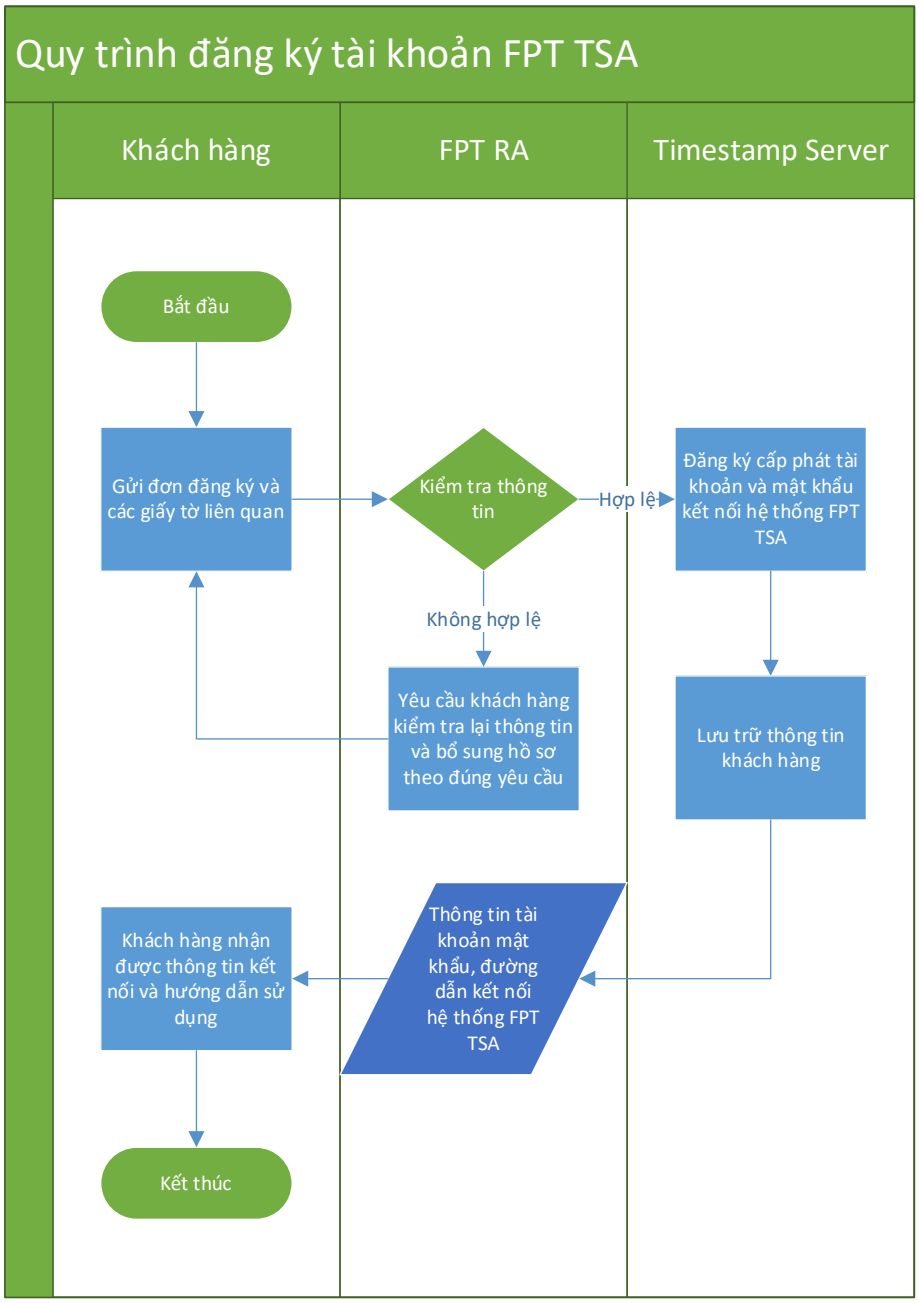
- Đăng ký tài khoản sử dụng dịch vụ dấu thời gian.
- Hủy tài khoản sử dụng dịch vụ dấu thời gian.
- Gán dấu thời gian cho tài liệu

I.3.3.1. Đăng ký tài khoản sử dụng dịch vụ dấu thời gian

Khi người dùng có nhu cầu sử dụng dịch vụ dấu thời gian, người dùng này cần tạo một yêu cầu xin cấp tài khoản dịch vụ dấu thời gian cho bộ phận quản lý đăng ký (FPT-RA). Người dùng cung cấp thông tin và hồ sơ thuê bao gửi tới FPT-RA thông qua phương thức bản giấy hoặc bản điện tử. RA sẽ chịu trách nhiệm kiểm tra tính hợp lệ của yêu cầu này. Nếu yêu cầu không hợp lệ RA sẽ trả lại yêu cầu cho người dùng đó và từ chối cấp tài khoản. Trong trường hợp yêu cầu hợp lệ RA tiếp tục chuyển yêu cầu tới FPT TSA.

Yêu cầu này sẽ được gửi tới RA qua một kênh truyền an toàn. Thông thường quá trình đăng ký này là gặp mặt trực tiếp (face-to-face) và xuất trình các tài liệu chứng minh định danh của thuê bao như chứng minh thư, hộ chiếu… Trong trường hợp không thể gặp mặt trực tiếp thì các thông tin và hồ sơ thuê bao được người dùng cung cấp thông qua phương thức điện tử gửi tới RA thông qua môi trường web được mã hóa theo giao thức SSL 128 bit.

Quy trình đăng ký cấp tài khoản dịch vụ dấu thời gian theo phương thức điện tử bao gồm:



- KHỞI TẠO YÊU CẦU

Người dùng khởi tạo yêu cầu đề nghị cấp tài khoản dịch vụ dấu thời gian thông qua phương thức điện tử.

- THU THẬP THÔNG TIN ĐĂNG KÝ CỦA THUÊ BAO VÀ HỒ SƠ THUÊ BAO

Người dùng cung cấp thông tin và hồ sơ thuê bao gửi tới FPT-RA thông qua phương thức điện tử.

- XÁC MINH CÁC THÔNG TIN ĐĂNG KÝ CỦA THUÊ BAO VÀ HỒ SƠ THUÊ BAO

FPT-RA tiếp nhận và xác minh thông tin và hồ sơ thuê bao của người dùng cung cấp.

- KHỞI TẠO TÀI KHOẢN

Sau khi nhận được yêu cầu xin cấp tài khoản dấu thời gian từ phía RA, FPT TSA tiến hành tạo tài khoản và mật khẩu dựa trên các thông tin có trong yêu cầu này. Dựa theo yêu cầu trong đơn đăng ký để đảm bảo lưu lượng sử dụng của tài khoản dấu thời gian.

- THÔNG BÁO KẾT QUẢ VÀ LƯU TRỮ THÔNG TIN ĐĂNG KÝ

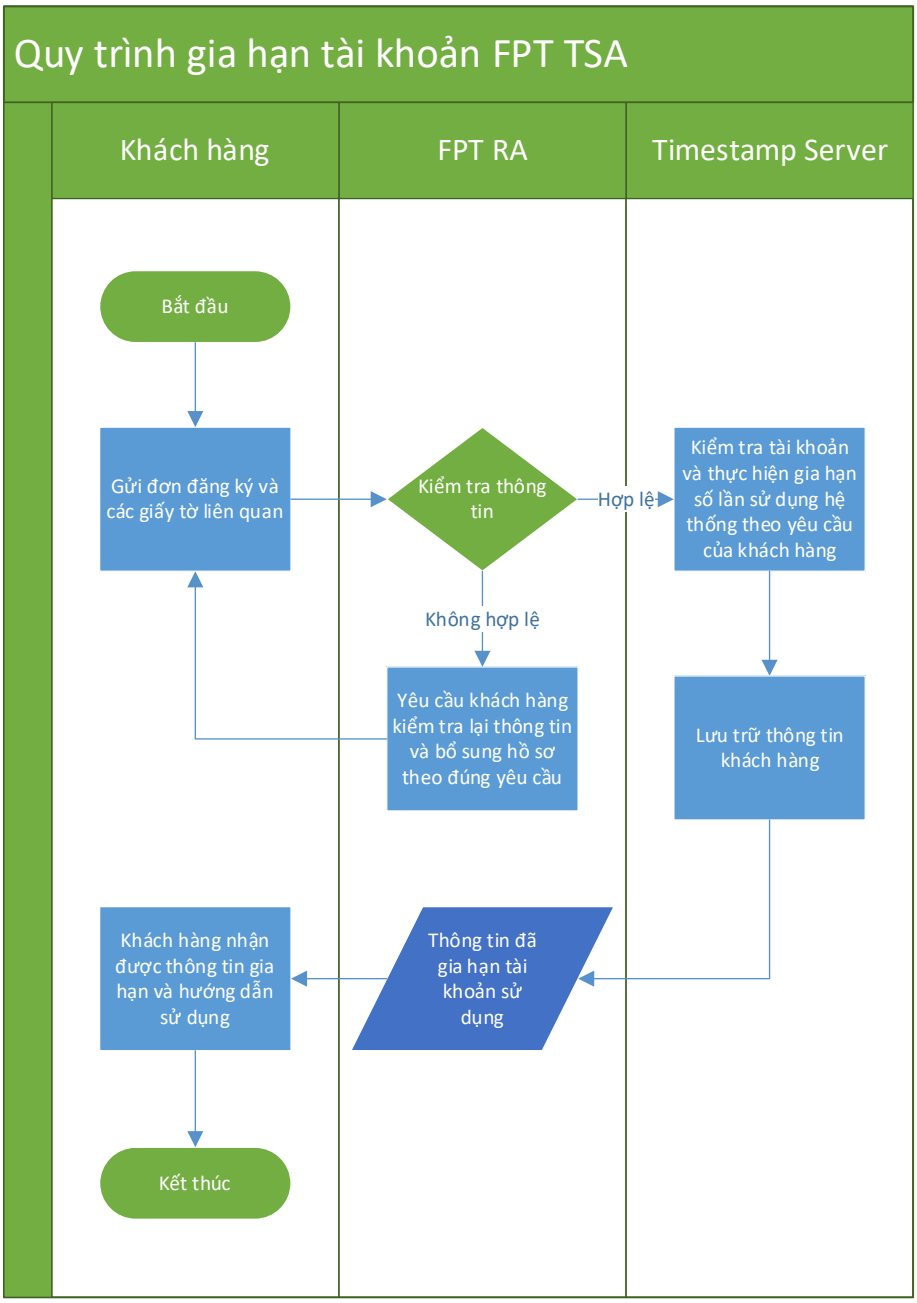
Sau khi đã đối chiếu thông tin với người đề nghị, FPT-RA trả kết quả (từ chối cấp hoặc cấp tài khoản) cho người đề nghị theo quy định của pháp luật.

FPT-CA là đơn vị chịu trách nhiệm về kết quả của việc xác minh tính chính xác của hồ sơ thuê bao.

I.3.3.2. Gia hạn tài khoản sử dụng dịch vụ dấu thời gian

Khi người dùng có nhu cầu gia hạn số lượt sử dụng dịch vụ dấu thời gian, người dùng này cần tạo một yêu cầu xin gia hạn tài khoản dịch vụ dấu thời gian cho bộ phận quản lý đăng ký (FPT-RA). Người dùng cung cấp thông tin và hồ sơ thuê bao gửi tới FPT-RA thông qua phương thức bản giấy hoặc bản điện tử. RA sẽ chịu trách nhiệm kiểm tra tính hợp lệ của yêu cầu này. Nếu yêu cầu không hợp lệ RA sẽ trả lại yêu cầu cho người dùng đó và từ chối gia hạn tài khoản. Trong trường hợp yêu cầu hợp lệ RA tiếp tục chuyển yêu cầu tới FPT TSA.

Quy trình gia hạn tài khoản dịch vụ dấu thời gian theo phương thức điện tử bao gồm:



- KHỞI TẠO YÊU CẦU

Người dùng khởi tạo yêu cầu đề nghị gia hạn tài khoản dịch vụ dấu thời gian thông qua phương thức điện tử.

- THU THẬP THÔNG TIN ĐĂNG KÝ CỦA THUÊ BAO VÀ HỒ SƠ THUÊ BAO

Người dùng cung cấp thông tin và hồ sơ thuê bao gửi tới FPT-RA thông qua phương thức điện tử.

- XÁC MINH CÁC THÔNG TIN ĐĂNG KÝ CỦA THUÊ BAO VÀ HỒ SƠ THUÊ BAO

FPT-RA tiếp nhận và xác minh thông tin và hồ sơ thuê bao của người dùng cung cấp.

- GIA HẠN TÀI KHOẢN

Sau khi nhận được yêu cầu xin cấp tài khoản dấu thời gian từ phía RA, FPT TSA tiến hành gia hạn số lần sử dụng tài khoản dựa trên các thông tin có trong yêu cầu này. Dựa theo yêu cầu trong đơn đăng ký để đảm bảo thông tin tài khoản là chính xác và không có thay đổi trong quá trình sử dụng của người dùng sau này.

- THÔNG BÁO KẾT QUẢ VÀ LƯU TRỮ THÔNG TIN GIA HẠN

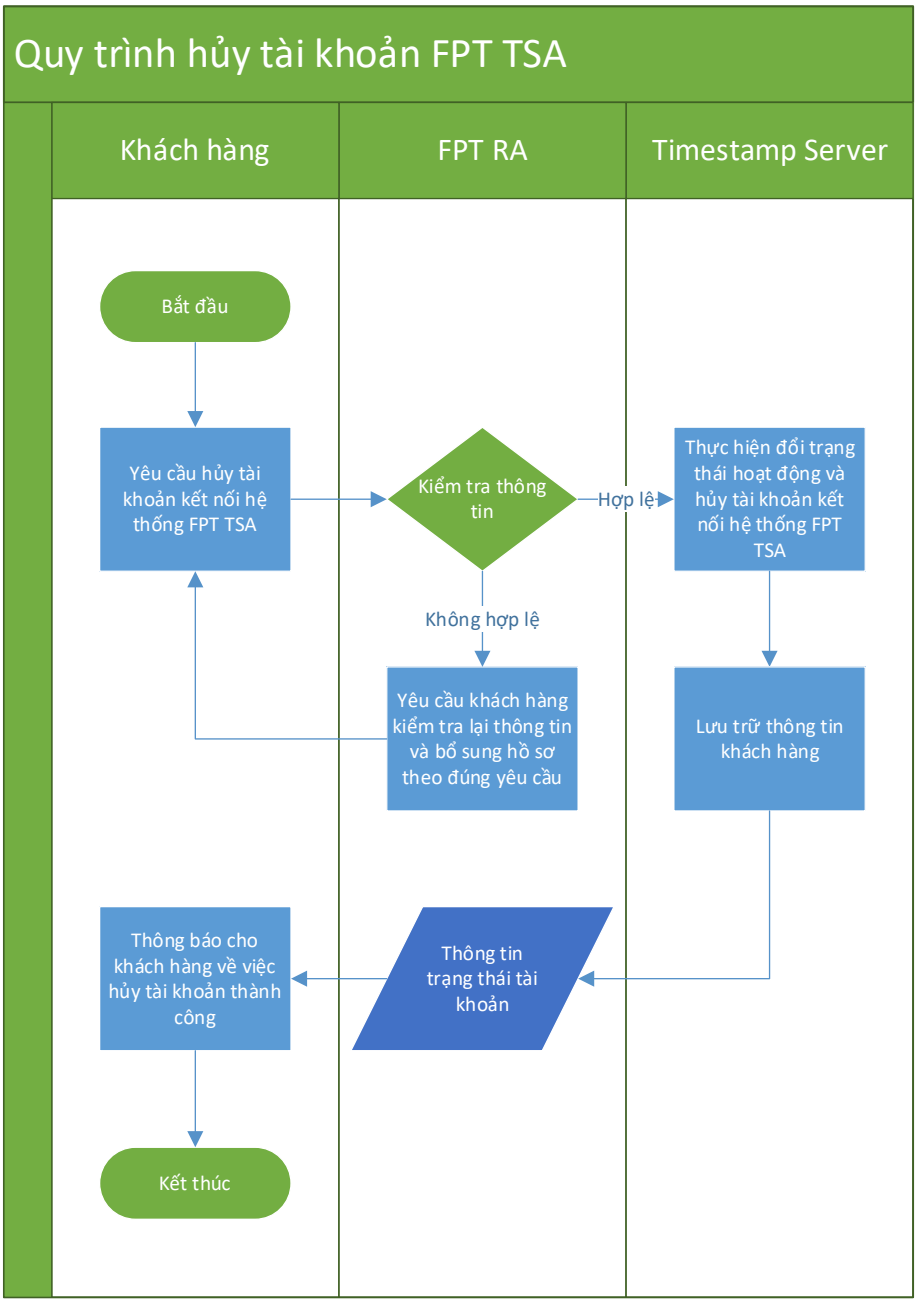
Sau khi đã đối chiếu thông tin với người đề nghị, FPT-RA trả kết quả (từ chối cấp hoặc gia hạn tài khoản) cho người đề nghị theo quy định của pháp luật.

FPT-CA là đơn vị chịu trách nhiệm về kết quả của việc xác minh tính chính xác của hồ sơ thuê bao.

I.3.3.3. Thu hồi tài khoản

Khi người dùng có nhu cầu ngưng sử dụng dịch vụ dấu thời gian, người dùng này cần tạo một yêu cầu xin hủy tài khoản dịch vụ dấu thời gian cho bộ phận quản lý đăng ký (FPT-RA). Người dùng cung cấp thông tin và hồ sơ thuê bao gửi tới FPT-RA thông qua phương thức bản giấy hoặc bản điện tử. RA sẽ chịu trách nhiệm kiểm tra tính hợp lệ của yêu cầu này. Nếu yêu cầu không hợp lệ RA sẽ trả lại yêu cầu cho người dùng đó và từ chối hủy tài khoản. Trong trường hợp yêu cầu hợp lệ RA tiếp tục chuyển yêu cầu tới FPT TSA.

Yêu cầu này sẽ được gửi tới RA qua một kênh truyền an toàn. Thông thường quá trình đăng ký này là gặp mặt trực tiếp (face-to-face) và xuất trình các tài liệu chứng minh định danh của thuê bao như chứng minh thư, hộ chiếu… Trong trường hợp không thể gặp mặt trực tiếp thì các thông tin và hồ sơ thuê bao được người dùng cung cấp thông qua phương thức điện tử gửi tới RA thông qua môi trường web được mã hóa theo giao thức SSL 128 bit.



Quy trình hủy tài khoản dịch vụ dấu thời gian theo phương thức điện tử bao gồm:

- KHỞI TẠO YÊU CẦU HỦY

Người dùng khởi tạo yêu cầu đề nghị hủy tài khoản dịch vụ dấu thời gian thông qua phương thức điện tử.

- THU THẬP THÔNG TIN CỦA THUÊ BAO VÀ HỒ SƠ THUÊ BAO

Người dùng cung cấp thông tin và hồ sơ thuê bao gửi tới FPT-RA thông qua phương thức điện tử.

- XÁC MINH CÁC THÔNG TIN CỦA THUÊ BAO VÀ HỒ SƠ THUÊ BAO

FPT-RA tiếp nhận và xác minh thông tin và hồ sơ thuê bao của người dùng cung cấp.

- HỦY TÀI KHOẢN

Sau khi nhận được yêu cầu xin hủy tài khoản dấu thời gian từ phía RA, FPT TSA tiến hành tạo đổi trạng thái hoạt động của tài khoản khách hàng trên hệ thống FPT TSA từ hoạt động sang ngưng hoạt động trong trường hợp tạm ngừng, nếu khách hàng của yêu cầu hủy bỏ tài khoản thì hệ thống FPT TSA sẽ xóa thông tin tài khoản trên hệ thống.

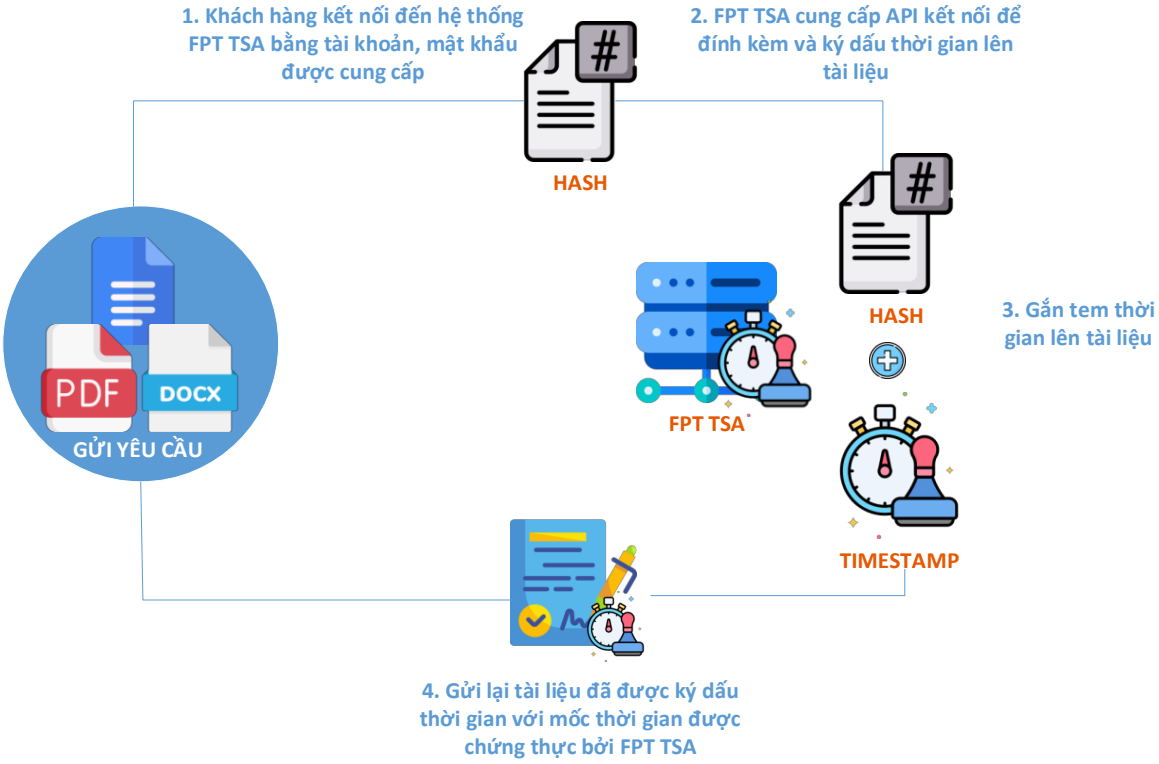
- THÔNG BÁO KẾT QUẢ VÀ LƯU TRỮ THÔNG TIN ĐĂNG KÝ

Sau khi hoàn tất quá trình hủy/tạm ngưng tài khoản, FPT-RA trả kết quả cho người đề nghị theo quy định của pháp luật.

I.3.3.4. Gán dấu thời gian lên tài liệu

Quy trình gắn dấu thời gian dựa trên chữ ký điện tử và các hàm băm. Đầu tiên, Dữ liệu trước khi được vào được thông qua hàm băm để tạo ra dữ liệu băm. Hàm băm là một loại dấu vân tay kỹ thuật số của dữ liệu gốc: một chuỗi các bit không thể trùng lặp với bất kỳ tập hợp dữ liệu nào khác. Nếu dữ liệu ban đầu bị thay đổi thì điều này sẽ dẫn đến một dữ liệu băm hoàn toàn khác. Dữ liệu băm này được gửi đến TSA. TSA nối một dấu thời gian với hàm băm và tính toán hàm băm của quá trình ghép nối này. Hàm băm này lần lượt được ký số bằng khóa riêng của hệ thống TSA. Hàm băm đã ký cùng với dấu thời gian này được gửi lại cho người yêu cầu dấu thời gian để lưu trữ chúng cùng với dữ liệu ban đầu (xem sơ đồ).

Vì dữ liệu gốc không thể được tính toán từ hàm băm (vì hàm băm là một hàm một chiều), TSA không bao giờ xem được dữ liệu gốc, điều này cho phép sử dụng phương pháp này cho dữ liệu bí mật, đảm bảo TCVN 7818-3:2010 về hàm băm



I.4.Chính sách quản trị

I.4.1. Tổ chức quản lý văn bản

Công ty hệ thống thông tin FPT trực thuộc tập đoàn FPT chịu trách nhiệm tổ chức quản lý văn bản quy chế chứng thực này.

I.4.2. Liên hệ

Mọi thông tin liên hệ, phản hồi về bản quy chế chứng thực có thể liên hệ với công ty hệ thống thông tin FPT, tầng 22, tòa nhà Keangnam Landmark 72, Lô E6, Phạm Hùng, Mễ Trì, Nam Từ Liêm, Hà Nội.

Các thông tin cập nhật, bổ sung bản quy chế chứng thực sẽ được thông báo qua trang web: http://www.dichvudientu.fpt.com.vn.

I.4.3. Tổ chức xác định CPS phù hợp với chính sách

Bộ Thông Tin và Truyền Thông và Công ty FPT xác định sự phù hợp và tính khả dụng CPS này.

I.4.4. Thủ tục phê chuẩn CPS

FPT sẽ phê chuẩn CPS và những thay đổi kế tiếp. Các thay đổi được ghi trong một tài liệu chứa các sửa đổi mẫu (dạng) của CPS hay các thông về quá trình cập nhật.

II.CÔNG BỐ VÀ LƯU TRỮ

II.1. Công bố thông tin

Các thông tin cần được công bố bao gồm:

- CPS trên toàn hệ thống

FPT sẽ liên tục phát hành phiên bản cập nhật của:

- Quy chế chứng thực (CPS) của dịch vụ FPT TSA.
- Các thỏa thuận với khách hàng.
- Các thỏa thuận với các relying party.

II.2. Lưu trữ

Chứng thư số sử dụng cho hệ thống FPT TSA được cấp bởi Bộ Truyền thông thông tin cho toàn hệ thống. Sau khi được cấp phép, chứng thư số sẽ được công bố công khai trên trang chủ rootca.gov.vn

Ngoài ra, thông tin về tài khoản và mật khẩu của người dùng được lưu trữ dưới dạng mã hóa trên các máy chủ Directory theo chuẩn LDAP X509 v3.

Hệ thống FPT TSA lưu trữ đầy đủ dữ liệu log gồm: logs máy chủ ứng dụng chạy hệ thống FPT TSA, logs máy chủ chạy hệ điều hành, logs cơ sở dữ liệu, logs HSM. Các logs này được lưu trữ trên máy chủ và thiết bị được backup thường xuyên sang thiết bị khác. Đảm bảo khi có sự cố xảy ra sẽ lấy được dữ liệu log của từng ứng dụng để xử lý.

- Logs máy chủ ứng dụng chạy hệ thống FPT TSA lưu tại thư mục riêng. Đây là logs toàn bộ hoạt động liên quan tới vận hành hệ thống FPT TSA ghi rõ chi tiết thông tin thời gian (ngày, giờ, phút giây) có hoạt động. Ví dụ như hoạt động đăng nhập, tạo thông tin khách hàng, sửa thông tin khách hàng, tạo tài khoản mật khẩu khách hàng cũng như các lỗi hệ thống nếu có. Khi cần truy xuất thông tin để kiểm tra, bảo trì hay khắc phụ sự cố liên quan tới vận hành quản trị chỉ cần truy cập thư mục và mở thông tin logs này lên để kiểm tra. Dữ liệu logs này được đồng bộ tức thời sang hệ thống dự phòng với địa chỉ và lưu trữ trong các thư mục tương tự.
- Logs máy chủ chạy hệ điều hành được lưu và truy xuất trực tiếp. Thường thì hệ thống máy chủ của FPT TSA được cài đặt license bản quyền, cài đặt hệ thống theo dõi hoạt động, ngăn ngừa nguy cơ tấn công, truy cập từ mọi

phía. Quản trị cũng có thể truy xuất dữ liệu trực tiếp trên các hệ thống này để kiểm tra hoạt động của Windows.

- Logs cơ sở dữ liệu: FPT TSA sử dụng hệ quản trị cơ sở dữ liệu mạnh mẽ nhất. Đây là logs toàn bộ hoạt động liên quan tới dữ liệu hệ thống FPT TSA như việc lớn lên của dữ liệu, đăng nhập, thêm người dùng. Khi cần truy xuất thông tin để kiểm tra, bảo trì hay khắc phụ sự cố liên quan tới vận hành quản trị chỉ cần truy cập thư mục và mở thông tin logs này lên để kiểm tra. Dữ liệu logs này được đồng bộ tức thời sang hệ thống dự phòng với địa chỉ và lưu trữ trong các thư mục tương tự.
- Logs HSM: Do là thiết bị đặc thù nên HSM sử dụng phần mềm riêng để lấy danh sách nhật ký. Đây là phần mềm chạy trên máy chủ ứng dụng để kết nối tới HSM để lấy logs.

Phần mềm có thể chạy trên các nền tảng:

- SUN Solaris 8, 10 (on the SUN/SPARC architecture) with Java 1.4
- SuSE Linux 10.0 with Java 1.4 and 1.5
- SuSE Linux 8.0 with Java 1.4
- Red Hat Linux 9.0 with Java 1.4
- Microsoft Windows

II.3. Quyền truy cập kho lưu trữ chứng thư

- Đối với thuê bao, FPT không giới hạn truy cập tới CPS. FPT yêu cầu người truy nhập phải tuân theo các thỏa thuận với đối tác tin cậy hoặc thỏa thuận sử dụng. Thỏa thuận này như điều kiện để truy cập. FPT triển khai các kiểm soát nhằm ngăn chặn việc truy cập bất hợp pháp vào kho lưu trữ nhằm thêm, xóa hay sửa đổi các mục trong kho lưu trữ.

III. NHẬN DẠNG VÀ XÁC THỰC

III.1. Đặt tên

Tên xuất hiện trong chứng thư số sử dụng cho hệ thống FPT TSA được cấp phát phải được Bộ TTTT xác thực.

III.1.1. Kiểu tên

- Tên trong trường Subject name của chứng thư thuê bao cuối được đặt theo chuẩn X.501. Tên của chứng thư thuê bao cuối chứa thành phần tên chung (CN=). Thành phần tên chung có thể là tên miền, địa chỉ thư điện tử của FPT TSA, tên hợp pháp của FPT TSA hoặc tên đại diện hợp pháp của FPT TSA.

III.1.2. Tính duy nhất của tên chứng thư số

Tên chứng thư số của dịch vụ FPT TSA sẽ là duy nhất với một cấp chứng thư xác định trong miền của dịch vụ FPT TSA.

III.2. Xác định danh tính thuê bao

III.2.1. Xác thực danh tính cá nhân

Chứng thực của thông tin cấp phát tài khoản sử dụng dấu thời gian dựa trên sự có mặt của người xin cấp tài khoản sử dụng dấu thời gian trước khi RA hay một nhà chức trách có thể kiểm định được tính hợp pháp. RA kiểm tra nhận dạng của người xin cấp tài khoản sử dụng dịch vụ dấu thời gian dựa trên thủ tục để nhận dạng của chính phủ, như hộ chiếu, hoặc giấy phép lái xe...

Trên thực tế, để đảm bảo tính bảo mật và tránh các trường hợp giả mạo, thuê bao cần xuất trình các giấy tờ sau đây khi xin cấp tài khoản từ FPT TSA:

- Hộ chiếu hoặc chứng minh thư nhân dân.
- Bản sao giấy khai sinh có công chứng nhà nước. Tên của thuê bao trên giấy khai sinh phải trùng với tên ghi trên hộ chiếu hoặc chứng minh thư nhân dân.
- Bản sao hộ khẩu hoặc giấy đăng ký tạm trú có chứng nhận của phường, xã… Trong trường hợp thay đổi địa điểm cư trú, thuê bao cần thông báo lại chỗ ở mới của mình tại cơ quan đăng ký để cập nhật vào cơ sở dữ liệu.

Các thông tin được xác minh như trên đảm bảo xác thực chính xác định danh của thuê bao, địa điểm cư trú để có thể dễ dàng thông báo đến thuê bao trong trường hợp xảy ra sự cố hoặc tranh chấp.

FPT cũng có thể kiểm tra đơn xin cấp tài khoản sử dụng dấu thời gian cho người quản trị của mình, người này phải hoàn toàn được tin cậy trong một tổ chức. Trong trường hợp này, việc chứng thực cho đơn xin cấp tài khoản được nhận dạng qua các mối quan hệ với nhân viên bằng hợp đồng và kiểm tra lai lịch.

III.2.2. Xác thực danh tính tổ chức, doanh nghiệp

Các thông tin của tổ chức, doanh nghiệp được xác minh theo những thủ tục được ghi trong tài liệu của dịch vụ FPT TSA.

Tối thiểu, dịch vụ FPT TSA sẽ xác minh các thông tin sau:

- Xác định sự tồn tại hợp lệ của một tổ chức bằng cách sử dụng ít nhất một dịch vụ hay cơ sở dữ liệu kiểm lỗi của đối tác thứ ba, hoặc tài liệu xác nhận sự tồn tại của tổ chức được cấp bởi cơ quan hợp pháp của chính phủ hay nhà chức trách. Ví dụ giấy phép đăng ký kinh doanh.
- Xác nhận bằng điện thoại, thư tín… các thông tin của tổ chức mà người xin cấp tài khoản sử dụng dấu thời gian đưa ra, rằng tổ chức đó đã phê duyệt đơn xin cấp tài khoản TSA. Khi tài khoản sử dụng cho cá nhân thuộc là một đại diện hợp pháp tổ chức, việc cá nhân là đại diện cho một tổ chức cũng phải được xác nhận.

III.2.3. Các tiêu chí hoạt động

Dịch vụ FPT TSA sẽ hoạt động tuân thủ theo CPS như các chính sách cần thiết khác được bổ sung.

IV. THỦ TỤC, QUY TRÌNH CẤP PHÁT TÀI KHOẢN TSA

IV.1. Thủ tục xin cấp tài khoản

IV.1.1. Các đối tượng có thể xin cấp chứng thư.

Những người sau đây có thể đệ trình đơn xin cấp tài khoản:

- Các thuê bao có nhu cầu sử dụng dấu thời gian cho mục đích bảo mật giao dịch.
- Đại diện của các tổ chức, doanh nghiệp, cá nhân.

IV.1.2. Hồ sơ xin cấp tài khoản dịch vụ dấu thời gian.

Đối với doanh nghiệp

- Đơn xin cấp tài khoản dịch vụ dấu thời gian.
- Sao y bản chính Giấy phép Đăng ký kinh doanh (có xác nhận của Doanh nghiệp)
- Sao y bản chính Giấy đăng ký thuế (có xác nhận của Doanh nghiệp)
- Photo CMND hoặc Hộ chiếu của người đại diện theo pháp lý

Đối với cá nhân

- Đơn xin cấp tài khoản dấu thời gian
- Bảo sao có công chứng CMND hoặc hộ chiếu

FPT TSA sẽ rà soát kỹ các hồ sơ trước khi tiến hành cấp tài khoản cho người dùng. Trong trường hợp phát hiện hồ sơ thiếu mà hết thời hạn bổ sung FPT TSA sẽ thực hiện thu hồi tài khoản theo chỉ đạo của Bộ Thông tin và Truyền thông.

IV.2. Xử lý đơn xin cấp tài khoản

IV.2.1. Chức năng nhận biết và xác thực

Một RA sẽ nhận biết và chứng thực các thông tin khách hàng.

IV.2.2. Phê duyệt hoặc từ chối các đơn xin cấp tài khoản

RA sẽ phê chuẩn đơn xin cấp tài khoản khi tuân theo các tiêu chuẩn sau đây:

- Nhận biết và xác thực các thông tin về khách hàng..
- Phí dịch vụ đã thanh toán.

RA sẽ từ chối đơn xin cấp một chứng thư theo tiêu chí sau đây:

- Nhận biết và xác thực các thông tin về thuê bao không thành công.
- Thuê bao không cung cấp tài liệu hỗ trợ theo yêu cầu.
- Thuê bao không trả lời yêu cầu trong thời gian quy định.
- Phí dịch vụ chưa thanh toán.
- RA có lý do tin rằng việc cung cấp tài khoản cho thuê bao có thể gây bất lợi cho FPT.

IV.2.3. Thời gian xử lý các đơn xin cấp tài khoản

RA có trách nhiệm xử lý các đơn xin cấp tài khoản dấu thời gian trong khoảng thời gian phù hợp. Không quy định thời gian hoàn thành quá trình xử lý một đơn xin cấp tài khoản dấu thời gian trừ khi được đưa ra trong hợp đồng với thuê bao, trong CPS hoặc thoả thuận giữa các bên của dịch vụ FPT TSA. Thông thường, nếu không có vướng mắc, hệ thống cung cấp dịch vụ FPT TSA có thể khởi tạo một tài khoản tối đa trong 05 ngày làm việc.

IV.3. Thông báo

IV.3.1. Hoạt động FPT trong suốt quá trình phát hành tài khoản

FPT duy trì hoạt động của mình liên tục 24/7 trong suốt quá trình cấp phát tài khoản dấu thời gian. Bất cứ sự cố hay việc bảo trì hệ thống đều được thông báo trước đến các thuê bao trong khoảng thời gian hợp lý

IV.3.2. Thông báo của FPT đến thuê bao về việc cấp tài khoản

FPT cấp phát tài khoản trực tiếp tới thuê bao hoặc thông qua RA. FPT thông báo cho thuê bao rằng tài khoản của họ đã được tạo đồng thời cung cấp cho thuê bao quyền truy cập tới đường dẫn và tài khoản mật khẩu sử dụng cho dịch vụ dấu thời gian.

IV.4. Hủy và tạm dừng tài khoản

IV.4.1. Các trường hợp Hủy

Chỉ trong các tình huống được liệt kê dưới đây, tài khoản thuê bao dùng cuối sẽ bị FPT hủy và được thông báo tới thuê bao. Dựa vào yêu cầu không sử dụng của thuê bao với lý do không nằm trong các lý do liệt kê bên dưới. FPT sẽ đánh dấu tài khoản là không hoạt động trong cơ sở dữ liệu.

Một tài khoản sẽ bị hủy nếu:

- Trung tâm xử lý, khách hàng hay thuê bao có lý do để tin hoặc nghi ngờ tài khoản của thuê bao bị lộ.
- Trung tâm xử lý hoặc khách hàng có lý do để tin rằng thuê bao vi phạm nghĩa vụ, trách nhiệm, hoặc hợp đồng thuê bao.
- Mối quan hệ giữa khách hàng doanh nghiệp với thuê bao kết thúc hoặc chấm dứt theo cách nào đó.
- Trung tâm xử lý hoặc khách hàng có lý do để tin rằng chứng thư được ban hành không phù hợp với quy định được yêu cầu bởi CPS.
- Trung tâm xử lý hoặc khách hàng có lý do để tin rằng các tài liệu trong đơn xin cấp tài khoản dấu thời gian là không hợp lệ.
- Trung tâm xử lý hoặc khách hàng xác định được tài liệu đầu tiên để cấp tài khoản không thoả mãn.
- Việc tiếp tục sử dụng dịch vụ dấu thời gian gây hại cho FPT.

Khi xem xét việc sử dụng dịch vụ dấu thời gian có hại cho FPT hay không, các RA xem xét các yếu tố sau:

- Nguồn gốc và số lượng của các khiếu nại nhận được.
- Xác nhận người khiếu nại.
- Cưỡng chế theo luật.
- Trả lời cho sử dụng gây hại của thuê bao.

FPT có thể thu hồi tài khoản quản trị nếu thẩm quyền của người quản trị kết thúc.

Thoả thuận với thuê bao yêu cầu thuê bao thông báo cho FPT ngay lập tức về những thông tin và nghi ngờ về việc lộ tài khoản và mật khẩu.

Thoả thuận yêu cầu thuê bao ngay lập tức thông báo với trung tâm xử lý khi có nghi ngờ về việc lộ tài khoản và mật khẩu.

IV.4.2. Đối tượng có thể yêu cầu Hủy

Những thuê bao cá nhân có thể yêu cầu hủy tài khoản dấu thời gian cá nhân của chính họ. Trong trường hợp tài khoản của tổ chức, một đại diện được uỷ quyền hợp pháp của tổ chức được quyền yêu cầu hủy tài khoản đã ban hành cho tổ chức. Đại diện được uỷ quyền hợp pháp của FPT hoặc RA sẽ được quyền yêu cầu hủy tài khoản.

IV.4.3. Thủ tục yêu cầu hủy tài khoản

Theo trình tự hủy tài khoản, CA xác nhận thuê bao yêu cầu hủy khoản là cá nhân hay tổ chức được chấp nhận đơn xin cấp tài khoản. Trình tự xác nhận yêu cầu hủy của thuê bao bao gồm:

- Thuê bao thông báo nội dung yêu cầu hủy tài khoản liên quan với tài khoản hủy.
- Thông báo cho các thuê bao các lý do chắc chắn về cấp tài khoản mà cá nhân hay tổ chức yêu cầu. Trên thực tế, việc thông tin với các thuê bao phụ thuộc vào nhiều trường hợp khác nhau nhưng có thể là một trong các cách sau: điện thoại, fax, thư điện tử, thư tín hay các dịch vụ đưa tin khác.

Thuê bao gửi yêu cầu hủy tới nhà quản lý FPT hoặc các RA qua các trung tâm của FPT. FPT xác nhận nhận dạng của người quản trị thông qua điều khiển truy cập sử dụng SSL và xác thực khách hàng trước khi cho phép họ thực hiện chức năng hủy.

IV.4.4. Thời gian cho một yêu cầu hủy

Những yêu cầu huỷ bỏ sẽ được đệ trình ngay khi có thể với thời gian hợp lý.

IV.4.5. Những yêu cầu đặc biệt liên quan đến vấn đề bị lộ khoá

Các thành viên của FPT sẽ được thông báo về việc vị lộ khoá bí mật của TSA hoặc nghi ngờ lộ khoá bí mật TSA sử dụng các biện pháp thương mại hợp lý. Trung tâm xử lý sẽ áp dụng các biện pháp thương mại hợp lý để thông báo tới đối tác tin cậy nếu họ phát hiện ra hoặc có lý do để tin rằng khoá bí mật của TSA bị lộ.

IV.5. Dịch vụ kiểm tra trạng thái chứng thư số

IV.5.1. Dịch vụ hỗ trợ

Trạng thái của chứng thư số sử dụng cho hệ thống dấu thời gian luôn được báo cáo sẵn sàng qua CRL, thư mục LDAP và qua phản hồi OCSP.

Dịch vụ cung cấp trạng thái hoạt động của chứng thư luôn sẵn sàng trực 24/7 (24giờ/ngày, 7ngày/tuần).

IV.5.2. Các đặc tính tuỳ chọn

OCSP là đặc tính dịch vụ kiểm tra trạng thái tuỳ chọn, không sẵn có cho mọi sản phẩm và phải được kích hoạt đối với từng dịch vụ.

IV.6. Kết thúc hợp đồng

Một thuê bao có thể kết thúc đăng ký sử dụng dịch vụ dấu thời gian của FPT khi:

- Để số lần sử dụng của tài khoản kết thúc hoặc về 0 mà không làm mới hay gia hạn tài khoản đó .
- Thu hồi tài khoản trước khi tài khoản hết số lần sử dụng mà không thay thế bằng một tài khoản khác.

IV.7. Cam kết

IV.7.1. Cam kết và nghĩa vụ của thuê bao khi đăng ký dịch vụ dấu thời gian

- Phải chắc chắn rằng bất kỳ thông tin nào được trình lên CA (RA) khi cấp, gia hạn hay yêu cầu hủy dịch vụ phải đầy đủ và chính xác
- Bảo vệ tài khoản và mật khẩu và tuân thủ tất các các yêu cầu nhằm tránh bị mất, bị lộ, thay đổi hay bị sử dụng bất hợp phát tài khoản mật khẩu của thuê bao đó.

V. KIỂM SOÁT BẢO MẬT HỆ THỐNG FPT TSA

V.1. Tạo cặp khoá và cài đặt

V.1.1. Tạo cặp khoá

Để khắc phục các nhược điểm về lưu trữ, bảo mật việc tạo khóa của hệ thống FPT TSA được thực hiện theo quy trình như sau:

- Đối với khóa của nhà cung cấp dịch vụ (FPT TSA), các cặp khóa của các thành phần như TSA, RA sẽ được sinh trực tiếp tại các thiết bị HSM chuyên dụng. Việc bảo vệ khóa bí mật của TSA trong các thiết bị phần cứng chuyên dụng sẽ giúp giảm thiểu nguy cơ lộ khóa bí mật (kẻ tấn công có thể sử dụng khóa bí mật của CA để làm giả các dấu thời gian trong toàn bộ hệ thống). Hệ thống FPT TSA hoàn toàn tương thích với những nhà cung cấp HSM hàng đầu thế giới hiện tại như AEP, Luna SA, nCipher, Thales, Utimaco…

V.1.2. Chuyển giao khoá công khai tới tổ chức ban hành chứng thư

FPT RA trình khoá công khai của họ tới FPT cho các chứng thư số thông qua việc sử dụng yêu cầu ký chứng thư PCKS # 10 (CSR) hoặc các gói chứng thư trong một phiên làm việc được đảm bảo bởi SSL.

V.1.3. Chuyển giao khoá công khai của CA tới các đối tác tin cậy

Khóa công khai của hệ thống FPT TSA được công bố rộng rãi trên hệ thống web server và LDAP directory để các đối tác tin cậy kiểm tra tính xác thực của các chứng thư số do Root CA cung cấp.

V.1.4. Kích thước khoá

Các cặp khoá cần có chiều dài thích hợp để ngăn việc lộ khoá bí mật trong thời gian sử dụng cặp khóa. Chuẩn hiện tại của dịch vụ FPT TSA yêu cầu chiều dài tối thiểu của cặp khoá để đảm bảo mức độ mã hoá đủ mạnh là 2048 bits RSA cho PCAs.

V.2. Bảo vệ khoá bí mật và kiểm soát phương thức mã hoá

V.2.1. Kiểm soát và chuẩn hoá mô đun mã hoá

Khóa bí mật nằm trong hệ thống FPT TSA sẽ được bảo vệ bởi hệ thống tin cậy và người nắm giữ khoá bí mật sẽ giữ chức năng phòng ngừa để ngăn chặn sự mất mát, bị tiết lộ, sử đổi và sử dụng bất hợp pháp khoá bí mật phù hợp với CPS này,

nghĩa vụ hợp đồng và yêu cầu được cung cấp nằm trong văn kiện bảo mật riêng của FPT TSA. Khóa bí mật được bảo vệ bằng thẻ thông minh hoặc thẻ cứng khác.

V.2.2. Đa kiểm soát khoá bí mật (m out of n)

Đa kiểm soát được áp dụng để bảo vệ dữ liệu kích hoạt cho khoá bí mật TSA được lưu trữ tại trung tâm xử lý tuân theo các chuẩn trong chính sách bảo mật của FPT. Trung tâm xử lý sử dụng "Secret Sharing" để chìa khoá bí mật hoặc dữ liệu kích hoạt cần thiết thành các phần riêng biệt gọi là "Secret Shares". Các thành phần này được giữ bởi các "Shareholders". Chỉ có m trong tổng số n "Secret Shares" được yêu cầu để vận hành khoá bí mật.

Trung tâm xử lý sử dụng Secret Sharing để bảo vệ dữ liệu kích hoạt và các TSA khác trong các miền con tương ứng tuân theo các chuẩn trong chính sách bảo mật của FPT. Trung tâm xử lý cũng sử dụng Secret Sharing để bảo vệ khoá bí mật tại từng khu vực khôi phục sau thảm hoạ.

Theo đó việc tạo khóa, giữ khóa được thực hiện theo cơ chế m-n. Việc lộ khóa của FPT TSA là hoàn toàn không thể xảy ra, vì FPT TSA sử dụng các cán bộ là những người gắn bó với trung tâm, nếu thiếu một trong số họ khóa cũng có thể khôi phục tuy nhiên cần khôi phục được khóa thì phải cần đầy đủ cơ số người cùng giữ khóa mới có thể khôi phục. Đây là cơ chế giữ khóa bí mật an toàn nhất hiện nay.

V.2.3. Sao lưu dự phòng khoá bí mật của đơn vị cung cấp

CA tạo các văn bản lưu dự phòng khoá bí mật cho mục đích khôi phục sự cố hay khôi phục sau thảm hoạ phù hợp với chuẩn chính trong chính sách bảo mật của FPT. Các bản sao lưu dự phòng phải phù hợp với các chính sách được nêu trong CP và CPS. Các bản sao lưu dự phòng được tạo ra bằng cách sao chép các khoá bí mật và đưa chúng vào các mô đun mã hoá dự phòng.

Khóa bí mật được dự phòng là để được bảo vệ khỏi các sửa đổi bất hợp pháp hoặc bị tiết lộ thông qua phương tiện mã hoá hoặc phương tiện vật lý. Các bản sao lưu dự phòng được bảo vệ vật lý và mã hoá ngang bằng hoặc tốt hơn so với các mô đun mã hoá nằm trong khu vực TSA, như tại khu vực khôi phục sau thảm hoạ hoặc tại khu vực cần bên ngoài khác ví dụ như ngân hàng.

Các khóa bí mật được FPT TSA sao lưu dự phòng gồm: Khóa bí mật của TSA được tạo ra để gửi yêu cầu cấp chứng thư số tới Root CA.

V.2.4. Lưu trữ khoá bí mật của đơn vị cung cấp

Khi một chứng thư của FPT TSA hết hạn, những cặp khóa gắn với chứng thư ấy sẽ đảm bảo được lưu trữ trong khoảng thời gian ít nhất là 5 năm trong các mô đun phần cứng có cơ chế mã hoá đáp ứng được các yêu cầu của CPS. Những cặp khoá TSA này sẽ không được sử dụng trong bất kỳ chữ ký nào sau khi hết hạn sử dụng trừ khi các chứng thư TSA này được khôi phục trong các trường hợp của CPS.

Các khóa bí mật được FPT TSA lưu trữ gồm: Khóa bí mật của CA được tạo ra để gửi yêu cầu cấp chứng thư số tới Root CA.

V.2.5. Cách thức khoá bí mật được chuyển đến hoặc đi từ một mô đun mã hoá

Khóa bí mật chuyển đến mô đun mã hoá sẽ sử dụng các cơ chế để ngăn chặn sự mất, ăn trộm, sửa đổi, tiết lộ và sử dụng trái phép khoá bí mật này.

Trung tâm xử lý cấp phát các khoá bí mật của TSA hoặc RA trên mô đun mã hoá phần cứng và chuyển giao chúng vào trung mô đun mã hoá phần cứng khác để ngăn chặn sự mất mát, ăn trộm, sửa đổi, tiết lộ sử dụng trái phép khoá bí mật. Việc chuyển giao này sẽ bị giới hạn để tạo ra các bản sao dự phòng khoá bí mật trên thẻ cứng phù hợp với tài liệu chuẩn trong chính sách bảo mật của FPT. Các khoá bí mật sẽ được mã hoá trong suốt quá trình truyền.

V.2.6. Cách thức lưu trữ khoá bí mật trên mô đun mã hoá

Các khoá bí mật của hệ thống TSA hoặc RA được lưu trữ trên các mô đun mã hoá dưới dạng mật mã.

V.2.7. Mô đun mã hoá của RA

Các RA sử dụng mô đun mã hoá kết hợp với cơ chế quản lý khoá tự động hoặc dịch vụ quản lý khóa dựa trên mô hình PKI

Chuẩn dịch vụ FPT TSA dành cho việc bảo vệ các khoá bí mật của người quản trị sử dụng mô đun mã hoá yêu cầu:

- Sử dụng mô đun mã hoá cùng với một mật khẩu có cấu trúc sẽ được đề cập để xác thực người quản trị trước khi kích hoạt khoá bí mật
- Cân nhắc một giải pháp hợp lý cho việc bảo vệ về mặt vật lý đối với máy trạm có chứa đầu đọc mô đun mã hoá để ngăn chặn việc sử dụng may trạm và khoá bí mật cùng với mô đun mã hoá trái phép.

V.2.8. Huỷ khóa bí mật

Khi được yêu cầu, các khoá bí mật của TSA sẽ bị huỷ triệt để nhằm đảm bảo rằng các khoá đó sẽ không được khôi phục trong bất kỳ trường hợp nào. Nhân viên *trung tâm xử lý* sẽ giảm bớt nhiệm vụ trên khoá bí mật của TSA bởi hoạt động xoá có sử dụng chức năng của thẻ chứa khoá bí mật của CA đó để ngăn chặn nó được khôi phục sau khi bị xoá trong khi không có ảnh hưởng bất lợi nào tới các khoá bí mật khác được chứa trong thẻ. Quá trình này tuân theo tài liệu chuẩn trong chính sách bảo mật riêng của FPT

V.2.9. Xử lý khi lộ khóa bí mật

Lộ khóa bí mật của FPT TSA

Khóa bí mật của FPT TSA được lưu trữ trong thiết bị phần cứng HSM đạt tiêu chuẩn FIPS 140-2 level 3 của chính phủ Mỹ, đây là thiết bị tạo khóa, mã hóa và lưu trữ khóa bí mật đạt tiêu chuẩn bảo mật cao nhất hiện nay, được dùng cho các hệ thống chuyên dùng, hệ thống quân đội. Ngoài ra, thiết bị này được đặt trong hệ thống Data Center đạt chuẩn Tier-3 tuân thủ nghiêm ngặt an ninh, phòng cháy chữa cháy. Thiết bị chỉ kết nối với máy chủ TSA qua mạng LAN. Do đó không thể có sự tấn công từ bên ngoài, với các truy cập từ DC phải có quyền. Do đó, tuyệt đối không có sự lộ khóa bí mật của FPT TSA

V.3. Kiểm soát bảo mật máy tính

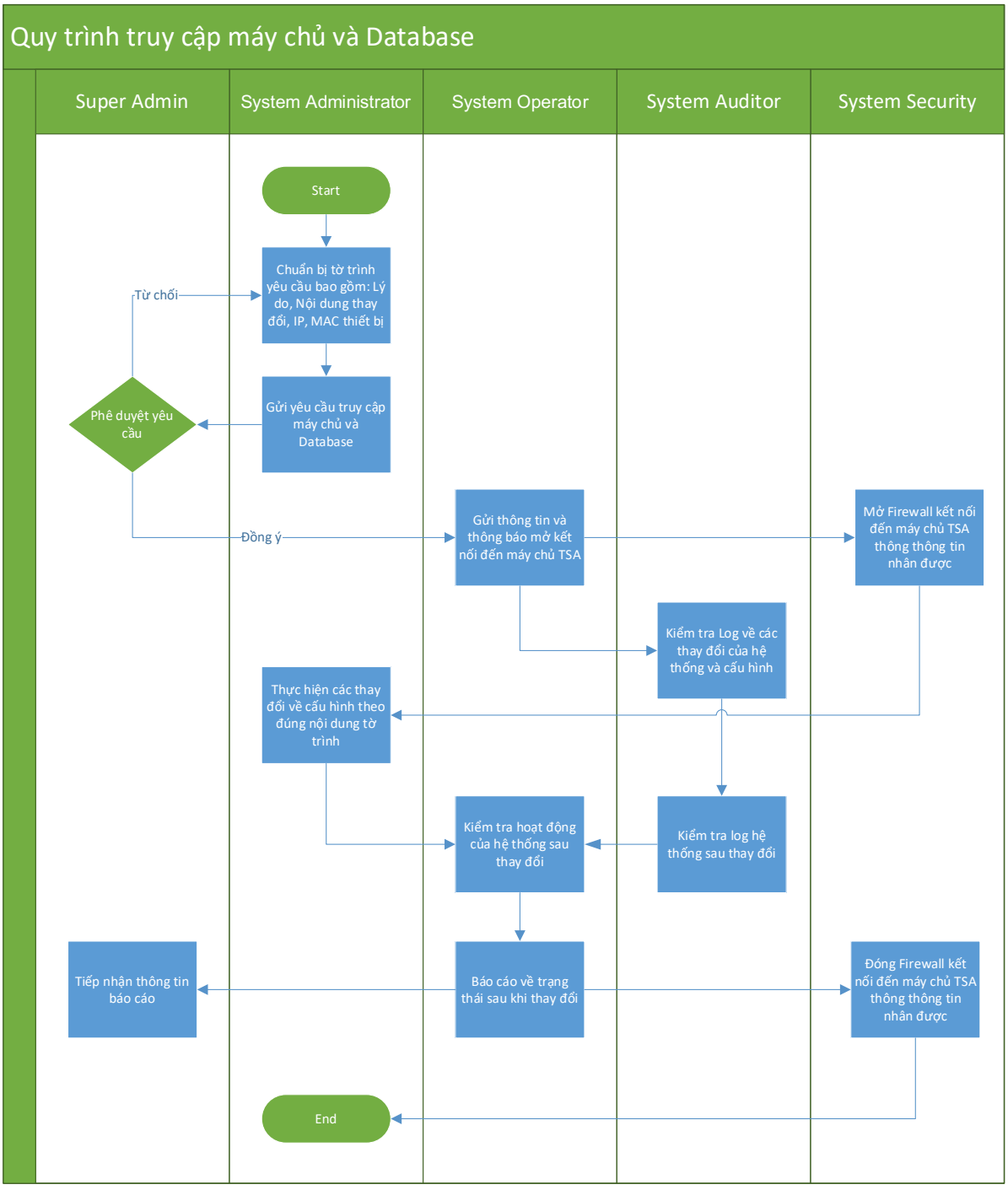
Dịch vụ FPT TSA thực hiện tất cả các chức năng của TSA và RA trên các hệ thống đáng tin cậy đáp ứng được các yêu cầu về bảo mật của dịch vụ FPT TSA.

Trung tâm xử lý sẽ phải đảm bảo chắc chắn rằng các hệ thống chứa phần mềm TSA và các tệp dữ liệu phải là hệ thống đáng tin cậy chống lại được các truy cập trái phép, điều này có thể được giải thích theo yêu cầu và tiêu chuẩn kiểm định. Thêm vào đó, trung tâm xử lý cũng giới hạn tối đa các truy cập đến máy chủ chính với những lý do quyền hạn để truy cập.

Trung tâm xử lý sẽ tạo ra các mạng tách biệt về mặt logic với những mạng khác. Sự tách biệt này nhằm ngăn chặn sự truy cập mạng trái phép ngoại trừ các tiến hành ứng dụng đã được định nghĩa. Trung tâm xử lý sẽ xử dụng tường lửa để bảo vệ hệ thống mạng trước nguy cơ xâm nhậm từ bên trong lẫn bên ngoài. Trung tâm xử lý sẽ yêu cầu sử dụng mật khẩu có đội dài tối thiểu và kết hợp giữa chữ cái với các ký tự đặc biệt, và yêu cầu mật khẩu phải được thay đổi trong một khoảng thời gian nhất định và những khi cần thiết. Việc truy cập trực tiếp dữ liệu của trung tâm xử lý được duy trì trong vùng nhớ của trung tâm xử lý sẽ bị giới hạn đối

với những người được tin tưởng trong nhóm hoạt động của trung tâm xử lý có những lý do hợp lệ để truy cập

V.4. Kiểm soát truy cập máy chủ và Database



Do tính năng đặc thù về việc lưu trữ các log và cấu hình của hệ thống TSA đảm bảo việc xác minh thời điểm sử dụng dịch vụ là rất quan trọng. Vậy nên để đảm bảo việc quản trị, cấu hình Server và hệ thống Database lưu trữ log của hệ thống, FPT-CA đã

xây dựng quy trình gồm nhiều bước để hệ thống được đảm bảo an toàn trong quá trình hoạt động.

- Bước 1: System Administrator chuẩn bị tờ trình cho Lãnh đạo (Super Admin) phê duyệt về:
  - Lý do truy cập Server và Database;
  - Nội dung các bước thực hiện tương tác hệ thống;
  - Địa chỉ IP, MAC thiết bị sử dụng để Remote hệ thống.
- Bước 2: Super Admin phê duyệt yêu cầu. Trong trường hợp nhận thấy có sai sót về tờ trình sẽ từ chối và yêu cầu System Administrator hoàn thiện lại tờ trình và cung cấp lại.
- Bước 3: Sau khi đồng ý Super Admin sẽ thông báo lại cho System Operator để thực hiện việc gửi thông tin thông báo về việc mở kết nối đến các cán bộ liên quan bao gồm: System Auditor và System Security.
- Bước 4: System Auditor sẽ kiểm tra lại các log của hệ thống trước khi thay đổi.
- Bước 5: System Security thực hiện việc mở kết nối từ máy chủ TSA đến máy tính quản trị của System Administrator trên Firewall thông qua IP và MAC của thiết bị. Sau đó thống báo lại tình trạng đã mở kết nối đến System Administrator.
- Bước 6: System Administrator thực hiện việc kết nối máy chủ TSA và thực hiện các thay đổi theo đúng nội dung của tờ trình. Sau khi, hoàn thành quá trình thay đổi sẽ thông báo lại về System Operator và System Auditor để kiểm tra hệ thống.
- Bước 8: System Auditor kiểm tra lại Log và cấu hình của hệ thống sau thay đổi và thông báo cho System Operator. System Operator sẽ kiểm tra hoạt động của hệ thống sau thay đổi.
- Bước 9: System Operator báo cáo về cho Super Admin trạng thái sau khi thay đổi và gửi yêu cầu cho System Security thực hiện đóng Firewall từ máy chủ quản trị đến server của hệ thống TSA.
- Bước 10: Thông báo kết thúc quy trình đến các cán bộ liên quan.

V.5. Kiểm soát chu kỳ kỹ thuật

V.5.1. Kiểm soát vấn đề quản lý bảo mật

Giải pháp An ninh mạng cho FPT TSA được thiết lập dựa trên các thành phần sau:

- Chính sách an ninh mạng được triển khai.
- Kiến trúc Module hóa các thành phần như: Core, Distribution, Edge, Access.
- Tường lửa Firwall: gồm Firewall Internet GW, Campus Firewall, Egde Firewall, Internal FW.
- Hệ thống phát hiện và chống thâm nhập mạng IPS/IPS Network Sensor
- Hệ thống phát hiện và chống thâm nhập các máy chủ ứng dụng IPS Host sensor.
- Hệ thống phòng chống Antivirus nhiều điểm: Internet Gateway, Mail server, spam mail, Client/server, quản lý tập trung.
- Hệ thống cập nhật bản vá cho máy chủ/máy trạm.
- Hệ thống quản trị an ninh : thành phần quản lý và giám sát an ninh tập trung, các thành phần dò tìm các lỗ hổng, thành phần thiết lập chính sách an ninh mạng, thành phần phân tích an ninh và báo cáo, thành phần cập nhật các bản vá cho HĐH mạng, thành phần quản lý và phân tích băng thông của mạng.

FPT có các cơ chế, chính sách để điều khiển và giám sát cấu hình của hệ thống FPT TSA. FPT tạo ra mã hoá đối với tất cả các gói phần mềm và các bản cập nhật của phần mềm dịch vụ FPT TSA. Mã hóa này được sử dụng để kiểm tra tính toàn vẹn của các phần mềm một cách thủ công. Dựa trên quá trình cài đặt và định kỳ sau này, FPT xác nhận tính vẹn toàn của hệ thống FPT TSA.

V.6. Bảo mật mạng cho hệ thống FPT TSA

Hệ thống tường lửa dành cho FPT TSA (Firewall)

Firewall sử dụng trong hệ thống FPT TSA thực hiện phân đoạn mạng thành các phần khác nhau và áp đặt các chính sách kiểm soát thông tin qua lại giữa các phân đoạn mạng đó.

Firewall cho FPT TSA áp dụng công nghệ Stateful Filtering là kỹ thuật cho phép lọc gói tin theo trạng thái. Khi sử dụng kỹ thuật này, Firewall duy trì một bảng trạng thái các kết nối được thiết lập, mỗi khi có kết nối được thiết lập từ bên

ngoài hay bên trong, thông tin về kết nối này được theo dõi và duy trì trong bảng trạng thái,thông tin này gồm có địa chỉ nguồn, địa chỉ đích, số cổng, thứ tự TCP. Các gói tin chỉ được cho phép đi qua Firewall nếu khi đối chiếu vào bảng trạng thái thấy khớp với các giá trị trong bảng này.

Bên cạnh chức năng truyền thống là lọc dữ liệu (với chức năng này Firewall chỉ đọc các header của gói tin, không đọc phần payload), những Firewall thiết kế cho FPT TSA đều có thêm những tính năng chống xâm nhập trên mạng qua những lỗ hổng bảo mật ở mức ứng dụng, nhận dạng tấn công dựa trên cơ sở dữ liệu về tấn công (gọi là signature database) và phản ứng lại các tấn công đó

Hệ thống tường lửa ứng dụng WEB (Web Application Firewall)

Ngoài các hệ thống Firwall để điều khiển truy cập, một trong những xu thế an ninh mạng rất phổ biến trên thế giới tập trung vào tấn công các hệ thống Website của các cơ quan, các tổ chức, các doanh nghiệp và các thiết bị bảo mật thông thường rất khó phát hiện các cuộc tấn công vào cổng dịch vụ TCP 80 này. Chính vì thế giải pháp bảo mật cho hệ thống mạng của FPT TSA sử dụng một loại Firewall đặc chủng, chuyên dụng để bảo vệ các máy chủ Web Server trước những nguy cơ rất lớn từ bên ngoài Internet vào hệ thống Website.

Hệ thống phát hiện và ngăn chặn tấn công (Intrusion Prevention System – IPS)

Song song với hệ thống Firewall là hệ thống dò tìm phát hiện chống xâm nhập bất hợp pháp – IPS (Intrusion Prevention System). Về cơ bản, thực chất IPS là một hệ thống giám sát, phân tích các thông tin và sự kiện trên mạng với tốc độ rất cao và có những cơ chế đặc biệt để nhận dạng các cuộc tấn công, sự lan tràn của virus, phát hiện sự thâm nhập bất hợp pháp thông qua các lỗ hổng bảo mật trong hệ thống... từ đó đưa ra những phản ứng tích cực tới.

VI. PHƯƠNG TIỆN, VẤN ĐỀ QUẢN LÝ VÀ ĐIỀU HÀNH HOẠT ĐỘNG

VI.1. Kiểm soát bảo mật mức vật lý

FPT có tài liệu chi tiết điều khiển vật lý và có những chính sách đảm bảo an toàn cho các máy chủ của dịch vụ dấu thời gian. Những chính sách này bao gồm yêu cầu kiểm tra độc lập, được mô tả ở mục VIII. Những tài liệu chứa thông tin nhạy cảm chỉ sẵn sàng khi có sự đồng ý của FPT. Khái quát về yêu cầu mô tả dưới đây.

VI.1.1. Cấu trúc và khoanh vùng

Môi trường cho các hoạt động của dịch vụ FPT TSA sẽ tuân theo yêu cầu an toàn và các yêu cầu kiểm tra của FPT, nhằm ngăn cản và phát hiện việc truy cập, tiết lộ và sử dụng hệ thống và thông tin nhạy cảm bất hợp pháp.

Các yêu cầu an toàn và yêu cầu kiểm tra của một phần dựa trên sự thiết lập an toàn lớp vật lý. Một lớp như hàng rào, như cửa được khoá nhằm cung cấp sự điều khiển truy nhập uỷ nhiệm cho những cá nhân (cửa hoặc cửa mở khoá hay mở) thực hiện tới vùng tiếp theo. Mỗi lớp cung cấp nhiều sự truy nhập hạn chế hơn và an toàn vật lý chống lại xâm nhập hay được cho phép truy cập. Hơn nữa, mỗi lớp an ninh vật lý đóng gói lớp bên trong tiếp theo, sao cho một lớp bên trong phải hoàn toàn nằm bên trong một lớp bên ngoài.

VI.1.2. Truy cập vật lý

Truy cập tới mỗi tầng an ninh vật lý có thể kiểm tra và giám sát. Vì vậy mỗi tầng có thể truy nhập bởi cấp phép riêng.

Phòng đặt hệ thống TSA của hệ thống dịch vụ dấu thời gian FPT được đặt trong không gian riêng với hệ thống Camera giám sát an ninh 24/7. Quyền ra vào nơi đặt thiết bị được kiểm soát bởi hệ thống nhận dạng vân tay và nhân viên bảo vệ. Bản thân nhân viên bảo vệ cũng không có quyền truy nhập hệ thống máy chủ TSA. Trách nhiệm của những nhân viên này là ngăn chặn các truy cập từ bên ngoài ở mức vật lý. Như vậy thiết kế về mặt kiểm soát vật lý của hệ thống FPT TSA đáp ứng mô hình 4 lớp về bảo mật truy cập vật lý với hệ thống pulic CA.

1. Hệ thống nhân viên an ninh kiểm soát vật lý (TIER 1).
2. Hệ thống truy nhập bằng thẻ từ vào/ ra của hệ thống dịch vụ dấu thời gian, có sự hỗ trợ của Camera giám sát (TIER 2).

3. Hệ thống truy nhập bằng sinh trắc học, Camera giám sát 24/24 tại phòng đặt máy chủ TSA (TIER 3). Phía sau lớp 3 sẽ có hai điểm truy cập.
    - Hệ thống máy chủ TSA hoạt động.
    - Hệ thống máy chủ back up (off –line).
4. Để thực hiện các thao tác với hệ thống TSA TIER 4 (tạo file CSR, sinh key trên HSM, cấu hình hệ thống) đòi hỏi quản trị viên phải dùng hệ thống smart card theo mô hình M/N (Đòi hỏi nhất M quản trị viên trong tổng số N người sử dụng smart card của mình để thực hiện các thao tác quản trị và vận hành hệ thống TSA). Truy nhập khu vực này đòi hỏi các kiểm tra bảo mật về sinh trắc học và hệ thống thẻ từ.

VI.1.3. Điều kiện không khí, nguồn điện, phòng tránh thảm họa.

Các thiết bị của FPT và RA trong bị với 2 thành phần là chính và dự phòng. hệ thống nguồn điện cần đảm bảo luôn liên tục, không bị gián đoạn truy cập. Các hệ thống nhiệt độ, thông gió, không khí cũng được trang bị để điều khiển nhiệt độ và độ ẩm

Thiết bị an toàn của FPT TSA và các RA được xây dựng để bổ sung phương án phòng ngừa để ngăn chặn vấn đề nước xâm nhập và hệ thống.

Thiết bị an toàn của FPT TSA và các RA được trang bị, bổ sung án phòng ngừa để ngăn chặn và dập tắt lửa hay các thảm hoạ khác có thể gây cháy hay khói. Hệ thống thiết kế để phù hợp với tiêu chuẩn phòng cháy chữa cháy.

VI.1.4. Phương tiện lưu trữ

FPT và các RA được bảo vệ trong các đĩa quang, từ sao lưu dữ liệu hệ thống hay thông tin nhậy cảm khỏi nước, lửa hay môi trường huỷ hoại và bảo vệ tránh sửa dụng truy cập trái phép hay phá huỷ.

VI.1.5. Bảo mật thông tin và tiêu huỷ rác

FPT và RA bổ sung quy trình huỷ rác như (tài liệu, giấy, đĩa quang hay bất kỳ loại rác nào) nhằm ngăn chặn sử dụng truy cập trái phép hay bị lộ thông tin bí mật/cá nhân.

VI.1.6. Dự phòng từ xa

FPT và các RA bảo dưỡng sao lưu hệ thống dữ liệu then chốt hay bất kỳ thông tin nhậy cảm bao gồm dữ liệu kiểm định trong dự phòng an toàn.

Hệ thống dự phòng của FPT TSA được đặt tại các trung tâm Data Center khác trong FPT. Hệ thống này duy trì hoạt động thông suốt thông qua việc đồng bộ dữ

liệu thường xuyên với hệ thống chính. Hệ thống này hoàn toàn là một bản back up đầy đủ của hệ thống chính. Ngay khi xảy ra sự cố , hệ thống này sẽ được sử dụng để truy trì hoạt động mà không làm ảnh hưởng đến giao dịch.

Việc đồng bộ, sao lưu định kỳ ở hệ thống dự phòng diễn ra hoàn toàn tự động dưới sự kiểm soát chặt chẽ từ các chuyên gia công ty FPT.

VI.2. Các kiểm soát thủ tục

VI.2.1. Các thành viên trực thuộc tổ chức.

Nhân viên, nhà thầu, nhân viên tư vấn đều có thể được xem xét để trở thành người tin cậy. Những người được chọn là người tin cậy làm việc tại vị trí tin cậy đáp ứng yêu cầu của CPS.

Thành viên tin cậy bao gồm tất cả các nhân viên, kỹ sư, tư vấn có sự truy cập tới hay điều khiển quá trình xác thực hoặc mã hóa có thể gây ảnh hưởng lớn tới:

- Quá trình kiểm tra thông tin trong đơn xin cấp tài khoản dấu thời gian.
- Việc chấp nhận, từ chối hay các xử lý khác của đơn xin tài khoản dấu thời gian, yêu cầu gia hạn, yêu cầu cấp mới, hoặc các thông tin đăng ký.
- Những người được tin cậy có thể bao gồm các đối tượng như sau:
- Nhân viên phục vụ khách hàng
- Nhân viên quản trị hệ thống
- Kỹ sư thiết kế
- Bộ phận được giao nhiệm vụ quản lý sự tin cậy về cơ sở hạ tầng.

VI.2.2. Số lượng thành viên cho mỗi công việc

FPT và các RA thiết lập, duy trì và có các yêu cầu nghiêm ngặt về thủ tục điều khiển để đảm bảo sự phân công nhiệm vụ dựa trên khả năng làm việc và đảm bảo rằng nhiều người được tin cậy sẽ cùng thực hiện các công việc có tính chất nhạy cảm.

Chính sách và thủ tục được thực hiện để đảm bảo sự phân công nhiệm vụ dựa trên khả năng làm việc. Những công việc mang tính nhạy cảm cao, chẳng hạn truy cập và quản lý hệ thống phần cứng mã hoá (đơn vị mã hoá chữ ký CSU) và các công việc liên quan đền khoá, yêu cầu nhiều người được tin tưởng tham gia.

Những thủ tục điều khiển ở bên trong được thiết kế để ít nhất hai cá nhân được tin tưởng cùng tham gia truy cập tới mức vật lý hoặc mức logic của thiết bị. Truy

cập tới phần cứng mã hoá yêu cầu chặt chẽ phải có nhiều người được tin tưởng cùng tham gia toàn bộ quá trình làm việc, từ việc nhận và kiểm tra cho tới bước cuối cùng là huỷ về logic và/hoặc về vật lý. Mỗi một lần mô đun này được kích hoạt trong các thao tác liên quan đến khoá, các truy cập xa hơn nữa sẽ bị thu hồi để duy trì việc phân cách giữa điều khiển các truy cập vật lý và mức logic tới thiết bị. Những người truy cập vật lý tới các mô đun không giữ "Secret Shares" (những thàng phần riêng biệt có chứa các thành phần riêng biệt của khoá bí mật hoặc dữ liệu kích hoạt và ngược lại.

VI.2.3. Nhận dạng và xác thực cho từng thành viên

FPT và các RA xác nhận nhận dạng và quyền cho mọi cá nhân trở thành người tin cậy là:

- Được cấp phép truy cập và cấp truy cập tới các tiện nghi cần thiết.
- Được cấp các tài liệu điện tử để có thể truy cập và thực hiện một số chứng năng trên các hệ thống thông tin và hệ thống FPT hay RA.

Việc xác thực nhận dạng bao gồm hoạt động của các các nhân tin cậy hoặc các chứng năng bảo mật trong tổ chức và kiểm tra thông tin nhận dạng, ví dụ như hộ chiếu, bằng lái xe. Tổ chức có trách nhiệm xác minh tuân theo các thủ tục được đưa ra trong CPS.

VI.2.4. Phân chia trách nhiệm

Những vai trò yêu cầu phân chia trách nhiệm bao gồm (nhưng không giới hạn):

- Xác thực thông tin trong đơn xin cấp tài khoản dấu thời gian
- Quá trình chấp nhận, từ chối, hoặc các quá trình khác của đơn xin cấp tài khoản dấu thời gian, yêu cầu gia hạn, cấp mới hay các thông tin đăng ký.
- Quá trình ban hành, hủy tài khoản, bao gồm những tác nhân được truy cập tới những phần hạn chế truy cập của kho lưu trữ.
- Quá trình chuyển giao những thông tin tài khoản, mật khẩu hay các yêu cầu từ khách hàng.
- Quá trình tạo, gia hạn hay huỷ một tài khoản kết nối
- Quá trình tải, gia hạn chứng thư số cho hệ thống dấu thời gian.

VI.3. Kiểm soát nhân sự

FPT ban hành những tài liệu về kiểm soát nhân sự và chính sách bảo mật cho TSA và RA. Việc tuân thủ những chính sách bao gồm các yêu cầu kiểm tra độc lập được mô tả ở mục VIII. Những tài liệu này chứa thông tin bảo mật nhạy cảm và chỉ dành riêng cho bên tham gia dịch vụ FPT TSA dưới sự đồng ý của FPT.

TSA và các RA yêu cầu những nhân viên đang mong muốn được trở thành người được tin cậy chứng minh được lai lịch tốt, có năng lực tốt và kinh nghiệm cần thiết để thực hiện tốt các yêu cầu công việc trong tương lai, cũng như việc được tin tưởng, nếu có, cần thiết để thực hiện các dịch vụ về chứng thư theo hợp đồng quản lý.

VI.3.1. Quy trình kiểm tra lai lịch

TSA và các RA kiểm tra lai lịch các ứng viên trở thành người được tin cậy. Việc kiểm tra lai lịch sẽ được lặp lại tối thiểu 5 năm một lần . Những thủ tục này tuân theo luật địa phương. Việc mở rộng một trong các yêu cầu không được trái luật địa phương.

Những nhân tố phát hiện trong lai lịch là cơ sở để xem xét việc loại trừ những ứng viên khỏi vị trí tin cậy như được đề cập trong bản hướng dẫn về yêu cầu kiểm tra và bảo mật của FPT, bao gồm bố điểm sau:

- Sự xuyên tạc của ứng viên hay người tin cậy.
- Thông tin tham chiếu của ứng viên không đáng tin cậy.
- Kiểm tra tiền án tiền sự.
- Có dấu hiệu không tốt về thông tin tài chính, tín dụng.

Bản báo cáo chứa thông tin đánh giá của bộ phận nhân sự và bộ phận an ninh, bộ phận này sẽ thực hiện các hoạt động kiểm tra khách chưa có trong bản kiểm tra lai lịch. Những điều này là thước đo để từ chối ứng viên cho vị trí tin cậy hay loại bỏ người tin cậy. Cách vận dụng thông tin đánh giá phải tuân theo luật.

Điều tra lai lịch cá nhân của ứng viên người tin cậy bao gồm:

- Sự xác nhận của nhân viên tiền nhiệm.
- Kiểm tra tham khảo đồng nghiệp.
- Kiểm tra trình độ ứng viên.
- Kiểm tra tiền án tiền sự (ở địa phương, thành phố, và quốc gia).

- Kiểm tra thông tin về tài chính, tín dụng.
- Trung tâm xử lý và dịch vụ của FPT cũng tiến hành điều tra thêm:
- Kiểm tra giấy phép lái xe
- Kiểm tra thông tin an ninh xã hội

VI.3.2. Yêu cầu về đào tạo

TSA và các RA cung cấp cho các cá nhân chương trình đào tạo theo yêu cầu công việc. Những chương trình đào tạo được kiểm tra định kỳ

Chương trình đào tạo gửi những phần liên quan tới cụ thể nhân viên được đào tạo, bao gồm:

- Cơ chế và nguyên tắc bảo mật của FPT.
- Các phiên bản phần cứng và phần mềm đang được sử dụng
- Trách nhiệm cá nhân.
- Báo cáo, chuyển giao các thoả hiệp và các vấn đề liên quan.
- Thủ tục khôi phục sau thảm hoạ và duy trì công việc

TSA và các RA thường xuyên đào tạo lại và cập nhật thông tin cho nhân viên của mình với mức độ và tần xuất phù hợp để nhân viên duy trì mức độ tin tưởng và thực hiện tốt công việc của mình.

VI.3.3. Kỷ luật đối với các hoạt động không hợp pháp

TSA và RA thiết lập, duy trì và áp đặt các chính sách đối với hành động bất hợp pháp. Các biện pháp kỷ luật có thể bao gồm đánh giá, và có thể chấm dứt phụ thuộc vào tần suất và mức độ nghiêm trọng của các hành động bất hợp pháp.

VI.3.4. Yêu cầu đối với các nhà thầu độc lập

TSA và các RA và các nhà thầu hay nhà tư vấn độc lập trở thành người tin cậy, tuân thủ theo các điều kiện sau đây:

- Tổ chức sử dụng các nhà thầu hay nhà tư vấn độc lập trở thành người tin cậy nếu tổ chức đó không có nhân viên thích hợp đóng vai trò người tin cậy.
- Nhà thầu hoặc nhân viên tư vấn được tổ chức tin cậy như một nhân viên của mình.

VI.3.5. Cung cấp tài liệu cho nhân viên

FPT cung cấp chương trình đào tạo cho nhân viên của mình khi cần thiết và cung cấp các tài liệu để họ hoàn thành tốt các công việc của mình.

VI.4. Kiểm tra truy cập

VI.4.1. Các loại bản ghi sự kiện

Các sự kiện có thể kiểm định phải được ghi lại bởi TSA và các RA của FPT. Mọi bản ghi, điện tử hay bằng tay, chứa thời gian của sự kiện, và nhận dạng của đơn vị thực hiện. TSA đưa ra các loại bản ghi sự kiện trong CPS

Các dạng sự kiện có thể kiểm định bao gồm:

- Các sự kiện:
    1. Tạo khoá TSA,
    2. Bật tắt các hệ thống và ứng dụng,
    3. Thay đổi khoá TSA,
    4. Sự kiện có liên quan đến quản lý chu kỳ mã hoá,
    5. Quá Trình xử lý dữ liệu kích hoạt cho khoá bí mật của TSA, các bản ghi truy cập vật lý,
    6. Bảo trì và thay đổi cấu hình hệ thống,
    7. Bản ghi huỷ bỏ các phương tiện chứa khoá, dữ liệu kích hoạt, hoặc thông tin thuê bao. Các sự kiện về chu kỳ sống của tài khoản hệ thống (bao gồm cấp phát, gia hạn, hủy, tạm dừng)
- Sự kiện liên quan tới nhân viên tin cậy (bao gồm (1) hành động truy cập hay thoát ra, (2) tạo và xoá bỏ mật khẩu hay thay đổi đặc quyền của người sử dụng, (3) thay đổi nhân sự).
- Báo cáo về việc truy nhập vào mạng và các hệ thống không được cấp quyền
- Lỗi trong việc sử dụng hệ thống dấu thời gian/
- Thay đổi chính sách tạo dấu thời gian, nguồn thời gian hợp lệ

VI.4.2. Xử lý bản ghi sự kiện

Bản ghi kiểm định được xem lại tương ứng với các cảnh báo không định kỳ và có liên quan trong hệ thống TSA/RA. Các trung tâm xử lý so sánh bản ghi với sự

hỗ trợ bản ghi bằng tay hay điện tử hệ thống của FPT và Trung tâm dịch vụ khi có bất kỳ hoạt động nghi ngờ nào.

Quá trình xử lý bản ghi kiểm định bao gồm quá trình xem xét các bản ghi kiểm định và ghi lại nguyên nhân của tất cả các sự kiện quan trọng trong bản tóm tắt việc xem xét lại bao gồm một quá trình phê chuẩn dữ liệu đó không bị trộn lẫn, sự thanh tra lại tất cả các dữ liệu và quá trình đánh giá của các cảnh báo hay các bản ghi bất thường. Các hành động được thực hiện dựa trên quá trình xem xét các bản ghi kiểm định được ghi lại thành tài liệu.

VI.4.3. Thời gian duy trì lưu trữ cho bản ghi kiểm định

Bản ghi kiểm định sẽ được lưu giữ ít nhất hai tháng sau khi đã được xử lý.

VI.4.4. Bảo vệ các bản ghi kiểm định

Bản ghi kiểm định sẽ được bảo vệ bằng hệ thống bản ghi kiểm định điện tử bao gồm các cơ chế bảo vệ các bàn ghi log khỏi các truy nhập, sửa đổi, xoá bỏ hoặc can thiệp bất hợp pháp.

VI.4.5. Thủ tục sao lưu dự phòng cho các bảng ghi kiểm định

Hàng ngày, các bảng ghi kiểm định sẽ được sao lưu những phần thay đổi, bổ sung, và hàng tuần sẽ được sao lưu dự phòng toàn bộ.

VI.4.6. Đánh giá điểm yếu

Các sự kiện trong quá trình kiểm định sẽ được ghi lại kiểm soát các điểm yếu của hệ thống. Sự đánh giá lỗi bảo mật logic (LSVAs) là được thực hiện, xem xét và sửa chữa theo sự kiểm tra các sự kiện được giám sát. LSVAs căn cứ vào các dữ liệu ghi lại tự động theo thời gian thực và được thực hiện hàng ngày, hàng tháng, hàng năm. LSVA hàng năm sẽ trở thành dữ liệu cho việc đánh giá kiểm toán hàng năm.

VI.5. Lưu trữ các bản ghi

VI.5.1. Những kiểu bản ghi được lưu trữ cho dịch vụ FPT TSA:

- Dữ liệu kiểm toán.
- Thông tin về đơn xin cấp tài khoản dấu thời gian.
- Tài liệu hỗ trợ những đơn xin cấp tài khoản dấu thời gian.
- Thông tin về chu kỳ làm việc của tài khoản, ví dụ: các thông tin hủy, khôi phục, gia hạn lưu lượng sử dụng.

VI.5.2. Thời gian duy trì tài liệu lưu trữ

Các dữ liệu sẽ được lưu trong một khoảng thời gian nhất định trước ngày tài khoản hết số lần sử dụng hoặc bị huỷ bỏ.

Các thông tin về hệ thống TSA của hệ thống FPT được lưu trữ tối thiểu là 5 năm.

VI.5.3. Bảo mật tài liệu lưu trữ

Có một bộ phận sẽ chịu trách nhiệm đảm bảo chỉ có những người tin tưởng có thẩm quyền mới có được truy nhập các dữ liệu lưu trữ. Các dữ liệu lưu trữ được bảo vệ để không bị truy cập bất hợp pháp, xem, thay đổi, xoá, sửa hay phá hoại bên trong hệ thống tin cậy. Phương tiện lưu trữ dữ liệu và các ứng dụng được yêu cầu xử lý dữ liệu sẽ được duy trì nhằm đảm bảo các dữ liệu lưu trữ có thể được truy cập trong khoảng thời gian đã được thiết lập trong CPS.

VI.5.4. Thủ tục sao lưu dự phòng dữ liệu

FPT sẽ thực hiện việc sao lưu dự phòng những phần cần thay đổi của dữ liệu điện tử có chứa thông tin về chứng thư được ban hành, và thực hiện việc sao lưu dự phòng toàn bộ hàng tuần. Những bản sao lưu bằng giấy được cất giữ trong phương tiện đựoc đảm bảo an ninh từ xa.

VI.5.5. Yêu cầu thời gian cho dữ liệu

Tài khoản và toàn bộ cơ sở dữ liệu về việc hủy sẽ chứa thông tin về ngày tháng. Những thông tin này cần ở dạng không mã hoá.

VI.5.6. Hệ thống thu nhập dữ liệu và lưu trữ

Hệ thống thu nhập thông tin dữ liệu lưu trữ của một tổ chức là hệ thống nội bộ, ngoại trừ trường hợp các khách hàng là RA. Trung tâm xử lý sẽ giúp đỡ các RA nảy trong việc bảo quản dữ liệu kiển toán. Như vậy hệ thống thu nhập dữ liệu này là ở bên ngoài doanh nghiệp RA. Mặt khác ,tổ chức tham gia dịch vụ FPT TSA sẽ tận dụng hệ thống thu nhập dữ liệu này.

VI.5.7. Thủ tục thu nhập và kiểm tra thông tin lưu trữ

Chỉ những cá nhân được tin tưởng và có thẩm quyền mới có quyền truy cập vào các dữ liệu lưu trữ. Tính toàn vẹn của thông tin được kiểm tra khi nó được khôi phục.

VI.6. Thay đổi khóa

Một chứng thư số TSA có thể được cấp mới nếu thực thể cấp cao của CA (CA'sSE) xác nhận lại nhận dạng của CA đó. Sau khi xác nhận lại, SE sẽ chấp thuận hay từ chối việc xin cấp mới đó.

Nếu chấp thuận với yêu cầu cấp mới, SE sẽ điều khiển một quá trình phát sinh khoá để tạo ra một cấp khoá mới cho TSA đó. Trong suốt quá trình phát sinh khoá, SE sẽ ký và cấp phát cho TSA đó một chứng thư mới. Như vậy quá trình phát sinh khoá tuân theo những yêu cầu được đề cập tới trong chính sách bảo mật của FPT. Chứng thư TSA mới sẽ chứa khoá công khai TSA được cấp phát trong quá trình phát sinh khoá sẽ có giá trị đối với đối tác tin cậy.

VI.7. Thoả thuận và khôi phục sau thảm họa

VI.7.1. Các thủ tục xử lý vấn đề lộ khoá và sự cố

Các bản sao lưu dự phòng các thông tin của TSA đực lưu trữ trong phương tiện từ xa và được đảm bảo tính sẵn sàng khi xảy ra thảm họa hay có sự phá hoại: các dữ liệu về đơn xin cấp tài khoản dấu thời gian, dữ liệu kiểm toán, các cơ sở dữ liệu cho các tài khoản đã ban hành, các bản ghi của hệ thống. Bản sao lưu dự phòng của các khoá bí mật TSA sẽ được tạo ra và duy trì theo mục VI.2.4 có trong CPS. Trung tâm xử lý sẽ duy trì các bản sao lưu dự phòng của các thông tin TSA của họ, cũng như các TSA của các khách hàng doanh nghiệp nằm trong miền con.

VI.7.2. Hành vi tiêu cực đối với tài nguyên máy tính, phần mềm và dữ liệu

Trong trường hợp tài nguyên, phần mềm và các dữ liệu được sử dụng với mục đích nguy hiểm, báo cáo về sự cố và trả lời cho sự cố đó sẽ được TSA và RA thực hiện ngay lập tức tuân theo các thủ tục của FPT được nêu trong tài liệu CPS này.

VI.7.3. Lộ khoá bí mật của TSA

Trong trường hợp lộ khoá bí mật của TSA, TSA sẽ bị thu hồi chứng thư. Trung tâm xử lý sẽ áp dụng các biện pháp thương mại hợp lý để lưu ý các đối tác tin cậy nếu họ phát hiện ra hoặc có lý do để tin rằng khoá bí mật của TSA bị lộ trong miền con của FPT.

VI.7.4. Khả năng duy trì liên tục trong kinh doanh sau thảm hoạ

FPT tiến hành bảo mật cho các hoạt động phát triển, kiểm tra, bảo trì của TSA và RA. FPT sẽ triển khai kế hoạch khôi phục sau thảm hoạ. Kế hoạch khôi phục sau thảm hoạ. Kế hoạch khôi phục sau thảm hoạ đặt ra tập trung vào việc khôi

phục hệ thống thông tin và các chức năng thương mại quan trọng. Khu vực khôi phục sau thảm hoạ sẽ có bảo vệ vật lý được FPT chỉ rõ.

Trung tâm xử lý có khả năng hồi phục hay khôi phục dữ liệu trong khoảng 72 giờ sau khi một thảm hoạ xảy ra. Trung tâm sẽ hỗ trợ tối thiểu các chức năng sau:

- Cấp phát tài khoản dấu thời gian.
- Gia hạn tài khoản dấu thời gian.
- Hủy tài khoản dấu thời gian.
- Gán dấu thời gian lên tài liệu
- Cung cấp các thông tin kết nối cho khách hàng.

Cơ sở dữ liệu khôi phục thảm hoạ của Trung tâm xử lý được đồng bộ hoá thường xuyên với cơ sở dữ liệu sản xuất trong một khoảng thời gian giới hạn theo Chỉ dẫn về yêu cầu an ninh và kiểm toán (Security and Audit Requirements Guide). Các thiết bị để khôi phục sau thảm hoạ của Trung tâm xử lý sẽ được bảo vệ vật lý tương ứng với mức an ninh vật lý được đề cập đến trong chính sách bảo mật của FPT.

Trung tâm dịch vụ có chức năng công bố thảm hoạ tên website của họ bằng ngôn ngữ địa phương và tiếng Anh thông báo trực tiếp tới khách hàng, đối tác tin cậy và những người quan tâm.

Kế hoạch khôi phục sau thảm hoạ của Trung tâm dịch vụ và trung tâm xử lý được thiết kế để tạo ra khả năng khôi phục hoàn toàn trong khoảng một tuần từ khi thảm hoạ xảy ra tại khu vực chính của Trung tâm dịch vụ và Trung tâm xử lý được thiết kế để tạo ra khả năng khôi phục hoàn toàn trong khoảng một tuần từ khi thảm hoạ xảy ra tại khu vực chính của Trung tâm dịch vụ và Trung tâm xử lý. Trung tâm dịch vụ và Trung tâm xử lý cài đặt và kiểm tra các thiết bị của họ tại khu vực chính để hộ trợ chứng năng TSA/RA theo mọi tình huống ngoại trừ một thảm hoạ lớn có thểm làm cho toàn bộ hệ thống không thể hoạt động được. Như vậy thiết bị đó phải được dự phòng và có khả năng chịu đựng hỏng hóc.

VI.8. Kết thúc sự hoạt động của TSA hay RA

Việc kết thúc các tổ chức tham gia dịch vụ FPT TSA (ngoại trừ RA) này sẽ nằm trong thoả thuận giữa CA và SE. Các bên sử dụng sự tin tưởng và áp dụng các biện pháp thương mại hợp lý để đi đến thoải thuận kế hoạch kế thúc nhằm giải thiểu tối đa tác động tới khách hàng, thuê bao và các đối tác. Kế hoạch kết thúc có thể bao gồm các bước:

- Thông báo đến các bên liên quan tới quá trình chấm dứt hoạt động như thuê bao, các đối tác, khách hàng.
- Xử lý các chi phí cho các thông báo đó.
- SE thu hồi chứng thư đã phát hành tới TSA.
- Lưu trữ các dữ liệu của TSA trong một khoảng thời gian được đề cập đến trong CPS.
- Tiếp tục hỗ trợ dịch vụ cho các khách hàng và thuê bao.
- Hoàn lại phí (nếu cần) cho những khách hàng có tài khoản chưa bị hết hạn và chưa bị thu hồi vừa bị thu hồi trong quá trình chấm dứt hay cung cấp.
- Sắp xếp khoá bí mật của TSA và thẻ phần cứng chứa khoá bí mật.
- Cung cấp các chuyển giao cần thiết của dịch vụ TSA tới các TSA đang hoạt động.

VII. KHUÔN DẠNG CỦA CHỨNG THƯ

VII.1. Khuôn dạng của chứng thư

Các chứng thư sử dụng cho hệ thống FPT TSA tuân theo ITU-T Recommendation x.509 (1997): Information Technology – Open Systems Interconnection-The Directory: Authentication Framework, June 1997 and (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008 ("RFC 5280").

Tối thiểu, các chứng thư X.509 bao gồm các trường cơ bản và các giá trị bắt buộc được chỉ ra hoặc phải tuân theo các ràng buộc trong bảng dưới đây:

Tên trường	Giá trị
Serial Number	Duy nhất cho một lssuer DN
Signature Algorithm	Định danh thuật toán được sử dụng để ký chứng thư
Issuer DN	Xem mục VII.1.4
Valid From	Thời điểm chứng thư bắt đầu có hiệu lực. Được đồng bộ với Master Clock của U.S Naval Observatory. Được mã hoá theo tiêu chuẩn RFC 5280
Valid To	Thời điểm chứng thư hết hiệu lực. Được đồng bộ với Master Clock của U.S Naval Observatory. Được mã hoá theo tiêu chuẩn RFC 5280
Subject DN	Xem mục VII.1.4
Subject Public Key	Được mã hoá theo tiêu chuẩn RFC 5280
Signature	Được sinh và mã hoá phù hợp với tiêu chuẩn RFC 5280

VII.1.1. Phiên bản

Chứng thư số của FPT TSA là các chứng thư X.509 phiên bản 3 nhưng chứng thư gốc (Root Certificates) có thể là chứng thư X.509 phiên bản 3 nhưng chứng thư gốc (Root Certificates) có thể là chứng thư X.509 phiên bản 1 để hỗ trợ kế thừa của hệ thống. Các chứng thư CA là các chứng thư X.509 phiên bản 1 hoặc phiên bản 3. Các chứng thư cho thuê bao cuối là chứng thư X.509 phiên bản 3.

VII.1.2. Phần mở rộng của chứng thư

FPT tạo ra chứng thư X.509 phiên bản 3 với sự mở rộng đực yêu cầu trong mục 7.1.2.1-7.1.2.8. Sự mở rộng riêng biệt có thể chấp nhận được, nhưng việc sử dụng các sự mở rộng riêng biệt không được đảm bảo trong CP và CPS trừ khi có các tham chiếu đặc biệt kèm theo.

6.1.1.1. Sử dụng khoá

Các chứng thư X.509 phiên bản 3 nói chung được phù hợp với RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.

Ghi chú: Mặt dù bit chống từ chối không được thiết lập cho phần mở rộng sử dụng khoá, nhưng FPT vẫn hỗ trợ các tính năng chống từ chối cho các chứng thư này. Bit chống từ chối không được yêu cầu thiết lập trong các chứng thư này bởi vì công nghệ PKI chưa đạt tới sự thống nhất về định nghĩa bit chống từ chối nghĩa. Cho đến khi đạt được sự thống nhất thì bit chống từ chối sẽ không có ý nghĩa đối với các đối tác tin cậy tiềm năng. Hơn thế nữa, các ứng dụng phổ biến nhất không nhận biết được bit chống từ chối.

7.1.1.1. Phần mở rộng của các chính sách chứng thư

Phần mở rộng của các chính sách chứng thư của X.509 phiên bản 3 được biết đến là việc nhận biết đối tượng của CPS theo mục VII.1.6 và hạn định chính sách tuân theo mục VII.1.8.

8.1.1.1. Tên thay thế của chủ thể (subjectAltName)

Trường mở rộng *subjectAltName* của chứng thư FPT TSA X.509 phiên bản 3 tuân theo chuẩn RFC 5280.

9.1.1.1. Rằng buộc cơ bản (BasicConstraints)

Với chứng thư X.509 phiên bản 3 cho CA, trường mở rộng *BasicConstraints* có giá trị CA được thiết lập là TRUE. Với chứng thư thuê bao cuối thì trường mở rộng *BasicConstraints* được thiết lập là một chuỗi rỗng. Trường *criticality* được thiết lập là TRUE cho chứng thư CA.

Trường "pathLen Constraint" của trường mở rộng BasicConstraints là giá trị lớn nhất của đường dẫn chứng thư. Nếu trường này có giá trị bằng 0 , thì chứng thư chỉ được cấp cho thuê bao thuê bao cuối.

10.1.1.1. Việc sử dụng khoá mở rộng

Với chứng thư thuê bao cuối X.509 phiên bản 3 của dịch vụ FPT TSA, trường mở rộng *ExtendedKeyUsage* được cấu hình bao gồm các khoá OID (object identifiers).

11.1.1.1. Điểm phân bố CRL

Trong chứng thư số FPT TSA X.509 phiên bản 3, trường mở rộng cRLDistributionPoints chứa các URL để đối tác tin cậy có thể lấy được CRL để kiểm tra trạng thái chứng thư.

12.1.1.1. Định danh khoá cho đơn vị cấp chứng thư.

Trong chứng thư FPT TSA X.509 phiển bản 3, phương pháp nhận dạng khoá dựa vào khoá công khai do TSA phát hành tuân theo phương thức được mô tả trong RFC 3208.

VII.1.3. Thuật toán nhận biết dối tượng

Dịch vụ FPT TSA sử dụng các thuật toán sau:

- SHA-256

Chữ ký số sử dụng các thuật toán này tuân theo tiêu chuẩn FIPS PUB 180-4. Sử dụng hàm băm SHA-256 có nhiều ưu điểm hơn so với SHA-1. Do thuật toán SHA-1 về lý thuyết có thể bị phá.

Phiên bản hiện tại của trung tâm xử lý sử dụng thuật mã hoá SHA-256 cho hệ thống FPT TSA

VII.1.4. Cấu trúc tên

Tên của chứng thư FPT TSA tuân theo mục III.1.1

VII.1.5. Ràng buộc tên

Không có sự ràng buộc nào về tên.

VII.1.6. Chính sách nhận biết đối tượng

Việc nhận biết đối tượng cho chính sách chứng thư tương ứng với mỗi cấp được thiết lập trong mục I.2. Mở rộng chính sách chứng thư trong mỗi chứng thư FPT TSA X.509 phiên bản 3 tuần theo mục I.2.

VII.1.7. Cách dùng của sự mở rộng chính sách ràng buộc

Không có ràng buộc nào.

VII.1.8. Chính sách hạn định cấu trúc và ngữ nghĩa

Chứng thư FPT TSA X.509 phiên bản 3 chứa hạn định chính sách trong phần mở rộng chính sách chứng thư. Nói chung, chứng thư bao gồm một CPS pointer qualifier trỏ đến bản thoả thuận với đối tác tin cậy hoặc CPS của FPT.

VII.2. Khuôn dạng danh sách thu hồi chứng thư CRL

Các chứng thư có chứa ngày hết hạn hiệu lực (trong trường thời gian hiệu lực), tuy nhiên đáng tiếc là đôi khi cần thu hồi (ngắt hiệu lực) của một chứng thư trước thời gian vì một vài lý do nào đó. TSA cần một phương tiện để cập nhật thông tin trạng thái chứng thư của mọi chứng thư sử dụng cho hệ thống. Một phương tiên hữu hiệu là danh sách thu hồi chứng thư chuẩn X.509 (*CRL – Certificate Revocation List*).

Danh sách thu hồi chứng thư X.509 được bảo vệ bởi chữ ký số của SE phát hành. Những người dùng sẽ chắc chắn rằng nội dung của CRL không bị thay đổi bằng cách xác thực chữ ký của SE trên CRL đó. Các chứng thư chứa một tập hợp các trường chuẩn và một tập các trường mở rộng tuỳ chọn. Những trường chuẩn bao gồm:

- **Version – Phiên bản**: Trường này miêu tả cú pháp của CRL (Thông thường trường phiên bản sẽ là 2).
- **Signature - Chữ ký**: Trường này chứa thông tin về kỹ thuật nhận diện cho chữ ký số mà CA sử dụng để ký vào CRL.
- **Issuer – Phát hành**: Trường này chứa tên theo chuẩn X.500 của CA phát hành CRL.
- **This Update - Cập nhật hiên tại**: Trường này chứa thông tin ngày phát hành (cập nhật) CRL.
- **Next update - Cập nhật sắp tới**: Trường này chứa thông tin ngày sẽ cập nhật tiếp theo gần nhất.
- **Revoked certificates – Chứng thư số bị thu hồi**: Trường này chứa thông tin về các chứng thư bị thu hồi (bao gồm Serial number, time of revoke certification - Thời gian chứng thư bắt đầu bị thu hồi, và một số thông tin mở rộng khác.) Các thông tin mở rộng khác được sử dụng để cung cấp thông tin bổ sung. Trường này chỉ xuất hiện trong các CRL phiên bản 2.

  Những trường mở rộng phổ biến được sử dụng bao gồm:

- **CRL number**: Số phát hành của CRL.
- **Authority key identifier**: Chúng ta đã biết mỗi CA có thể có nhiều cặp khóa khác nhau vì vậy trường này giúp người dùng biết cần chọn lựa khoá công khai nào để xác thực chữ ký số của CA đã ký trên CRL để có thể xác định độ tin cậy của CRL.

- **Issuer alternative name**: Trường Issuer ở trên đã chứa thông tin tên chuẩn X.500 của CA phát hành CRL, tuy nhiên một số ứng dụng đặc biết không thể hiểu chuẩn đặt tên này. Do đó trường Issuer alternative name chứa thông tin về CA phát hành CRL theo một cú pháp thích hợp khác. Ví dụ…dạng DNS hay e-mail chẳng hạn: CA1@xyz.vn.

- **Issuing distribution points**: Trường này để kết hợp cùng với trường mở rộng CRL distribution point trong chứng thư X.509.

- **Reason code**: Trường này được dùng để đưa ra lý do vì sao một chứng thư cụ thể bị thu hồi. (Nhằm giúp người dùng xử lý mềm dẻo hơn).

- **Certificate issuer**: Đôi khi một CA nào đó chuyển chức năng phát hành CRL với các chứng thư mà nó phát hành cho một CA khác. Trường này được dùng để xem thông tin về CA nào phát hành ra các chứng thực xuất hiện trong một CRL.

VIII. KIỂM ĐỊNH TÍNH TUÂN THỦ VÀ CÁC ĐÁNH GIÁ KHÁC

FPT sẽ tiến hành kiểm toán định kỳ nhằm đảm bảo việc tuân thủ các tiêu chuẩn của dịch vụ FPT TSA sau khi đi vào hoạt động.

Bên cạnh đó, các tiêu chuẩn của dịch vụ FPT TSA sẽ được dùng để tiến hành đánh giá và thanh tra nhằm đảm bảo tính trung thực của FPT, bao gồm những điều sau:

Các tiêu chuẩn của dịch vụ FPT TSA sẽ được dùng để thanh tra hay đánh giá FPT, hay thuê bao là các doanh nghiệp. Trong trường hợp FPT hoặc Superior Entity được kiểm tra và kết quả cho thấy các thực thể không đạt các tiêu chuẩn của dịch vụ FPT TSA, sẽ được tiếp tục hoạt động hoặc không được hoạt động tuỳ thuộc vào mức độ và hậu quả của tổn thất gây ra. Những lỗi hay những tổn thất, cho thấy mối đe doạ tiềm ẩn và thực sự đối với an ninh hay tính toàn vẹn của FPT TSA .

Các tiêu chuẩn của dịch vụ FPT TSA sẽ được dùng để tiến hành các đánh giá về quản lý rủi ro bổ sung của chính FPT hay của thuê bao theo những phát hiện về việc không tuân thủ đầy đủ hoặc có những ngoại lệ trong kết quả cuộc kiểm toán quá trình tuân thủ và đó cũng là một phần của quá trình quản lý rủi ro tổng thể.

Các tiêu chuẩn của dịch vụ FPT TSA sẽ được dùng để tiến hành kiểm toán, đánh giá và thanh tra các thực thể hoặc hãng kiểm toán đóng vai trò là bên thứ 3. Các thực thể chịu sự kiểm toán, đánh giá và thanh tra sẽ phải hợp tác với FPT để tiến hành kiểm toán, đánh giá và thanh tra này.

VIII.1. Tần suất và các trường hợp đánh giá

Các cuộc kiểm soát quá trình tuân thủ được tiến hành ít nhất mỗi năm một lần với chi phí phụ thuộc về thực thể được kiểm toán.

VIII.2. Danh tính và khả năng của người kiểm toán

Hãng kiểm toán đóng vai trò là bên thứ 3 sẽ tiến hành kiểm toán quá trình tuân thủ của FPT.

Việc đánh giá và kiểm toán trên lại được kiểm tra bởi một công ty kế toán nhà nước đã được cấp chứng thư trong sự giám định của an ninh máy tính hoặc bởi các chuyên gia có uy tín về an ninh máy tính do ban cố vấn an ninh chỉ định. Công ty này cũng sẽ phải giám định về an ninh công nghệ thông tin và việc thực hiện cấp phát dấu thời gian.

VIII.3. Mối quan hệ giữa kiểm toán viên và thực thể được kiểm toán

Việc kiểm toán mà được thực hiện bởi hãng kiểm toán đóng vai trò là bên thứ 3 sẽ được tiến hành kiểm tra bởi các hãng độc lập với thực thể được kiểm toán. Sẽ không có bất kì sự tranh cãi nào về lợi ích gây cản trở tới việc thực hiện các dịch vụ kiểm toán.

VIII.4. Những đối tượng trong quá trình đánh giá

Chủ thể kiểm toán của mỗi loại thực thể sẽ được đưa ra như dưới đây. Thực thể được kiểm tra có thể tiến hành kiểm toán việc thực hiện theo một mô mình là một phần của cuộc kiểm tra tổng thể hàng năm về hệ thống thông tin của thực thể.

FPT sẽ được kiểm toán dựa theo những hướng dẫn có trong các tuyên bố số 70 về chuẩn kiểm toán (SAS) do Viện kế toán công chứng Hoa Kỳ (American Institule of Certificate Public Accounts) đưa ra và các báo cáo về quá trình giao dịch của các tổ chức dịch vụ.

VIII.5. Giải quyết khi kết quả bị đánh giá là thiếu sót.

Sau khi nhận được báo cáo kiểm toán, SE của thực thể được kiểm toán sẽ liên lạc với bên kiểm toán để thảo luận về những trường hợp ngoại lệ và những thiếu sót mà kết quả cuộc kiểm toán chỉ ra. Các tiêu chuẩn của dịch vụ FPT TSA sẽ được sử dụng để thảo luận về những trường hợp ngoại lệ và những thiết sót với bên kiểm toán. Thực thể được kiểm toán và SE sẽ dùng những nỗ lực thương mại để thoả thuận kế hoạch hành động đúng đắn để giải quyết các vấn đề do các trường hợp ngoại lệ và thiếu sót gây ra và để thực hiện kế hoạch đó.

Trong trường hợp bên thực thể được kiểm toán thất bại trong việc đưa ra một kế hoạch hành động hoặc thất bại trong việc thực hiện nó, hoặc nếu bản báo cáo chỉ ra những ngoại lệ và những thiếu sót mà FPT và SE tin rằng chúng là mối đe doạ tức thì tới an ninh và tính thống nhất của FPT:

(a) FPT và SE sẽ khẳng định có cần thiết phải thu hồi hay thoả hiệp báo cáo hay không.

(b) FPT và SE sẽ được phép tạm dừng dịch vụ để tiến hành kiểm toán

(c) Nếu cần thiết, FPT và SE có thể sẽ chấm dứt dịch vụ và những điều khoản trong hợp đồng giữa thực thể được kiểm toán và SE của nó.

VIII.6. Thông báo kết quả

Theo như bất kì một cuộc kiểm toán nào thì bên thực thể được kiểm toán sẽ cung cấp cho FPT và SE (nếu SE không phải là FPT) bản báo cáo và các chứng nhận hàng năm dựa trên kết quả kiểm toán hoặc tự kiểm toán trong vòng 14 ngày sau khi kết thúc kiểm toán hoặc không quá 44 ngày sau ngày bắt đầu các hoạt động.

IX. CÁC VẤN ĐỀ THƯƠNG MẠI VÀ PHÁP LÝ KHÁC

IX.1. Lệ phí

IX.1.1. Lệ phí cấp tài khoản hoặc gia hạn tài khoản

Khách hàng sử dụng dịch vụ FPT TSA phải trả phí khi xin cấp, gia hạn tài khoản dịch vụ dấu thời gian, quản lý hệ thống dấu thời gian cho nhà cung cấp.

IX.1.2. Lệ phí sử dụng dịch vụ dấu thời gian

Các thuê bao của dịch vụ FPT TSA và RA không phải trả phí để tạo ra dữ liệu tài khoản.

IX.1.3. Phí truy cập thông tin về trạng thái chứng thư và việc thu hồi chứng thư.

Chứng thư số sử dụng cho hệ thống cấp phát dấu thời gian sẽ do Bộ Truyền thông thông tin cấp phép nên các đường dẫn CRLs hay OCSP của chứng thư số sẽ do Bộ Truyền thông thông tin quản lý.

IX.1.4. Lệ phí sử dụng cho các dịch vụ khác

Các thành phần tham gia dịch vụ FPT TSA không phải trả phí khi truy cập CP hoặc CPS. Việc sử dụng văn bản với các mục đích khác như sao chép, phân bổ lại, sửa chữa hoặc tạo mới các công viên phát sinh sẽ phải tuân theo thoả thuận hợp pháp với người đang nắm giữ bản quyền của văn bản này.

IX.1.5. Chính sách hoàn trả phí

FPT sẽ đưa ra phạm vi cho việc áp dụng chính sách hoàn trả phí. Chính sách này sẽ được đưa lên website (bao gồm một danh sách các kho dữ liệu), hoặc đưa vào bản thoả thuận với khách hàng hay đưa vào trong bản CPS.

IX.2. Trách nhiệm tài chính

IX.2.1. Bảo hiểm

FPT sẽ duy trình tính thương mại hợp lý cho các mức bảo hiểm đối với các lỗi hay thiếu sót, hoặc thông qua các chương trình bảo hiểm lỗi hay thiếu sót với các hãng bảo hiểm hoặc tự cam kết bảo hiểm. Các yêu cầu bảo hiểm này không áp dụng với các tổ chức chính trị.

13.1.1.1. Các trường hợp FPT tiến hành đề bù bảo hiểm và mức đền bù bảo hiểm

FPT tiến hành đền bù bảo hiểm cho các trường hợp sau:

- Lỗi do TS gây ra, bao gồm lỗi kỹ thuật khi phát hành tài khoản theo trách nhiệm của FPT TSA.
- FPT đưa ra các mức đền bù bảo hiểm theo các mức bảo hiểm chứng thư khác nhau.
- Việc đề bù bảo hiểm thực hiện theo đúng hợp đồng với thuê bao.

14.1.1.1. Các trường hợp không được hưởng đền bù bảo hiểm

FPT sẽ không chịu trách nhiệm trong các trường hợp:

- Các trường hợp sử dụng chứng thư không được đề cập đến trong CP, CPS.
- Các trường hợp giả mạo xử lý chứng từ.
- Các trường hợp sử dụng, cấu hình không phù hợp, không nằm trong trách nhiệm của TSA được sử dụng trong quá trình xử lý chứng thư.
- Khách hàng đánh mất hoặc để lộ tài khoản mất khẩu sử dụng cho hệ thống dịch vụ dấu thời gian.
- Lỗi của RA, bao gồm lỗi xác thực việc nhận biết dữ liệu, số chứng thư, giá trị khoá công khai, RA không gửi yêu cầu phù hợp... Khi có lỗi xảy ra, RA sẽ chịu hoàn toàn trách nhiệm với khách hàng.Việc đề bù được thực hiện theo hợp đồng với thuê bao.

IX.2.2. Các tài sản khác

FPT có quền tự chủ tài chính để duy trì hoạt động và thực hiện các nhiệm vụ của mình, đồng thời có trách nhiệm pháp lý đối với các rủi ro cho thuê bao và các đối tác tin cậy.

IX.2.3. Thông tin bảo đảm mở rộng.

FPT đưa ra chương trình bảo đảm mở rộng cung cấp các SSL và bảo vệ chữ ký số không bị mất hay phá huỷ từ những thiếu sót trong quá trình cấp chứng nhận hoặc từ việc vi phạm hợp đồng. FPT đưa ra các chương trình bảo đảm mở rộng được yêu cầu trong CPS.

IX.3. Tính bảo mật của thông tin kinh doanh

IX.3.1. Phạm vi của thông tin cần bảo mật

Những dữ liệu sau của thuê bao, như đề cập đến ở mục IX.3.2 sẽ được đảm bảo tính mật và riêng tư (“thông tin mật/riêng tư”)

- Các dữ liệu TSA, được phê chuẩn hoặc không được phê chuẩn
- Các dữ liệu đơn xin cấp tài khoản dấu thời gian
- Các khóa bí mật của hệ thống sử dụng hệ thống quản lý khoá công khai và các thông tin cần thiết để khôi phục các khoá này.
- Các dữ liệu chuyển đổi (dữ liệu đầy đủ và các dữ liệu kiểm toán của quá trình chuyển đổi).
- Các dữ liệu kiểm toán tạo hoặc lưu giữ bởi FPT hoặc một thuê bao.
- Các báo cáo kiểm toán tạo bởi FPT hay thuê bao (cho việc đánh giá những báo cáo này), hoặc những kiểm toán viên (nội bộ hoặc là bên ngoài).
- Các dự án khôi phục do tại nạn hay khôi phục sau thảm hoạ.
- Quản lý mức độ an ninh trong hoạt động của phần cứng, phần mềm, các quản trị viên của dịch vụ chứng thư và của các dịch vụ khác.

IX.3.2. Thông tin không nằm trong phạm vi của quá trình đảm bảo tính mật

Chứng thư, thu hồi chứng thư và các thông tin về trạng thái của chứng thư, nơi lưu giữ của FPT cùng các thông tin chứa bên trong không được coi là các thông tin mật/riêng tư. Các thông tin không được xem là mật/riêng tư trong muc 9.3.1 sẽ không riêng tư hoặc không bí mật. Phần này tuân theo luật riêng tư.

IX.3.3. Trách nhiệm bảo vệ thông tin mật

FPT đảm bảo an ninh cho các thông tin riêng tư không bị tiết lộ với bên thứ 3.

IX.4. Tính bí mật của thông tin cá nhân

IX.4.1. Kế hoạch đảm bảo tính riêng tư

FPT sẽ tiến hành triển khai chính sách đảm bảo tính riêng , tuân theo luật riêng tư, FPT sẽ không tiết lộ tên hay bất cứ một thông tin nào về các đơn xin cấp chứng thư của thuê bao ra bên ngoài.

IX.4.2. Thông tin riêng tư

Tất cả những thông tin về thuê bao không được công bố công khai, bao gồm tài khoản mật khẩu khách hàng sử dụng cho hệ thống, và các CRL trực tuyến được coi là thông tin riêng tư.

IX.4.3. Thông tin không riêng tư

Tất cả các thông tin được công khai trong chứng thư số sử dụng cho hệ thống được coi như không phải là thông tin riêng tư.

IX.4.4. Trách nhiệm bảo vệ thông tin riêng tư

Những người tham gia vào dịch vụ FPT TSA nhận các thông tin mật phải đảm bảo tính mật cho những thông tin này không bị tiết lộ với bên thứ 3 và phải tuân theo những luật riêng tư trong phạm vi quyền hạn của mình.

IX.4.5. Thông báo và cho phép sử dụng thông tin mật

Theo luật riêng tư hay theo thoả thuận, các thông tin riêng tư sẽ không được sử dụng mà không có sự cho phép của người sở hữu những thông tin này. Phần này tuân theo luật từng riêng tư.

IX.5. Cung cấp thông tin

FPT sẽ được phép công bố những thông tin mật/riêng tư nếu:

- Quá trình công bố là cần thiết khi có yêu cầu của toà án và tìm kiếm thông tin xác nhận.
- Quá trình công bố là cần thiết đáp ứng yêu cầu của toà án, quá trình quản trị hay các quá trình liên quan đến luật pháp, các hoạt động quản lý như thẩm vấn của toà án, yêu cầu xác nhận, yêu cầu cho quá trình tạo tài liệu.

IX.5.1. Những trường hợp làm lộ thông tin khác

Những chính sách riêng tư bao gồm các điều khoản liên quan đến việc tiết lộ các thông tin bí mật/riêng.

IX.6. Quyền sở hữu trí tuệ

IX.6.1. Quyền sở hữu trong CPS

Các bên liên quan trong dịch vụ FPT TSA chấp nhận rằng FPT có quyền sở hữu đối với CPS và các điều khoản ghi trong CPS.

IX.6.2. Quyền sở hữu tên

FPT TSA có quyền sở hữu đối với thương hiệu, tên dịch vụ trong các đơn xin tài khoản dấu thời gian , và với tên phân biệt (distinguished name) trong chứng thư sử dụng cho hệ thống dấu thời gian của FPT.

IX.6.3. Quyền sở hữu khoá và các tài liệu của khoá

Cặp khoá tương ứng với chứng thư của TSA và thuê bao là tài sản của TSA và thuê bao và được lưu trữ bảo vệ theo quyền sở hữu trí tuệ.

IX.7. Vấn đề đại diện và bảo lãnh

IX.7.1. Đại diện của CA và vấn đề bảo lãnh

Dịch vụ FPT TSA bảo đảm:

- Không có những thông tin không phù hợp với thực tế trong chứng thư.
- Chứng thư của TSA phù hợp với yêu cầu trong CP và CPS.
- Dịch vụ hủy tài khoản và sử dụng kho lưu trữ phù hợp với tiêu chuẩn trong CP và CPS.

Thoả thuận với khách hàng có thể có thêm các tuyên bố và cam kết khác.

IX.7.2. Đại diện của RA và vấn đề bảo lãnh

Các RA của dịch vụ FPT TSA bảo đảm:

- Không có thiếu sót trong quá trình khởi tạo tài khoản, mật khẩu và kết nối tới hệ thống FPT TSA.
- Những chứng thư của RA tuân theo các yêu cầu trong CPS này.
- Dịch vụ thu hồi tài khoản và sử dụng kho lưu trữ phù hợp với tiêu chuẩn trong CPS.

Thoả thuận với khách hàng có thể có thêm các tuyên bố và cam kết khác.

IX.7.3. Đại diện của khách hàng và sự bảo lãnh

Khách hàng cam kết rằng:

- Tài khoản và mật khẩu được cung cấp bởi FPT TSA phải đảm bảo an toàn, bí mật trong toàn bộ quá trình sử dụng.
- Không chia sẽ hay trao đổi tài khoản với bên thứ 3 nếu chưa được sự chấp nhận hoặc cấp phép từ FPT TSA
- Tất cả các cam kết được đưa ra bởi khách hàng trong đơn xin cấp tài khoản dấu thời gian là đúng sự thật.
- Dịch vụ dấu thời gian được sử dụng cho các mục đích hợp pháp và tuân theo những yêu cầu trong CPS.

Thoả thuận khách hàng có thể có thêm các tuyên bố và cam kết khác.

IX.7.4. Đại diện cho các đối tác tin cậy và vấn đề bảo lãnh

Thoả thuận với đối tác tin cậy yêu cầu đối tác tin cậy phải có đủ thông tin để đưa ra một quyết định dựa vào các thông tin trong chứng thư. Họ có trách nhiệm quyết định tin tưởng hay không vào các thông tin trong chứng thư. Relying Rarties có trong CPS.

Thoả thuận về bên đối tác có thể bao gồm thêm các tuyên bố và cam kết khác.

Trách nhiệm pháp lý của đối tác tin cậy sẽ được thiết lập trong hợp đồng đối tác tin cậy.

IX.8. Vấn đề bồi thường

IX.8.1. Vấn đề bồi thường của khách hàng

Khi pháp luật yêu cầu, khách hàng phải bồi thường cho FPT nếu xuất hiện:

- Những thông tin không hợp lệ do khách hàng cung cấp trên đơn xin cấp tài khoản dấu thời gian.
- Lỗi của khách hàng để lộ những nhân tố, yếu tố liên quan đến đơn xin cấp tài khoản dấu thời gian, sự bỏ sót do sự cẩu thả hay với mục đích lừa đảo.
- Lỗi của khách hàng trong việc bảo vệ tài khoản, mật khẩu, sử dụng hệ thống tin cậy, hoặc không thực hiện các biện pháp phòng ngừa cần thiết để tránh gây hậu quả.
- Việc sử dụng tên của khách hàng (kể cả việc không giới hạn tên chung, tên miền, hoặc địa chỉ thư điện tử) vi phạm quyền sở hữu trí tuệ của bên thứ 3.

Hợp đồng với khách hàng có thể có những bổ sung phù hợp.

IX.8.2. Vấn đề bồi thường của các đối tác tin cậy

Khi được pháp luật cho phép, bản thỏa thuận với đối tác tin cậy sẽ yêu cầu dối tác tin cậy bồi thường cho FPT hay các thành phần tham gia dịch vụ FPT TSA vì:

- Lỗi của đối tác tin cậy trong việc thực thi bổn phận của một bên đối tác
- Sự tin cậy của đối tác về dịch vụ dấu thời gian không được đáp ứng trong một số trường hợp.
- Lỗi của đối tác tin cậy trong việc kiểm tra trạng thái của tài khoản để xác dịnh tài kharon đã hết hạn hay bị thu hồi.

Thỏa thuận với đối tác tin cậy sẽ bao gồm thêm một số nghĩa vụ khác.

IX.9. Thời hạn

IX.9.1. Thời hạn

CPS bắt đầu có hiệu lực khi được công bố từ kho lưu trữ của dịch vụ FPT TSA. Các điều sửa đổi bổ sung cho CPS này cũng bắt đầu có hiệu lực khi có sự công bố từ kho lưu trữ của dịch vụ FPT TSA.

IX.10. Sự kết thúc

IX.10.1. Sự kết thúc

CPS này được bổ sung, sửa đổi sẽ vẫn giữ hiệu lực cho đến khi được thay thế bởi một văn bản mới.

IX.10.2. Ảnh hưởng của sự kết thúc và những tồn tại

Khi CPS hết hiệu lực, các thành phần của dịch vụ FPT TSA sẽ không bị giới hạn bởi các điều khoản còn hiệu lực của chứng thư đã được ban hàng.

IX.11. Thông báo riêng và thỏa thuận giữa các bên

FPT sẽ sử dụng các biện pháp thương mại để giao thiệp giữa các bên, hoặc sử dụng các thỏa thuận trong hợp đồng ký hết khi một điều khoản nào đó được ghi rõ trong hợp đồng.

IX.12. Sự sửa đổi

IX.12.1. Các thủ tục sửa đổi

Những sửa đổi của CPS sẽ được thực hiện bởi Cấp quản lý chính sách có thẩm quyền của FPT. Những điều sửa đổi có thể ở dạng tài liệu chứa tất cả những điều sửa đổi cho CPS hoặc ở dạng cập nhật.

IX.13. Các trường hợp cần sửa đổi nhận diện đối tượng (OID)

Nếu cần thiết, FPT có thể thay đổi OID cho các chính sách chứng thư tương ứng với từng cấp chứng thư. Nếu không, việc sửa đổi sẽ không bao gồm việc sửa đổi OID.

IX.13.1. Cách thức và thời hạn thông báo

FPT có quyền quyết định việc thay đổi là cần thiết hay không cần thiết.

FPT tập hợp những thay đổi về CPS từ các thành phần tham gia vào dịch vụ FPT TSA. Nếu FPT cho rằng một sự thay đổi nào đó nên làm thì sẽ đề xuất thực

hiện sự thay đổi đó. FPT sẽ đưa ra thông báo về sự thay đổi đó phù hợp với mục này.

Trái ngược với một số điều trong CPS, nếu FPT cho rằng sự thay đổi CPS là cần thiết để ngăn chặn sự xâm phạm đến an toàn của dịch vụ FPT TSA, FPT sẽ có quyền thay đổi CPS. Công bố về sự thay đổi sẽ ngay lập tức có hiệu lực. Sau khi công bố, FPT sẽ thông báo tới các bên liên quan.

15.1.1.1. Thời điểm đưa ra sự sửa đổi

Thời gian sửa đổi là 15 nagỳ kể từ ngày được công bố trên kho lưu trữ của dịch vụ FPT TSA. Bất kỳ ai tham gia vào dịch vụ FPT TSA cũng có quyền đề xuất ý kiến tới FPT cho đến lúc hết thời gian sửa đổi.

16.1.1.1. Cơ chế xử lý các sửa đổi

FPT sẽ xem xét tất cả các đề xuất liên quan đến vấn đề sửa đổi bổ sung. FPT có thể:

(a) Cho phép các đề xuất có hiệu lực mà không cần sửa đổi.

(b) Sửa đổi các đề xuất và tái bản nếu cần.

(c) Hủy bỏ những đề xuất sửa đổi.

FPT có quyền hủy bỏ các đề xuất sửa đổi, và đưa ra ghi chú trong phần tài liệu về "Cập nhật và các ghi chú thực thi" của FPT TSA. Những sửa đổi có hiệu lực sau khi hết hạn sửa đổi.

IX.14. Thủ tục tranh chấp

IX.14.1. Thủ tục tranh chấp giữa FPT, cộng tác và thuê bao

Việc giải quyết tranh chấp giữa FPT, các bên và thuê bao phải tuân thủ theo các điều khoản được ghi trong hợp đồng.

IX.14.2. Thủ tục tranh chấp giữa thuê bao và đối tác tin cậy

Những cuộc tranh chấp có liên quan đến dịch vụ FPT TSA yêu cầu thời gian đàm phán là 60 ngày, sau đó có thể được đưa lên toà án có đủ quyền để xử lý.

IX.15. Luật quản trị

Tuân theo luật của nước CHXHCN Việt Nam và luật Thương mại điện tử của Việt Nam, các đối tượng sẽ bị cưỡng chế thực hiện, xây dựng, giải thích và hợp lệ hóa CPS này, không quan tâm tới sự lựa chọn các văn bản luật khác, và không yêu cầu thiết lập mối quan hệ thương mại ở Việt Nam. Việc lựa chọn luật này

nhằm đảm bảo tính thống nhất của các thủ tục và giải thích cho những người tham gia dịch vụ FPT TSA, bất kể họ ở đâu.

CPS này tùy thuộc vào hệ thống các điều luật, quy tắc, các điều chỉnh, quy định, các sắc lệnh và mệnh lệnh thuộc phạm vi địa phương, bang, quốc gia, nhưng không giới hạn hay hạn chế trong lĩnh vực xuất khẩu hay nhập khẩu phần mềm, phần cứng và các thông tin kỹ thuật.

IX.16. Sự tuân thủ luật

CPS này tùy thuộc vào hệ thống các điều luật, quy tắc, các điều chỉnh, quy định, các sắc lệnh và mệnh lệnh thuộc phạm vi địa phương, bang, quốc gia, nhưng không giới hạn hay hạn chế cho lĩnh vực xuất khẩu phần mềm, phần cứng và các thông tin kỹ thuật.

IX.16.1. Trách nhiệm

Trách nhiệm của các bên được quy định và giới hạn theo hợp đồng đã ký kết.

IX.16.2. Tính độc lập của các điều khoản

Trong trường hợp một điều khoản hay sự sửa đổi bổ sung của CPS được giữ lại không thể thi hành được bởi một phiên tòa hay một cuộc xét xử có thẩm quyền, phần còn lại của CPS vẫn có hiệu lực.

IX.16.3. Sự thực thi (quyền ủy nhiệm và quyền khước từ)

Bất kỳ một bên nào chiếm ưu thế trong những tranh cãi nảy sinh ngoài hợp đồng đều được quyền ủy nhiệm hoặc quyền khước từ do sự vi phạm một trong các điều khoản trong hợp đồng.

IX.16.4. Chính sách bắt buộc thực thi

Trong phạm vi luật pháp cho phép, thỏa thuận của thuê bao và thỏa thuận bên liên quan bắt buộc phải tuân theo các điều khoản bảo vệ dịch vụ FPT TSA.

IX.17. Các quy định khác

IX.17.1. Nhiệm vụ, vai trò, trách nhiệm của hệ thống FPT TSA

Xem thêm mục I.3.1.

17.1.1.1. Quy trình hoạt động.

Xem thêm mục I.3.3.

18.1.1.1. Kết thúc RA, TSA.

Xem thêm mục VI.4.

19.1.1.1. Lệ phí, bảo lãnh, trách nhiệm tài chính và bồi thường.

Xem thêm mục IX.1., IX.2., IX.6. và IX.7.

20.1.1.1. Trách nhiệm báo cáo thông tin với Trung tâm Chứng thực điện tử quốc gia.

FPT cam kết tuân thủ đầy đủ trách nhiệm báo cáo thông tin lên Trung tâm Chứng thực điện tử quốc gia với các yêu cầu được nêu rõ.

IX.17.2. Nhiệm vụ, vai trò và trách nhiệm của thuê bao

21.1.1.1. Định nghĩa.

Xem thêm mục I.3.2.

22.1.1.1. Nhận dạng và xác thực.

Xem thêm mục III.1.2. và III.2.

23.1.1.1. Cam kết và nghĩa vụ của thuê bao.

Xem thêm mục IV.7.

24.1.1.1. Lệ phí và bồi thường

Xem thêm mục IX.1. và IX.8