CÔNG TY CỔ PHẦN CHỮ KÝ SỐ FASTCA

----------0O0----------

QUY CHẾ CHỨNG THỰC

DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG (FASTCA)

Hà nội, 02/2020

MỤC LỤC

THUẬT NGỮ VÀ TỪ VIẾT TẮT

#	Định nghĩa/ Từ viết tắt	Giải thích
1.	3DES (Triple DES)	Thuật toán mã hóa dữ liệu được cải tiến từ DES bằng các thêm các vòng mã hóa.
2.	AES (Advanced Encryption Standard)	Chuẩn mã hóa dữ liệu nâng cao được phát triển nhằm thay thế DES.
3.	CA (Certification Authority)	Tổ chức chứng thực
4.	CP (Certificate Policy)	Chính sách chứng thư số
5.	CPS (Certificate Practice Statement)	Quy chế chứng thực
6.	CRL (Certificate Revocation List)	Danh sách các chứng thư số bị thu hồi
7.	DC (Digital Certificate)	Chứng thư số
8.	DES (Data Encription Standard)	Chuẩn mã hóa dữ liệu đối xứng
9.	FastCA (Fast Certification Authority)	Tổ chức cung cấp dịch vụ chứng thực chữ ký số FastCA
10.	HSM (Hardware Security Module)	Thiết bị phần cứng bảo mật dùng để tạo, lưu trữ và bảo vệ các khóa sử dụng trong mã hóa. Trong hệ thống PKI, HSM thường được dùng để bảo vệ các cặp khóa quan trọng như các cặp khóa của RootCA và SubCA.
11.	LDAP (Lightweight Directory Access Protocol)	Giao thức truy nhập thư mục chứng thư số
12.	PKI (Khóa công khai Infrastructure)	Hạ tầng khoá công khai
13.	OCSP (Online Certificate Status Protocol)	Giao thức kiểm tra trạng thái chứng thư số trực tuyến
14.	RA (Registration Authority)	Cơ quan đăng ký
15.	RootCA (Root Certification Authority)	Hệ thống cấp phát chứng thư số gốc
16.	RSA	Thuật toán mật mã khóa công khai RSA, dùng để sinh cặp khóa
17.	SubCA (Subordinate Certification Authority)	Hệ thống cấp phát chứng thư số con
18.	USB Token	Thiết bị lưu trữ khóa của người dùng trong hệ thống PKI (USB Token hoặc Smartcard…)

I- GIỚI THIỆU

I.1 Tổng quan

FastCA là tên gọi của dịch vụ chứng thực chữ ký số công cộng do Công ty cổ phần chữ ký số FastCA cung cấp. Các quy định về chính sách chứng thư số của dịch vụ FastCA được trình bày trong tài liệu này gồm có các quy trình quản lý cấp phát, gia hạn, thu hồi, tạm dừng, khôi phục, hủy bỏ chứng thư số cho các thuê bao là cá nhân, tổ chức doanh nghiệp,...

Bản quy chế chứng thực mô tả các thủ tục và cơ chế thực thi của nhà cung cấp chứng thư số của hệ thống FastCA: mô tả các điều khoản và điều kiện thực hiện của nó nhằm cung cấp tới các cơ quan quản lý cũng như người sử dụng những mô tả rõ ràng về các dịch vụ của hệ thống và các điều kiện để sử dụng chúng. Ngoài ra, nó cũng đưa ra những đảm bảo về mặt an toàn bảo mật và an toàn thông tin của hệ thống FastCA và các dịch vụ chứng thực chữ ký số cung cấp cho khách hàng.

Hệ thống FastCA được tuân thủ theo Nghị định 130/2018/NĐ-CP của Chính phủ quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số và Thông tư 06/2015/TT-BTTTT quy định danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số bắt đầu có hiệu lực.

I.2 Tên tài liệu và nhận dạng

Tài liệu này được gọi là Quy chế chứng thực (CPS) của Nhà cung cấp dịch vụ chứng thư số FastCA. Bản quy chế này được chấp nhận bởi đơn vị quản lý của Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia (RootCA) là Trung tâm Chứng thực điện tử Quốc gia (NEAC), Bộ thông tin và truyền thông. Các chứng thư số do FastCA phát hành có số Object Identifier (OID), do Trung tâm NEAC cấp để chỉ ra đường dẫn của bản CPS này.

I.3 Đối tượng tham gia

- Hệ thống dịch vụ chứng thực chữ ký số Quốc gia do Bộ Thông tin và Truyền thông quản lý là hệ thống RootCA Quốc gia.
- Hệ thống FastCA là hệ thống CA cấp dưới của RootCA Quốc gia, được Bộ Thông tin và Truyền thông cấp phép hoạt động theo quy định của pháp luật.
- Bộ phận xử lý đăng kí RA (Registration Authority – RA): Chịu trách nhiệm tiếp nhận các yêu cầu đăng ký, hủy bỏ, tạm dừng, thu hồi, gia hạn của thuê bao và kiểm tra, xác thực các yêu cầu này. Đây cũng có thể coi là các đại lý của hệ thống FastCA, các chức năng chính:

- Xác nhận nhận dạng của một cá nhân, tổ chức, doanh nghiệp.
- Khởi tạo quá trình cấp, gia hạn, thu hồi, tạm dừng chứng thư số với CA trên vai trò đại diện cho người dùng cuối.
- Có thể hỗ trợ tạo khoá cho người dùng cuối trên thiết bị lưu khóa PKI Token.
- Thực hiện chức năng quản lý vòng đời của chứng thư số.

– Các thực thể cuối (End Entities – EE): là những thuê bao sẽ sử dụng dịch vụ chứng thực chữ ký số của hệ thống FastCA. Thực thể có thể là người sử dụng, tổ chức, doanh nghiệp hoặc một chương trình phần mềm, thiết bị, dịch vụ web, thư điện tử. Có thể sở hữu chứng thư số, hoặc truy vấn đến chứng thư số. Các nhóm thực thể cuối bao gồm:

– Thuê bao (Subscriber) là một người, một tổ chức, hay một chương trình phần mềm, thiết bị phần cứng, dịch vụ web, thư điện tử.

– Đối tác tin tưởng (Relying Party) là một người, một tổ chức, hay một thực thể sử dụng chứng thư số của hệ thống FastCA và các thông tin khác từ kho lưu trữ chứng thư số để xác thực chứng thư số và xác thực chữ ký số của thuê bao.

I.4 Sử dụng chứng thư

I.4.1 Sử dụng chứng thư số hợp lệ

I.4.1.1 Chứng thư số của FastCA

Chứng thư số của FastCA được cấp bởi RootCA quốc gia với mục đích sử dụng chính như sau:

digitalSignature, nonrepudiation, keyAgreement, dataEncipherment và keyEncipherment (các trường trong Key Usage của chứng thư số).

Chứng thư số FastCA được sử dụng để ký phát hành chứng thư số cho thuê bao, các danh sách hủy bỏ CRLs của FastCA, chứng thư số cho hệ thống kiểm tra chứng thư số trực tuyến OCSP; để xác thực các chứng thư số do FastCA cấp và xác thực dữ liệu đã ký số.

I.4.1.2 Các chứng thư số do FastCA cung cấp

FastCA cung cấp các chứng thư số cho khách hàng thuê bao, gồm:

– Chứng thư số cho cá nhân: chứng thư được sử dụng với mục đích với định danh cá nhân. Phục vụ ký số, xác thực tài liệu điện tử, xác thực đăng nhập, SSL, mail và giao dịch điện tử trong lĩnh vực công cộng.

- Chứng thư số cho tổ chức: chứng thư được cấp cho một tổ chức, doanh nghiệp sử dụng với mục đích với định danh tổ chức. Phục vụ ký số, đại diện tổ chức, doanh nghiệp giao dịch điện tử trong lĩnh vực công cộng (B2G, B2B, B2C).

Sử dụng trên các thiết bị:

- PKI Token hoặc PKI Token đạt chuẩn FIPS PUB 140-2 tối thiểu level 2.
- HSM đạt chuẩn FIPS PUB 140-2 tối thiểu level 3.

Định dạng theo chuẩn X509, hàm băm SHA-256, cặp khóa RSA có độ dài 2048-bit, 4096-bit tùy theo yêu cầu của khách hàng thuê bao.

Thời gian có hiệu lực của các chứng thư số thông thường sẽ chia theo các gói: 1 năm, 2 năm, 3 năm hoặc theo nhu cầu của khách hàng nhưng không vượt quá thời hạn của chứng thư số SubCA của FastCA được cấp.

I.4.2 Các trường hợp bị cấm

Sử dụng chứng thư số sai mục đích, không được nêu ở mục I.1.4.1 theo các thuộc tính của chứng thư (Key Usage) sẽ bị cấm.

I.5 Quản lý quy chế chứng thực

I.5.1 Tổ chức quản lý quy chế chứng thực

Công ty FastCA là tổ chức viết và cập nhật Quy chế chứng thực.

Quy chế chứng thực có thể được tải tại địa chỉ http://fastca.vn/download/CPS

I.5.2 Thông tin liên hệ

Địa chỉ: Tầng 6, tòa nhà MD Complex, số 68 Nguyễn Cơ Thạch, phường Cầu Diễn, quận Nam Từ Liêm, thành phố Hà Nội, Việt Nam;

Email: info@fastcavn

Website: www.fastca.vn

I.5.3 Phạm vi, hiệu lực của Quy chế chứng thực

- Quy chế chứng thực này mô tả quyền và nghĩa vụ của các bên liên quan, vấn đề pháp luật và đặc điểm hạ tầng kỹ thuật của hệ thống FastCA.
- Quy chế đề cập đến các thỏa thuận giữa FastCA và các thành viên trong miền quản lý của FastCA, áp dụng cho RA, thuê bao, người nhận.
- Quy chế chứng thực này có hiệu lực trong toàn bộ thời gian cung cấp dịch vụ của FastCA.

I.5.4 Thủ tục phê duyệt Quy chế chứng thực

Công ty FastCA sẽ phê duyệt Quy chế chứng thực và phát hành quy chế trên website.

Phiên bản được cập nhật có tính ràng buộc đối với tất cả thuê bao bao gồm thuê bao và các bên dựa vào các chứng thư số đã được ban hành theo một phiên bản trước của Quy chế chứng thực.

I.6 Định nghĩa và từ viết tắt

(Chi tiết trong Danh mục từ viết tắt)

II- Các trách nhiệm công bố và lưu trữ chứng thư số

II.1 Lưu trữ

- CPS:

  http://fastca.vn/download/CPS

- Chứng thư số của FastCA:

  http://fastca.vn/download/fastca.crt

- Chứng thư số của thuê bao:

  Website: https://cts.fastca.vn/

- CRL:

  http://crl.fastca.vn/fastca.crl

- OCSP:

  http://ocsp.fastca.vn/

II.2 Công bố thông tin chứng thư số

Các thông tin cần được công bố bao gồm:

- CPS trên toàn hệ thống
- Chứng thư của CA và thuê bao
- Danh sách chứng thư số bị thu hồi (CRL)

Kho lưu trữ chứng thư của FastCA sử dụng giao diện web, cho phép đối tác tin cậy thực hiện các yêu cầu truy vấn trực tuyến về thu hồi chứng thư hay truy vấn thông tin trạng thái các chứng thư.

II.3 Thời gian công bố và bàn giao chứng thư số

Tối đa 1 tuần làm việc thuê bao có thể nhận được chứng thư số kể từ khi đăng ký.

Khách hàng cần phải ký xác nhận về tính chính xác của thông tin trên chứng thư số theo mẫu "Giấy xác nhận thông tin khách hàng" mà FastCA cung cấp khi khách hàng tiếp nhận usb token chứa chứng thư số.

Chứng thư số của thuê bao được công bố tối đa trong 1 giờ sau khi thuê bao gửi xác minh tính chính xác của thông tin trên chứng thư số về FastCA.

Danh sách thu hồi chứng thư số CRL được cập nhật chu kỳ tối thiểu 1 ngày cập nhật 1 lần.

II.4 Quyền truy cập kho lưu trữ chứng thư

- Cập nhật CPS: chỉ FastCA mới có quyền cập nhật CPS.
- Đối với thuê bao, không giới hạn truy cập tới CPS, CPS, chứng thư, thông tin chứng thư, hay CRLs. FastCA yêu cầu người truy nhập phải tuân theo các thỏa thuận với đối tác tin cậy hoặc thỏa thuận sử dụng CRLs. Thỏa thuận này như điều kiện để truy cập chứng thư, thông tin chứng thư hay CRLs. FastCA 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.1 Đặt tên thuê bao trong chứng thư số

III.1.1 Kiểu của tên

Phần sau đây định nghĩa cấu trúc đặt tên theo Quy chế chứng thực.

- Đối với chứng thư số cho cá nhân, thành phần tên chung CN của đối tượng tên phân biệt định danh duy nhất thuê bao như sau:
    - UserID= CMND:[số chứng minh nhân dân] hoặc HC:[số hộ chiếu] hoặc CCCD:[số thẻ căn cước công dân]
    - CN= Họ và Tên (Tên của thuê bao được cấp chứng thư số)
    - ST= Tên của tỉnh/TP nơi sống/làm việc của thuê bao bằng tiếng Việt, có dấu, các chữ cái đầu viết hoa
    - C= VN
    - Email = abc@xyz.com [thư điện tử của thuê bao – mục này là không bắt buộc]
- Đối với chứng thư số cho tổ chức, thành phần tên chung CN của đối tượng tên phân biệt định danh duy nhất thuê bao như sau:
    - UserID= MST:[mã số thuế] hoặc MNS:[mã quan hệ ngân sách] hoặc BHXH:[mã số bảo hiểm xã hội]
    - CN= Họ và Tên (Tên của thuê bao được cấp chứng thư số)
    - ST= Tên của tỉnh/TP nơi sống/làm việc của thuê bao bằng tiếng Việt, có dấu, các chữ cái đầu viết hoa
    - C=VN
    - Email = abc@xyz.com [thư điện tử của thuê bao – mục này là không bắt buộc]
- Đối với các chứng thư số khác theo quy định của Bộ Thông tin và Truyền thông.

III.1.2 Tính duy nhất của tên thuê bao

Tên thuê bao của dịch vụ FastCA sẽ là duy nhất với một cấp chứng thư xác định trong miền của dịch vụ FastCA. Một thuê bao có thể có hai hoặc nhiều chứng thư có cùng tên.

III.1.3 Nhận dạng, xác thực và vai trò của thương hiệu

Đối tượng đăng ký chứng thư số không được sử dụng các tên đã được sở hữu và đăng ký bởi tổ chức, cá nhân theo quy định của pháp luật.

Trong trường hợp cần thiết, FastCA có thể yêu cầu thuê bao cung cấp bằng chứng, tài liệu chứng minh quyền sở hữu đối với tên đăng ký.

FastCA không chịu trách nhiệm trong mọi tranh chấp về tên của đối tượng đăng ký. FastCA có quyền chấm dứt hoặc tạm dừng chứng thư số của thuê bao trong trường hợp có tranh chấp xảy ra.

III.2 Xác minh đề nghị cấp chứng thư số lần đầu

III.2.1 Xác minh thuê bao cá nhân

Bộ phận đăng ký RA kiểm tra nhận dạng của người xin cấp chứng thư dựa trên thủ tục để nhận dạng của chính phủ, như hộ chiếu, hoặc giấy phép lái xe...

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 chứng thư số từ FastCA:

- Hộ chiếu hoặc chứng minh thư nhân dân hoặc thẻ căn cước công dân
- Bản sao giấy khai sinh có công chứng.
- 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.

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

Đối với tổ chức, doanh nghiệp, FastCA 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 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 chứng thư đưa ra, rằng tổ chức đó đã phê duyệt đơn xin cấp chứng thư. Khi một chứng thư bao gồm tên một cá nhân là một đại diện hợp pháp tổ chức, việc cá nhân là đại diện cho một tổ chức cũng phải được xác nhận. Khi tên miền hoặc địa

chỉ thư điện tử có trong chứng thư, tổ chức có toàn quyền sử dụng đối với tên miền hay địa chỉ thư điện tử đó.

III.2.3 Những thông tin của thuê bao không được xác thực

Thông tin của thuê bao không được xác thực gồm có:

- Các đơn vị, phòng ban thuộc tổ chức (Organization Unit)
- Bất kì một thông tin nào được coi là không cần xác thực trong chứng thư.

III.3 Xác minh đề nghị thay đổi cặp khóa

Trước khi chứng thư hết hạn cần phải đăng ký để có được một chứng thư mới nhằm duy trì sự liên tục của việc sử dụng chứng thư. Các bộ phận đăng ký RA yêu cầu thuê bao phải xin cấp một cặp khóa mới để thay thế cặp khóa đã hết hạn (gọi là "Re-key"), trong một số trường hợp có thể yêu cầu một chứng thư mới thay thế cho một cặp khóa đã tồn tại (gọi là "Renewal").

III.3.1 Quy trình nhận diện và xác thực thủ tục cấp lại khoá (Re-key)

Thủ tục thay đổi cặp khóa đảm bảo rằng cá nhân hay một tổ chức muốn cấp lại khóa cho chứng thư là chủ thuê bao của chứng thư đó.

Khi thuê bao có yêu cầu tiếp tục sử dụng chứng thư số thì chứng thư mới sẽ được tự động cấp phát. Sau khi cấp lại khoá, FastCA hoặc bộ phận đăng ký RA sẽ xác nhận lại việc định danh của thuê bao sao cho phù hợp với các yêu cầu xác thực và định danh của đơn xin cấp chứng thư ban đầu.

III.3.2 Nhận diện và xác thực việc cấp lại khoá sau khi đã bị thu hồi (Renewal)

Các trường hợp không được cấp lại khoá sau khi bị thu hồi.

- Chứng thư số vi phạm hợp đồng giữa thuê bao với FastCA.
- Phát hiện có sự thiếu sót trong việc thẩm định các giấy tờ khi đăng ký chứng thư số (Chứng minh thư hoặc hộ chiếu giả, hộ khẩu không hợp lệ…)
- Chứng thư bị thu hồi vì đã sử dụng vào các mục đích trái pháp luật…

Quá trình khôi phục chứng thư của một tổ chức là hoàn toàn có thể được phép, miễn là quá trình khôi phục đảm bảo rằng tổ chức yêu cầu khôi phục chứng thư thực sự là khách hàng đã sử dụng chứng thư đó, đồng thời lý do khôi phục chứng thư là hợp lệ. Ví dụ: lộ khóa bí mật, mất thiết bị lưu trữ khóa bí mật, lộ khóa của CA… Chứng thư của một tổ chức được khôi phục sẽ chứa cùng các thông tin đặc trưng như của chứng thư cũ.

Việc khôi phục chứng thư của một cá nhân bị thu hồi chứng thư cũng cần đảm bảo rằng người đang yêu cầu được khôi phục chính là khách hàng đang sử dụng chứng thư đó.

III.4 Xác minh đề nghị thu hồi chứng thư số

Khi có yêu cầu thu hồi chứng thư số, FastCA phải kiểm tra và xác thực đúng nếu có yêu cầu sự huỷ bỏ chứng thư từ thuê bao của dịch vụ FastCA. Các thủ tục được dùng gồm:

- Nhận các thông báo từ thuê bao về yêu cầu thu hồi
- Xác minh thuê bao thông báo thu hồi, xác minh sự sở hữu chứng thư số cần thu hồi của thuê bao (qua điện thoại, email).
- Thông báo tới thuê bao các lý do chắc chắn về cấp chứng thư mà các 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.

IV - Các yêu cầu đối với vòng đời chứng thư số của thuê bao

IV.1 Cấp chứng thư số cho thuê bao

FastCA thực hiện thủ tục cấp chứng thư số cho các khách hàng cá nhân hoặc tổ chức doanh nghiệp dựa trên yêu cầu của khách hàng. Hồ sơ cấp chứng thư số của thuê bao:

- Đơn cấp chứng thư số theo mẫu của FastCA.
- Giấy tờ kèm theo bao gồm:

  + Đối với cá nhân: bản sao chứng minh nhân dân hoặc căn cước công dân hoặc hộ chiếu;

  + Đối với tổ chức: bản sao quyết định thành lập hoặc quyết định quy định về chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức hoặc giấy chứng nhận đăng ký doanh nghiệp hoặc giấy chứng nhận đầu tư; chứng minh nhân dân, hoặc căn cước công dân hoặc hộ chiếu của người đại diện theo pháp luật của tổ chức.

  (Cá nhân, tổ chức có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc nộp bản sao xuất trình kèm bản chính để đối chiếu).

FastCA cấp chứng thư số cho thuê bao sau khi kiểm tra được các nội dung sau đây:

- Thông tin trong hồ sơ đề nghị cấp chứng thư số của thuê bao là chính xác;
- Khóa công khai trên chứng thư số sẽ được cấp là duy nhất và cùng cặp với khóa bí mật của tổ chức, cá nhân đề nghị cấp chứng thư số.

FastCA công bố chứng thư số đã cấp cho thuê bao trên cơ sở dữ liệu về chứng thư số của mình sau khi có xác nhận của thuê bao về tính chính xác của thông tin trên chứng thư số đó; thời hạn để công bố chậm nhất là 24 giờ sau khi đã có xác nhận của thuê bao; trừ trường hợp có thỏa thuận khác.

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

Những người sau đây có thể đệ trình đơn xin cấp chứng thư số:

- Các thuê bao có nhu cầu xin chứng thư cho mục đích ký số và xác thực trong các giao dịch điện tử.
- Đại diện của các tổ chức, doanh nghiệp.
- Các đại lý đăng ký làm RA cho FastCA.

IV.1.2 Tiến trình xử lý và trách nhiệm của thuê bao chứng thư.

Thuê bao chứng thư sẽ kê khai vào các phần có liên quan bao gồm cả phần đại diện và phần đảm bảo và chịu trách nhiệm về quá trình xử lý bao gồm:

- Hoàn thành bảng kê khai và cung cấp các thông tin đúng, chính xác.
- Tự tạo khoá hoặc yêu cầu FastCA tạo cặp khoá trên thiết bị PKI Token an toàn.
- Cung cấp khoá công khai đến RA, đến trung tâm xử lý và chứng minh sự tương thích giữa khoá bí mật và khoá công khai cho trung tâm xử lý.

IV.1.2.1 Chứng thư số của RA

Người đăng ký chứng thư số cho RA sẽ làm hợp đồng với FastCA. RA sẽ cung cấp tài liệu chứng tỏ nhận dạng và cung cấp các thông tin trong hợp đồng trong quá trình ký hợp đồng. Trong quá trình ký hợp đồng, đầu tiên là nghi lễ sinh khóa tạo ra cặp khóa cho RA, sau đó người yêu cầu cấp chứng thư số sẽ hợp tác với FastCA để xác định tên đặc trưng phù hợp và thông tin còn lại trong chứng thư số sẽ được tạo ra.

IV.2 Xử lý đơn xin cấp chứng thư

IV.2.1 Chức năng nhận biết và xác thực

Một RA sẽ nhận biết và chứng thực các thông tin khách hàng theo mục III.2

IV.2.2 Phê duyệt hoặc từ chối các đơn xin cấp chứng thư

RA sẽ phê chuẩn một chứng thư khi tuân theo các tiêu chuẩn sau đây:

- Nhận biết và xác thực các thông tin về khách hàng theo mục III.2.
- Phí dịch vụ đã thanh toán.

RA sẽ từ chối 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 chứng thư cho thuê bao có thể gây bất lợi cho FastCA.

IV.2.3 Thời gian xử lý các đơn xin cấp chứng thư

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

IV.3 Sinh chứng thư số

IV.3.1 Các hành động của FastCA trong quá trình sinh chứng thư số

Một chứng thư số được tạo và cấp sau khi FastCA chấp nhận một yêu cầu cấp chứng thư số hoặc sau khi nhận được một yêu cầu cấp chứng thư số của RA. FastCA tạo và cấp cho người yêu cầu cấp chứng thư số một chứng thư số dựa trên những thông tin trong yêu cầu cấp chứng thư số sau khi yêu cầu này được chấp nhận.

IV.3.2 Thông báo cho thuê bao khi CA đã tạo xong chứng thư số

FastCA cấp các chứng thư số cho thuê bao sẽ (trực tiếp hoặc gián tiếp thông qua RA) thông báo thuê bao đã tạo chứng thư số qua thư điện tử hoặc tin nhắn và cho phép thuê bao tải chứng thư số về từ trang web hoặc qua thư điện tử.

IV.4 Công bố chứng thư

IV.4.1 Chấp nhận chứng thư

Khi thuê bao tải về và cài đặt chứng thư từ thông báo của FastCA, điều này chứng minh việc chấp thuận của thuê bao đó đối với chứng thư số

Khi thuê bao không trả lời thông báo của FastCA trong khoảng thời gian quy định. Chứng thư coi như được khách hàng chấp thuận.

IV.4.2 Công khai chứng thư của FastCA

Trung tâm xử lý công bố chứng thư số mà họ đã phát hành đồng thời có trách nhiệm đăng thông tin về chứng thư mới của thuê bao tới kho lưu trữ LDAP và website của FastCA.

IV.4.3 Thông báo việc phát hành chứng thư đến các đối tượng khác

FastCA có trách nhiệm gửi thông báo cho RA về việc phát hành chứng thư.

IV.5 Tạo khóa và phân phối khóa cho thuê bao

- Tổ chức, cá nhân đề nghị cấp chứng thư số có thể tự tạo cặp khóa hoặc yêu cầu bằng văn bản để FastCA tạo cặp khóa cho mình.
- Trường hợp tổ chức, cá nhân đề nghị cấp chứng thư số tự tạo cặp khóa, FastCA cần đảm bảo chắc chắn rằng tổ chức, cá nhân đó đã sử dụng thiết bị theo đúng tiêu chuẩn quy định của Thông tư 06/2015/TT-BTTTT để tạo ra và lưu trữ cặp khóa.
- Trường hợp FastCA tạo cặp khóa thì phải đảm bảo sử dụng các phương thức an toàn để chuyển giao khóa bí mật đến tổ chức, cá nhân đề nghị cấp chứng thư số và chỉ được lưu bản sao của khóa bí mật khi tổ chức, cá nhân đề nghị cấp chứng thư số có yêu cầu bằng văn bản.

IV.5.1 Cách sử dụng chứng thư và khoá bí mật của thuê bao

Việc sử dụng khoá bí mật tương ứng với khoá công khai trong chứng thư chỉ được cho phép khi thuê bao đồng ý với bản thoả thuận thuê bao và thuê bao chấp nhận chứng thư. Chứng thư sẽ được sử dụng hợp pháp dựa theo bản thoả thuận thuê bao với các điều khoản có trong CPS của nhà cung cấp chứng thư. Chứng thư sử dụng phải khớp với quy định tại trường *KeyUsage* có trong chứng thư (ví dụ: KeyUsage quy định chứng thư số chỉ dùng để ký thì không được dùng chứng thư số này để mã dữ liệu).

Thuê bao có trách nhiệm bảo vệ khoá bí mật khỏi việc truy cập bất hợp pháp và sẽ không được sử dụng khoá bí mật khi chứng thư hết hạn hay khi bị thu hồi chứng thư.

IV.5.2 Cách sử dụng chứng thư và khoá công khai của các đối tác tin cậy

Các đối tác tin cậy phải đồng ý với các điều khoản trong bản thoả thuận đối tác tin cậy để tin cậy chứng thư.

Tính tin cậy của chứng thư phải phù hợp với từng hoàn cảnh cụ thể. Nếu hoàn cảnh chỉ ra rằng phải cần thêm sự đảm bảo, thì đối tác tin cậy phải đạt được sự bảo đảm cần thiết.

Trước khi tin cậy, các đối tác tin cậy sẽ đánh giá một cách độc lập:

- Sử dụng chứng thư một cách phù hợp và xác định rằng chứng thư sẽ được sử dụng cho mục đích mà nó không bị ngăn cấm hoặc bị giới hạn bởi CPS, FastCA và các RA không có trách nhiệm đánh giá việc sử dụng chứng thư.
- Chứng thư đang sử dụng theo đúng phần mở rộng của trường KeyUsage trong chứng thư.
- Trạng thái của chứng thư và tất cả các CA trong mắt xích chịu trách nhiệm phát hành chứng thư phải còn hiệu lực. Nếu bất cứ chứng thư nào trong chuỗi chứng thư bị thu hồi, đối tác tin cậy sẽ điều tra xem tính tin cậy của chữ ký số trong chứng thư của thuê bao để việc thu hồi chứng thư là hợp lý.
- Giả thiết rằng việc sử dụng chứng thư là hợp lý, các đối tác tin cậy sẽ sử dụng phần mềm thực hiện việc xác thực chữ ký số hoặc các phương pháp khác như một điều kiện để tin cậy. Các phương pháp này bao gồm việc định danh một mắt xích chứng thư và xác thực các chữ ký số trên tất cả các chứng thư trong chuỗi chứng thư.

IV.6 Gia hạn chứng thư số cho thuê bao

Gia hạn chứng thư số là sự cấp một chứng thư số mới cho thuê bao khi chứng thư số cũ đã hết (hoặc sắp hết) thời hạn sử dụng. Thuê bao có thể chọn việc gia hạn chứng thư số giữ nguyên cặp khóa hoặc thay đổi cặp khóa mới.

- Ít nhất là 30 ngày trước ngày hết hạn của chứng thư số, thuê bao có quyền yêu cầu gia hạn chứng thư số.
- Khi nhận được yêu cầu gia hạn của thuê bao, FastCA có nghĩa vụ hoàn thành các thủ tục gia hạn chứng thư số trước khi hết hiệu lực.
- Trường hợp thay đổi khóa công khai trên chứng thư số được gia hạn, thuê bao phải yêu cầu rõ; việc tạo khóa, phân phối khóa và công bố chứng thư số được gia hạn thực hiện theo các quy định tại các Điều 24 và 25 của Nghị định 130/2018/NĐ-CP.

IV.6.1 Khóa công khai mà đối tác tin tưởng giữ và phạm vi sử dụng

Trước khi hết hạn, thuê bao cần phải gia hạn một chứng thư số mới để duy trì sử dụng chứng thư số. Một chứng thư số cũng có thể được gia hạn sau khi hết hạn.

IV.6.2 Ai có thể yêu cầu gia hạn

Chỉ người đăng ký của một chứng thư số cá nhân hay được ủy quyền đại diện cho tổ chức mới có thể gia hạn.

IV.6.3 Xử lý yêu cầu gia hạn

Thủ tục gia hạn đảm bảo rằng cá nhân hay tổ chức đang muốn gia hạn một chứng thư số là chủ nhân của nó.

Thuê bao phải được xác minh cá nhân để chứng minh được quyền sở hữu khóa cá nhân (Khóa bí mật). Thuê bao chọn và đệ trình với thông tin đã được cung cấp. Sau khi gia hạn một chứng thư số, nếu một thuê bao vượt qua được các kiểm tra xác minh và các thông tin này chưa bị thay đổi, một chứng thư số gia hạn tự động được tạo ra.

Ngoài thủ tục này hay các thủ tục duyệt khác, những yêu cầu cho xác thực yêu cầu cấp chứng thư số gốc sẽ được sử dụng để gia hạn.

IV.6.4 Thông báo về sự tạo ra chứng thư số mới cho thuê bao

Thông báo về sự gia hạn chứng thư số cũng giống như thông báo khi chứng thư số được cấp mới.

IV.6.5 Sự chấp nhận chứng thư số gia hạn

Tương tự như sự chấp nhận chứng thư số được cấp mới.

IV.6.6 Công bố chứng thư số được gia hạn

Chứng thư số được gia hạn sẽ được công bố vào kho để có thể truy xuất.

IV.6.7 Thông báo tạo chứng thư số mới cho các thực thể khác

RA có thể nhận được thông báo nếu các yêu cầu cấp chứng thư số mà nó chấp nhận được CA tạo chứng thư số

IV.7 Thay đổi cặp khóa cho thuê bao

Đổi khóa là một quá trình sinh cặp khóa mới thay thế cho cặp khóa cũ đã được cấp chứng thư số của thuê bao. Thông tin của thuê bao trên chứng thư số được giữ nguyên trạng, chỉ thay đổi thành phần cặp khóa công khai và chứng thư số mới được tạo ra tương ứng với các thông tin này. Đổi khóa được hỗ trợ cho mọi lớp chứng thư số.

IV.7.1 Các tình huống đổi khóa

Trước khi hết hạn một chứng thư số, thuê bao cần đổi khóa chứng thư số này để tiếp tục duy trì giá trị sử dụng của chứng thư số. Một chứng thư số có thể được đổi khóa sau khi đã hết hạn. Hoặc trong trường hợp cần đổi khóa khẩn cấp đối với chứng thư.

Trong trường hợp thuê bao có nhu cầu thay đổi cặp khóa, thuê bao phải có đơn đề nghị thay đổi cặp khóa. Việc tạo khóa, phân phối khóa và công bố chứng thư số với khóa công khai mới thực hiện theo các quy định tại các Điều 24 và 25 của Nghị định 130/2018/NĐ-CP.

IV.7.2 Ai có thể yêu cầu đổi khóa

Chỉ thuê bao của chứng thư số cá nhân hay một đại diện được ủy quyền mới có thể yêu cầu đổi khóa.

IV.7.3 Xử lý yêu cầu đổi khóa

Thủ tục đổi khóa đảm bảo rằng cá nhân hay tổ chức đang muốn đổi khóa của một chứng thư số là chủ sở hữu của chứng thư số.

Thuê bao phải được xác minh cá nhân để chứng minh được quyền sở hữu khóa cá nhân (Khóa bí mật). Thuê bao chọn và đệ trình với thông tin đã được cung cấp. Sau khi gia hạn một chứng thư số, nếu một thuê bao vượt qua được các kiểm tra xác minh và các thông tin này chưa bị thay đổi, một cặp khóa tự động được tạo ra.

Ngoài thủ tục này hay các thủ tục duyệt khác, những yêu cầu cho xác thực yêu cầu cấp chứng thư số gốc sẽ được sử dụng để gia hạn.

IV.7.4 Thông báo về sự tạo ra chứng thư số mới cho thuê bao

Thông báo về sự đổi khóa chứng thư số cũng giống như thông báo khi chứng thư số được cấp mới.

IV.7.5 Sự chấp nhận chứng thư số đổi khóa

Tương tự như sự chấp nhận chứng thư số được cấp mới.

IV.7.6 Công bố chứng thư số được đổi khóa

Chứng thư số được đổi khóa sẽ được công bố vào kho để có thể truy xuất.

IV.7.7 Thông báo tạo chứng thư số mới cho các thực thể khác

RA có thể yêu cầu thông báo về việc tạo chứng thư số mà họ đã duyệt.

IV.8 Thay đổi chứng thư số

IV.8.1 Các tình huống thay đổi chứng thư số

Sự thay đổi chứng thư số nói đến các thủ tục liên quan đến việc tạo một chứng thư số mới để thay đổi thông tin trong một chứng thư số đã tồn tại (không chỉ thay đổi Khóa công khai) .

Sự thay đổi chứng thư số được coi như một yêu cầu cấp chứng thư số mới

IV.8.2 Ai có thể yêu cầu thay đổi chứng thư số

Chỉ người đăng ký của một chứng thư số cá nhân hay được ủy quyền đại diện cho tổ chức mới có thể yêu cầu thay đổi chứng thư số.

IV.8.3 Xử lý yêu cầu thay đổi chứng thư số

Một RA sẽ thực hiện nhận dạng và xác thực mọi thông tin thuê bao.

IV.8.4 Thông báo chứng thư số mới cho CA

Thông báo về sự đổi khóa chứng thư số cũng giống như thông báo khi chứng thư số được cấp mới.

IV.8.5 Thủ tục chấp nhận chứng thư số mới được thay đổi

Tương tự như sự chấp nhận chứng thư số được cấp mới.

IV.8.6 Công bố chứng tư số mới cho CA

Chứng thư số được đổi khóa sẽ được công bố vào kho để có thể truy xuất

IV.8.7 Thông báo cho các thực thể khác

RA có thể yêu cầu thông báo về việc tạo chứng thư số mà họ đã duyệt. Các thuê bao khác có thể tìm chứng thư số tại kho chứng thư số được công bố.

IV.9 Thu hồi chứng thư số của thuê bao

IV.9.1 Các tình huống thu hồi chứng thư số

Chứng thư số của thuê bao bị thu hồi trong những trường hợp sau đây:

- Khi thuê bao yêu cầu bằng văn bản và yêu cầu này đã được FastCA xác minh là chính xác;
- Khi thuê bao là cá nhân đã chết hoặc mất tích theo tuyên bố của tòa án hoặc thuê bao là tổ chức giải thể hoặc phá sản theo quy định của pháp luật;
- Cơ quan chức năng nhà nước có thẩm quyền;.
- Theo điều kiện thu hồi chứng thư số đã được quy định trong hợp đồng giữa thuê bao và FastCA.

Chỉ trong những trường hợp được liệt kê dưới đây, chứng thư số sẽ bị thu hồi bởi một thuê bao hay các đối tượng có thẩm quyền (RA, Admin) và được công bố trên một danh sách chứng thư số bị thu hồi (CRL). Nhờ yêu cầu từ một thuê bao, người mà có thể không còn sử dụng chứng thư số (hay không muốn sử dụng) với lý do không được liệt kê dưới đây, FastCA sẽ đặt cờ cho chứng thư số là không hoạt động trong cơ sở dữ liệu nhưng sẽ không công bố chứng thư số lên CRL.

Một chứng thư số bị thu hồi nếu:

- Một thuê bao, RA, FastCA có lý do để tin tưởng hay nghi ngờ rằng khóa bí mật của thuê bao đã bị làm lộ, bị đánh cắp.
- RA, FastCA có lý do tin tưởng rằng thuê bao đã vi phạm một trong các điều khoản nghiêm trọng trong các thỏa thuận với FastCA.
- Thỏa thuận với thuê bao đã kết thúc
- Sự ủy quyền của một tổ chức cho một thuê bao đã kết thúc .
- Một thành viên khác có lý do tin tưởng rằng một yêu cầu cấp chứng thư số thực tế bị sai
- Một thành viên khác xác định rằng một điều kiện tiên quyết thiết yếu để tạo chứng thư số đã không thỏa mãn hay khước từ
- Trong trường hợp chứng thư số của tổ chức, tên thuê bao tổ chức bị thay đổi
- Thông tin trong chứng thư số, ngoài những thông tin không được xác minh, không chính xác hay đã bị thay đổi.
- Sự tiếp tục sử dụng chứng thư số làm tổn hại tới FastCA.

Khi xem xét việc sử dụng chứng thư số có làm hại đến FastCA không, một CA và/hoặc RA sẽ xem xét những vấn đề khác nữa:

- Nhận được nhiều phản ánh.

- Nhân dạng của những người phản ánh.
- Liên quan chặt chẽ đến luật pháp
- Những phản ứng lại việc sử dụng gây hại từ người dùng được đưa ra mà chưa được chứng minh

IV.9.2 Ai có thể yêu cầu thu hồi chứng thư số

- Thuê bao cá nhân có thể yêu cầu thu hồi chứng thư số cá nhân của họ. Trong trường hợp chứng thư số của tổ chức, một đại diện được ủy quyền của tổ chức sẽ được cho quyền yêu cầu thu hồi những chứng thư số được cung cấp cho tổ chức. Một đại diện được ủy quyền của FastCA, hay một RA sẽ được cho quyền yêu cầu thu hồi một chứng thư số của RA Admin.
- FastCA có thể thu hồi chứng thư số trong trường hợp phát hiện thuê bao thực hiện không đúng hợp đồng, vi phạm luật pháp
- Cơ quan có thẩm quyền.

IV.9.3 Thủ tục thu hồi chứng thư số

Khi có căn cứ thu hồi chứng thư số, FastCA thu hồi chứng thư số, đồng thời thông báo ngay cho thuê bao và công bố trên cơ sở dữ liệu về chứng thư số việc thu hồi.

Trước khi thu hồi một chứng thư số, CA kiểm lại xem thu hồi đã được yêu cầu bởi thuê bao hay thực thể mà chấp nhận yêu cầu cấp chứng thư số. Thủ tục xác thực yêu cầu thu hồi gồm:

- Thuê bao đệ trình lên các thông tin và xác thực quyền sở hữu khóa đối với chứng thư số bị thu hồi cơ sở dữ liệu của FastCA.
- Nhận một thông điệp có nội dung từ Thuê bao yêu cầu thu hồi một chữ ký có thể kiểm tra với tham chiếu tới chứng thư số bị thu hồi.
- Đối thoại với thuê bao cung cấp sự đảm bảo hợp lý về lớp chứng thư số mà thuê bao yêu cầu thu hồi. Tùy vào tình huống cụ thể, phương tiện đối thoại có thể là điện thoại, mail...

CA/RA admin được quyền yêu cầu thu hồi chứng thư số của người dùng cuối trong miền con của CA/RA. FastCA sẽ xác thực nhân dạng của Admin qua điều khiển truy cập sử dụng SSL và xác thực client trước khi cho phép thực hiện chức năng thu hồi.

RA sử dụng phần mềm tự động có thể đệ trình một gói các yêu cầu thu hồi tới FastCA. Mỗi yêu cầu được xác thực qua một chữ ký với Khóa bí mật trong thiết bị lưu trữ vật lý của RA.

IV.9.4 Thời hạn yêu cầu thu hồi chứng thư số

Yêu cầu thu hồi sẽ được đệ trình ngay lập tức trong một khoảng thời gian hợp lý về phương diện thương mại.

IV.9.5 Giới hạn thời gian xử lý yêu cầu thu hồi chứng thư số của CA

Chứng thư số bị thu hồi ngay lập tức, sau khi FastCA xác thực các thông tin thu hồi.

IV.9.6 Kiểm tra những yêu cầu thu hồi cho đối tác tin tưởng

Người nhận sẽ kiểm tra trạng thái các chứng thư số mà họ tin tưởng. Một phương pháp mà người nhận sử dụng có thể kiểm tra trạng thái chứng thư số là kiểm tra hầu hết các CRL gần đây của FastCA. Một lựa chọn khác, người nhận có thể khớp những yêu cầu này bằng cách kiểm tra trạng thái của chứng thư số sử dụng OCSP (nếu được).

FastCA sẽ cung cấp cho người nhận thông tin làm thế nào để tìm được CRL, địa chỉ Web, hay OCSP responder (nếu có) phù hợp để kiểm tra trạng thái thu hồi.

IV.9.7 Tần suất tạo CRL mới

CRL cho chứng thư số người dùng cuối được cập nhật một ngày một lần.

IV.9.8 Giới hạn trễ cho CRL

CRL được đưa vào kho trong một khoảng thời gian phù hợp sau khi được tạo ra, cần một thời gian ngắn để cập nhật CRL.

IV.9.9 Kiểm tra trạng thái chứng thư số trực tuyến

Đường dẫn của OCSP được ghi vào trong chứng thư số do FastCA cấp. Khi kiểm tra trạng thái chứng thư số trực tuyến, các bên thứ ba có thể sử dụng đường dẫn này để kết nối tới OCSP kiểm tra trạng thái chứng thư số trực tuyến..

IV.9.10 Các yêu cầu kiểm tra trạng thái trực tuyến

Người nhận phải kiểm tra trạng thái của một chứng thư số mà trên đó anh ấy/chị ấy/nó tin tưởng. Nếu người nhận không kiểm tra trạng thái của một chứng thư số bằng cách kiểm tra các CRL liên quan, người nhận sẽ kiểm tra trạng thái chứng thư số bằng cách kiểm tra OCSP responder phù hợp (nếu OCSP có hiệu lực).

IV.9.11 Các dạng thông tin trạng thái thu hồi khác

Không quy định

IV.9.12 Những ràng buộc đặc biệt liên quan đến việc khóa bị lộ

Các thuê bao của FastCA sẽ được thông báo trong trường hợp khóa Khóa bí mật của CA bị lộ

IV.10 Tạm dừng hoặc phục hồi chứng thư số của thuê bao

IV.10.1 Các tình huống tạm dừng hoặc phục hồi chứng thư số

- Khóa bí mật tương ứng với chứng thư số bị nghi là đã bị lộ, tạm dừng sử dụng chứng thư số để kiểm tra. Nếu kiểm tra không có vấn đề thì phục hồi chứng thư số của thuê bao.
- Người sử dụng chứng thư số có nhu cầu không sử dụng trong một thời gian vì một mục đích hợp lý, thuê bao cần yêu cầu bằng văn bản và yêu cầu này đã được FastCA xác minh là chính xác. Hết thời gian tạm dừng thì sẽ phục hồi lại theo yêu cầu của thuê bao.
- Khi Khi FastCA có căn cứ để khẳng định rằng chứng thư số được cấp không tuân theo các quy định tại các Điều 24 và 25 Nghị định 1130/2018/NĐ-CP hoặc khi phát hiện ra bất cứ sai sót nào có ảnh hưởng đến quyền lợi của thuê bao và người nhận;
- Khi có yêu cầu của cơ quan chức năng nhà nước có thẩm quyền;
- Theo điều kiện tạm dừng chứng thư số đã được quy định trong hợp đồng giữa thuê bao và FastCA.

IV.10.2 Ai có thể yêu cầu tạm dừng hoặc phục hồi các chứng thư số

- Thuê bao cá nhân có thể yêu cầu tạm dừng và phục hồi chứng thư số cá nhân của họ. Trong trường hợp chứng thư số của tổ chức, một đại diện được ủy quyền của tổ chức sẽ được cho quyền yêu cầu tạm dừng và phục hồi những chứng thư số được cung cấp cho tổ chức. Một đại diện được ủy quyền của FastCA, hay một RA sẽ được cho quyền yêu cầu tạm dừng và phục hồi một chứng thư số của RA Admin.
- FastCA có thể tạm dừng chứng thư số trong trường hợp phát hiện thuê bao thực hiện không đúng hợp đồng, vi phạm luật pháp.
- Cơ quan chức năng nhà nước có thẩm quyền;.

IV.10.3 Thủ tục tạm dừng hoặc phục hồi chứng thư số

- Khi có căn cứ tạm dừng chứng thư số, FastCA tiến hành tạm dừng, đồng thời, thông báo cho thuê bao và công bố trên cơ sở dữ liệu về chứng thư số việc tạm dừng, thời gian bắt đầu và kết thúc việc tạm dừng.
- FastCA phục hồi chứng thư số khi không còn căn cứ để tạm dừng chứng thư số hoặc thời hạn tạm dừng theo yêu cầu đã hết.

IV.10.4 Giới hạn xử lý tạm dừng hoặc phục hồi chứng thư số

Chứng thư số bị tạm dừng hoặc phục hồi ngay lập tức, sau khi FastCA xác thực các thông tin yêu cầu.

IV.11 Dịch vụ cung cấp thông tin trạng thái chứng thư số

IV.11.1 Đặc điểm

Trạng thái của chứng thư số được xác định trong CRL thông qua một trang Web, LDAP directory và qua OCSP responder.

IV.11.2 Tính sẵn sàng của dịch vụ

Dịch vụ trạng thái chứng thư số được duy trì 24x7 (khi có vấn đề về dịch vụ FastCA sẽ thông báo kế hoạch xử lý trên website của FastCA).

IV.11.3 Kết thúc thuê bao

Sự kết thúc thuê bao có hiệu lực trong các trường hợp sau:

- Thuê bao đã hết hạn mà không gia hạn
- Thu hồi chứng thư số xảy ra mà không xin cấp một chứng thư số mới

IV.12 Quản lý khóa của một bên thứ ba và sự phục hồi khóa

Khóa của thuê bao được lưu trữ an toàn và duy nhất trong thiết bị PKI Token hoặc thiết bị an ninh phần cứng an toàn do thuê bao quản lý và phục vụ mục đích ký số, xác thực, không phục vụ mã hóa bảo mật dữ liệu vì vậy FastCA không cung cấp dịch vụ lưu trữ và phục hồi khóa cho thuê bao.

IV.13 Thủ tục xác thực thông tin thuê bao

- Thủ tục xác thực thông tin thuê bao được thực hiện khi có yêu cầu của khách hàng trong các trường hợp cấp chứng thư số, gia hạn, thay đổi cặp khóa, tạm dừng, khôi phục và thu hồi chứng thư số. Việc xác thực để đảm bảo rằng cá nhân hay tổ chức đang muốn thực hiện các yêu cầu này là chủ sở hữu thực sự.
- Việc xác thực dựa trên yêu cầu của khách hàng, hồ sơ kèm theo và cặp khóa, chứng thư số hiện tại (nếu có).

V- CÁC KIỂM SOÁT THIẾT BỊ, QUẢN LÝ VÀ VẬN HÀNH

V.1 Các kiểm soát an ninh vật lý

V.1.1 Truy cập vật lý

Việc truy cập về mặt vật lý vào hệ thống của FastCA được kiểm soát bằng hệ thống của các đơn vị cung cấp dịch vụ IDC như CMC và Viettel.

Để truy nhập vào hệ thống vật lý FastCA phải qua các lớp kiểm soát như sau:

- Kiểm soát bảo vệ tòa nhà.
- Tổ kiểm tra giám sát phòng máy theo từng ca trực.
- Xác thực bằng thẻ từ lần thứ nhất để vào trung tâm dữ liệu IDC.
- Xác thực bằng khóa tủ RACK lần thứ hai khi vào vùng chứa máy chủ: LDAP, OCSP, CRL, RA, CA, …
- Xác thực bằng thẻ từ lần thứ ba khi vào HSM.

V.1.2 Điều kiện không khí, nguồn điện, phòng tránh thảm họa.

Các thiết bị của FastCA trang bị với 2 thành phần là chính và dự phòng. Hệ thống nguồn điện cần đảm bảo liên tục, không bị gián đoạn. 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 FastCA được trang bị, bổ sung phòng ngừa để ngăn chặn và dập tắt lửa hay các thảm hoạ khác có thể gây cháy hay khói. Hệ thống thiết kế phù hợp với tiêu chuẩn phòng cháy chữa cháy.

V.1.3 Phương tiện lưu trữ

Dữ liệu của FastCA được bảo vệ trong các ổ cứng chuyên dụng như thiết bị lưu trữ, ổ cứng local trên các máy chủ cũng như việc đồng bộ dữ liệu ở hệ thống dự phòng, nhằm đảm bảo sao lưu dữ liệu hệ thống hay thông tin nhạy cảm khỏi nước, lửa hay môi trường huỷ hoại và bảo vệ tránh sử dụng truy cập trái phép hay phá huỷ.

V.1.4 Dự phòng từ xa

FastCA bảo trì sao lưu hệ thống dữ liệu then chốt hay bất kỳ thông tin nhạy cảm bao gồm dữ liệu kiểm định trong dự phòng an toàn.

Hệ thống dự phòng của FastCA được đặt tại các trung tâm Data Center của Viettel IDC ở Khu công nghệ cao Hòa Lạc, Km 29 Đại lộ Thăng, Thạch Thất, Hà Nội. 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 backup đầy đủ của hệ thống chính. Ngay khi

xảy ra sự cố, hệ thống này sẽ được sử dụng để duy trì hoạt động mà không làm ảnh hưởng đến giao dịch.

Việc đồng bộ, sao lưu dữ liệu định kỳ ở hệ thống dự phòng diễn ra hoàn toàn tự động dưới sự kiểm soát chặt chẽ từ các chuyên gia của FastCA. Thành phần cặp khóa trong HSM được thực hiện trực tiếp định kỳ theo chính sách của FastCA. Đối với mã nguồn của các máy chủ ứng dụng sẽ được đồng bộ chỉ khi có nâng cấp thay đổi.

V.2 Quy trình kiểm soát

V.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 chứng tư số.
- Việc chấp nhận, từ chối hay các xử lý khác của đơn xin cấp chứng thư số, yêu cầu thu hồi, yêu cầu cấp mới, hoặc các thông tin đăng ký.
- Ban hành, thu hồi chứng thư của các nhân viên có truy cập tới các thành phần bị hạn chế của hệ thống.
- 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.

V.2.2 Số lượng thành viên cho mỗi công việc

FastCA 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 và các công việc liên quan đến 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 lần, module 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 module không giữ "Secret Shares" (những thành phần riêng biệt có chứa các thành phần riêng biệt của khoá bí mật hoặc dữ liệu kích hoạt và ngược lại.

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

FastCA 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 vùng, thiết bị cần thiết.
- Được cấp các tài liệu điện tử để có thể truy cập và thực hiện một số chức năng trên các hệ thống thông tin và hệ thống FastCA.

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

V.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 chứng thư
- Quá trình chấp nhận, từ chối, hoặc các quá trình khác của đơn xin cấp chứng thư, yêu cầu thu hồi, cấp mới hay các thông tin đăng ký.
- Quá trình ban hành, thu hồi các chứng thư, 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 thuê bao hay các yêu cầu từ khách hàng.
- Quá trình tạo, ban hành hay tiêu huỷ một chứng thư số.

V.3 Quản lý nhân sự

Các thành viên của FastCA đều phải sử dụng nhân sự đảm bảo chất lượng và được huấn luyện, kiểm tra thường xuyên. Các thông tin nhạy cảm chỉ được phép chia sẻ trong nội bộ FastCA.

FastCA ban hành những tài liệu về kiểm soát nhân sự và chính sách bảo mật cho CA và RA. Những tài liệu này chứa thông tin bảo mật nhạy cảm và chỉ dành riêng cho bên tham gia dịch vụ FastCA dưới sự đồng ý của FastCA.

CA và các RA yêu cầu những nhân viên 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.

V.3.1 Quy trình kiểm tra lai lịch

CA 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 FastCA, bao gồm:

- Kê khai thông tin không đúng 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 FastCA cũng tiến hành điều tra thêm:
- Kiểm tra chứng minh thư nhân dân, giấy phép lái xe
- Kiểm tra thông tin an ninh xã hội

V.3.2 Yêu cầu về đào tạo

CA 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 FastCA.
- 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

CA 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.

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

CA 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.

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

CA 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.

V.3.5 Cung cấp tài liệu cho nhân viên

Nhân viên được giao quản lý hệ thống FastCA phải được cung cấp các tài liệu sau:

- Tài liệu Quy chế chứng thực
- FastCA – Hướng dẫn thủ tục và điều hành
- Sách giáo khoa - PKI do FastCA cung cấp
- Hướng dẫn cài đặt PKI do FastCA cung cấp

V.4 Các quy trình ghi nhật ký kiểm toán

V.4.1 Các loại bản ghi sự kiện

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

Hệ thống PKI có thể ghi lại các sự kiện sau:

1. Các sự kiện quản lý vòng đời chứng thư người đăng ký và CA, bao gồm:
   - Tạo khóa, sao lưu, lưu trữ, phục hồi, lưu trữ, và hủy bỏ;
   - Sự kiện quản lý vòng đời thiết bị mã hóa.
2. Các sự kiện quản lý vòng đời chứng thư người đăng ký và CA, bao gồm:
   - Yêu cầu chứng thư, gia hạn, tạm ngưng, khôi phục và yêu cầu khóa và thu hồi;
   - Tất cả các hoạt động xác minh được quy định trong các Yêu cầu này và Quy chế chứng thực;
   - Ngày, giờ, số điện thoại được sử dụng, người nói chuyện và kết quả cuối cùng của các cuộc điện thoại xác minh;
   - Phê duyệt và từ chối yêu cầu chứng thư;
   - Phát hành chứng thư;
   - Tạo danh sách Thu hồi Giấy chứng thư và các mục OCSP.
3. Các sự kiện bảo mật, bao gồm:
   - Các nỗ lực truy cập hệ thống PKI thành công và không thành công;
   - Các hoạt động của hệ thống an ninh và PKI được thực hiện;
   - Thay đổi hồ sơ bảo mật;
   - Sự cố hệ thống, lỗi phần cứng và các bất thường khác;
   - Các hoạt động của Firewall
   - Vào và ra khỏi cơ sở của CA.

V.4.2 Tần suất xử lý ghi chép

Các ghi chép được xử lý (lưu trữ) 1 tháng 1 lần.

V.4.3 Thời gian lưu trữ nhật ký kiểm toán

Thời gian lưu trữ 5 năm theo luật pháp Việt Nam.

V.4.4 Bảo vệ nhật ký kiểm toán

Tất cả các tệp ghi chép phải được bảo vệ toàn vẹn.

V.4.5 Các thủ tục sao lưu nhật ký kiểm toán

FastCA sẽ đảm bảo rằng sao lưu nhật ký kiểm toán phải được bao gồm trong thủ tục sao lưu.

V.4.6 Hệ thống thu thập kiểm toán (bên trong và bên ngoài)

FastCA sẽ đảm bảo rằng tất cả các sản phẩm thuộc phạm vi của FastCA có hệ thống kiểm toán nội bộ. Hệ thống kiểm toán ngoài có thể được thực hiện.

V.4.7 Thông báo tới đối tượng thực hiện sự kiện.

Không có điều khoản.

V.4.8 Đánh giá tính dễ bị tổn thương.

Quản lý rủi ro được thực hiện 2 năm một lần, bao gồm đánh giá tính dễ bị tổn thương.

V.5 Lưu trữ hồ sơ

V.5.1 Các loại hồ sơ được lưu trữ

FastCA phải đảm bảo rằng các hồ sơ sau được lưu trữ: chứng thư được cấp, các tệp ghi chép, các tệp cấu hình và khóa cá nhân mã hóa.

Các mục lưu trữ:

- Chứng thư
- Tệp ghi chép
- Thông tin cấu hình - Tệp cấu hình
- Khóa cá nhân mã hóa

V.5.2 Thời gian lưu trữ

Ít nhất 5 năm theo luật Việt Nam.

V.5.3 Bảo vệ lưu trữ

Lưu trữ phải được thực hiện trên phương tiện truyền thông chỉ ghi một lần. Kho lưu trữ ở mức tối thiểu bao gồm:

- Các tệp ghi chép kiểm toán cho khoảng thời gian lưu trữ
- Chứng thư được cấp cho khoảng thời gian lưu trữ

Một khi lưu trữ được thực hiện, một hàm băm SHA-256 của kho lưu trữ được thực hiện. Việc này phải được ghi lại để đảm bảo bảo vệ toàn vẹn.

Kho lưu trữ được vận chuyển qua các phương tiện an toàn tới trang web dự phòng và được lưu trữ dưới sự kiểm soát truy cập thích hợp để đảm bảo tính bảo mật.

V.5.4 Các thủ tục sao lưu lưu trữ

Các thủ tục sao lưu lưu trữ phải bao gồm: viết trên phương tiện truyền thông chỉ ghi một lần, tính giá trị băm, vận chuyển an toàn đến một vị trí an toàn.

- Sao lưu lưu trữ bao gồm các mục sau:
- Hệ thống tệp – Tất cả các hệ thống tệp được lưu trữ 1 lần/ tuần
- Tệp nhật ký - Các tệp nhật ký được gửi đến một tệp tin syslog ngoại trừ tệp nhật ký được ghi chép vào cơ sở dữ liệu. Các mục đăng nhập này là
- Cơ sở dữ liệu – Sao lưu cơ sở dữ liệu được thực hiện

V.5.5 Các yêu cầu cấp dấu thời gian của hồ sơ

Không áp dụng

V.5.6 Hệ thống lưu trữ (bên trong hoặc bên ngoài)

FastCA sẽ sử dụng hệ thống lưu trữ bên ngoài thông qua hệ thống lưu trữ riêng.

V.5.7 Các thủ tục thu thập và xác minh thông tin lưu trữ

FastCA sẽ đảm bảo rằng thông tin lưu trữ có thể xác minh. Tối thiểu, giá trị hàm băm và cấp dấu giá trị có thể được xác minh.

V.6 Thay đổi khóa

Chứng thư số của FastCA có thể được Bộ Thông tin và Truyền thông gia hạn, cấp mới với điều kiện thời gian hiệu lực còn lại của chứng thư số FastCA lớn hơn thời gian hiệu lực của chứng thư số cấp cho thuê bao là 90 ngày.

V.7 Thoả thuận và khôi phục sau thảm họa

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

Các bản sao lưu dự phòng các thông tin của CA được 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 chứng thư số, dữ liệu kiểm toán, các cơ sở dữ liệu cho các chứng thư đã ban hành. Trung tâm xử lý sẽ duy trì các bản sao lưu dự phòng của các thông tin CA của họ, cũng như các CA của các khách hàng doanh nghiệp nằm trong miền con.

V.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 CA và RA thực hiện ngay lập tức tuân theo các thủ tục của FastCA được nêu trong tài liệu này.

V.7.3 Lộ khoá bí mật của CA

Trong trường hợp lộ khoá bí mật của CA, CA 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 CA bị lộ trong miền con của FastCA.

V.7.4 Khả năng duy trì liên tục hệ thống sau thảm hoạ

FastCA tiến hành bảo mật cho các hoạt động phát triển, kiểm tra, bảo trì của CA và RA. FastCA 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 FastCA chỉ rõ.

Trung tâm xử lý có khả năng hồi phục hay khôi phục dữ liệu trong khoảng 24 giờ sau khi một thảm hoạ xảy ra. Trung tâm sẽ hỗ trợ tối thiểu các chức năng sau:

- Ban hành chứng thư.
- Thu hồi chứng thư.
- Công khai các thông tin thu hồi.
- Cung cấp các thông tin khôi phục khoá cho khách hàng doanh nghiệp sử dụng hạ tầng quản lý PKI.

Cơ sở dữ liệu khôi phục thảm hoạ của Trung tâm xử lý được đồng bộ hoá thường xuyên với cơ sở dữ liệu chính 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 FastCA.

Trung tâm dịch vụ có chức năng công bố thảm hoạ tên website, 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 hỗ trợ chức năng CA/RA theo mọi tình huống ngoại trừ một thảm hoạ lớn có thể 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.

V.7.5 Kết thúc sự hoạt động của CA hay RA

V.7.5.1 Chấm dứt CA

CA có thể bị chấm dứt vì bất kỳ lý do nào nhưng quyết định phải được Bộ Thông tin và Truyền thông phê duyệt. Trong trường hợp chấm dứt hoạt động của CA vì bất kỳ lý do nào, FastCA phải thông báo kịp thời và chuyển giao trách nhiệm cho các đơn vị kế tiếp, duy trì các hồ sơ, và các biện pháp khắc phục. Trước khi chấm dứt các hoạt động CA của mình, FastCA sẽ có thể thực hiện theo các bước sau

- Cung cấp cho người đăng ký chứng thư hợp lệ với thông báo chín mươi (90) ngày về ý định chấm dứt hoạt động như một CA
- Thu hồi tất cả các chứng chỉ vẫn chưa bị thu hồi hoặc chưa hết hạn vào cuối thời hạn chín mươi (90) ngày,
- Thông báo thời gian mà không cần sự cho phép của người đăng ký.
- Thông báo kịp thời về việc hủy bỏ đối với mỗi người đăng ký bị ảnh hưởng.
- Sắp xếp hợp lý để giữ hồ sơ theo CP / CPS này.
- Bảo lưu quyền cung cấp sự sắp xếp kế tiếp cho việc tái cấp chứng thư bởi một người kế nhiệm CA có tất cả các quyền liên quan để làm việc và tuân thủ tất cả các quy tắc cần thiết, trong khi hoạt động của nó ít nhất phải an toàn như các CA công cộng khác.

Các yêu cầu có thể thay đổi theo hợp đồng, những sửa đổi đó chỉ ảnh hưởng đến các bên ký kết hợp đồng.

V.7.5.2 Chấm dứt RA

Cơ quan đăng ký có thể bị chấm dứt vì bất kì lý do nào. Mọi quyết định được phê duyệt bởi FastCA. Trong trường hợp chấm dứt RA vì bất kỳ lý do nào, FastCA phải thông báo kịp thời và chuyển giao trách nhiệm cho đơn vị kế tiếp, duy trì hồ sơ và các biện pháp khắc phục. Trước khi chấm dứt các hoạt động của RA. FastCA có thể thực hiện các bước sau:

- Cung cấp cho thuê bao do RA quản lý thông báo chín mươi (90) ngày về ý định chấm dứt hoạt động như một RA.

- Cung cấp giải pháp thay thế cho các thuê bao, tổ chức, cá nhân, doanh nghiệp thuộc RA quản lý.
- Dừng chấp nhận yêu cầu chứng thư ba mươi (30) ngày sau khi ban hành thông báo chấm dứt.
- Sắp xếp hợp lý để bảo quản hồ sơ theo đúng tài liệu này.

Các yêu cầu có thể thay đổi theo hợp đồng, những sửa đổi đó chỉ ảnh hưởng đến các bên ký kết hợp đồng.

VI - VẤN ĐỀ AN TOÀN, AN NINH KỸ THUẬT

VI.1 Sinh khóa và cài đặt

VI.1.1 An ninh sinh cặp khóa cho FastCA

- Đối với khóa của nhà cung cấp dịch vụ (FastCA), các cặp khóa của các thành phần như CA, RA sẽ được sinh trực tiếp tại các thiết bị HSM chuyên dụng. Việc bảo vệ khóa bí mật của CA 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 chứng thư số trong toàn bộ hệ thống). Hệ thống FastCA hoàn toàn tương thích với những nhà cung cấp HSM hàng đầu thế giới hiện tại như Utimaco, AEP, SafeNet, nCipher, Thales…

VI.1.2 An ninh sinh cặp khóa cho thuê bao

- Thuê bao tự sinh khóa trên thiết bị PKI Token an toàn hoặc thiết bị HSM, thuộc sự quản lý của thuê bao và thông báo đến FastCA quá trình sinh khóa trên thiết bị PKI Token.
- RA hoặc các đại lý RA của FastCA hỗ trợ thuê bao sinh khóa trên thiết bị PKI Token an toàn hoặc thiết bị HSM.
- FastCA sinh khóa cho thuê bao trên thiết bị PKI Token an toàn và chuyển cho thuê bao.
- FastCA không lưu trữ bất kỳ khóa bí mật (Khóa bí mật) nào của thuê bao

VI.1.3 Gửi khóa bí mật cho thuê bao

- Dịch vụ FastCA cho phép khách hàng lựa chọn đăng ký việc sinh khóa và chứng thư số trên thiết bị USB Token/Smart Card của khách hàng tại nhà cung cấp dịch vụ hoặc sinh khóa trên thiết bị USB Token/Smart Card của khách hàng tại máy tính cá nhân của người đăng ký dịch vụ. Như vậy cặp khóa của người dùng sẽ chỉ được lưu trên thiết bị USB Token/Smart Card của khách hàng và chỉ chứng thư số của người dùng được lưu tại hệ thống CA Server của nhà cung cấp dịch vụ.
- Trong trường hợp, cặp khóa được sinh ra trên thiết bị USB Token/Smart Card của khách hàng tại máy tính cá nhân của người đăng ký dịch vụ, quá trình chuyển giao khóa bí mật tới người dùng cuối là không cần thiết. Tuy nhiên để đảm bảo thông tin truyền tải từ hệ thống CA đến máy tính cá nhân người dùng được bảo vệ, FastCA triển khai giao thức SSL cho các kết nối này nhằm mã hóa dữ liệu truyền tải trên đường truyền không bị đánh cắp và thay đổi thông tin. Về SSL mà FastCA

sử dụng chi tiết được mô tả tại mục 6.4 bên trên. Quy trình phân phối khóa cho thuê bao đối với trường hợp cặp khóa được tạo bởi thuê bao như sau:

- Thuê bao hoàn thành các thủ tục về đăng ký sử dụng dịch vụ theo quy định của FastCA. Chi tiết xem tại quy chế chứng thực kèm hồ sơ này.
- Thuê bao nhận thiết bị lưu khóa là USB Token qua các văn phòng đại diện, các đại lý chính thức của FastCA trên toàn quốc, hoặc qua đường bưu điện đảm bảo.
- Trước quá trình sinh khóa và truyền tải chứng thư tới thuê bao, thuê bao sẽ nhận được một mật khẩu do hệ thống CA tự động sinh ra (một cách ngẫu nhiên) qua thư điện tử. Thuê bao thực hiện nhập mã kích hoạt, độ dài khóa, loại thiết bị lưu trữ USB Token để kích hoạt tạo chứng thư số của mình. Quá trình kết nối và lưu chuyển thông tin giữa hệ thống CA và máy tính cá nhân của người dùng được thực hiện qua kết nối truyền thông bảo mật (SSL) nên đảm bảo tính an toàn của thông tin. Tương tự về SSL mà FastCA sử dụng chi tiết được mô tả tại mục 6.4 bên trên.
- Nếu thuê bao để lộ cả tài khoản và mật khẩu thì cặp khóa và chứng thư sẽ rơi vào tay người khác. Trong trường hợp này, trách nhiệm hoàn toàn thuộc về thuê bao sử dụng dịch vụ. Tuy nhiên, thuê bao cần xác minh thông tin và có thể yêu cầu tới hệ thống đăng ký để hệ thống có thể thu hồi cặp khóa và chứng thư đã bị lộ.
- Sau khi hoàn thiệt các bước xác minh thông tin thì thuê bao có thể sinh ra cặp khóa mới và hệ thống CA sẽ ký một chứng thư số mới cho người đăng ký.

– Trong trường hợp người dùng lựa chọn việc sinh khóa trên thiết bị USB Token/Smart Card của khách hàng và chứng thư số tại nhà cung cấp FastCA thì quy trình thực hiện phân phối khóa như sau:

- Thuê bao hoàn thành các thủ tục về đăng ký sử dụng dịch vụ theo quy định của FastCA. Chi tiết xem tại quy chế chứng thực kèm hồ sơ này.
- FastCA nhập các thông tin cần thiết mà thuê bao đã cung cấp lên hệ thống và thực hiện cấp chứng thư số cho cặp khóa của thuê bao do PKI Token FastCA khởi tạo.
- FastCA thực hiện bàn giao chứng thư số và yêu cầu thuê bao kiểm tra, xác nhận tính chính xác của thông tin thuê bao trên chứng thư số do FastCA cấp theo đề nghị của thuê bao.

- Thuê bao xác nhận tính chính xác của thông tin được cấp trong chứng thư số và ký nhận biên bản bàn giao token.
- FastCA sẽ tiến hành bàn giao mã PIN của thuê bao sau khi thuê bao đã nhận token và có xác nhận hợp lệ.
- Sau khi đã giao thiết bị USB PKI token cho thuê bao, thuê bao phải xác nhận trước khi FastCA công bố chứng thư số của thuê bao trên cơ sở dữ liệu trực tuyến về chứng thư số của FastCA.

VI.1.4 Gửi khóa công khai cho FastCA

Khi một khóa công khai được truyền tới FastCA để thực hiện chứng thực, nó sẽ được gửi qua một cơ chế đảm bảo rằng Khóa công khai này không bị thay thế trong quá trình vận chuyển và người yêu cầu cấp chứng thư số sở hữu Khóa bí mật tương ứng. Cơ chế được sử dụng để gửi khóa công khai là một gói chứng thư số được ký PKCS#10 hay phương pháp tương đương. Đảm bảo rằng:

- Khóa công khai không bị thay thế, sửa đổi trên đường truyền
- Yêu cầu cấp chứng thư số sở hữu Khóa bí mật tương ứng

Trung tâm xử lý thực hiện quá trình sinh khóa, truyền Khóa công khai từ module mã hóa nơi nó được tạo ra tới module mã hóa của CA cấp trên, bằng cách đóng gói nó trong một gói chứng thư số được ký PKCS#10.

Trong trường hợp sinh chứng thư số cho FastCA, cặp khóa FastCA được sinh trên HSM và gửi yêu cầu đăng ký chứng thư số của FastCA định dạng PKCS#10 lên RootCA Quốc gia để xin cấp chứng thư số cho FastCA.

VI.1.5 Gửi Khóa công khai của CA cho người nhận

Chứng thư số khóa công khai của FastCA và RootCA quốc gia được công bố công khai trên website của FastCA và RootCA quốc gia.

Các chứng thư số khóa công khai của người dùng được công bố trên kho lưu trữ chứng thư số của FastCA, người dùng có thể tải về để sử dụng, không cần cơ chế phân phối đặc biệt.

VI.1.6 Độ dài của khóa

Cặp khóa có độ dài đủ để chống lại việc sử dụng tấn công mã để xác định Khóa bí mật trong suốt thời gian sử dụng cặp khóa. FastCA hiện tại sử dụng cặp khóa có độ dài nhỏ nhất tương đương với 2048-bit trong RSA cho CA.

FastCA chỉ chấp nhận cặp khóa có độ dài tối thiểu tương đương 2048 bit RSA cho các chứng thư số.

VI.1.7 Các tham số sinh Khóa công khai và kiểm tra chất lượng

Thành viên FastCA sử dụng chữ ký số chuẩn sẽ sinh ra các tham số khóa được yêu cầu tương ứng với FIPS 140-2 level 3 hoặc chuẩn tương đương được quy định tại Thông tư số 06/2015/TT-BTTT. Khi thành viên FastCA sử dụng chữ ký số chuẩn, chất lượng của những tham số khóa sẽ được kiểm tra theo FIPS 140-2 level 3 hoặc chuẩn tương đương được quy định tại Thông tư số 06/2015/TT-BTTT.

VI.1.8 Đa kiểm soát khoá bí mật (m out of n)

Cơ chế này sử dụng để bảo đảm an toàn cho khóa bí mật của FastCA lưu trữ trong thiết bị HSM.

Đa kiểm soát được áp dụng để bảo vệ dữ liệu kích hoạt cho khoá bí mật CA được lưu trữ tại trung tâm xử lý tuân theo các chuẩn trong chính sách bảo mật của FastCA. 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 CA khác trong các miền con tương ứng tuân theo các chuẩn trong chính sách bảo mật của FastCA. Trung tâm xử lý cũng sử dụng Secret Sharing để bảo vệ khoá bí mật tại từng khu vực khôi phục sau thảm hoạ.

VI.1.9 Sao lưu dự phòng khoá bí mật

CA tạo các bản lưu dự phòng khoá bí mật cho mục đích khôi phục sự cố hay khôi phục sau thảm hoạ phù hợp với chuẩn trong chính sách bảo mật của FastCA. Các bản sao lưu dự phòng phải phù hợp với các chính sách được nêu trong Quy chế chứng thực. Các bản sao lưu dự phòng được tạo ra bằng cách sao chép các khoá bí mật và đưa chúng vào các module mã hoá dự phòng (thường là các thẻ thông minh được chia sẻ và bảo mật).

Khóa bí mật được dự phòng là để được bảo vệ 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 module mã hoá nằm trong khu vực CA, như tại khu vực khôi phục sau thảm hoạ hoặc tại khu vực bên ngoài khác, ví dụ như ngân hàng.

VI.1.10 Lưu trữ khoá bí mật

Khi một chứng thư của FastCA 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 module phần cứng có cơ chế mã hoá đáp ứng được các yêu cầu của CPS. Những cặp khoá CA này sẽ không

được sử dụng trong bất kỳ chữ ký nào sau khi hết hạn sử dụng trừ khi các chứng thư CA này được khôi phục trong các trường hợp cần thiết.

VI.1.11 Cách thức khoá bí mật được chuyển đến hoặc đi từ một module mã hoá

Khóa bí mật chuyển đến module 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 CA hoặc RA trên module mã hoá phần cứng và chuyển giao chúng vào module 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 FastCA. Các khoá bí mật sẽ được mã hoá trong suốt quá trình truyền.

VI.1.12 Cách thức lưu trữ khoá bí mật trên module mã hoá

Các khoá bí mật của CA hoặc RA được lưu trữ trên các module mã hoá dưới dạng mật mã.

VI.1.13 Sử dụng khoá bí mật đối với thuê bao

Thuê bao có nghĩa vụ bảo vệ khoá bí mật của mình. Phải đảm bảo khóa bí mật được lưu trữ trong các thiết PKI Token an toàn, không được đọc, sao chép ra ngoài.

VI.1.14 Huỷ khóa bí mật

Khi được yêu cầu, các khoá bí mật của CA sẽ bị huỷ để đảm bảo các khoá đó sẽ không được khôi phục trong bất kỳ trường hợp nào. Quá trình này tuân theo tài liệu chuẩn trong chính sách bảo mật riêng của FastCA

VI.2 Dữ liệu kích hoạt

VI.2.1 Quá trình tạo và cài đặt dữ liệu kích hoạt

FastCA tạo và cài đặt dữ liệu kích hoạt (Activation Data) cho khoá bí mật sử dụng những phương pháp để bảo vệ dữ liệu kích hoạt đối với các phạm vi cần thiết nhằm tránh sự mất mát, sự ăn cắp, sự cải biến, sự tiết lộ trái phép, hoặc sử dụng trái phép các khoá bí mật.

Đối với phạm vi mật khẩu được sử dụng cho dữ liệu kích hoạt, những người đăng ký sẽ thiết lập mật khẩu, những mật khẩu này không dễ dàng bị đoán nhận hoặc bị tấn công bởi kiểu tấn công từ điển.

VI.2.2 Bảo vệ dữ liệu kích hoạt

FastCA sẽ bảo vệ dữ liệu kích hoạt cho những khoá bí mật của họ bằng các phương pháp nhằm để tránh sự mất mát, sự ăn cắp, sự cải biến, sự tiết lộ trái phép, hoặc sử dụng trái phép các khoá bí mật.

Thuê bao đầu cuối sẽ bảo vệ dữ liệu kích hoạt cho những khoá bí mật trong bất cứ trường hợp nào, đối với phạm vi cần thiết nhằm tránh sự mất mát, sự ăn cắp, sự cải biến, sự tiết lộ trái phép, hoặc sử dụng trái phép các khoá bí mật.

Trung tâm xử lý sử dụng *Secret Sharing* tuân theo Quy chế chứng thực và những chính sách bảo mật của dịch vụ FastCA. Trung tâm xử lý cung cấp các thủ tục và các giá trị cho phép *Shareholders* có những đề phòng cần thiết để tránh sự mất mát, sự ăn cắp, sự cải biến, sự tiết lộ trái phép hoặc sử dụng trái phép *Secret Shares*, những cái mà họ sở hữu. *Shareholders* sẽ không làm những việc sau:

- Sao lưu, tiết lộ, hoặc làm cho hãng thứ 3 biết được Secret Share, hoặc sử dụng bất hợp pháp Secret Share đó, hoặc
- Tiết lộ trạng thái cá nhân như là Shareholder đến bên thứ 3.

Secret Share và bất cứ thông tin bị tiết lộ đến *Shareholder* được gắn liền với trách nhiệm cá nhân như một *Shareholder* thiết lập các thông tin bí mật hoặc các thông tin riêng.

Trung tâm xử lý có kế hoạch khôi phục thảm hoạ nhằm đảm bảo *Secret Share* luôn sẵn sàng tại vị trí khôi phục thảm hoạ sau khi thảm họa xảy ra. Mỗi trung tâm xử lý duy trì dấu vết kiểm định của *Secret Share* và *Secrete Holders* sẽ tham gia vào quá trình duy trì các kiểm định đó.

VI.2.3 Các vấn đề khác của dữ liệu kích hoạt

VI.2.3.1 Vấn đề chuyển tải dữ liệu kích hoạt

Để chuyển giao các dữ liệu kích hoạt cho các khoá bí mật, các thành viên thuộc dịch vụ FastCA sẽ sử dụng các biện pháp chống lại các nguy cơ mất mát, bị đánh cắp, bị sửa đổi, bị tiết lộ hoặc bị sử dụng trái phép đối với các khóa riêng. Trong phạm vi môi trường Windows và đăng nhập mạng thì sự kết hợp tên sử dụng/mật khẩu (username/password) sẽ được sử dụng như là dữ liệu kích hoạt cho thuê bao cuối, mật khẩu được truyền đi trên mạng sẽ được bảo vệ khỏi sự truy cập của những thuê bao không được phép.

VI.2.3.2 Huỷ dữ liệu kích hoạt

Dữ liệu kích hoạt khóa bí mật của CA sẽ bị vô hiệu hoá bằng cách sử dụng biện pháp nhằm chống lại nguy cơ mất mát, bị đánh cắp, bị sửa đổi, bị tiết lộ hoặc bị sử dụng trái phép đối với các khoá bí mật mà dữ liệu kích hoạt đó bảo vệ. Sau khi hết thời gian lưu trữ, dịch vụ FastCA sẽ vô hiệu hoá dữ liệu kích hoạt bằng cách ghi đè hoặc tiến hành huỷ vật lý.

VI.3 Kiểm soát bảo mật máy tính

Dịch vụ FastCA thực hiện tất cả các chức năng của CA và RA trên các hệ thống đáng tin cậy đáp ứng được các yêu cầu về bảo mật của dịch vụ FastCA. Các thuê bao tổ chức phải sử dụng hệ thống đáng tin cậy.

Trung tâm xử lý phải đảm bảo chắc chắn rằng các hệ thống chứa phần mềm CA và các tệp dữ liệu là hệ thống đáng tin cậy chống lại các truy cập trái phép, điều này có thể được giải thích theo yêu cầu và tiêu chuẩn kiểm định trong mục 4.5.1. 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. Thuê bao thông thường sẽ không có tài khoản trên máy chủ chính.

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 truy cập mạng trái phép, ngoại trừ các tiến hành ứng dụng đã được định nghĩa. Trung tâm xử lý sẽ sử dụng tường lửa để bảo vệ hệ thống mạng trước nguy cơ xâm nhập 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 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

VI.4 An ninh mạng

Việc thiết kế an toàn chung cho hệ thống, FastCA dựa trên các tiêu chuẩn an toàn như ISO 27001 để thiết kế, có các mục sau:

- Chính sách an ninh mạng.
- Tường lửa Firewall.
- Hệ thống phát hiện và chống thâm nhập mạng IPS
- Hệ thống phát hiện và chống thâm nhập các máy chủ ứng dụng.
- Hệ thống phòng chống Antivirus.
- 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, thành phần quản lý và phân tích băng thông của mạng.

Dựa vào các thành phần này, hệ thống an ninh mạng của FastCA được xây dựng để đảm bảo các yêu cầu:

- An toàn và tin cậy
- Ngăn chặn các tấn công trong và ngoài mạng hiệu quả.
- Chính sách an ninh mạng thống nhất chặt chẽ.
- Tính sẵn sàng cao của hệ thống 99,99%
- Dễ dàng bổ sung thêm các thành phần (module) và nâng cấp.
- Không làm giảm và ảnh hưởng đến hiệu suất (Performance) của toàn mạng.
- Dễ dàng cô lập những điểm bị tấn công và tổn thương.
- Quản lý tập trung, tạo các báo cáo an ninh dễ hiểu tường minh và chính xác.
- Khả năng mở rộng:
- Dễ dàng mở rộng và bổ sung các thiết bị Firewall.
- Dễ dàng mở rộng và bổ sung các thiết bị chống thâm nhập trái phép trên mạng IPS.
- Dễ dàng bổ sung các Module khác khi mạng lưới phát triển.

– **Tính bảo mật:** Mạng có tính bảo mật cao, có nhiều biện pháp phòng chống sự truy nhập bất hợp pháp vào mạng. Mạng phải chống lại được các hiện tượng lấy cắp hay thay đổi thông tin.

– Đảm bảo khả năng phòng thủ theo chiều sâu, nhiều lớp.

– Tích hợp đa công nghệ: FW, IPS, AV, Content Filtering, Patch Management, AAA, …..

– Tiếp cận mạng tự phòng vệ.

– **An toàn dữ liệu:** An toàn dữ liệu là một yêu cầu quan trọng đối với một mạng cung cấp dịch vụ như FastCA, nó phải đảm bảo dữ liệu cung cấp phải được bảo vệ tránh mất mát, hư hỏng dữ liệu.

– **Tính tương thích:** Mạng cần có tính tương thích cao, cho phép chạy được những phần mềm thông dụng, cho phép nối ghép với các mạng khác trong hệ thống cũng như nối ra quốc tế khi có nhu cầu.

– **Tính mềm dẻo:** Cho phép dễ dàng thay đổi kiến trúc, vị trí đặt máy của mạng. Cho phép thay đổi được các phần mềm ứng dụng cũng như phần mềm hệ thống cho mạng cũng như cho từng trạm làm việc.

– **Bảo mật phân cấp nhiều mức:** Mạng phải đảm bảo thiết lập an ninh ở nhiều mức khác nhau như sau:

- Bảo mật mức mạng : thiết bị kết nối mạng, thiết bị mã hóa, thiết bị tối ưu băng thông, cân bằng tải, ...
- Bảo mật truy cập: Firewall, IDS/IPS,...
- Bảo mật mức thiết bị.
- Bảo mật mức máy chủ.
- Bảo mật mức hệ điều hành.
- Bảo mật mức CSDL.
- Bảo mật mức ứng dụng.

VI.4.1.1 Hệ thống tường lửa dành cho FastCA (Firewall)

Firewall sử dụng trong hệ thống FastCA 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.

Trước kia, khi công nghệ Firewall còn chưa phát triển, thì Firewall mới thực hiện được chức năng lọc gói tin ở lớp 3 gọi là packet filtering. Chức năng này có nhược điểm rất lớn là khó mở rộng và kiểm soát khi có nhiều chính sách được thực hiện và cũng không thích ứng với những ứng dụng multimedia là những loại ứng dụng thay đổi cổng kết nối một cách linh hoạt.

Firewall cho FastCA 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 FastCA 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.

VI.4.1.2 Hệ thống phát hiện và ngăn chặn tấn công (Intrusion Prevention System – IPS)

Hệ thống FastCA được đặt tại datacenter đã được bảo vệ, ngăn chặn các cuộc tấn công bất hợp pháp vào hệ thống máy chủ đặt tại DC theo quy chuẩn Quốc tế. Tuy nhiên hệ thống FastCA bổ sung thêm hệ thống IPS để ngăn chặn truy cập trái phép. Giúp quản trị hệ thống kịp thời xử lý, kết hợp với dịch vụ theo dõi lưu lượng đường truyền của DC để

kiểm tra, phát hiện. Giải pháp IPS sử dụng ở đây là một module mở rộng trên thiết bị Firewall cứng:

- Tường lửa (firewall) là một thiết bị mạng truyền thống trong việc bảo vệ hệ thống mạng. Với những thiết bị tường lửa đời đầu chủ yếu hoạt động theo kiểu Packet Filtering, các chính sách được thiết lập để cho phép hoặc ngăn chặn một gói tin ra/vào các vùng mạng do tường lửa phân tách. Nhưng trước nguy cơ an ninh mạng ngày càng nhiều, tường lửa UTM được ra đời nhằm giải quyết các bài toán này.
- Với những thiết bị/ứng dụng tường lửa truyền thống như Iptable, pfsense...hoạt động theo cơ chế Packet Filtering, chỉ lọc một số thông tin chính trên gói tin như địa chỉ nguồn, đích, port...Chứ không quan tâm nhiều đến nội dung gói tin. Cơ chế hoạt động đơn giản cho phép các thiết bị/ứng dụng tường lửa hoạt động nhanh, nhẹ nhưng lại không thể bảo vệ hệ thống một cách hoàn hảo.
- Trên Internet hiện nay tồn tại nhiều nguy hiểm đến từ: Virus, spyware, malware...đã làm điêu đứng bao nhiêu người dùng, hệ thống nhờ cơ chế lây lan, lan truyền đơn giản. Email spam gây ra sự khó chịu cho người dùng. Malsite là những website có chứa mã độc. Tấn công mạng dựa vào các lỗ hổng trên máy chủ, thiết bị mạng. Tấn công DDoS/DOS làm tê liệt hệ thống, gây nghẽn mạng làm người dùng không truy cập được các dịch vụ. Ứng dụng nguy hiểm là các ứng dụng được cài đặt ngầm vào hệ thống, gây chậm máy, đánh cắp dữ liệu...
- Với firewall hoạt động dựa theo cơ chế Packet Filtering có thể giúp người dùng bảo vệ hệ thống trước những nguy cơ trên không? Câu trả lời là không và tường lửa UTM (firewall Unified Threat Management) ra đời. Ngay từ tên gọi đã cho thấy firewall UTM có thể quản lý tập trung các mối nguy hiểm. Tường lửa UTM bao gồm các module như Antivirus, Antispam, IPS, Application Control, WebBlocker, DDoS Defense...giúp bảo vệ hệ thống.

Từ những tính năng cao cấp trên: Hệ thống FastCA đã chọn sử dụng công nghệ Firewall UTM tích hợp các tính năng Antivirus, Antispam, IPS, Application Control, WebBlocker, DDoS Defens. Cho khả năng cấm ngay lập tức lưu thông mạng không mong muốn. Trợ giúp các điều tra chứng cứ để chỉ ra nguồn gốc của các cuộc tấn công và phạm vi của chúng. Đơn giản hóa triển khai và quản trị IPS. Chống lại các nguy cơ mới thông qua dịch vụ Smart Defense Servies.

VI.4.1.3 Hệ thống ghi nhật ký (log files)

Mọi hành động, thao tác hệ thống được ghi lại nhằm mục đích theo dõi, duy trì tìm ra nguyên nhân sự cố khi hệ thống không hoạt động. Các nội dung sau được ghi nhật ký:

– Các sự kiện :

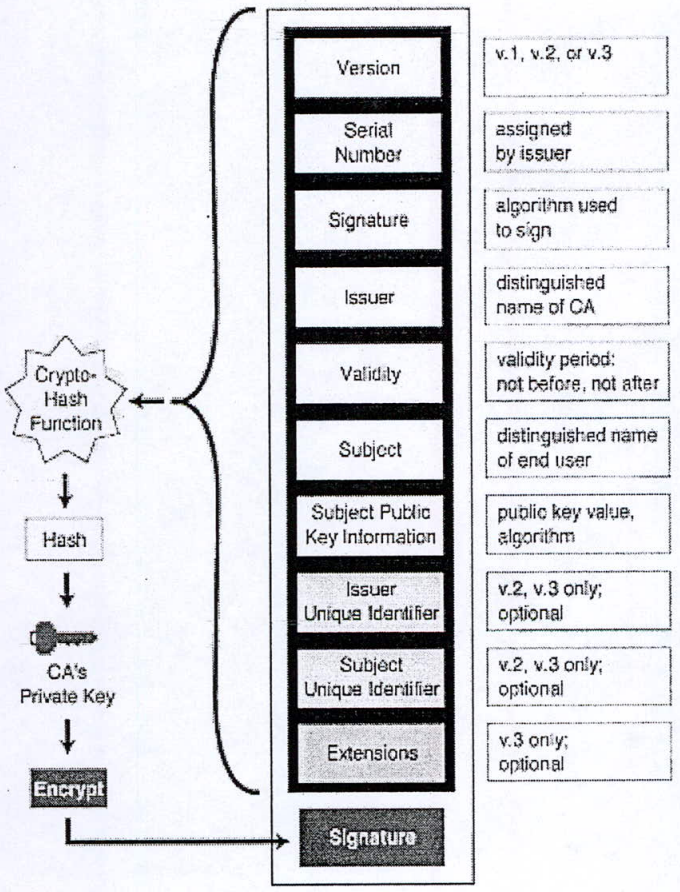
- Bật tắt các thành phần hệ thống và ứng dụng
- Tạo khóa và thay đổi khóa
- Các sự kiện về quản lý chu kỳ của chứng thư số : cấp phát, hủy bỏ, thu hồi,…
- Quản trị hệ thống
- Truy cập từ xa
- Tạo và xóa mật khẩu hay thay đổi đặc quyền người sử dụng
- Thay đổi nhân sự
- Các hành động truy nhập vào mạng và các hệ thống không được cấp quyền
- Lỗi trong việc đọc ghi
- Thay đổi chính sách, thời gian của chứng thư số

VII- ĐẶC TẢ VỀ CHỨNG THƯ SỐ VÀ DANH SÁCH CHỨNG THƯ BỊ THU HỒI (CRL)

VII.1 Đặc tả về chứng thư số

Chứng thư có thể hiểu đơn giản một mẩu tin cung cấp nhân dạng của người sở hữu khóa công khai. Giống như tấm hộ chiếu hay chứng minh thư, chứng thư cung cấp bằng chứng nhận dạng của một người hay một thực thể. Chứng thư được kí và được lưu chuyển bởi một tổ chức thứ ba đáng tin cậy gọi là nhà cung cấp chứng thư số - CA. Đến chừng nào mà cả người gửi và người nhận còn tin tưởng vào CA, thì khóa công khai của người được cấp chứng thư vẫn có giá trị khẳng định người đó.

VII.1.1 Cấu trúc của chứng thư số



VII.1.2 Cấu trúc của một chứng thư số

Các chứng thư số hiện nay được xây dựng theo chuẩn X.509, bao gồm những trường thông tin chính sau:

- **Phiên bản:** phiên bản của chứng thư số, ví dụ: X.509 v1, v2 hoặc v3.
- **Số serial:** một số duy nhất (ID) để nhận dạng chứng thư số này so với những chứng thư số khác của CA.

- **Chữ kí:** số nhận dạng (ID) của các thuật toán đã dùng để tạo chữ kí số lên chứng thư số, cùng các tham số được sử dụng trong các thuật toán đó. VD: OID là số nhận dạng của thuật toán SHA-1 kết hợp với RSA. Điều này chỉ ra rằng, một giá trị băm được tạo ra từ thuật toán SHA-1, sau đó được mã hóa bởi thuật toán RSA, sinh ra chữ kí số trên chứng thư số này.
- **Người phát hành (Issuer):** Tên phân biệt của CA đã phát hành chứng thư số này (bao gồm các thông tin như: Tên nước, tên thành phố, tên địa phương, tên tổ chức, tên đơn vị, tên thường gọi, địa chỉ email …). Trường này luôn phải có.
- **Hiệu lực (Validity):** Khoảng thời gian có hiệu lực của chứng thư số.
- **Chủ thể (Subject):** Tên phân biệt của người sở hữu chứng thư số. Trường này không được để trống trừ khi có một trường khác như trường Mở rộng (Extension) thay thế.
- **Thông tin về khóa công khai của chủ thể (Subject Khóa công khai Info):** khoá công khai của chủ thể và ID của các thuật toán mã hóa đã sử dụng. Trường này luôn phải có.
- Số ID của người phát hành (Issuer Unique ID): chỉ có ở phiên bản 2 và 3.
- Số ID của chủ thể (Subject Unique ID): chỉ có ở phiên bản 2 và 3.
- **Trường mở rộng:** chỉ có ở phiên bản 3, bao gồm những thông tin như: Authority Key Identifier, Subject Key Identifier, Key Usage, Extended Key Usage, CRL Distribution Point, Private Key Usage Period, Certificate Policies, Policy Mappings, Subject Alternate Name, Issuer Alternate Name, Subject Directory Attributes, Basic Constraints, Name Constraints, Policy Constraints, Inhibit Any Policy, Freshest CRL Pointer, Authority Information Access, Subject Information Access.
- Chữ kí số của CA lên chứng thư.

VII.2 Đặc tả về danh sách chứng thư số bị thu hồi

Trường	Giá trị
Version	Phiên bản của CRL
Signature Algorithm	Thuật toán để ký CRL
Issuer	Nhà cung cấp

Trường	Giá trị
Effective Date	Ngày bắt đầu có hiệu lực
Next Update	Thời gian có CRL tiếp theo
Revoked Certificate	Danh sách chứng thư bị thu hồi, được liệt kê bằng các số serial

VII.3 Đặc tả về OCSP

Được khuyến nghị trong RFC2560.

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

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

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

Các tiêu chuẩn của dịch vụ FastCA sẽ được dùng để thanh tra hay đánh giá FastCA, hay thuê bao là các doanh nghiệp. Trong trường hợp FastCA hoặc Superior Entity được kiểm tra và kết quả cho thấy các thực thể không đạt các tiêu chuẩn của dịch vụ FastCA, 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 FastCA .

Các tiêu chuẩn của dịch vụ FastCA sẽ được dùng để tiến hành các đánh giá về quản lý rủi ro bổ sung của chính FastCA 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 FastCA 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 FastCA 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.1.1 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 FastCA.

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 PKI.

VIII.1.2 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.1.3 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 hình là một phần của cuộc kiểm tra tổng thể hàng năm về hệ thống thông tin của thực thể.

FastCA 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.1.4 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 FastCA sẽ được sử dụng để thảo luận về những trường hợp ngoại lệ và những thiếu 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 FastCA và SE tin rằng chúng là mối đe doạ tức thì tới an ninh và tính thống nhất của FastCA:

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

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

(c) Nếu cần thiết, FastCA 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.1.5 Thông báo kết quả

Theo như bất kì một cuộc kiểm toán nào thì bên thực thể được kiểm toán sẽ cung cấp cho FastCA 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 Chứng thư hoặc gia hạn Chứng thư

Khách hàng sử dụng dịch vụ FastCA phải trả phí khi xin cấp chứng thư, quản lý và tạo mới chứng thư cho nhà cung cấp.

IX.1.2 Lệ phí sử dụng Chứng thư

Các thuê bao của dịch vụ FastCA và RA không phải trả phí để tạo ra kho chứng thư hay dịch vụ cung cấp thông tin chứng thư trực tuyến cho đối tác tin cậy.

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

Các thành phần tham gia dịch vụ FastCA không phải trả phí cho việc tạo ra các CRLs. Tuy nhiên CA được trả phí khi cung cấp các dịch vụ CRLs, OCSP hoặc các dịch vụ thu hồi giá trị gia tăng, dịch vụ cung cấp thông tin trạng thái khác.

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

Các thành phần tham gia dịch vụ FastCA không phải trả phí khi truy cập Quy chế chứng thực. 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

FastCA 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

FastCA sẽ duy trì 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.

IX.2.1.1 Các trường hợp FastCA tiến hành đền bù bảo hiểm và mức đền bù bảo hiểm

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

- Lỗi do CA gây ra, bao gồm lỗi kỹ thuật khi phát hành chứng thư theo trách nhiệm của CA.

- FastCA đưa ra các mức đền bù bảo hiểm theo các mức bảo hiểm chứng thư khác nhau.
- Việc đền bù bảo hiểm thực hiện theo đúng hợp đồng với thuê bao.

IX.2.1.2 Các trường hợp không được hưởng đền bù bảo hiểm

FastCA 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 thư.
- Các trường hợp sử dụng, cấu hình thiết bị không phù hợp, không nằm trong trách nhiệm của CA được sử dụng trong quá trình xử lý chứng thư.
- Khóa bí mật bị mất, bị phá huỷ do khách hàng.
- Khách hàng đánh mất hoặc để lộ code PIN bảo vệ khoá bí mật.
- 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 đền bù được thực hiện theo hợp đồng với thuê bao.

IX.2.2 Các tài sản khác

FastCA có quyền 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.

FastCA 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. FastCA 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 9.3.2 sẽ được đảm bảo tính mật và riêng tư ("thông tin mật/riêng tư")

- Các dữ liệu CA, được phê chuẩn hoặc không được phê chuẩn
- Các dữ liệu đơn xin cấp chứng thư

- Các khóa bí mật của thuê bao doanh nghiệp 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 FastCA hoặc một thuê bao.
- Các báo cáo kiểm toán tạo bởi FastCA 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 FastCA 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 mục 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

FastCA 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

FastCA sẽ tiến hành triển khai chính sách đảm bảo tính riêng , tuân theo luật riêng tư, FastCA 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 danh mục chứng thư 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 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 FastCA 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 riêng tư.

IX.4.6 Cung cấp thông tin mật theo yêu cầu của luật pháp hay cho quá trình quản trị

FastCA 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.4.7 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.5 Quyền sở hữu trí tuệ

IX.5.1 Quyền sở hữu trong chứng thư và thông tin thu hồi chứng thư.

CA có tất cả quyền sở hữu liên quan đến chứng thư và các thông tin thu hồi chứng thư mà họ đã ban hành. FastCA và khách hàng cho phép tái tạo và phân phối chứng thư mà không cần trả phí, với điều kiện chúng được tái tạo toàn bộ sử dụng chứng thư tuân theo thoả thuận với đối tác tin cậy. FastCA và khách hàng cũng cho phép đối tác tin cậy sử dụng các thông tin thu hồi để thực hiện chức năng của mình tuân theo thoả thuận sử dụng CRL, thoả thuận với đối tác tin cậy hay các thoả thuận thích hợp khác.

IX.5.2 Quyền sở hữu trong CPS

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

IX.5.3 Quyền sở hữu tên

Người đăng ký chứng thư có quyền sở hữu đối với thương hiệu, tên dịch vụ trong các đơn xin cấp chứng thư , và với tên phân biệt (distinguished name) trong chứng thư cấp.

IX.5.4 Quyền sở hữu khoá và các tài liệu của khoá

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

IX.6 Vấn đề đại diện và bảo lãnh

IX.6.1 Đại diện của CA và vấn đề bảo lãnh

Dịch vụ FastCA bảo đảm:

- Không có những thông tin không phù hợp với thực tế trong chứng thư.
- Không có thiếu sót ở các thông tin trong chứng thư.
- Chứng thư của CA phù hợp với yêu cầu trong CP và CPS.
- Dịch vụ thu hồi chứng thư 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.6.2 Đại diện của RA và vấn đề bảo lãnh

Các RA của dịch vụ FastCA bảo đảm:

- Không có những thông tin không phù hợp với thực tế trong chứng thư.
- Không có thiếu sót ở các thông tin trong chứng thư.
- Những chứng thư của RA tuân theo các yêu cầu trong CPS này.
- Dịch vụ thu hồi chứng thư 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.6.3 Đại diện của khách hàng và sự bảo lãnh

Khách hàng cam kết rằng:

- Mỗi chữ ký số được tạo sử dụng khoá bí mật tương ứng với khoá công khai liệt kê trong chứng thư là chữ ký điện tử của khách hàng. Chứng thư được chấp nhận và hoạt động (khi chưa hết hạn hay bị thu hồi) trong thời gian chữ ký số này được tạo.
- Khoá bí mật được bảo vệ và người không có thẩm quyền không thể truy cập vào khoá này.
- Tất cả các cam kết được đưa ra bởi khách hàng trong đơn xin cấp chứng thư là đúng sự thật.

- Tất cả những thông tin cung cấp bởi khách hàng và chứa bên trong chứng thư là đúng sự thật.
- Chứng thư được sử dụng cho các mục đích hợp pháp và tuân theo những yêu cầu trong CPS.
- Khách hàng là thuê bao cuối và không phải là một CA, không được phép sử dụng khoá bí mật kết hợp với bất kì khoá công khai nào được liệt kê trong chứng thư cho các mục đích ký số, hay đưa ra CRL, như là một CA.

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

IX.6.4 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.7 Vấn đề bồi thường

IX.7.1 Vấn đề bồi thường của khách hàng

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

- Những thông tin không hợp lệ do khách hàng cung cấp trên đơn xin cấp chứng thư.
- Lỗi của khách hàng để lộ những nhân tố, yếu tố liên quan đến đơn xin cấp chứng thư, sự bỏ sót do sự cẩu thả hay với mục đích lừa đảo.
- Lỗi của khách hàng trong việc bảo vệ khóa bí mật, 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.7.2 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 bồi thường cho FastCA hay các thành phần tham gia dịch vụ FastCA như CA và RA 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 một chứng thư không được đáp ứng trong một số trường hợp.
- Lỗi của đối tác tin cậy trong việc kiểm tra trạng thái của chứng thư để xác định chứng thư đã hết hạn hay bị thu hồi.

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

IX.8 Thời hạn và sự kết thúc

IX.8.1 Thời hạn

CPS bắt đầu có hiệu lực khi được công bố từ kho lưu trữ của dịch vụ FastCA. 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 FastCA.

IX.8.2 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.8.3 Ảnh hưởng của sự kết thúc và những tồn tại

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

IX.9 Thông báo riêng và thỏa thuận giữa các bên

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

IX.9.1 Sự sửa đổi

IX.9.1.1 Các thủ tục sửa đổi

Những sửa đổi của CPS sẽ được thực hiện bởi Cấp quản lý chính sách có thẩm quyền của FastCA. 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.9.1.2 Các trường hợp cần sửa đổi nhận diện đối tượng (OID)

Nếu cần thiết, FastCA 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.9.1.3 Cách thức và thời hạn thông báo

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

FastCA tập hợp những thay đổi về CPS từ các thành phần tham gia vào dịch vụ FastCA. Nếu FastCA cho rằng một sự thay đổi nào đó nên làm thì sẽ đề xuất thực hiện sự thay đổi đó. FastCA sẽ đưa ra thông báo về sự thay đổi đó phù hợp với mục này.

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

A. Thời điểm đưa ra sự sửa đổi

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

B. Cơ chế xử lý các sửa đổi

FastCA sẽ xem xét tất cả các đề xuất liên quan đến vấn đề sửa đổi bổ sung. FastCA 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.

FastCA 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 FastCA. Những sửa đổi có hiệu lực sau khi hết hạn sửa đổi.

IX.10 Thủ tục tranh chấp

IX.10.1 Thủ tục tranh chấp giữa FastCA, cộng tác và thuê bao

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

IX.10.2 Thủ tục tranh chấp giữa thuê bao và đối tác tin cậy

Những tranh chấp có liên quan đến dịch vụ FastCA 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.11 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 FastCA, 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.11.1 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.11.1.1 Trách nhiệm

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

IX.11.1.2 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.11.1.3 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.11.1.4 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 FastCA.