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, 06/2021

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 công cộng 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…)

1. GIỚI THIỆU

1.1 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.

1.2 Tên tài liệu và nhận dạng

- Tài liệu này được gọi là Quy chế chứng thực (CPS) của Nhà cung cấp dịch vụ chứng thực chữ ký số công cộng FastCA (gọi tắt là "Quy chế chứng thực của 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.

1.3 Đối tượng tham gia

a) FastCA

- FastCA là dịch vụ chứng thực chữ ký số công cộng của Công ty cổ phần chữ ký số FastCA.

b) RA (Registration Authority – RA)

- RA là một bộ phận của FastCA có 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.
- Đại lý của FastCA là một RA
- Bản thân FastCA cũng là một RA

c) Thuê bao (Subscriber):

- Thuê bao của FastCA là một đối tượng sở hữu chứng thư số do FastCA cung cấp.

d) Đối tượng khác

- Ngoài các đối tượng FastCA, RA, Thuê bao, FastCA không quản lý đối tượng nào khác

1.4 Sử dụng chứng thư số của FastCA

1.4.1 Sử dụng chứng thư số hợp lệ

- Chứng thư số của FastCA được cấp bởi RootCA quốc gia với các "Mục đích sử dụng" chính như sau: digitalSignature, nonrepudiation, keyAgreement, dataEncipherment và keyEncipherment (các trường trong Key Usage của chứng thư số).
- Thuê bao được sử dụng chứng thư số vào các mục đích được quy định bởi trường "Mục đích sử dụng" (KeyUsage) trong chứng thư số.
- Mục đích sử dụng không bị cấm bởi pháp luật, chính sách chứng thư số của RootCA, chính sách chứng thư số và quy chế chứng thực của FastCA và thỏa thuận của thuê bao với FastCA

1.4.2 Các trường hợp bị cấm

- Sử dụng chứng thư số sai mục đích, không được nêu ở mục 1.4.1 theo các thuộc tính của chứng thư (Key Usage) sẽ bị cấm.
- Chứng thư số do FastCA cấp không được sử dụng vào các mục đích như đảm bảo an ninh cho lĩnh vực hạt nhân, hệ thống điều khiển vũ khí…

- Chứng thư số do FastCA cấp không được sử dụng ngoài mục đích dân sự như trong lĩnh vực an ninh, quân sự, đảm bảo an ninh quốc gia.
- Chứng thư số do FastCA cấp không được sử dụng vào các mục đích vi phạm pháp luật.
- Chứng thư số của thuê bao FastCA không được sử dụng làm chứng thư số của CA khác.

1.5 Quản lý quy chế chứng thực

1.5.1 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 https://fastca.vn/download/CPS

1.5.2 Thông tin liên hệ

- Địa chỉ: Tầng 5, Tòa Nhà Sudico, Đường Mễ Trì, Phường Mễ Trì, Quận Nam Từ Liêm, Hà Nội, Việt Nam;
- Số điện thoại tổng đài: 1900.2158
- Email: info@fastcavn
- Website: www.fastca.vn

1.5.3 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 lý 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.
- Quy chế chứng thực này có hiệu lực trong toàn bộ thời gian cung cấp dịch vụ của FastCA.

1.5.4 Thủ tục phê duyệt Quy chế chứng thực

- Công ty cổ phần chữ ký số FastCA sẽ phê duyệt Quy chế chứng thực và phát hành quy chế trên website.

- Chứng thư số do FastCA cấp không được sử dụng ngoài mục đích dân sự như trong lĩnh vực an ninh, quân sự, đảm bảo an ninh quốc gia.
- Chứng thư số do FastCA cấp không được sử dụng vào các mục đích vi phạm pháp luật.
- Chứng thư số của thuê bao FastCA không được sử dụng làm chứng thư số của CA khác.

1.5 Quản lý quy chế chứng thực

1.5.1 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 https://fastca.vn/download/CPS

1.5.2 Thông tin liên hệ

- Địa chỉ: Tầng 5, Tòa Nhà Sudico, Đường Mễ Trì, Phường Mễ Trì, Quận Nam Từ Liêm, Hà Nội, Việt Nam;
- Số điện thoại tổng đài: 1900.2158
- Email: info@fastcavn
- Website: www.fastca.vn

1.5.3 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 lý 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.
- Quy chế chứng thực này có hiệu lực trong toàn bộ thời gian cung cấp dịch vụ của FastCA.

1.5.4 Thủ tục phê duyệt Quy chế chứng thực

- Công ty cổ phần chữ ký số 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.

1.6 Định nghĩa và từ viết tắt

(Chi tiết trong Danh mục từ viết tắt)

2. CÁC TRÁCH NHIỆM CÔNG BỐ VÀ LƯU TRỮ CHỨNG THƯ SỐ

2.1 Lưu trữ

- FastCA chịu trách nhiệm duy trì các địa chỉ lưu trữ các thông tin, cho phép truy nhập từ internet. FastCA sẽ công bố chứng thư số và thông tin thu hồi chứng thư số lên địa chỉ công cộng này. Các địa chỉ truy nhập được cụ thể trong các phần bên dưới.

2.2 Công bố thông tin chứng thư số

- 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.
- Các thông tin cần được công bố bao gồm:
  + CPS – Quy chế chứng thực:

    https://fastca.vn/download/CPS
  + Chứng thư số của FastCA:

    https://fastca.vn/download/fastca.crt
  + Chứng thư số của thuê bao:

    https://cts.fastca.vn/
  + CRL – Danh sách chứng thư số thu hồi:

    http://crl.fastca.vn/fastca.crl
  + OCSP – Trạng thái chứng thư số trực tuyến:

    http://ocsp.fastca.vn/
  + FastCA công bố các thông tin CA:

    https://fastca.vn

2.3 Tần suất công bố

- Quy chế chứng thực: được cập nhật khi FastCA có sự thay đổi về chính sách và sẽ công bố tại đường link đã trình bầy tại mục 2.2.

- Thỏa thuận thuê bao: được cập nhật khi cần thiết.
- Chứng thư số: được công bố khi chứng thư số được ban hành, thời gian tối đa cập nhật là 24h sau khi thuê bao xác minh tính chính xác của thông tin trên chứng thư số tới FastCA.
- Trạng thái chứng thư số: được công bố ngay lập tức lên OCSP.
- Danh sách chứng thư số bị thu hồi: được cập nhật hằng ngày.

2.4 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.

3. ĐỊNH DANH VÀ XÁC THỰC

3.1 Đặt tên thuê bao trong chứng thư số

3.1.1 Kiểu của tên

- Chứng thư số chứa một tên thuê bao, để phân biệt với các chứng thư số khác (Distinguished Names – DN) theo chuẩn X.501 trong trường Issuer và Subject.
- Các thuộc tính trong một DN mà FastCA sử dụng được mô tả trong bảng dưới đây:

Thuộc tính	Giá trị
Quốc gia (C)	Hai chữ cái chỉ tên quốc gia theo ISO, Việt Nam được ký hiệu là "VN"
Tên của thuê bao (CN)	Tên đối tượng sở hữu chứng thư số, tên miền nếu là chứng thư số SSL
Tổ chức (O)	Tên tổ chức/đơn vị quản lý đối tượng sở hữu chứng thư số.
Bộ phận tổ chức (OU)	Bộ phận thuộc tổ chức/đơn vị (O) mà đối tượng sở hữu chứng thư số thuộc. (*Chỉ đối với chứng thư số của cá nhân thuộc tổ chức*)
Tỉnh/Thành Phố (S)	Tên Tỉnh, Thành phố nơi sống/làm việc của đối tượng sở hữu chứng thư số bằng tiếng Việt, các chữ cái đầu viết hoa.
Địa chỉ email (E)	Địa chỉ email của đối tượng sở hữu chứng thư số
Mã duy nhất (UID)	Mã định danh của đối tượng sở hữu chứng thư số. - Đối với cá nhân Mã số định danh sẽ là: CMND:[số chứng minh nhân dân] hoặc HC:[số hộ chiếu] hoặc CCCD:[số thẻ căn cước công dân]. - Đối với cơ quan tổ chức mã đinh danh FastCA sẽ sử dụng là: MST:[mã số thuế] hoặc MNS:[mã quan hệ ngân sách] hoặc BHXH:[mã số bảo hiểm xã hội] hoặc SQĐ: [Số quyết định thành lập].

- Đối với các chứng thư số khác theo quy định của Bộ Thông tin và Truyền thông.

3.1.2 Tính duy nhất của tên thuê bao

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

3.1.3 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.

3.2 Xác minh đề nghị cấp chứng thư số lần đầu

3.2.1 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, định danh của chính phủ.
- Để đảm bảo tính bảo mật và tránh các trường hợp giả mạo, thuê bao cần xuất trình một trong các giấy tờ sau đây khi xin cấp chứng thư số từ FastCA:
  - CMND: [chứng minh nhân dân]
  - HC: [hộ chiếu]
  - CCCD: [thẻ căn cước công dân]
- 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.
- Hồ sơ xin cấp gồm có:
  + Đơn xin cấp chứng thư (theo mẫu của FastCA)
  + Giấy tờ xác thực nhận dạng cá nhân
  + Các giấy tờ liên quan (nếu có)
- Quy trình xác thực nhận dạng của cá nhân đăng ký chứng thư số như sau:

+ Người đăng ký nộp hồ sơ cho FastCA /RA.

+ FastCA /RA xác minh thông tin trên hồ sơ với các thông tin trên Giấy tờ xác thực nhận dạng cá nhân.

3.2.2 Xác thực danh tính tổ chức, doanh nghiệp

- Đối với tổ chức, doanh nghiệp, FastCA sẽ xác minh các thông tin sau:

  - Thông tin xác định sự tồn tại của tổ chức, gồm có: tên tổ chức, giấy chứng nhận đăng ký kinh doanh hoặc giấy phép hoạt động, địa chỉ.

  - FastCA, hoặc các RA của FastCA thực hiện xác thực nhận dạng của tổ chức theo các thông tin nêu trên.

  - Khi chứng thư số của tổ chức có chứa tên cá nhân làm đại diện, cần thực hiện các thủ tục xác thực sự ủy quyền như 3.2.4.

  - Tên miền hay email chứa trong chứng thư số khi cần xác thực cũng được xác minh về quyền sở hữu của tổ chức với tên miền, email đó. Tên miền được xác thực dựa vào giấy đăng ký tên miền hoặc thông qua cơ sở dữ liệu của nhà cung cấp tên miền. Địa chỉ email được xác thực bằng cách yêu cầu trả lời lại email đã được gửi từ FastCA.

3.2.3 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 số.

3.2.4 Xác thực sự ủy quyền

- Khi chứng thư số của tổ chức, doanh nghiệp có chứa tên cá nhân làm đại diện, cần thực hiện các thủ tục xác thực sự ủy quyền, các thủ tục xác thực này bao gồm:

  - Xác thực sự tồn tại của tổ chức, doanh nghiệp như 3.2.2.

  - Xác thực cá nhân như 3.2.1 và xác thực sự ủy quyền của tổ chức đối với cá nhân đó bằng giấy ủy quyền. Trong một số trường hợp cần làm rõ, FastCA sẽ xác thực bổ sung bằng cách gọi điện hoặc xác thực trực tiếp tại tổ chức về cá nhân đó.

3.3 Xác minh đề nghị thay làm mới chứng thư số

- 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"). Như vậy đối với FastCA việc làm mới chứng thư số có thể có 2 trường hợp:
    - Sinh một cặp khóa mới thay thế cặp khóa trong chứng thư số đã hết hạn (đổi khóa - rekey).
    - Tạo chứng thư số mới cho một cặp khóa đang tồn tại (gia hạn - renewal).

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

- Thời hạn xin làm mới của thuê bao: trước khi chứng thư số hết hạn. Sau khi chứng thư số hết hạn, yêu cầu làm mới chứng thư số sẽ không được chấp nhận, thuê bao phải thực hiện lại các bước như đăng ký mới.
- Thủ tục thay đổi cặp khóa đảm bảo rằng cá nhân hay một tổ chức có nhu cầu 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 FastCA hoặc RA có trách nhiệm xác thực yêu cầu làm mới của thuê bao. Sau khi xác thực, FastCA cấp chứng thư số mới cho thuê bao. Sau khi cấp lại chứng thư số mới, FastCA hoặc 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.

3.3.2 Nhận diện và xác thực việc cấp lại chứng thư 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, đăng ký kinh doanh không hợp lệ…)
    - Chứng thư số đã sử dụng vào các mục đích trái pháp luật, các hoạt động ảnh hưởng tới uy tín của FastCA.

- 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 tổ chức đã sử dụng chứng thư đó, đồng thời lý do khôi phục chứng thư là hợp lệ. Chứng thư của một tổ chức được khôi phục sẽ chứa 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.

3.4 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 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 hoặc các phương tiện truyền thông khác).
  - Thông báo tới thuê bao các lý do chắc chắn về cấp chứng thư mà cá nhân hay tổ chức yêu cầu, trên thực tế việc thông tin với các thuê bao phụ thuộc vào nhiều trường hợp khác nhau nhưng có thể là một trong các cách sau: điện thoại, fax, thư điện tử, thư tín hay các dịch vụ đưa tin và các phương tiện truyền thông.

4. CÁC YÊU CẦU ĐỐI VỚI VÒNG ĐỜI CHỨNG THƯ SỐ CỦA THUÊ BAO

4.1 Đăng ký 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.
- ***Ghi chú:*** 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.

4.1.1 Các đối tượng có thể xin cấp chứng thư số.

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

+ Bất cứ cá nhân nào đủ điều kiện theo quy định của pháp luật và CPS này có như cầu sử dụng chứng thư số.

+ Đại diện theo pháp luật của tổ chức, doanh nghiệp đủ điều kiện theo quy định của pháp luật và CPS này có nhu cầu sử dụng chứng thư số.

+ Các đại lý đăng ký làm RA cho FastCA.

4.1.2 Tiến trình xử lý và trách nhiệm của thuê bao chứng thư số.

4.1.2.1 Chứng thư số của thuê bao cá nhân, tổ chức

- Thuê bao làm thủ tục và ký một thỏa thuận với FastCA, các điều khoản và cam kết trong thỏa thuận được mô tả trong phần 9.6.3

- Thuê bao có thể lựa chọn một trong 2 hình thức sau:

  + Tạo khóa phía FastCA/RA: Thuê bao hoàn thành đơn đăng ký chứng thư số và cung cấp tài liệu xác minh thông tin đã kê khai.

  + Tạo khóa phía thuê bao: thuê bao đăng ký thực hiện các bước sau:

    - Thuê bao hoàn thành đơn đăng ký chứng thư số và cung cấp tài liệu xác minh thông tin đã kê khai.

    - Tạo hoặc chuẩn bị cặp khóa

    - Gửi khóa công khai trực tiếp cho FastCA hoặc thông qua RA

    - Chứng minh quyền sở hữu và tính duy nhất của khóa bí mật tương ứng với khóa công khai vừa gửi theo 3.2.1.

4.1.2.2 Chứng thư số của RA

- Để đăng ký cấp chứng thư số từ FastCA, RA phải thực hiện việc ký hợp đồng với FastCA và tiến hành các thủ tục đăng ký cấp chứng thư số tương tự như các thuê bao.

- FastCA sẽ thực hiện sinh khóa cho RA.

- Trách nhiệm của RA được làm rõ trong phần 9.6.2.

4.2 Xử lý đơn xin cấp chứng thư

4.2.1 Chức năng nhận biết và xác thực

- FastCA/RA sẽ nhận biết và xác thực các thông tin khách hàng theo mục 3.2

4.2.2 Phê duyệt hoặc từ chối các đơn xin cấp chứng thư

- FastCA/RA sẽ chấp nhận yêu cầu cấp một hoặc nhiều chứng thư số khi tuân theo các tiêu chuẩn sau đây:
  + Nhận biết và xác thực các thông tin về khách hàng theo mục 3.2.
  + Phí dịch vụ đã thanh toán.
- FastCA/RA sẽ từ chối yêu cầu cấp một hoặc nhiều chứng thư số theo tiêu chí sau đây:
  + Nhận biết và xác thực các thông tin về đối tượng đăng ký cấp chứng thư số không thành công theo mục 3.2.
  + Đối tượng yêu cầu cấp chứng thư số không cung cấp tài liệu theo yêu cầu.
  + Đối tượng yêu cầu cấp chứng thư số không trả lời yêu cầu trong thời gian quy định.
  + Phí dịch vụ chưa thanh toán.
  + FastCA/RA có lý do tin rằng việc cung cấp chứng thư cho thuê bao có thể gây ảnh hưởng đến uy tín của FastCA.

4.2.3 Thời gian xử lý các đơn xin cấp chứng thư

- Thời gian xử lý một yêu cầu cấp chứng thư số được quy định trong bản thỏa thuận giữa thuê bao với FastCA.

4.3 Sinh chứng thư số

4.3.1 Vai trò của FastCA trong quá trình sinh chứng thư số

Chứng thư số được tạo và cấp sau khi FastCA chấp nhận yêu cầu cấp chứng thư số hoặc sau khi nhận được một yêu cầu cấp chứng thư số của RA. FastCA tạo và cấp chứng thư số dựa trên những thông tin trong bản yêu cầu cấp chứng thư số sau khi yêu cầu này được xác thực định danh.

4.3.2 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 đồng thời cung cấp phương thức truy cập tới chứng thư số đó để kiểm tra tính sẵn sàng của chứng thư.

- Chứng thư số có hiệu lực sẽ cho phép thuê bao tải chứng thư số từ trang web hoặc FastCA gửi trực tiếp tới thuê bao.

4.4 Công bố chứng thư số

4.4.1 Chấp nhận chứng thư số của thuê bao

- Thuê bao thể hiện sự chấp nhận chứng thư số khi ký vào bản xác nhận thông tin trên chứng thư số chính xác với thông tin thuê bao đăng ký, bản xác nhận này được FastCA lưu trữ.

4.4.2 Công khai chứng thư của FastCA

- FastCA công bố chứng thư số 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.

4.4.3 Thông báo việc phát hành chứng thư đến các đối tượng khác

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

4.5 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.
- 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.

4.5.1 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.

4.5.2 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 về độ tin cậy của chứng thư số với FastCA.
- 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.
- Người nhận cần dựa vào các thông tin sau để đánh giá sự tin cậy một cách độc lập của chứng thư số:
    - 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.

4.6 Gia hạn chứng thư số cho thuê bao

- Gia hạn chứng thư số là việc cấp phát 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.

4.6.1 Các tình huống gia hạn chứng thư số

- 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.

4.6.2 Ai có thể yêu cầu gia hạn

- Chỉ có thuê bao cá nhân hoặc đại diện theo pháp luật của tổ chức đối với thuê bao tổ chức mới được yêu cầu gia hạn chứng thư số.

4.6.3 Xử lý yêu cầu gia hạn

- Thuê bao cần tiến hành kê khai đầy đủ thông tin yêu cầu trong giấy đề nghị gia hạn chứng thư số và các thủ tục đã đề cập tại 4.1.2
- FastCA/RA tiến hành xác thực thông tin của thuê bao trong giấy đề nghị gia hạn chứng thư số theo phần 3.2. Nếu thông tin xác thực, việc gia hạn được tiến hành. Nếu thông tin sai lệch, yêu cầu bị từ chối.

4.6.4 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.

4.6.5 Sự chấp nhận chứng thư số gia hạn

- Tương tự mục 4.4.1

4.6.6 Công bố chứng thư số được gia hạn

- Tương tự mục 4.4.2

4.6.7 Thông báo tạo chứng thư số mới cho các thực thể khác

- Tương tự mục 4.4.3

- Tương tự như sự chấp nhận chứng thư số được cấp mới. Chi tiết đã trình bầy tại phần 4.4.1.

4.7.6 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. Chi tiết đã trình bầy tại phần 4.4.2.

4.7.7 Thông báo tạo chứng thư số mới cho các thực thể khác

- Tương tự đã trình bầy tại phần 4.4.3.

4.8 Thay đổi thông tin chứng thư số

4.8.1 Các tình huống thay đổi chứng thư số

- Khi thông tin chứng thư số cần thay đổi, trừ những trường hợp đã nêu trong 4.6 và 4.7

4.8.2 Ai có thể yêu cầu thay đổi chứng thư số

- Chỉ thuê bao cá nhân hoặc đại diện theo pháp luật của tổ chức đối với thuê bao tổ chức mới có thể yêu cầu thay đổi chứng thư số. Xem phần 4.1.

4.8.3 Xử lý yêu cầu thay đổi chứng thư số

- FastCA/RA sẽ thực hiện nhận dạng và xác thực mọi thông tin thuê bao. Xem phần 3.2.

4.8.4 Thông báo chứng thư số mới cho CA

- Thông báo về sự đổi chứng thư số cũng giống như thông báo khi chứng thư số được cấp mới. Xem phần 4.3.2.

4.8.5 Thủ tục chấp nhận chứng thư số mới được thay đổi

- Tương tự như sự chấp nhận chứng thư số được cấp mới. Xem phần 4.4.1.

4.8.6 Công bố chứng thư số mới bởi CA

- Chứng thư số được đổi khóa sẽ được công bố vào kho để có thể truy xuất. Xem phần 4.4.2.

4.8.7 Thông báo cho các thực thể khác

- Xem phần 4.4.3.

4.9 Thu hồi chứng thư số của thuê bao

4.9.1 Các tình huống thu hồi chứng thư số

- Chỉ trong những trường hợp được liệt kê dưới đây, yêu cầu chứng thư số sẽ bị thu hồi khi thuê bao hay các đối tượng có thẩm quyền (RA, FastCA) yêu cầu và được công bố lên 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.
- 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 tổ chức cung cấp dịch vụ chứng thực chữ ký số của mình 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;
  + Khi có yêu cầu của cơ quan chức năng nhà nước có thẩm quyền hoặc Bộ Thông tin và Truyền thông;
  + Theo điều kiện thu hồi chứng thư số đã được quy định trong hợp đồng giữa thuê bao và FastCA.
- Thuê bao cần nêu rõ lý do yêu cầu thu hồi chứng thư số đến FastCA:
  + 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 hoặc CPS này;
  + Thỏa thuận với thuê bao đã kết thúc hoặc sự ủy quyền của một tổ chức cho một thuê bao đã kết thúc;
  + FastCA có lý do tin tưởng rằng một yêu cầu cấp chứng thư số thực tế bị sai;
  + FastCA 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 hay không, FastCA/RA sẽ xem xét những yếu tố sau:

+ Nhận được nhiều phản ánh.

+ Mức độ tin cậy của thông tin phản ánh.

+ Các phàn nàn liên quan đến các yếu tố pháp luật

+ Phàn nàn về thiệt hại gây ra do việc sử dụng chứng thư số của thuê bao.

+ Nếu FastCA đơn phương thu hồi chứng thư số, FastCA sẽ thông báo cho thuê bao và công bố trên cơ sở dữ liệu về chứng thư số việc thu hồi.

4.9.2 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, đại diện theo pháp luật 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 chức năng có thẩm quyền hoặc Bộ Thông tin và Truyền thông.

4.9.3 Thủ tục thu hồi chứng thư số

- Khi có căn cứ thu hồi chứng thư số, FastCA thực hiện 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, FastCA 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 gửi các thông tin và xác thực quyền sở hữu khóa đối với chứng thư số bị thu hồi cơ sở dữ liệu của FastCA.
  + FastCA nhận một thông điệp từ thuê bao yêu cầu thu hồi chứng thư số, yêu cầu thu hồi này được ký bằng chứng thư số được cấp hoặc có chứa thông tin chứng thư số để có thể kiểm tra và tham chiếu tới chứng thư số bị thu hồi.
  + FastCA liên hệ xác thực để đảm bảo chắc chắn yêu cầu thu hồi là của chủ sở hữu chứng thư số đó. Tùy vào tình huống cụ thể, phương tiện đối thoại có thể là điện thoại, email, thư tín hay thông qua các phương tiện truyền thông khác.
- CA/RA được quyền yêu cầu thu hồi chứng thư số của người dùng cuối trong miền con của CA/RA. FastCA sẽ xác thực nhận 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.

4.9.4 Thời hạn yêu cầu thu hồi chứng thư số

- Thuê bao sẽ gửi yêu cầu thu hồi chứng thư số ngay lập tức khi phát hiệt hay nghi ngờ khóa bí mật bị mất/lộ.
- Quản trị hệ thống BkavCA/RA sẽ gửi yêu cầu thu hồi chứng thư số ngay khi nhận được yêu cầu từ thuê bao hoặc nhận sau khi xác thực thông tin phàn nàn.

4.9.5 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.

4.9.6 Tần suất tạo CRL mới

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

4.9.7 Giới hạn trễ cho CRL

- CRL được công bố ngay lập tức sau khi được tạo ra

4.9.8 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.

4.9.9 Các yêu cầu kiểm tra trạng thái trực tuyến

- Người nhận phải kiểm tra trạng thái của một chứng thư số nếu muốn 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.

4.9.10 Các dạng thông tin trạng thái thu hồi khác

- FastCA không sử dụng dạng thông tin trạng thái thu hồi nào khác ngoài CRL và OCSP.

4.9.11 Những ràng buộc đặc biệt liên quan đến việc khóa bị lộ

- Khi khóa bí mật FastCA bị mất/lộ hoặc nghi ngờ mất/lộ, FastCA thực hiện:
    - Lập tức báo cho RootCA về việc bị mất/lộ hoặc nghi ngờ mất/lộ khóa.
    - Tạm dừng cấp phát chứng thư số cho tới khi có kết quả xác minh.
    - Thực hiện theo hướng dẫn của RootCA nếu bị mất/lộ khóa.

4.10 Tạm dừng hoặc phục hồi chứng thư số của thuê bao

4.10.1 Các tình huống tạm dừng hoặc phục hồi chứng thư số

Chứng thư số của thuê bao bị tạm dừng trong các 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 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 130/2018/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 tiến hành tố tụng, cơ quan công an hoặc Bộ Thông tin và Truyền thông;
- Theo điều kiện tạm dừng chứng thư số đã được quy định trong hợp đồng giữa thuê bao và FastCA.
- Khi có căn cứ tạm dừng chứng thư số, FastCA sẽ tiến hành tạm dừng, đồng thời, thông báo ngay 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.

- ***Chứng thư số của thuê bao được phục hồi khi không còn căn cứ để tạm dừng chứng thư số hoặc thời hạn tạm dừng theo yêu cầu đã hết.***

4.10.2 Ai có thể yêu cầu tạm dừng hoặc phục hồi các chứng thư số

- Những đối tượng sau có thể yêu cầu tạm dừng chứng thư số:
  - Thuê bao
  - FastCA
  - Cơ quan tố tụng, cơ quan công an hoặc Bộ Thông tin và Truyền thông

4.10.3 Thủ tục tạm dừng hoặc phục hồi chứng thư số

- Theo quy định trong hợp đồng giữa thuê bao và FastCA

4.10.4 Giới hạn xử lý tạm dừng hoặc phục hồi chứng thư số

- Không có quy định cụ thể về giới hạn xử lý tạm dừng chứng thư số.

4.11 Dịch vụ cung cấp thông tin trạng thái chứng thư số

4.11.1 Đặc điểm

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

4.11.2 Tính sẵn sàng của dịch vụ

- Dịch vụ trạng thái chứng thư số được duy trì 24/7 (khi có vấn đề về dịch vụ FastCA sẽ thông báo kế hoạch xử lý trên website của FastCA).

4.11.3 Tùy chọn đặc biệt

- OCSP là dịch vụ tùy chọn, miễn phí.

4.12 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.

4.13 Lưu trữ và phục hồi khóa bí mật của thuê bao

- Hiện tại, FastCA không thực hiện việc lưu trữ khóa bí mật của thuê bao cũng như cung cấp dịch vụ phục hồi khóa. Khóa bí mật được bảo quản bởi chính thuê bao.
- Tuy nhiên, cơ chế này hoàn toàn có thể thay đổi, phụ thuộc vào yêu cầu của luật pháp.

5. CÁC KIỂM SOÁT THIẾT BỊ, QUẢN LÝ VÀ VẬN HÀNH

5.1 Các kiểm soát an ninh vật lý

5.1.1 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 các tài khoản truy cập vào từng thành phần hệ thống, trang thiết bị lần thứ ba.

5.1.2 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.

5.1.3 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.

5.1.4 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 CMC IDC tại tòa nhà CMC, Duy Tân, Dịch Vọng Hậu, Cầu Giấy, 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.

5.2 Quy trình kiểm soát

5.2.1 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 số.
  + Việc quản lý thông tin thuê bao, thông tin yêu cầu từ thuê bao.
- Những người được tin cậy có thể bao gồm nhưng không giới hạn các đối tượng sau:
  + Người đứng đầu hệ thống.

+ Người quản trị hệ thống và bộ phận quản trị hệ thống.
+ Người phụ trách cấp phát chứng thư số và bộ phận phụ trách cấp phát chứng thư số.

- Những người được tin tưởng đều được xác minh về nhân thân, khả năng đảm bảo đáp ứng yêu cầu công việc trước khi được giao nhiệm vụ.

5.2.2 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.

5.2.3 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, căn cước công dân, hộ chiếu. Tổ chức có trách nhiệm xác minh tuân theo các thủ tục được đưa ra trong CPS.

5.2.4 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 số.
+ Quản lý thông tin, yêu cầu của thuê bao.

5.3 Quản lý nhân sự

5.3.1 Khả năng chuyên môn, kinh nghiệm và các yêu cầu chứng minh sự trong sạch

- Những người tin cậy của FastCA được xác minh dựa trên: khả năng và kinh nghiệm chuyên môn đáp ứng các nhu cầu công việc, các bằng chứng chứng minh sự trong sạch về lý lịch.
- Các thành viên của FastCA đều phải đảm bảo chất lượng và được huấn luyện, kiểm tra thường xuyên.

5.3.2 Các thủ tục kiểm tra lý lịch, trình độ.

- Trước khi bổ nhiệm nhân viên vào một nhiệm vụ cần được tin tưởng, FastCA kiểm tra các thông tin sau:
  + Kiểm tra, xác minh thông tin theo sơ yếu lý lịch.
  + Xác minh trình độ học vấn cao nhất đạt được.
  + Xem xét các thông tin tiền án/tiền sự (nếu có).
  + Xem xét dấu hiệu không tốt về thông tin tài chính, tín dụng.

5.3.3 Yêu cầu về đào tạo

- FastCA 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 chính sách và thủ tục của FastCA.
  + Các phiên bản phần cứng và phần mềm đang được sử dụng.
  + Trách nhiệm công việc.

+ Sử dụng và vận hành các thiết bị phần cứng và phần mềm.

+ Xử lý các sự cố.

+ Các thủ tục duy trì tính liên tục của dịch vụ khi có thảm họa.

5.3.4 Tần suất đào tạo và đào tạo lại

- FastCA 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.

5.3.5 Kỷ luật đối với các hoạt động không hợp pháp

- FastCA 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.

5.3.6 Yêu cầu đối với các nhà thầu độc lập

- Trong một số trường hợp, các cố vấn độc lập có thể được thuê để thực hiện một số công việc cần sự tin tưởng của FastCA. Những người này cũng phải tuân theo các tiêu chuẩn an ninh như nhân viên của FastCA. Nếu các cố vấn không đáp ứng đủ các tiêu chí trong 5.3.2, họ chỉ được phép thực hiện công việc khi có sự giám sát của người được tin tưởng của FastCA.

5.3.7 Cung cấp tài liệu cho nhân viên

- FastCA cung cấp các tài liệu cần thiết cho nhân viên, đảm bảo các nhân viên có thể thực hiện tốt công việc với các tài liệu được cung cấp.

5.4 Các quy trình ghi nhật ký kiểm toán

5.4.1 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 được thực hiện tự động hay và thủ công tùy vào từng trường hợp:

a. 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, yêu cầu khóa và thu hồi chứng thư số;

+ Tất cả các hoạt động xác minh được quy định trong các Yêu cầu này và Quy chế chứng thực;
+ Phê duyệt và từ chối yêu cầu chứng thư;
+ Phát hành chứng thư;
+ Tạo danh sách, ban hành CRL và các truy vấn OCSP.

b. Các sự kiện liên quan đến an ninh bảo mật, bao gồm:

+ Các nỗ lực truy cập hệ thống PKI thành công và không thành công;
+ Hành động đọc, ghi hoặc xóa các file, bản ghi nhạy cảm.
+ 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.

5.4.2 Tần suất xử lý ghi chép

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

5.4.3 Thời gian lưu trữ nhật ký kiểm toán

Nhật ký sẽ được giữ tại hệ thống ít nhất 2 tháng sau khi xử lý và sau đó được chuyển sang khu vực lưu trữ (phần 5.5.2)

5.4.4 Bảo vệ nhật ký kiểm toán

Nhật ký được bảo vệ với trước các hành động xem, thay đổi, xóa hay các tác động khác mà không được phép.

5.4.5 Các thủ tục sao lưu nhật ký kiểm toán

Nhật ký được backup theo chế độ backup chung của FastCA

5.4.6 Hệ thống thu thập kiểm toán (bên trong và bên ngoài)

- Các log ứng dụng, hệ điều hành và mạng được ghi lại tự động
- Một số log được ghi bằng tay bởi nhân viên.

5.4.7 Thông báo tới đối tượng thực hiện sự kiện.

Không có điều khoản.

5.4.8 Đánh giá tính dễ bị tổn thương.

Dữ liệu nhật ký sẽ được đưa vào phân tích, kết quả phân tích sẽ cho biết các nguy cơ tiềm tàng trong hệ thống, từ đó có phương án khắc phục

5.5 Lưu trữ hồ sơ

5.5.1 Các loại hồ sơ được lưu trữ

- Mọi dữ liệu nhật ký trong phần 5.4.
- Thông tin đơn xin cấp chứng thư số.
- Các thông tin bổ sung của đơn xin cấp chứng thư số.
- Thông tin vòng đời chứng thư số như: thu hồi, đổi khóa, làm mới…
- Các thông tin khác theo quy định của Bộ TTTT

5.5.2 Thời gian lưu trữ

Ít nhất 5 năm kể từ ngày chứng thư số hết hạn hoặc hủy bỏ.

5.5.3 Bảo vệ lưu trữ

Hệ thống lưu dữ liệu lưu trữ được bảo vệ để chỉ những người được phép mới có thể truy nhập. Dữ liệu lưu trữ được bảo vệ theo các phương pháp cần thiết, chống lại việc xem, thay đổi, xóa hay các thao tác khác không được cho phép. Hệ thống chứa dữ liệu lưu trữ và ứng dụng xử lý dữ liệu lưu trữ được duy trì để đảm bảo dữ liệu lưu trữ có thể được truy nhập trong khoảng thời gian được quy định trong quy chế chứng thực này.

5.5.4 Các thủ tục sao lưu lưu trữ

Dữ liệu lưu trữ được backup theo chế độ backup chung của FastCA

5.5.5 Dán nhãn thời gian của các bản ghi

Chứng thư số, CRL chứa thông tin thời gian, ngày tháng. Thông tin thời gian này không cần được mã hóa.

5.5.6 Hệ thống lưu trữ (bên trong hoặc bên ngoài)

FastCA sẽ sử dụng hệ thống lưu trữ tập trung, trừ trường hợp trừ trường hợp khách hàng doanh nghiệp với vai trò là RA.

5.5.7 Các thủ tục thu thập và xác minh thông tin lưu trữ

- Chỉ những người được cấp quyền mới được phép truy nhập tới thông tin lưu trữ.
- Thông tin lưu trữ sẽ được kiểm tra tính toàn vẹn khi được lấy ra.

5.6 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.
- Trước khi chứng thư số của FastCA hết hạn, theo quy định, FastCA sẽ xin cấp một chứng thư số mới và sử dụng chứng thư số mới để ban hành chứng thư số mới này cho các thuê bao.
- Cặp khóa của FastCA sẽ không được sử dụng quá thời gian có hiệu lực của nó được quy định trong quy chế này. Chứng thư số của FastCA có thể được gia hạn (đổi khóa) khi trước khi cặp khóa cũ hết hạn.
- Trước khi hết hạn chứng thư số của FastCA, các thủ tục được ban hành cho phép chuyển tiếp (changeover) từ cặp khóa cũ sang cặp khóa mới cho các thực thể thuộc phạm vi quản lý của FastCA. Quá trình chuyển tiếp khóa của FastCA đảm bảo rằng:
  + FastCA chỉ ban hành chứng thư số mới cho thuê bao trước thời điểm nhất định so với ngày hết hạn cặp khóa. Thời điểm này là thời điểm tạm dừng ban hành chứng thư số, do pháp luật quy định.
  + Khi nhận được yêu cầu ban hành chứng thư số sau thời điểm tạm dừng ban hành chứng thư số trên, FastCA sử dụng cặp khóa mới để ban hành chứng thư số cho thuê bao.
- FastCA tiếp tục ký lên CRL bằng cặp khóa cũ đến khi nào hết hạn toàn bộ chứng thư số được ban hành bởi cặp khóa cũ.

5.7 Xử lý khi có sự cố và thảm họa

5.7.1 Các thủ tục kiểm soát sự cố và thảm họa

- Các thông tin sau được backup đề phòng có sự cố và thảm họa: dữ liệu về đơn xin cấp chứng thư số, dữ liệu nhật ký, và các bản ghi chứng thư số được tạo ra.
- Khi có sự cố, các dữ liệu được phục hồi theo các thủ tục đã có.

5.7.2 Sự cố về máy tính, phần mềm và dữ liệu

Khi có các sự cố về máy tính, phần mềm và dữ liệu, các thủ tục xử lý sự cố được thực hiện. Mỗi sự cố sẽ có các quy trình xử lý khác nhau. Nếu sự cố nghiêm trọng, các thủ tục phục hồi sẽ được thực hiện.

5.7.3 Thủ tục xử lý khi làm mất/lộ khoá bí mật

- Khi khóa bí mật của FastCA nghi ngờ bị mất/lộ, FastCA sẽ thực hiện thủ tục xử lý khi khóa bị lộ. Đội xử lý sự cố an ninh của FastCA chịu trách nhiệm điều phối thực hiện các bước trong thủ tục này. Đội xử lý sự cố an ninh bao gồm người đứng đầu FastCA, người phụ trách kỹ thuật và người phụ trách cấp phát chứng thư số.
- Nếu chứng thư số của FastCA bị thu hồi, các thủ tục sau sẽ được thực hiện:
  + Trạng thái thu hồi chứng thư số của FastCA sẽ được công bố bởi RootCA.
  + FastCA cố gắng thông báo cho toàn bộ thuê bảo trong hệ thống FastCA dừng sử dụng các chứng thư số do FastCA ban hành.
  + FastCA xin cấp chứng thư số mới từ RootCA và ban hành chứng thư số cho các thuê bao của mình để họ tiếp tục sử dụng.

5.7.4 Khả năng phục hồi hệ thống sau thảm hoạ

- FastCA thực hiện các kế hoạch dự phòng, đảm bảo hoạt động liên tục kể cả có thảm họa. Kế hoạch này được xây dựng này được kiểm tra, thử nghiệm và xem xét định kỳ.
- FastCA có khả năng phục hồi những hoạt động quan trọng trong vòng 24 giờ sau khi một thảm họa xảy ra. Ít nhất các hoạt động sau sẽ được phục hồi:
  + Ban hành chứng thư số.
  + Thu hồi chứng thư số.

+ Công bố thông tin thu hồi chứng thư số.

- Cơ sở dữ liệu của FastCA phục hồi thảm họa sẽ được đồng bộ với cơ sở dữ liệu chính trong thời gian phù hợp, ít nhất là một ngày một lần đồng bộ.
- Kế hoạch phục hồi của FastCA được thiết kế có khả năng phục hồi hoạt động toàn bộ hệ thống trong vòng một tuần.
- FastCA dự phòng các thiết bị phần cứng và phần mềm cung cấp dịch vụ. Khóa bí mật của FastCA cũng được dự phòng và duy trì phục vụ cho mục đích phục hồi hệ thống.

5.8 Kết thúc sự hoạt động của CA hay RA

- Khi không còn hoạt động, FastCA hoặc RA dùng mọi biện pháp cố gắng thông báo cho thuê bao các đối tượng khác trước khi dừng hoạt động. FastCA, RA sẽ có kế hoạch kết thúc nhằm giảm thiểu thiệt hại nhất cho khách hàng. FastCA thực hiện kế hoạch kết thúc như sau:
  + Chuẩn bị thông báo cho các thành viên bị ảnh hưởng (thuê bao, RA nếu cần).
  + Chịu chi phí cho các thông báo.
  + Bảo quản dữ liệu lưu trữ và bản ghi của CA trong thời gian được quy định bởi quy chế này.
  + Tiếp tục dịch vụ hỗ trợ thuê bao và khách hàng tới khi các chứng thư số do FastCA ban hành hết hạn.
  + Tiếp tục dịch vụ ban hành CRL và duy trì OCSP tới khi các chứng thư số do FastCA ban hành hết hạn.
  + Thu hồi chứng thư số của thuê bao nếu cần thiết.
  + Có chính sách trả lại tiền cho thuê bao bị thu hồi chứng thư số nếu chứng thư số của họ chưa hết hạn, chưa bị thu hồi nhưng phải thu hồi do kế hoạch dừng hoạt động. Trong trường hợp có thể, FastCA thỏa thuận cùng thuê bao bị thu hồi chứng thư số về việc thuê bao chuyển sang sử dụng dịch vụ tại nhà cung cấp dịch vụ khác, chi phí và các thủ tục cần thiết sẽ do FastCA đảm nhiệm.
  + Thực hiện các thủ tục chuẩn bị trước khi chuyển các dịch vụ chứng thực sang cho CA khác.

6. VẤN ĐỀ AN TOÀN, AN NINH KỸ THUẬT

6.1 Sinh khóa và cài đặt

6.1.1 An ninh sinh cặp khóa cho FastCA

- Đối với khóa của nhà cung cấp dịch vụ FastCA, các cặp khóa sẽ được sinh trực tiếp tại các thiết bị HSM chuyên dụng đạt chuẩn FIPS 140-2 level 3.
- 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…

6.1.2 An ninh sinh cặp khóa cho thuê bao

- Thuê bao tự sinh khóa trên thiết bị an toàn đáp ứng tối thiểu tiêu chuẩn FIPS 140-2 level 2 như PKI Token hoặc thiết bị HSM, thuộc sự quản lý của thuê bao.
- FastCA hoặc các đại lý RA của FastCA hướng dẫn thuê bao sinh khóa trên thiết bị PKI Token an toàn hoặc thiết bị HSM.
- FastCA không lưu trữ bất kỳ khóa bí mật (Khóa bí mật) nào của thuê bao.

6.1.3 Gửi khóa bí mật cho thuê bao

- Khách hàng tự sinh khóa trên thiết bị USB Token/Smart Card tại máy tính cá nhân. 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. 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 nhằm tránh việc bị đánh cắp và thay đổi thông tin. 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.

+ 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.

+ 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 liên hệ với FastCA để được hỗ trợ cho việc thu hồi chứng thư đã bị lộ.

+ Sau khi hoàn thiện các bước xác minh thông tin thì thuê bao có thể sinh ra cặp khóa mới và hệ thống CA của FastCA trả về một chứng thư số cho người đăng ký.

6.1.4 Gửi khóa công khai cho FastCA

- Khi một khóa công khai từ thuê bao 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 thông điệp dạng 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.

- Nếu cặp khóa được tạo bên phía FastCA, việc gửi khóa cho CA là không cần thiết.

6.1.5 Gửi Khóa công khai của FastCA 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.

6.1.6 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.

6.1.7 Các tham số sinh Khóa công khai và kiểm tra chất lượng

Quá trình sinh khóa công khai tuân theo tiêu chuẩn PKCS#1 đáp ứng theo tiêu chuẩn được quy định tại Thông tư số 06/2015/TT-BTTT.

6.1.8 Mục đích sử dụng khóa (trường Key Usage của X.509 v3)

Xem phần 7.1.2.1

6.2 Bảo vệ khóa bí mật và kiểm soát module mã hóa

6.2.1 Tiêu chuẩn module mã hóa

FastCA sử dụng thiết bị mã hóa phần cứng chuyên dụng (Hardware Security Module) để lưu trữ khóa bí mật của FastCA. Thiết bị HSM của FastCA đáp ứng chuẩn chuẩn FIPS 140-2 level 3.

6.2.2 Cơ chế kiểm soát khóa bí mật

- Cơ chế kiểm soát khóa bí mật được FastCA sử dụng là cơ chế phân chia role. Bao gồm các Role như sau:
  + HSM Security Officer (SO): chịu trách nhiệm khởi tạo HSM, thiết lập và thay đổi Chính sách HSM (dựa trên Khả năng của HSM), tạo và xóa phân vùng ứng dụng.

+ Partition Security Officer (PO): chịu trách nhiệm khởi tạo vai trò Crypto Officer (CO) trên phân vùng, đặt lại mật khẩu, cài đặt và thay đổi chính sách cấp phân vùng.

+ Crypto Officer (CO): chịu trách nhiệm khởi tạo vai trò Crypto User (CU) tạo và sửa đổi các đối tượng mật mã trong phân vùng HSM

+ Auditor (Au): chịu trách nhiệm quản lý ghi nhật ký kiểm toán HSM, độc lập với các vai trò khác trên HSM

+ Crypto User (CU): chịu trách nhiệm sử dụng các đối tượng mật mã (mã hóa / giải mã, ký / xác minh ...) trong phân vùng HSM.

6.2.3 Lưu giữ ngoài khóa bí mật của thuê bao

FastCA không lưu giữ khóa bí mật của thuê bao

6.2.4 Dự phòng khóa bí mật

- FastCA sẽ dự phòng (backup) khóa bí mật của mình để đề phòng thảm họa và trục trặc thiết bị. Khóa bí mật của FastCA được lưu trữ dự phòng trong các thiết bị HSM.

- FastCA không dự phòng khóa bí mật cho RA. Khóa bí mật của thuê bao được dự phòng như 6.2.3. Khóa bí mật được lưu trữ trong các thiết bị như USB Token sẽ không được dự phòng.

6.2.5 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 HSM. Khoá CA này sẽ không được sử dụng trong bất kỳ hoạt động nào của FastCA.

- FastCA không lưu trữ khóa bí mật của RA, của thuê bao khi không có yêu cầu của pháp luật.

6.2.6 Chuyển khóa bí mật

- FastCA giữ khóa trên một HSM và một bản sao khóa để dự phòng phục vụ cho trường hợp phục hồi hệ thống trên một HSM khác. Khóa bí mật sẽ được mã hóa trong quá trình chuyển giữa 2 HSM.

6.2.7 Lưu khóa bí mật trong trên module mã hóa

FastCA giữ khóa bí mật trong các HSM, khóa bí mật được lưu trong dạng được mã hóa.

6.2.8 Phương thực kích hoạt khóa bí mật

- Các thành viên FastCA sẽ có các biện pháp bảo vệ kích hoạt khóa bí mật phù hợp, cụ thể:
  + Đối với thuê bao: khóa bí mật được lưu trong USB token, việc kích hoạt khóa bí mật yêu cầu mật khẩu bảo vệ. Khi không sử dụng, khóa bí mật tồn tại ở dạng mã hóa.
  + Đối với quản trị hệ thống FastCA /RA: khóa bí mật được lưu trong USB token, việc kích hoạt khóa bí mật yêu cầu mật khẩu bảo vệ. Khi không sử dụng, khóa bí mật tồn tại ở dạng mã hóa.
  + Đối với RA: khóa bí mật được lưu trong USB token, việc kích hoạt khóa bí mật yêu cầu mật khẩu bảo vệ và phải xác thực được ít nhất 2 người quản trị. Khi không sử dụng, khóa bí mật tồn tại ở dạng mã hóa.
  + Đối với FastCA: sử dụng HSM để lưu trữ khóa bí mật, việc kích hoạt khóa bí mật yêu cầu các mã chia sẻ theo cơ chế được môt tả tại 6.2.2.

6.2.9 Phương pháp ngừng khóa bí mật

- Khóa bí mật của FastCA bị ngừng kích hoạt khi thiết bị HSM hay partion chưa khóa của FastCA ở chế độ ngừng hoạt động.
- Khóa bí mật của quản trị hệ thống, của RA và của thuê bao có thể bị ngừng kích hoạt sau mỗi nhiệm vụ, sau khi đăng xuất hệ thống hoặc sau khi loại bỏ USB Token khỏi máy tính. Trong mọi trường hợp, thuê bao phải có nghĩa vụ thực hiện các biện pháp bảo vệ khóa bí mật của mình.

6.2.10 Huỷ khóa bí mật

- Việc xóa khóa bí mật được thực hiện theo phương pháp an toàn, đảm bảo không thể phục hồi lại khóa đã xóa.
- Khóa bí mật lưu trên USB token được xóa bằng phần mềm quản trị USB token

- Khóa bí mật lưu trên HSM được xóa bằng chứng năng xóa khóa của HSM

6.2.11 Đánh giá module mã hóa

Xem mục 6.2.1

6.3 Các vấn đề khác của việc quản lý cặp khóa

6.3.1 Lưu trữ khóa công khai

- FastCA sẽ lưu trữ khóa công khai của mình, của RA và toàn bộ thuê bao.

6.3.2 Thời hạn sử dụng chứng thư số và thời hạn sử dụng cặp khóa

- Thời hạn sử dụng của chứng thư số sẽ kết thúc khi chứng thư số đó hết hạn hoặc bị thu hồi.
- Thời hạn sử dụng cặp khóa của thuê bao giống như thời hạn sử dụng của chứng thư số, ngoại trừ chức năng giải mã và kiểm tra chữ ký sau khi chứng thư số hết hạn.
- FastCA không ban hành các chứng thư số có thời hạn sử dụng vượt quá thời hạn sử dụng chứng thư số của CA.
- Chứng thư số mà FastCA cung cấp cho thuê bao tùy thuộc vào thỏa thuận với thuê bao.

6.4 Dữ liệu kích hoạt khóa bí mật

6.4.1 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.

6.4.2 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.
- Thuê bao của FastCA được lưu trữ khóa bí mật dưới dạng mã hóa sử dụng USB Token và mật khẩu bảo vệ.

6.4.3 Các vấn đề khác của dữ liệu kích hoạt

6.4.3.1 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.

6.4.3.2 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.

6.5 Kiểm soát an ninh hệ thống 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 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. 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.

6.6 Giám sát hệ thống 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.
  + Phát hiện và chống thâm nhập mạng IPS
  + Điều khiển ứng dụng (Application Control)
  + Phòng chống Antivirus.
  + Hệ thống cập nhật bản vá.
  + Hệ thống ghi log tập trung
- 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.

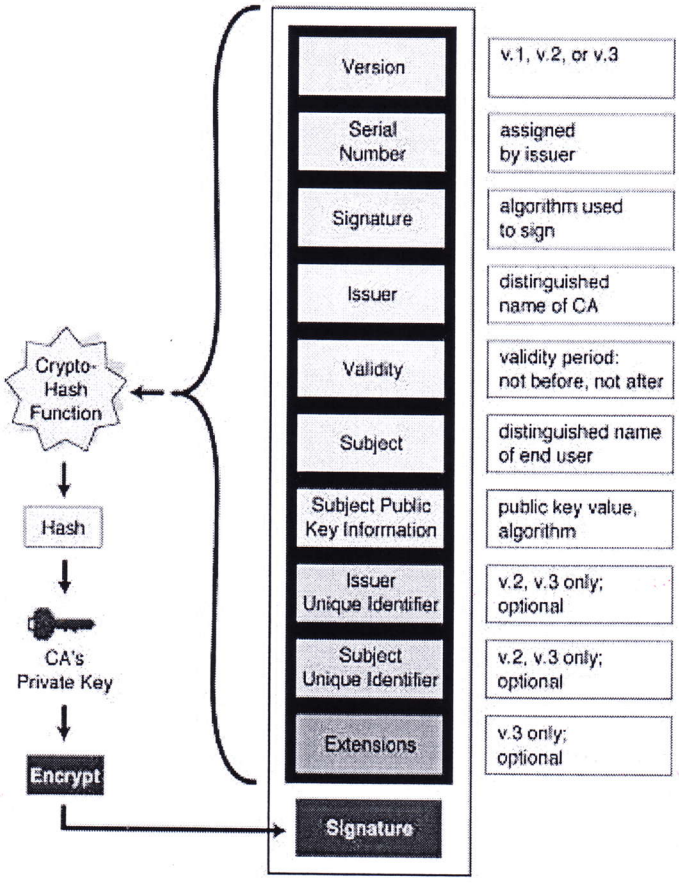
6.7 Time-Stamping

Chứng thư số, CRL và bản ghi cơ sở dữ liệu chứng thư số bị thu hồi chứa thông tin ngày giờ. Thông tin thời gian không cần được mã hóa.

7. ĐẶC TẢ VỀ CHỨNG THƯ SỐ, CRL VÀ OCSP

7.1 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 số 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.
- Cấu trúc chung của chứng thư số



- Cấu trúc chứng thư số của FastCA được xây dựng theo chuẩn X.509, bao gồm những trường thông tin chính sau:

Trường thông tin	**Giá trị/Ý nghĩa**
Serial Number	Giá trị là duy nhất đối với mỗi chứng thư số do FastCA ban hành

Trường thông tin	Giá trị/Ý nghĩa
Signature Algorithm	Định danh (OID) của thuật toán được sử dụng để ký lên chứng thư số (xem phần 7.1.3)
Issuer DN	Xem phần 7.1.4
Valid From	Thời điểm bắt đầu chứng thư số có hiệu lực, theo giờ UTC
Valid To	Thời điểm hết hiệu lực của chứng thư số, theo giờ UTC
Subject DN	Xem phần 7.1.4
Subject Public key	Khóa công khai, được mã hóa phù hợp với RFC 5280
Signature	Chữ ký của FastCA, được mã hóa phù hợp với RFC 5280

7.1.1 Phiên bản

- Chứng thư số của FastCA sử dụng phiên bản của chứng thư số X.509 Version 3.

7.1.2 Trường mở rộng

- FastCA ban hành chứng thư số X.509 phiên bản 3 với phần mở rộng được quy định như sau (từ mục 7.1.2.1 đến 7.1.2.8):

7.1.2.1 Key Usage

- Chứng thư số X.509 phiên bản 3 được ban hành theo RFC 5280. Phần mở rộng KeyUsage trong chứng thư số theo bảng sau.
- Chứng thư số do FastCA ban hành có sử dụng trường KeyUsage

Trường thông tin	Chứng thư số cá nhân và tổ chức	Chứng thư số Web Server (SSL)	Chứng thư số ký mã phần mềm (CodeSigning)
digitalSignature	Có	Có	Có
nonRepudiation	Có	Có	Có
keyEncipherment	Có	Có	Không
dataEncipherment	Không	Không	Không
keyAgreement	Không	Không	Không
keyCertSign	Không	Không	Không
CRLSign	Không	Không	Không
encipherOnly	Không	Không	Không
decipherOnly	Không	Không	Không

7.1.2.2 Certificate policies

- Chứng thư số do FastCA ban hành không có trường mở rộng này.

7.1.2.3 Subject Alternative Name

- Phần mở rộng subjectAltName của chứng thư số được gán giá trị theo RFC 5280.

7.1.2.4 Basic Constraints

- Phần mở rộng Basic Constraints của chứng thư số được gán giá trị theo RFC 5280.

7.1.2.5 Extended Key Usage

- Trường mở rộng ExtendedKeyUsage trong chứng thư số được cấu hình với giá trị thể hiện mục đích sử dụng của chứng thư số, chi tiết biểu diễn trong bảng dưới đây.

Trường thông tin	Chứng thư số cá nhân và tổ chức	Chứng thư số Web Server (SSL)	Chứng thư số ký mã phần mềm (CodeSigning)
ServerAuth	Không	Có	Không
ClientAuth	Có	Có	Không
CodeSigning	Không	Không	Có
EmailProtection	Có	Không	Không
TimeStamping	Không	Không	Không

7.1.2.6 CRL Distribution Points

- Chứng thư số do FastCA ban hành trường có mở rộng cRLDistributionPoints chứa URL vị trí mà người nhận có thể lấy được CRL để kiểm tra trạng thái của chứng thư số.

7.1.2.7 Authority Key Identifier

- Giá trị của trường này là định danh chứng thư số của FastCA, giá trị này trùng với trường Subject Key Identifier trong chứng thư của FastCA do Root CA ban hành.

7.1.2.8 Subject Key Identifier

- Giá trị định danh chứng thư số do FastCA ban hành.

7.1.3 Các thuật toán ký

- FastCA ký lên các chứng thư số, sử dụng thuật toán sau:

  + sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

- Thủ tục ký chứng thư số áp dụng lược đồ RSASSA-PSS được quy định trong PKCS #1 phiên bản 2.1

- Phiên bản của FastCA hỗ trợ sử dụng thuật toán mã hóa SHA-256, SHA-384 và SHA-512 trong chứng thư số.

7.1.4 Khuôn dạng tên

- FastCA ban hành chứng thư số với trường Issuer và Subject Distinguished Name mô tả trong phần 3.1.1. Ngoài ra, chứng thư số thường có thêm trường Organiztional Unit.

7.1.5 Ràng buộc tên

- FastCA không quy định cụ thể các ràng buộc cho việc đặt tên.

7.1.6 Định danh chính sách và quy chế chứng thư số

- Chứng thư số do FastCA ban hành không có trường mở rộng này.

7.1.7 Sử dụng ràng buộc mở rộng chính sách chứng thư số

- FastCA không quy định các ràng buộc sử dụng trưởng mở rộng chính sách chứng thư số.

7.1.8 Cú pháp và ngữ nghĩa của chính sách phân loại

- FastCA ban hành chứng thư số tuân theo các quy định trong quy chế chứng thực này và các thỏa thuận với thuê bao, thỏa thuận với người nhận liên quan.

7.1.9 Xử lý ngữ nghĩa của các trường mở rộng chính sách chứng thư số

- FastCA không quy định về xử lý ngữ nghĩa trường mở rộng chính sách chứng thư.

7.2 Đặc tả về CRL

CRL do FastCA công bố tuân theo chuẩn ITU-T X.509 và các quy định của RFC 5280. Tối thiểu, CRL do FastCA công bố có các trường và giá trị theo bảng dưới đây.

Trường thông tin	Giá trị/Ý nghĩa
Version	Phiên bản của CRL là Version 2
Issuer	Nhà cung cấp FastCA
Effective Date	Ngày bắt đầu có hiệu lực
Next Update	Thời gian có CRL tiếp theo
Signature Algorithm	Thuật toán để ký CRL là sha256RSA
Signature Hash Algorithm	Thuật toán để hash là sha256
Revoked Certificate	Danh sách chứng thư bị thu hồi, được liệt kê bằng các số serial number của các chứng thư số bị thu hồi và ngày thu hồi

7.2.1 Phiên bản

FastCA ban hành X.509 Version 2 CRL.

7.2.2 CRL và các trường mở rộng của CRL

CRL do FastCA ban hành không có quy định về các trường mở rộng.

7.3 Đặc tả về OCSP

OCSP là giao thức cho phép lấy thông tin cập nhật về trạng thái thu hồi của một chứng thư số cụ thể. Dịch vụ OCSP (OCSP Responder) tuân theo RFC 2560.

7.3.1 Phiên bản

FastCA cung cấp dịch vụ OCSP Version 1 theo RFC 2560.

7.3.2 Phần mở rộng OCSP

Không quy định.

8. KIỂM TOÁN KỸ THUẬT

- Việc kiểm toán kỹ thuật về các hoạt động FastCA được thực hiện định kỳ hàng năm hoặc theo yêu cầu từ RootCA.
- Ngoài các kiểm định trên, FastCA có thể thực hiện những kiểm định kỹ thuật khác để đảm bảo tính tin cậy của FastCA. Các kiểm toán kỹ thuật đó có thể được thực hiện bởi một đơn vị bên ngoài.

8.1 Tần suất và các tình huống đánh giá kỹ thuật

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

8.2 Danh tính và khả năng của người kiểm toán kỹ thuật

Người thực hiện kiểm toán kỹ thuật được chỉ định bởi RootCA để thực hiện các cuộc kiểm toán kỹ thuật FastCA.

8.3 Mối quan hệ giữa người kiểm toán kỹ thuật và thực thể được kiểm toán

Kiểm toán kỹ thuật được thực hiện bởi những người không phụ thuộc vào FastCA.

8.4 Các nội dung kiểm toán kỹ thuật

Các lĩnh vực được kiểm toán kỹ thuật bao gồm: hạ tầng hệ thống, các quy trình quản lý khóa, quy trình vận hàn hệ thống và các nội dung khác theo yêu cầu khác của đơn vị kiểm toán kỹ thuật.

8.5 Xử lý khi phát hiện sai sót.

- Sau khi có báo cáo kiểm toán kỹ thuật, FastCA sẽ làm việc với RootCA về những nội dung chưa phù hợp.
- FastCA sẽ nghiên cứu và đề ra và thực hiện phương án xử lý những nội dung chưa phù hợp trong thời gian thống nhất với RootCA.
- Dịch vụ của FastCA sẽ bị ngừng trong các tình huống sau:
  + Báo cáo kiểm toán kỹ thuật cho thấy có lỗi nghiêm trọng có thể ảnh hưởng ngay lập tức tới an an ninh của hệ thống FastCA.

+ FastCA thực hiện kế hoạch xử lý nhưng không có kết quả.

8.6 Thông báo kết quả

Báo cáo kết quả kiểm toán kỹ thuật được FastCA công bố tại website:

http://fastca.vn

9. CÁC VẤN ĐỀ THƯƠNG MẠI VÀ PHÁP LÝ KHÁC

9.1 Lệ phí

9.1.1 Lệ phí cấp Chứng thư hoặc gia hạn Chứng thư số

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. Mức phí sẽ tùy thuộc vào hợp đồng đối với từng thuê bao.

9.1.2 Lệ phí truy cập Chứng thư số

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

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

- FastCA sẽ không thu phí cho việc công bố CRL.
- FastCA sẽ thu phí cung cấp dịch vụ OCSP hoặc các dịch vụ tiện ích khác.
- FastCA không cho phép bên thứ ba truy nhập vào thông tin CRL, OCSP hoặc thông tin khác của FastCA với mục đích cung cấp các sản phẩm hay dịch vụ mà không có sự cho phép của FastCA bằng văn bản.

9.1.4 Lệ phí sử dụng cho các dịch vụ khác

- FastCA không thu phí truy cập vào quy chế chứng thực của mình. FastCA giữ bản quyền cùng với các tài liệu khác do FastCA công bố.
- Việc sử dụng quy chế chứng thực của FastCA với các mục đích khác như sao chép, phân bổ lại, sửa chữa hoặc tạo mới các công viên phát sinh sẽ phải được sự cho phép của FastCA.

9.1.5 Chính sách hoàn trả phí

- Thuê bao có thể yêu cầu FastCA thu hồi chứng thư số và hoàn lại phí trong các trường hợp sau:
  + Trong vòng 30 từ ngày ban hành chứng thư số
  + Nếu FastCA vi phạm điều khoản trong hợp đồng với thuê bao
- FastCA thực hiện việc hoàn phí cho thuê bao theo các điều khoản thỏa thuận với thuê bao.

9.2 Trách nhiệm về tài chính

- 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.
- FastCA đã thực hiện bảo lãnh thanh toán của một ngân hàng thương mại hoạt động tại Việt Nam không dưới 5 (năm) tỷ đồng, để giải quyết các rủi ro và các khoản đền bù có thể xảy ra trong quá trình cung cấp dịch vụ và thanh toán chi phí tiếp nhận và duy trì cơ sở dữ liệu của FastCA trong trường hợp bị thu hồi giấy phép.

9.3 Tính bảo mật của thông tin kinh doanh

9.3.1 Phạm vi của thông tin cần bảo mật

- Những thông tin sau được coi là thông tin bí mật:
  + Các thông tin được yêu cầu bởi pháp luật.
  + Hồ sơ đăng ký cấp chứng thư số.
  + Biên bản giao dịch.
  + Nhật ký kiểm tra FastCA.
  + Báo cáo kiểm tra FastCA.
  + Kế hoạch đối phó với sự cố và kế hoạch khôi phục lại sau thảm họa.
  + Phương pháp điều khiển hoạt động các thành phần FastCA: phần cứng, phần mềm và quản trị của dịch vụ của FastCA.

9.3.2 Thông tin không nằm trong phạm vi của quá trình đảm bảo tính mật

- Các thông tin không được coi là bí mật.
  + Chứng thư số, trạng thái thu hồi của chứng thư số và thông tin trạng thái khác, địa chỉ lưu trữ của FastCA và thông tin trên đó.
  + Không được chỉ rõ trong phần 9.3.1 được coi là không bí mật.

9.3.3 Trách nhiệm bảo vệ thông tin mật

FastCA đảm bảo an ninh cho các thông tin riêng tư không bị tiết lộ.

9.4 Bảo mật của thông tin cá nhân

9.4.1 Kế hoạch đảm bảo thông tin cá nhân

Chính sách bảo mật được công bố trên trang Web của FastCA.

9.4.2 Phạm vi các thông tin bí mật

Mọi thông tin thuê bao không được công bố qua nội dung của chứng thư số, dịch vụ Directory và CRL được coi là bí mật.

9.4.3 Những thông tin không bí mật

Tất cả các thông tin được công khai trong chứng thư được coi như không phải là thông tin bí mật.

9.4.4 Trách nhiệm bảo vệ thông tin riêng tư

FastCA thực hiện các biện pháp đảm bảo an ninh cho các thông tin bí mật của thuê bao, tuân theo yêu cầu của luật pháp.

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.

9.4.5 Thông báo và cho phép sử dụng thông tin mật

Thông tin bí mật sẽ không được sử dụng mà không có sự cho phép của người sở hữu thông tin hoặc đại điện sở hữu thông tin đó, trừ những trường hợp được quy định trong quy chế này hoặc trong các thỏa thuận cụ thể.

9.4.6 Cung cấp thông tin mật theo yêu cầu của của cơ quan luật pháp

FastCA sẽ cung cấp thông tin bí mật nếu có yêu cầu của cơ quan pháp luật có thẩm quyền và tuân thủ theo quy định của pháp luật.

9.4.7 Các tình huống cung cấp thông tin khác

FastCA không cung cấp thông tin cho các đối tượng nào khác ngoài đại diện có thẩm quyền của pháp luật

9.5 Quyền sở hữu trí tuệ

9.5.1 Quyền sở hữu thông tin chứng thư số và thông tin thu hồi chứng thứ.

- FastCA giữ mọi quyền sở hữu chứng thư số và thông tin thu hồi mà FastCA phát hành ra.
- FastCA cho phép thuê bao và 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.

9.5.2 Quyền sở hữu trong CPS

FastCA giữ mọi quyền sở hữu trí tuệ quy chế chứng thực này.

9.5.3 Quyền sở hữu tên

Đối tượng đăng ký chứng thư số phải có quyền sở hữu về nhãn hiệu đăng ký, nhãn hiệu dịch vụ, hoặc tên tổ chức (danh nghiệp) trong đơn xin cấp chứng thư số và tên đặc trưng trong chứng thư số.

9.5.4 Quyền sở hữu khoá

Cặp khoá tương ứng với chứng thư số của FastCA, RA, thuê bao được sở hữu bởi chính đối tượng là chủ thể của chứng thư số đó.

9.6 Tuyên bố và cam kết

9.6.1 Tuyên bố và cam kết của FastCA

- Dịch vụ FastCA bảo đảm:
  + Không thay đổi thông tin đăng ký chứng thư số được cung cấp bởi đối tượng đăng ký.
  + Không có lỗi trong quá trình duyệt và ban hành chứng thư số.
  + Chứng thư số do FastCA ban hành đáp ứng các yêu cầu trong quy chế này.
  + Cung cấp dịch vụ thu hồi và cho phép sử dụng địa chỉ lưu trữ phù hợp với quy chế chứng thực này.
- Chịu trách nhiệm về việc quản lý và xác minh các điều kiện hoạt động của RA theo quy định của pháp luật.

9.6.2 Tuyên bố và cam kết của RA

- RA đảm bảo rằng:
  + Không thay đổi thông tin đăng ký chứng thư số được cung cấp bởi đối tượng đăng ký.
  + Không có lỗi trong quá trình duyệt hồ sơ xin cấp chứng thư số và quá trình gửi thông tin cho FastCA.
  + Tuân thủ theo quy trình quản lý vòng đời chứng thư số của FastCA.
- RA có trách nhiệm ký hợp đồng với FastCA. Trong hợp đồng có quy định:
  + Loại chứng thư số mà RA được phép tham gia cung cấp.
  + Các bước trong quy trình cấp phát chứng thư số RA được thực hiện.
  + Chứng thư số chỉ được cấp sau khi FastCA đã nhận đầy đủ hồ sơ của thuê bao, và thông tin thuê bao được thẩm định.
  + Cam kết của RA với FastCA đúng như trong hợp đồng đã ký và theo quy định của pháp luật.
  + Nhân viên RA trực tiếp tham gia vào quy trình cung cấp chứng thư số phải có hiểu biết pháp luật về chữ ký số và dịch vụ chứng thực chữ ký số.

9.6.3 Tuyên bố và cam kết của thuê bao

- Thuê bao đảm bảo rằng:
  + Khi ký: sử dụng khóa bí mật tương ứng với khóa công khai trong chứng thư số; tại thời điểm ký, thuê bao chấp nhận chứng thư số và chứng thư số đang có hiệu lực (không hết hạn hoặc bị thu hồi).
  + Khóa bí mật của mình được bảo vệ và không cho người khác sử dụng.
  + Mọi thông tin cung cấp bởi thuê bao là đúng.
  + Sử dụng chứng thư số đúng mục đích của chứng thư số, phù hợp với quy định của pháp luật và quy chế chứng thực này
  + Không sử dụng chứng thư số được cấp thực hiện các chức năng của một CA.
  + Không sử dụng chứng thư số vào các mục đích giả mạo, gian lận, ...trái với pháp luật.

- Thỏa thuận thuê bao có thể bao gồm thêm những điều khoản khác. Nội dung thỏa thuận thuê bao được trình bày trong phần phụ lục.

9.6.4 Tuyên bố và cam kết của các đối tượng khác

Ngoài FastCA, RA và thuê bao; không có tuyên bố và cam kết của đối tượng nào khác được FastCA quy định.

9.7 Từ chối trách nhiệm

FastCA không quy định cụ thể về việc từ chối trách nhiệm.

9.8 Giới hạn bồi thường của FastCA

- Trong phạm vi được cho phép bởi pháp luật, thỏa thuận thuê bao sẽ giới hạn khoản tiền đền bù của FastCA. Trong mọi trường hợp, khoản tiền mà FastCA phải trả cho các đối tượng không vượt quá các ngưỡng theo bảng dưới đây:

Loại chứng thư số	Khoản tiền giới hạn phải trả
Chứng thư số Cá nhân/Tổ chức	5.000 USD
Chứng thư số Web Server	10.000 USD
Chứng thư số ký phần mềm	10.000 USD

- Khoản tiền phải trả cho thuê bao được quy định trong thỏa thuận thuê bao tương ứng.

9.9 Vấn đề bồi thường của khách hàng cho FastCA

- Khi pháp luật yêu cầu, khách hàng phải bồi thường cho FastCA nếu xuất hiện:
  - Cung cấp thông tin không đúng khi đăng ký cấp chứng thư số.
  - Thuê bao có lỗi trong việc bảo vệ khóa bí mật.
  - Lỗi của khách hàng trong việc bảo vệ khóa bí mật, 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.

- Hợp đồng với khách hàng có thể có những bổ sung khác.

9.10 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 RA nếu:
  - Lỗi của đối tác tin cậy trong việc thực thi trách nhiệm, quyền hạn theo hợp đồng thỏa thuận đã được ký.
  - 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 có thể bao gồm thêm một số nghĩa vụ khác.

9.11 Thời hạn bắt đầu và hết hiệu lực

9.11.1 Thời hạn bắt đầu có hiệu lực

Quy chế chứng thư số này có hiệu lực khi được công bố trên trang Web của FastCA. Các sự bổ sung cho quy chế chứng thư số này có hiệu lực khi được công bố.

9.11.2 Thời hạn hết hiệu lực

Quy chế này sẽ vẫn còn hiệu lực cho đến khi được thay thế bởi một phiên bản mới.

9.11.3 Ảnh hưởng của của quy chế chứng thực số hết hiệu lực

Khi quy chế này hết hiệu lực, các điều khoản của nó vẫn được áp dụng cho các chứng thư số được ban hành trong thời hạn của quy chế này cho đến khi chứng thư số hết hạn hoặc bị thu hồi.

9.12 Thông báo và trao đổi thông tin giữa các thành viên

Trừ khi được quy định rõ ràng, các thành viên FastCA sẽ sử dụng các phương pháp liên lạc hợp lý, tùy thuộc mức độ nguy cấp về nội dung của thông tin cần liên lạc.

9.13 Bổ sung và sửa đổi

9.13.1 Thủ tục bổ sung

- Quy chế này được bổ sung, sửa đổi bởi FastCA. Nội dung sửa đổi được lưu tại website: https://fastca.vn
- Nội dung sửa đổi sẽ thay thế các nội dung trong các điều khoản tương đương trong phiên bản quy chế chứng thực tương ứng và mọi tài liệu liên quan khác.

9.13.2 Cơ chế và thời hạn thông báo

- Đối với các thay đổi không quan trong như thay đổi URL, thông tin liên hệ, lỗi in ấn… FastCA có quyền thay đổi quy chế mà không cần thông báo về sự thay đổi.
- Đối với các thay đổi theo đề xuất từ các thành viên, FastCA sẽ xem xét yêu cầu thay đổi. Nếu quy chế cần thay đổi, FastCA sẽ đưa ra thông báo về sự thay đổi này.
- Trong một số trường hợp đặc biệt, liên quan tới an ninh của hệ thống, FastCA sẽ thực hiện sự thay đổi quy chế này lập tức, sau đó sẽ thông báo cho các thành viên.

9.13.2.1 Kỳ hạn góp ý

Các thành viên của FastCA được quyền góp ý cho quy chế chứng thư số trong vòng 15 ngày từ ngày quy chế được công bố.

9.13.2.2 Cơ chế quản lý góp ý

FastCA sẽ xem xét mọi góp ý sửa đổi. FastCA sẽ thực hiện một trong các tình huống sau:

+ Không thay đổi gì góp ý ban đầu; hoặc
+ Sửa đổi những góp ý sửa đổi và công bố lại chúng; hoặc
+ Hủy bỏ góp ý sửa đổi.

9.13.2.3 Các tình huống mà định danh quy chế chứng thực phải thay đổi

Định danh quy chế chứng thực được thay đổi theo yêu cầu của FastCA.

9.14 Thủ tục tranh chấp

9.14.1 Thủ tục tranh chấp giữa FastCA với RA

- Tranh chấp giữa FastCA và các RA sẽ được giải quyết theo các điều khoản được quy định trong hợp đồng thỏa thuận giữa FastCA và RA.

9.14.2 Thủ tục tranh chấp giữa FastCA với người dùng cuối

- Tranh chấp giữa FastCA và người dùng cuối sẽ được giải quyết theo các điều khoản được quy định trong thỏa thuận giữa FastCA và thuê bao.

9.15 Pháp luật

Pháp luật Việt Nam sẽ được sử dụng trong mọi trường hợp, kể cả có liên quan đến các yếu tố nước ngoài.

9.16 Phù hợp với pháp luật hiện hành

Nếu có quy định trong quy chế này xung đột với quy định của các văn bản pháp luật, lúc này quy định của văn bản pháp luật sẽ có hiệu lực.

9.17 Những điều khoản chung

9.17.1 Thỏa thuận bao trùm mọi thành viên

Quy chế chứng thực này là thỏa thuận mà mọi thành viên của FastCA phải tuân thủ.

9.17.2 Sự chuyển nhượng

Không có quy định nào cho phép chuyển nhượng quyền sử dụng chứng thư số. FastCA không quy định các trường hợp chuyển nhượng khác.

9.17.3 Tính độc lập của các điều khoản

Nếu như một số điều khoản trong quy chế chứng thực này không hợp pháp các điều khoản đó sẽ không có giá trị, nhưng không ảnh hưởng đến hiệu lực của các điều khoản khác

9.17.4 Sự ép buộc

Không có sự ép buộc nào đưa đến việc ban hành chứng thư của FastCA.

9.17.5 Trường hợp bất khả kháng

Thỏa thuận thuê bao và thỏa thuận người nhận sẽ có điều khoản về trường hợp bất khả kháng để bảo vệ cho FastCA.

9.18 Những điều khoản khác

Không có các điều khoản nào khác ngoài các điều khoản được quy định trong quy chế chứng thực này.