CÔNG TY CỔ PHẦN CÔNG NGHỆ TIN HỌC EFY VIỆT NAM

QUY CHẾ CHỨNG THỰC DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG (EFY-CA)

HÀ NỘI, 2024

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)	Ủy quyền 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 được sử dụng rộng rãi.
9.	EFY-CA (EFY Certification Authority)	Hệ thống cung cấp dịch vụ chứng thực chữ ký số EFY
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 chuẩn truy nhập thư mục
12.	PKI (Khóa công khai Infrastructure)	Hạ tầng khóa 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 mức 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 mức con
18.	USB Token	Thiết bị bảo vệ khóa của người dùng trong hệ thống PKI (USB Token hoặc Smartcard…)

I - GIỚI THIỆU

I.1 Tổng quan

EFY-CA là tên gọi của dịch vụ chứng thực chữ ký số công cộng do Công ty cổ phần công nghệ tin học EFY Việt Nam cung cấp. Các quy định về chính sách chứng thư số của dịch vụ EFY-CA 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 EFY-CA. Quy chế chứng thực 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 EFY-CA và các dịch vụ chứng thực chữ ký số cung cấp cho khách hàng.

Hệ thống EFY-CA được tuân thủ theo Nghị định số 130/2018/NĐ-CP ngày 27 tháng 9 năm 2018 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, Thông tư số 31/2020/TT-BTTTT ngày 30 tháng 10 năm 2020.

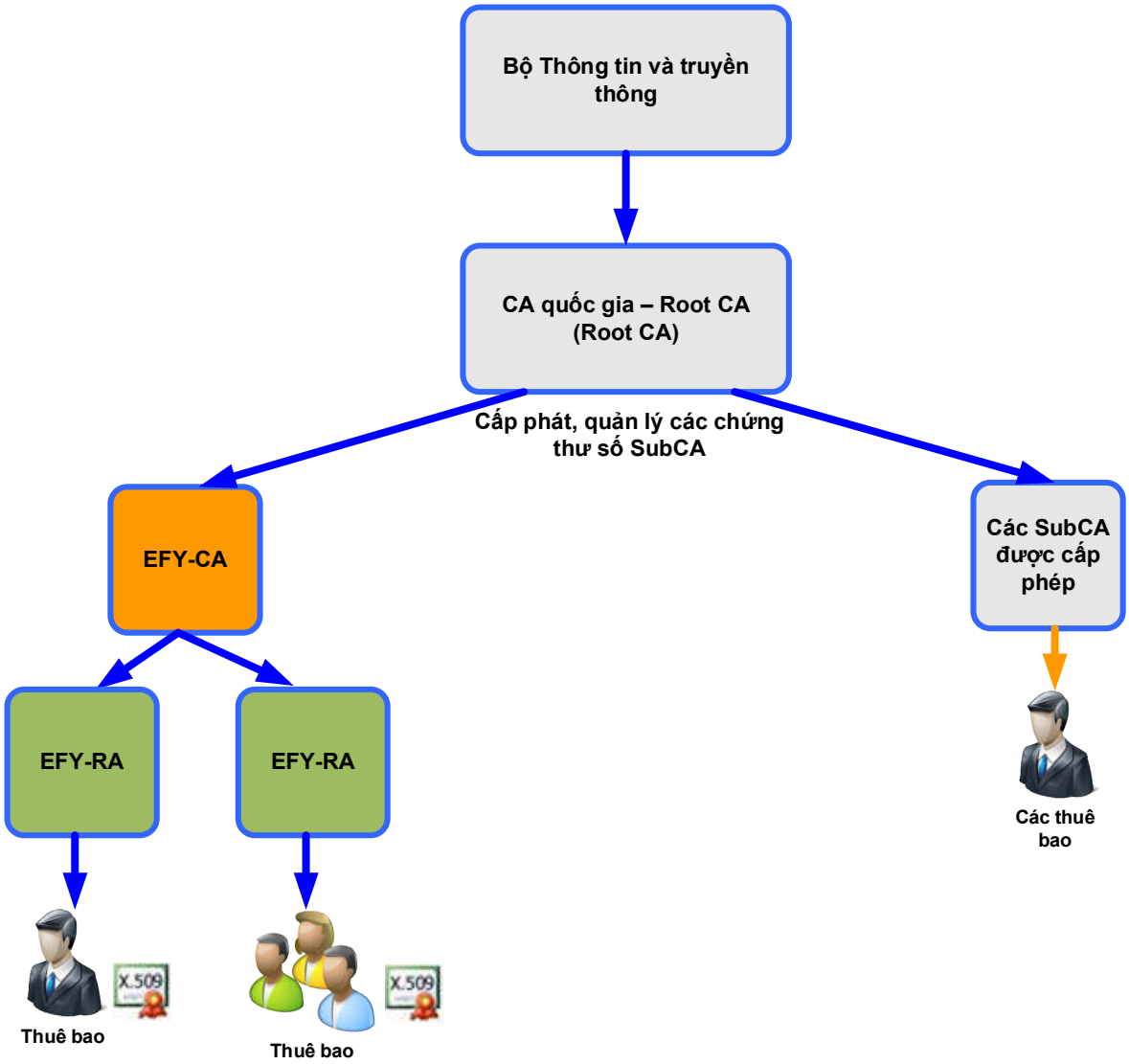
I.2 Tên và dấu hiệu nhận diện tài liệu

Tài liệu này được gọi là quy chế chứng thực của nhà cung cấp dịch vụ chứng thư số EFY-CA (EFY-CA/CPS). 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, Bộ Thông tin và Truyền thông (Trung tâm CTĐTQG, Bộ TT&TT).

I.3 Các thành phần trong hệ thống dịch vụ chứng thực chữ ký số

- 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 EFY-CA 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 ký EFY-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 EFY-CA, 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 khóa 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 EFY-CA. 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 EFY-CA 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 Mục đích sử dụng chứng thư

I.4.1 Sử dụng chứng thư số hợp lệ

I.4.1.1 *Chứng thư số của EFY-CA*

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

I.4.1.2 *Các chứng thư số do EFY-CA phát hành*

- Chứng thư được cấp cho cá nhân: chứng thư được sử dụng với mục đích cá nhân, xác định danh tính. Phục vụ ký số, xác thực tài liệu điện tử, xác thực đăng nhập, SSL, Mail.
- Chứng thư được cấp cho tổ chức: chứng thư được cấp cho một tổ chức, doanh nghiệp. Chứng thư số cho thiết bị HSM, SSL server, Mail server.
- Chứng thư số CodeSigning.

I.4.2 Các trường hợp bị cấm

Sử dụng chứng thư số sai mục đích, không được nêu ở mục 1.4 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

EFY-CA là tổ chức viết và cập nhật Quy chế chứng thực.

Quy chế chứng thực có thể được tải tại website: http://efyca.vn/download/CPS

I.5.2 Thông tin liên hệ

- Liên hệ:
- Địa chỉ: Tầng 9 Tòa nhà Sannam số 78 Duy Tân, Phường Dịch Vọng Hậu, Quận Cầu Giấy, TP Hà Nội;
- Số điện thoại: 024 6287 2290
- Email: contact@efy.com.vn
- Website công ty: http://efy.com.vn ; Website dịch vụ: http://efyca.vn

I.5.3 Thủ tục phê duyệt Quy chế chứng thực

EFY-CA dự thảo nội dung và gửi Quy chế chứng thực gửi RootCA phê duyệt nội dung. EFY-CA sẽ công bố Quy chế chứng thực và phát hành quy chế trên website dịch vụ sau khi được kiểm duyệt và cho phép bởi RootCA.

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 - Trách nhiệm lưu trữ và công bố thông tin

II.1 Lưu trữ

- CPS
  - http://efyca.vn/download/CPS
- Chứng thư số của Root and Sub CA certificates
  - https://rootca.gov.vn/crt/micnrca.crt (SHA1)
  - https://rootca.gov.vn/crt/vnrca256.p7b (SHA256)
  - http://va.efyca.vn/certs/efyca.crt (SHA1)
  - http://va.efyca.vn/certs/efyca256.crt (SHA256)
- Chứng thư số của thuê bao
  - LDAP
    - http://ldap.efyca.vn
  - Website:
    - https://efyca.vn/
- CRL
  - https://rootca.gov.vn/crl/micnrca.crl (CRL RootCA SHA1)
  - https://rootca.gov.vn/crl/vnrca256.crl (CRL RootCA SHA256)
  - http://va.efyca.vn/pub/CRL (CRL EFY-CA SHA1)
  - http://va.efyca.vn/pub/CRL256 (CRL EFY-CA SHA256)
- OCSP
  - http://ocsp.efyca.vn/

II.2 Công bố thông tin chứng thư số

Các thông tin cần được công bố bao gồm:

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

Kho lưu trữ chứng thư của EFY-CA sử dụng giao diện web hoặc LDAP, 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

Chứng thư số của thuê bao được công bố tối đa trong 1 giờ sau khi cấp.

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

Tối đa 1 ngày làm việc để công bố chứng thư số của thuê bao lên LDAP, website.

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

II.4 Kiểm soát truy nhập thông tin

- Cập nhật CPS: chỉ EFY-CA mới có quyền cập nhật CPS.
- Đối với thuê bao, không giới hạn truy cập tới CPS, chứng thư, thông tin chứng thư, hay CRLs. EFY-CA 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. EFY-CA triển khai các kiểm soát nhằm ngăn chặn việc truy cập bất hợp pháp vào kho lưu trữ nhằm thêm, xóa hay sửa đổi các mục trong kho lưu trữ.

III - Nhận dạng và xác thực yêu cầu xin cấp chứng thư số

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:
  - CN= Họ và Tên
  - C=VN
  - L = vị trí
  - Email = abc@xyz.com
- 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:
  - CN= Tên tổ chức
  - C=VN
  - L = vị trí
  - UserID=MST (trong trường hợp khai thuế, bảo hiểm qua mạng)
  - Email = abc@xyz.com
- Đối với chứng thư số cho dịch vụ, SSL, mail:
  - CN= Domain name
  - C=VN
  - L = vị trí
  - Email = abc@xyz.com
- Đối với các chứng thư số khác (codesigning,…) 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 EFY-CA sẽ là duy nhất với một cấp chứng thư xác định trong miền của dịch vụ EFY-CA. 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, EFY-CA có thể yêu cầu thuê bao cung cấp bằng chứng, tài liệu chứng minh quyền sở hữu đối với tên đăng ký.

EFY-CA không chịu trách nhiệm trong mọi tranh chấp về tên của đối tượng đăng ký. EFY-CA 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

III.2.1 Xác minh thuê bao cá nhân

Bộ phận đăng ký RA kiểm tra nhân dạng của người xin cấp chứng thư dựa trên thủ tục để nhận dạng của chính phủ, như CMND/CCCD/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 Hộ chiếu hoặc chứng minh thư nhân dân hoặc căn cước công dân khi xin cấp chứng thư số từ EFY-CA.

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, EFY-CA 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 khóa (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 khóa, EFY-CA 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 khóa sau khi đã bị thu hồi (Renewal)

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

- Chứng thư số vi phạm hợp đồng giữa thuê bao với EFY-CA.
- 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, EFY-CA phải kiểm tra và xác thực đúng nếu có yêu cầu sự huỷ bỏ chứng thư từ thuê bao của dịch vụ EFY-CA. 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 cá nhân hay tổ chức yêu cầu, trên thực tế việc thông tin với các thuê bao phụ thuộc vào nhiều trường hợp khác nhau nhưng có thể là một trong các cách sau: điện thoại, fax, thư điện tử, thư tín hay các dịch vụ đưa tin khác.

Chỉ EFY-CA mới được phép thu hồi chứng thư thuê bao.

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

IV.1 Yêu cầu cấp chứng thư

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 EFY-CA.

Hồ sơ cấp chứng thư số của thuê bao theo Nghị định 130/2018/NĐ-CP:

1. Đơn cấp chứng thư số theo mẫu của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng (EFY-CA).

2. Giấy tờ kèm theo bao gồm:

a) Đối với cá nhân: Chứng minh nhân dân hoặc căn cước công dân hoặc hộ chiếu;

b) Đối với tổ chức: 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.

3. 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.

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, hồ sơ đăng ký cấp chứng thư số và cung cấp các thông tin đúng, chính xác.
- Tự tạo khóa hoặc yêu cầu EFY-CA tạo cặp khóa trên thiết bị PKI Token an toàn.
- Cung cấp khóa công khai đến RA, đến trung tâm xử lý và chứng minh sự tương thích giữa khóa bí mật và khóa 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 EFY-CA. 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 EFY-CA 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 yêu cầu 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.

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.
- RA có lý do tin rằng việc cung cấp chứng thư cho thuê bao có thể gây bất lợi cho EFY-CA.

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 EFY-CA. Thông thường, nếu không có vướng mắc, hệ thống cung cấp dịch vụ EFY-CA có thể khởi tạo một chứng thư mới tối đa trong 05 ngày làm việc.

IV.3 Cấp chứng thư số

IV.3.1 Các hành động của EFY-CA trong quá trình sinh chứng thư số

Một chứng thư số được tạo và cấp sau khi EFY-CA chấp nhận một yêu cầu cấp chứng thư số hoặc sau khi nhận được một yêu cầu cấp chứng thư số của RA. EFY-CA 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

EFY-CA cấp các chứng thư số cho thuê bao sẽ (trực tiếp hoặc gián tiếp thông qua RA) thông báo thuê bao EFY 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 Xác nhận và Công bố công khai chứng thư số

IV.4.1 Chấp nhận chứng thư

Thuê bao hoàn thiện việc xác nhận thông tin chứng thư số là chính xác bằng văn bản hoặc điện tử và phản hồi lại cho EFY-CA.

- Xác nhận bằng văn bản

Thuê bao xác nhận thông tin chứng thư số vào mẫu giấy xác nhận thông tin chứng thư số do EFY-CA cung cấp (bản cứng) bằng cách ký tay, đóng dấu (đối với tổ chức) và gửi lại cho EFY-CA để kiểm tra, lưu trữ hồ sơ thuê bao.

- Xác nhận bằng điện tử

Thuê bao có thể xác nhận thông tin chứng thư số bằng phương thức điện tử, cụ thể:

Thuê bao xác nhận thông tin chứng thư số vào vào mẫu giấy xác nhận thông tin chứng thư số do EFY-CA cung cấp bằng cách ký số (sử dụng chữ ký số còn hiệu lực) và gửi lại file giấy xác nhận đã ký số cho EFY-CA để kiểm tra, lưu trữ hồ sơ thuê bao.

Hoặc

Thuê bao có thể thực hiện xác nhận thông tin chứng thư số trên phần mềm theo các bước như sau:

Bước 1: Thuê bao nhận thiết bị Token và thực hiện cài đặt phần mềm Token Manager. Sau khi cài đặt, bắt buộc thuê bao phải thực hiện đổi mã PIN của Token để có thể thực hiện cấp chứng thư số. (Thực hiện đối với trường hợp Token cấp mới; trong trường hợp đã có Token và gia hạn thì bỏ qua bước này)

Bước 2: Thuê bao nhập mã kích hoạt yêu cầu chứng thư số vào phần mềm (mã kích hoạt được gửi về email đăng ký khi yêu cầu cấp chứng thư số được EFY-CA duyệt). Thông tin về yêu cầu chứng thư số được hiển thị trên phần mềm Token Manager để thuê bao kiểm tra và đồng ý cấp phát chứng thư số. Trường hợp phát hiện sai thông tin, thuê bao phản hồi lại cho nhân viên hỗ trợ.

Bước 3: Yêu cầu cấp chứng thư số được tiếp tục thực hiện trên Token, sau khi đã cấp chứng thư số, trên phần mềm Token Manager hiển thị form xác nhận thông tin chứng thư số để thuê bao kiểm tra. Nếu xác nhận thông tin là chính xác, thuê bao click tích chọn và Xác nhận để hoàn tất cấp chứng thư số và thiết bị Token. Nếu không xác nhận, chứng thư số sẽ không thể hoàn tất quá trình nạp vào Token và chưa thể thực hiện ký số.

Trường hợp sai thông tin, thuê bao phản hồi lại cho nhân viên hỗ trợ.

Thông tin về việc xác nhận trên Token Manager được lưu vết nhật ký (log) trên hệ thống nhằm đảm bảo yêu cầu về quản lý hồ sơ thuê bao.

IV.4.2 Công khai chứng thư của EFY-CA

Trung tâm xử lý 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 EFY-CA.

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

EFY-CA có trách nhiệm gửi thông báo cho RA về việc phát hành chứng thư.

IV.5 Sử dụng cặp khóa và chứng thư

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

Việc sử dụng khóa bí mật tương ứng với khóa 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 CP và 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 khóa bí mật khỏi việc truy cập bất hợp pháp và sẽ không được sử dụng khóa bí mật khi chứng thư hết hạn hay khi bị thu hồi chứng thư.

IV.5.2 Cách sử dụng chứng thư và khóa 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, EFY-CA 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

Gia hạn chứng thư số là sự cấp một chứng thư số mới cho thuê bao mà không thay đổi Khóa công khai và thông tin khác trong chứng thư số. Gia hạn được hỗ trợ cho chứng thư số khi mà cặp khóa được tạo cho phép tạo một yêu cầu cấp chứng thư từ một cặp khóa đã tồn tại.

IV.6.1 Các trường hợp được gia hạn chứng thư số của thuê bao

- 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.

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.6.2 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 sẽ được sử dụng để gia hạn.

IV.6.3 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.6.4 Sự chấp nhận, xác nhận chứng thư số gia hạn

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

IV.6.5 Công bố chứng thư số được gia hạn

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

IV.6.6 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 của 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. Đổi khóa được hỗ trợ cho mọi lớp chứng thư số.

IV.7.1 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.7.2 Các trường hợp được yêu cầu thay đổi cặp 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.

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 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, xác nhận chứng thư số đổi khóa

Tương tự như sự chấp nhận, xác 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 thông tin 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 thư 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 và tạm dừng chứng thư số

IV.9.1 Các tình huống thu hồi chứng thư số

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, EFY-CA 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, EFY-CA có lý do để tin tưởng hay nghi ngờ rằng khóa bí mật của thuê bao đã bị làm lộ, bị đánh cắp.
- RA, EFY-CA có lý do tin tưởng rằng thuê bao đã vi phạm một trong các điều khoản nghiêm trọng trong các thỏa thuận với EFY-CA và EFY-CA/CPS.
- 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 EFY-CA.

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

- Nhận được nhiều phản ánh.
- Nhận 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 EFY-CA, hay một RA sẽ được cho quyền yêu cầu thu hồi một chứng thư số của RA Admin.
- EFY-CA 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

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 EFY-CA.
- 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, email...

CA/RA admin được quyền yêu cầu thu hồi chứng thư số của người dùng cuối trong miền con của CA/RA. EFY-CA 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 EFY-CA. 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 EFY-CA 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 EFY-CA. 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).

EFY-CA 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 EFY-CA 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 EFY-CA sẽ được thông báo trong trường hợp khóa Khóa bí mật của CA bị lộ.

IV.9.13 Các tình huống tạm dừng 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.
- Người sử dụng chứng thư số có nhu cầu không sử dụng trong một thời gian vì một mục đích hợp lý.

IV.9.14 Ai có thể yêu cầu tạm dừng các 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 EFY-CA, hay một RA sẽ được cho quyền yêu cầu thu hồi một chứng thư số của RA Admin.

- EFY-CA 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.9.15 Thủ tục tạm dừng chứng thư số

- Người yêu cầu treo chứng thư số thực hiện các thủ tục xác thực nhận dạng với CA/RA
- Người yêu cầu trình bày lý do phù hợp
- Yêu cầu treo chứng thư số được tạo và gửi cho CA.

IV.9.16 Giới hạn xử lý tạm dừng chứng thư số

Chứng thư số bị tạm dừng ngay lập tức, sau khi EFY-CA xác thực các thông tin thu hồi.

IV.10 Kiểm tra thông tin trạng thái chứng thư số

IV.10.1 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.10.2 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 EFY-CA sẽ thông báo kế hoạch xử lý trên website của EFY-CA).

IV.11 Chấm dứt dịch vụ của 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.

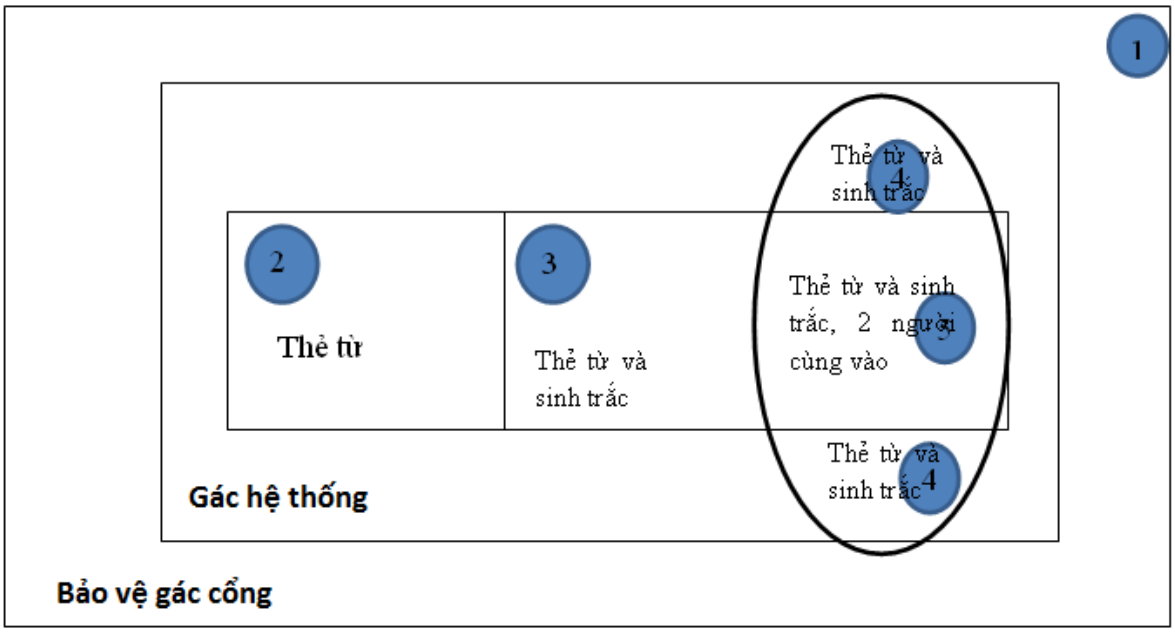
IV.12 Lưu trữ và phục hồi khóa bí mật của thuê bao

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 EFY-CA không cung cấp dịch vụ lưu trữ và phục hồi khóa cho thuê bao.

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

V.1 Các kiểm soát an toàn, an ninh vật lý

V.1.1 Truy cập vật lý



Truy cập tới mỗi tầng an ninh vật lý có thể kiểm tra và giám sát. Vì vậy mỗi tầng có thể truy nhập bởi cấp phép riêng. Phòng đặt hệ thống CA, RA của hệ thống chứng thực chữ ký số EFY-CA được đặt trong không gian riêng với hệ thống Camera giám sát an ninh 24/7. Quyền ra vào nơi đặt thiết bị được kiểm soát bởi hệ thống nhận dạng vân tay và nhân viên bảo vệ. Bản thân nhân viên bảo vệ cũng không có quyền truy nhập hệ thống máy chủ CA, RA. Trách nhiệm của những nhân viên này là ngăn chặn các truy cập từ bên ngoài ở mức vật lý. Như vậy thiết kế về mặt kiểm soát vật lý của hệ thống EFY-CA đáp ứng mô hình 4 lớp về bảo mật truy cập vật lý với hệ thống public CA:

- Hệ thống nhân viên an ninh kiểm soát vật lý.
- Hệ thống truy nhập bằng thẻ từ vào/ ra của hệ thống Public CA, có sự hỗ trợ của Camera giám sát (TIER 2).
- Hệ thống truy nhập bằng sinh trắc học, Camera giám sát 24/24 tại phòng đặt máy chủ CA/RA (TIER 3). Phía sau lớp 3 sẽ có hai điểm truy cập:
- Hệ thống máy chủ CA hoạt động.
- Hệ thống máy chủ back up (offline).
- Để thực hiện các thao tác với hệ thống CA (ký lên chứng thư số, cấu hình hệ thống) đòi hỏi quản trị viên phải dùng hệ thống smart card theo mô hình M/N (Đòi hỏi ít nhất M quản trị viên trong tổng số N người sử dụng smart card của mình để thực hiện các thao tác quản trị và vận hành hệ thống CA). Truy nhập khu vực này đòi hỏi các kiểm tra bảo mật về sinh trắc học và hệ thống thẻ từ.

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

Các thiết bị của EFY-CA 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 EFY-CA được trang bị, bổ sung phòng ngừa để ngăn chặn và dập tắt lửa hay các thảm họa 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

EFY-CA được bảo vệ trong các đĩa quang, từ 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

EFY-CA 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 EFY-CA được đặt tại các trung tâm Data Center khác. 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 định kỳ ở hệ thống dự phòng diễn ra hoàn toàn tự động dưới sự kiểm soát chặt chẽ từ các chuyên gia của EFY-CA.

V.1.5 Tiêu hủy rác, thông tin nhạy cảm

Các tài nguyên, tài liệu hồ sơ thông tin nhạy cảm được tiêu hủy nhằm không cho dữ liệu thông tin có thể phục hồi. Các phương tiện lưu trữ đảm bảo tính bảo mật khi lưu trữ các thông tin nhạy cảm trước khi được tiêu hủy.

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 thư 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

EFY 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 khóa, 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, mô đun này được kích hoạt trong các thao tác liên quan đến khóa, các truy cập xa hơn nữa sẽ bị thu hồi để duy trì việc phân cách giữa điều khiển các truy cập vật lý và mức logic tới thiết bị. Những người truy cập vật lý tới các mô đun không giữ "Secret Shares" (những thành phần riêng biệt có chứa các thành phần riêng biệt của khóa bí mật hoặc dữ liệu kích hoạt và ngược lại.

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

EFY-CA 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 EFY-CA.

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 như 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 Kiểm soát nhân sự

Các thành viên của EFY-CA 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 EFY-CA.

EFY-CA 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 EFY-CA dưới sự đồng ý của EFY-CA.

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 pháp 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 EFY-CA, bao gồm bốn điểm sau:

- 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 EFY-CA cũng tiến hành điều tra thêm.
- Kiểm tra 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 EFY-CA.
- Các phiên bản phần cứng và phần mềm đang được sử dụng.
- Trách nhiệm cá nhân.
- Báo cáo, chuyển giao các thỏa hiệp và các vấn đề liên quan.
- Thủ tục khôi phục sau thảm họa 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 suất 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 EFY-CA phải được cung cấp các tài liệu sau:

- Tài liệu Chính sách chứng thư
- Tài liệu Quy chế chứng thực
- EFY-CA – Hướng dẫn thủ tục và điều hành
- Tài liệu PKI do EFY-CA cung cấp
- Hướng dẫn cài đặt PKI do EFY-CA cung cấp.

V.4 Các quy trình ghi nhật ký hệ thống

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 EFY-CA. 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:

a. Tạo khóa, sao lưu, lưu trữ, phục hồi, lưu trữ, và hủy bỏ;

b. 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:

a. Yêu cầu chứng thư, gia hạn và yêu cầu tái khóa và thu hồi;

b. Tất cả các hoạt động xác minh được quy định trong các Yêu cầu này và Quy chế chứng thực;

c. Ngày, giờ, số điện thoại được sử dụng, người nói chuyện và kết quả cuối cùng của các cuộc điện thoại xác minh;

d. Phê duyệt và từ chối yêu cầu chứng thư;

e. Phát hành chứng thư;

f. Tạo danh sách Thu hồi Giấy chứng thư và các mục OCSP.

3. Các sự kiện bảo mật, bao gồm:

a. Các nỗ lực truy cập hệ thống PKI thành công và không thành công;

b. Các hoạt động của hệ thống an ninh và PKI được thực hiện;

c. Thay đổi hồ sơ bảo mật;

d. Sự cố hệ thống, lỗi phần cứng và các bất thường khác;

e. Các hoạt động của Firewall và router;

f. 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

EFY-CA 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)

EFY-CA sẽ đảm bảo rằng tất cả các sản phẩm thuộc phạm vi của EFY-CA 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 các bản ghi

V.5.1 Các loại hồ sơ được lưu trữ

EFY-CA 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.
- 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)

EFY-CA 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

EFY-CA 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 EFY-CA 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 EFY-CA lớn hơn thời gian hiệu lực của chứng thư số cấp cho thuê bao là 90 ngày.

Quy trình và thủ tục thay đổi cặp khóa được tuân theo nội dung Nghị định 130/2018/NĐ-CP.

V.7 Xử lý sự cố, thảm họa và phục hồi

V.7.1 Các thủ tục xử lý vấn đề lộ khóa 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 EFY-CA được nêu trong tài liệu này.

V.7.3 Lộ khóa bí mật của CA

Trong trường hợp lộ khóa 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 khóa bí mật của CA bị lộ trong miền con của EFY-CA.

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

EFY-CA tiến hành bảo mật cho các hoạt động phát triển, kiểm tra, bảo trì của CA và RA. EFY-CA sẽ triển khai kế hoạch khôi phục sau thảm họa. Kế hoạch khôi phục sau thảm họa. Kế hoạch khôi phục sau thảm họa 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 họa sẽ có bảo vệ vật lý được EFY-CA chỉ rõ.

Trung tâm xử lý có khả năng hồi phục hay khôi phục dữ liệu trong khoảng 72 giờ sau khi một thảm họa 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 khóa cho khách hàng doanh nghiệp sử dụng hạ tầng quản lý PKI.

Cơ sở dữ liệu khôi phục thảm họa 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 họa 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 EFY-CA.

Trung tâm dịch vụ có chức năng công bố thảm họa trên website, thông báo trực tiếp tới khách hàng, đối tác tin cậy và những người quan tâm.

Kế hoạch khôi phục sau thảm họa 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 họa 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 họa 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 họa 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.8 Dừng hoạt động

V.8.1 Kết thúc sự hoạt động của CA hay RA

V.8.1.1 *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, EFY-CA 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, EFY-CA 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.8.1.2 *Chấm dứt RA*

Cơ quan đăng ký có thể bị chấm dứt vì bất kỳ lý do nào. Mọi quyết định được phê duyệt bởi EFY-CA. Trong trường hợp chấm dứt RA vì bất kỳ lý do nào, EFY-CA 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. EFY-CA 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 - ĐẢM BẢO AN TOÀN, AN NINH VỀ KỸ THUẬT

VI.1 Tạo và phân phối cặp khóa

VI.1.1 An ninh sinh cặp khóa cho EFY-CA

- Đối với khóa của nhà cung cấp dịch vụ (EFY-CA), 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 EFY-CA hoàn toàn tương thích với những nhà cung cấp HSM hàng đầu thế giới hiện tại như Utimaco, AEP, Luna SA, 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 EFY-CA quá trình sinh khóa trên thiết bị PKI Token.
- EFY-RA hoặc các đại lý RA của EFY-CA hỗ trợ thuê bao sinh khóa trên thiết bị PKI Token an toàn hoặc thiết bị HSM.
- EFY-CA sinh khóa cho thuê bao trên thiết bị PKI Token an toàn và chuyển cho thuê bao.
- EFY-CA 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

- Trong trường hợp EFY-CA, EFY-RA, RA sinh khóa cho thuê bao trên thiết bị PKI Token, thiết bị sẽ được gửi tới thuê bao theo đường vật lý. Mã PIN của thiết bị được chuyển tới thuê bao theo đường thư điện tử, thư giấy…
- Sau khi nhận được thiết bị PKI Token, thuê bao phải đổi mã PIN của thiết bị.

VI.1.4 Gửi Khóa công khai cho EFY-CA

Khi một khóa công khai được truyền tới EFY-CA 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 EFY-CA, cặp khóa EFY-CA được sinh trên HSM và gửi yêu cầu đăng ký chứng thư số của EFY-CA định dạng PKCS#10 lên RootCA Quốc gia để xin cấp chứng thư số cho EFY-CA.

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

Chứng thư số khóa công khai của EFY-CA và RootCA quốc gia được công bố công khai trên website của EFY-CA 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 EFY-CA, 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. EFY-CA hiện tại sử dụng cặp khóa có độ dài nhỏ nhất tương đương với 2048 bit trong RSA cho CA.

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

VI.1.7 Cách thức khóa bí mật được chuyển đến hoặc đi từ một mô đun mã hoá

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

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

Những người tham gia dịch vụ EFY-CA có sẵn các khóa bí mật và chuyển chúng vào trong thẻ cứng, ví dụ: kiểm soát khóa bí mật đã được cấp phát của thuê bao cuối vào thẻ thông minh.

VI.1.8 Cách thức lưu trữ khóa bí mật trên mô đun mã hoá

Các khóa bí mật của CA hoặc RA được lưu trữ trên các mô đun mã hoá dưới dạng mật mã.

VI.1.9 Sử dụng khóa bí mật đối với thuê bao

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

VI.1.10 Huỷ khóa bí mật

Khi được yêu cầu, các khóa bí mật của CA sẽ bị huỷ diệt để đảm bảo các khóa 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 EFY-CA.

VI.2 Kiểm soát và bảo vệ khóa bí mật

VI.2.1 Tiêu chuẩn kỹ thuật đối với thiết bị mật mã

Thiết bị mật mã HSM EFY-CA sử dụng 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-BTTTT.

VI.2.2 Các cơ chế kiểm soát và bảo vệ khóa bí mật

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

Đa kiểm soát được áp dụng để bảo vệ dữ liệu kích hoạt cho khóa bí mật CA được lưu trữ tại trung tâm xử lý tuân theo các chuẩn trong chính sách bảo mật của EFY-CA. Trung tâm xử lý sử dụng “Secret Sharing” để chia khóa 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 khóa 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 EFY-CA. Trung tâm xử lý cũng sử dụng Secret Sharing để bảo vệ khóa bí mật tại từng khu vực khôi phục sau thảm họa

VI.2.3 Dự phòng khóa bí mật

CA tạo các bản lưu dự phòng khóa bí mật cho mục đích khôi phục sự cố hay khôi phục sau thảm họa phù hợp với chuẩn trong chính sách bảo mật của EFY-CA. 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 khóa bí mật và đưa chúng vào các mô đun 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 mô đun mã hoá nằm trong khu vực CA, như tại khu vực khôi phục sau thảm họa hoặc tại khu vực bên ngoài khác, ví dụ như ngân hàng.

Khi một chứng thư của EFY-CA hết hạn, những cặp khóa gắn với chứng thư ấy sẽ đảm bảo được lưu trữ trong khoảng thời gian ít nhất là 5 năm trong các mô đun phần cứng có cơ chế mã hoá đáp ứng được các yêu cầu của CPS. Những cặp khóa 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.3 Các vấn đề liên quan đến quản lý cặp khóa

VI.3.1 Lưu trữ khóa

Khóa được sinh và quản lý trên thiết bị đạt chuẩn bảo mật.

VI.3.2 Thời gian có hiệu lực của chứng thư và cặp khóa

Thời gian hoạt động của chứng thư số được tính từ thời điểm cấp phát chứng thư số và kết thúc tại thời điểm hết hạn được đề cập trong thuộc tính của chứng thư số ngoại trừ trường hợp chứng thư số bị thu hồi trước khi hết hạn.

Thời gian hoạt động của cặp khóa tương ứng với thời gian hoạt động của chứng thư số tương ứng ngoại trừ trường hợp cặp khóa dùng để mã hóa, kiểm tra chữ ký. Ngoài ra thời gian hoạt động của cặp khóa tuân theo các quy định của Bộ Thông tin và Truyền Thông.

VI.4 Dữ liệu kích hoạt

VI.4.1 Quá trình tạo và cài đặt dữ liệu kích hoạt

EFY-CA tạo và cài đặt dữ liệu kích hoạt (Activation Data) cho khóa 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 khóa 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.4.2 Bảo vệ dữ liệu kích hoạt

EFY-CA sẽ bảo vệ dữ liệu kích hoạt cho những khóa 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 khóa bí mật.

Thuê bao đầu cuối sẽ bảo vệ dữ liệu kích hoạt cho những khóa 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 khóa 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 EFY-CA. 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.
- 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 họa nhằm đảm bảo *Secret Share* luôn sẵn sàng tại vị trí khôi phục thảm họa 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.4.3 Các vấn đề khác của dữ liệu kích hoạt

VI.4.3.1 *Vấn đề chuyển tải dữ liệu kích hoạt*

Để chuyển giao các dữ liệu kích hoạt cho các khóa bí mật, các thành viên thuộc dịch vụ EFY-CA 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.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 khóa bí mật mà dữ liệu kích hoạt đó bảo vệ. Sau khi hết thời gian lưu trữ, dịch vụ EFY-CA sẽ vô hiệu hoá dữ liệu kích hoạt bằng cách ghi đè hoặc tiến hành huỷ vật lý.

VI.5 Kiểm soát an ninh máy tính

Dịch vụ EFY-CA 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 EFY-CA. 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.6 Kiểm soát an ninh quy trình sử dụng

Hệ thống EFY-CA sử dụng các cơ chế, chính sách, biện pháp bảo mật trong quá trình triển khai dịch vụ bao gồm việc giám sát các hoạt động triển khai, cấu hình, vận hành hệ thống. Đảm bảo các điều kiện hoạt động cho dịch vụ ký số, kiểm soát các vấn đề liên quan đến xác thực và quyền truy cập.

VI.7 Giám sát an ninh hệ thống mạng

Việc thiết kế an toàn chung cho hệ thống, EFY-CA 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: gồm Firewall Internet GW, Internal FW.
- Hệ thống phát hiện và chống thâm nhập mạng IPS/IPS Network Sensor.
- Hệ thống phát hiện và chống thâm nhập các máy chủ ứng dụng IPS Host sensor.
- Hệ thống phòng chống Antivirus nhiều điểm: Internet Gateway, Mail server, spam mail, Client/server, quản lý tập trung.
- Hệ thống cập nhật bản vá cho máy chủ/máy trạm.
- Hệ thống quản trị an ninh: thành phần quản lý và giám sát an ninh tập trung, các thành phần dò tìm các lỗ hổng, thành phần thiết lập chính sách an ninh mạng, thành phần phân tích an ninh và báo cáo, thành phần cập nhật các bản vá, thành phần quản lý và phân tích băng thông của mạng.

Dựa vào các thành phần này, hệ thống an ninh mạng của EFY-CA 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.

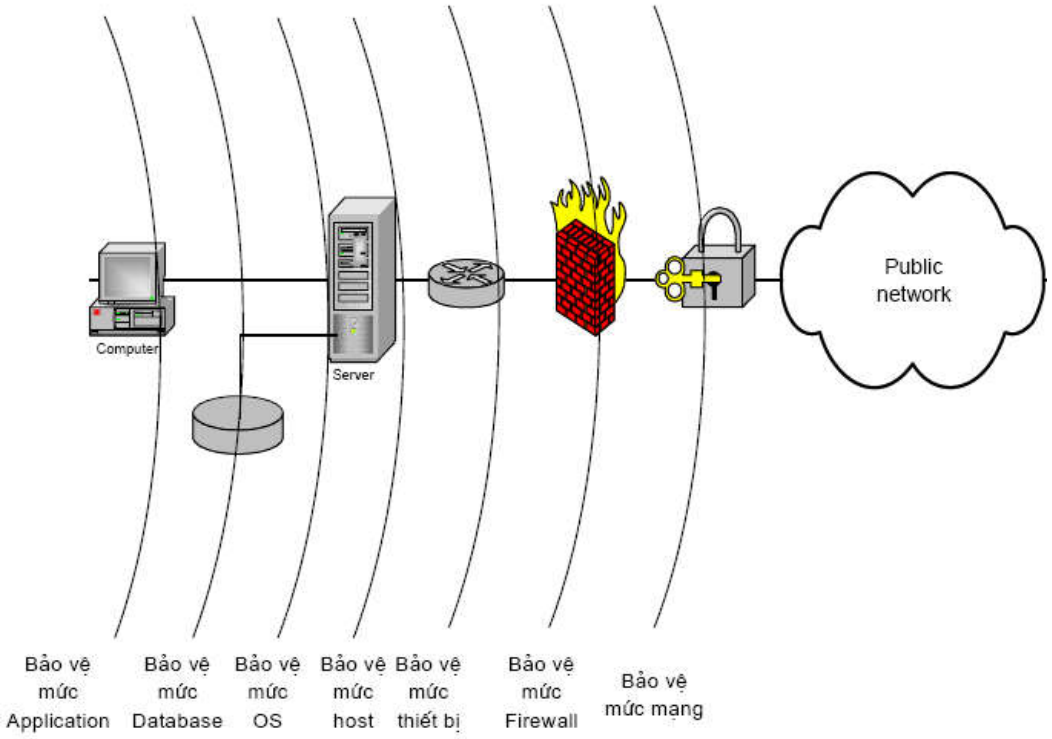
- Quản lý tập trung, tạo các báo cáo an ninh dễ hiểu tường minh và chính xác.

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 EFY-CA, 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.7.1.1 *Hệ thống tường lửa dành cho EFY-CA (Firewall)*

Firewall sử dụng trong hệ thống EFY-CA 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 EFY-CA 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 EFY-CA 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.7.1.2 *Hệ thống tường lửa ứng dụng WEB (Web Application Firewall)*

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

VI.7.1.3 *Hệ thống phát hiện và ngăn chặn tấn công (Intrusion Prevention System – IPS)*

Qua phân tích trên, hệ thống EFY-CA được thuê đặt tại DC của EFY-CA và Viettel (TIA 942 Tier3) 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 EFY-CA 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 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 EFY-CA 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.7.1.4 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.

VI.8 Dấu thời gian

- EFY-CA chưa cung cấp dịch vụ dấu thời gian.

VII - ĐỊNH DẠNG CHỨNG THƯ SỐ, DANH SÁCH THU HỒI CHỨNG THƯ (CRL), GIAO THỨC KIỂM TRA TRẠNG THÁI CHỨNG THƯ SỐ TRỰC TUYẾN (OCSP)

VII.1 Định dạng của chứng thư số

Chứng thư số có định dạng X509 v3 và RFC3280, theo Thông tư 06/2015/TT-BTTTT. Chứng thư số bao gồm tối thiểu các trường thông tin tuân theo quy định tại Thông tư 04/2019/TT-BTTTT như sau:

STT	Trường		Ý nghĩa	Quy định	
				Chứng thư số công cộng	Chứng thư số chuyên dùng Chính phủ
1	Version		Phiên bản của chứng thư số	Version 3 (value = 2)	
2	Serial Number		Số hiệu chứng thư số	Số nguyên dương ngẫu nhiên xác định duy nhất một chứng thư số do CA cấp cho thuê bao, độ dài không quá 20 octet (byte)	
3	Signature		Thuật toán ký chứng thư số của CA	Theo quy định của Bộ Thông tin và Truyền thông về tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số đang có hiệu lực	
4	Issuer	common Name	Tên của CA cấp chứng thư số	Tên giao dịch của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng trong hồ sơ đề nghị cấp chứng thư số	Tên sub-CA của Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ
		organizationName	Tên của tổ chức/doanh nghiệp vận hành CA	Tên của doanh nghiệp được cấp phép cung cấp dịch vụ chứng thực chữ ký số công cộng	Ban Cơ yếu Chính phủ
		countryName	Tên nước	VN	
5	Validity	notBefore	Thời điểm có hiệu lực của chứng thư số	- Trước năm 2050: UTCTime. - Từ năm 2050 trở đi: GeneralizedTime.	

		notAfter	Thời điểm hết hiệu lực của chứng thư số	- Trước năm 2050: UTCTime. - Từ năm 2050 trở đi: GeneralizedTime.
6	Subject	userID	Định danh của thuê bao	MST:[mã số thuế] hoặc MNS:[mã quan hệ ngân sách] hoặc BHXH:[mã số bảo hiểm xã hội] hoặc CMND:[số chứng minh nhân dân] hoặc HC:[số hộ chiếu] hoặc CCCD:[số thẻ căn cước công dân] *Các trường hợp khác theo thỏa thuận giữa thuê bao và tổ chức cung cấp dịch vụ chứng thực chữ ký số.*
		commonName	Tên của thuê bao	Tên của thuê bao được cấp chứng thư số
		organizationName	Tên của tổ chức/đơn vị quản lý thuê bao	Tên của tổ chức/đơn vị quản lý thuê bao (nếu có)
		stateOrProvinceName	Tên tỉnh/TP nơi sống/làm việc của thuê bao	Tên của tỉnh/TP nơi sống/làm việc của thuê bao bằng tiếng Việt, có dấu, các chữ cái đầu viết hoa.
		countryName	Tên nước	VN
7	Subject Public Key Info	algorithm	Thuật toán sinh khóa	Theo quy định của Bộ Thông tin và Truyền thông về tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số đang có hiệu lực
		subjectPublicKey	Khóa công khai của thuê bao	Theo quy định của Bộ Thông tin và Truyền thông về tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số đang có hiệu lực
8	signatureAlgorithm	Thuật toán ký chứng thư số của CA	Cùng thuật toán tại trường số 3	

9	signatureValue	Chữ ký số của CA trên chứng thư số	Chữ ký số của CA trên chứng thư số

Các thành phần mở rộng:

Cách sử dụng khóa (Key Usage) trong chứng thư số X.509 phiên bản 3 phải tuân theo quy định trong RFC 3280.

Phần mở rộng của chính sách chứng thư (Certificate Policies Extension) không được sử dụng trong chứng thư số của thuê bao.

Các ràng buộc cơ bản (Basic Constraints): Subject Type=End Entity, Path Length Constraint=None.

Điểm công bố danh sách chứng thư số bị thu hồi: Trường CRL Distribution Points của chứng thư số X.509 phiên bản 3 có chứa địa chỉ URL để người dùng truy cập tới CRL nhằm kiểm tra trạng thái chứng thư số.

- Đường dân giao thức kiểm tra trạng thái chứng thư số trực tuyến OCSP: Authority Info Access, Access Method=On-line Certificate Status Protocol, Alterative Name: URL=…

VII.2 Định dạng danh sách thu hồi chứng thư số

Trường	Giá trị
Version	Phiên bản của CRL
Signature Algorithm	Thuật toán để ký CRL
Issuer	Nhà cung cấp
Effective Date	Ngày bắt đầu có hiệu lực
Next Update	Thời gian có CRL tiếp theo
Revoked Certificate	Danh sách chứng thư bị hủy, 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

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

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

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

Các tiêu chuẩn của dịch vụ EFY-CA sẽ được dùng để tiến hành các đánh giá về quản lý rủi ro bổ sung của chính EFY-CA 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 EFY-CA 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 EFY-CA để tiến hành kiểm toán, đánh giá và thanh tra này.

VIII.1 Tần suất và các trường hợp đánh giá

Các cuộc kiểm tra đánh giá quá trình tuân thủ được tiến hành ít nhất mỗi năm một lần với chi phí phụ thuộc về thực thể được kiểm toán đáp ứng yêu cầu theo quy định.

VIII.2 Đơn vị, người thực hiện kiểm tra kỹ thuật

Việc kiểm tra kỹ thuật hệ thống được thực hiện bởi đơn vị, cá nhân có năng lực chuyên môn về hạ tầng kỹ thuật hệ thống CA và đảm bảo các yêu cầu về an toàn thông tin. Ngoài ra các đơn vị, cá nhân đã được chứng nhận bởi RootCA về đánh giá năng lực kiểm tra.

VIII.3 Các nội dung kiểm tra kỹ thuật

Các nội dung kiểm tra kỹ thuật bao gồm hạ tầng, môi trường hoạt động của hệ thống EFY-CA, các hoạt động quản lý khóa, quản trị hệ thống, quản trị vòng đời chứng thư số và các quy trình kiểm soát, vận hành khác có liên quan.

VIII.4 Xử lý khi phát hiện sai sót

Dựa vào kết quả kiểm tra đánh giá, bộ phận quản trị EFY-CA sẽ xây dựng các kế hoạch triển khai các biện pháp hợp lý nhằm xử lý các vấn đề gây ảnh hưởng hoặc có nguy cơ ảnh hưởng đến hoạt động của dịch vụ.

VIII.5 Công bố kết quả kiểm tra kỹ thuật

Kết quả kiểm tra kỹ thuật sẽ được EFY-CA công bố trên trang thông tin điện tử của mình.

VIII.6 Tần suất và các trường hợp đánh giá

Tần suất đánh giá kỹ thuật sẽ được thực hiện định kỳ hoặc tuân theo thời hạn chứng chỉ của các thành phần hệ thống.

VIII.7 Danh tính và khả năng của đơn vị, người kiểm tra

Việc kiểm tra kỹ thuật hệ thống được thực hiện bởi đơn vị, cá nhân có năng lực chuyên môn về hạ tầng kỹ thuật hệ thống CA và đảm bảo các yêu cầu về an toàn thông tin. Ngoài ra các đơn vị, cá nhân đã được chứng nhận bởi RootCA về đánh giá năng lực kiểm tra.

IX - CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC

IX.1 Phí/ Giá

Phí duy trì dịch vụ hệ thống kiểm tra trạng thái chứng thư số tuân theo quy định tại Thông tư 19/2022/TT-BTC ngày 23 tháng 3 năm 2022 Quy định mức thu, chế độ thu, nộp, quản lý và sử dụng dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số.

IX.1.1 Lệ phí cấp Chứng thư hoặc gia hạn Chứng thư

Khách hàng sử dụng dịch vụ EFY-CA 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 EFY-CA 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 EFY-CA 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 EFY-CA 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 việc 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

EFY-CA 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

EFY-CA 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 EFY-CA tiến hành đền bù bảo hiểm và mức đền bù bảo hiểm*

EFY-CA 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.
- EFY-CA 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*

EFY-CA 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 khóa bí mật.
- Lỗi của RA, bao gồm lỗi xác thực việc nhận biết dữ liệu, số chứng thư, giá trị khóa 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

EFY-CA 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.

EFY-CA 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. EFY-CA đưa ra các chương trình bảo đảm mở rộng được yêu cầu trong CPS.

IX.3 Bảo mật các thông tin nghiệp vụ

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 khóa công khai và các thông tin cần thiết để khôi phục các khóa 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 EFY-CA hoặc một thuê bao.
- Các báo cáo kiểm toán tạo bởi EFY-CA 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 tai nạn hay khôi phục sau thảm họa.
- 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 EFY-CA 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

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

IX.4 Bảo mật thông tin cá nhân

Chính sách bảo mật thông tin cá nhân được công bố trên trang tin điện tử của EFY-CA.

IX.4.1 Phạm vi thông tin bí mật cần được bảo vệ, kế hoạch bảo mật thông tin cá nhân

EFY-CA sẽ tiến hành triển khai chính sách đảm bảo tính riêng, tuân theo luật riêng tư, EFY-CA 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.

Tất cả những thông tin về thuê bao không được công bố công khai qua các nội dung bao gồm chứng thư số, danh mục chứng thư và các CRL trực tuyến được coi là thông tin bí mật.

IX.4.2 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.4.3 Trách nhiệm bảo vệ thông tin riêng tư

Những người tham gia vào dịch vụ EFY-CA nhận các thông tin bí mật phải đảm bảo tính mật cho những thông tin này không bị tiết lộ với bên thứ 3 và phải tuân theo những quy định về bảo vệ dữ liệu cá nhân trong phạm vi quyền hạn của mình.

IX.4.4 Thông báo và cho phép sử dụng thông tin mật

Theo quy định hay theo chính sách bảo mật, các thông tin bí mật sẽ không được sử dụng mà không có sự cho phép của người sở hữu hoặc đại diện chủ sở hữu những thông tin này. Trừ các trường hợp được quy định khác hoặc các thỏa thuận cụ thể.

IX.4.5 Cung cấp thông tin mật theo yêu cầu của cơ quan luật pháp

EFY-CA sẽ được phép công bố những thông tin mật/riêng tư nếu:

- Có yêu cầu của cơ quan quản lý nhà nước, chính phủ, cơ quan điều tra, tòa án,… tuân thủ theo quy định của pháp luật hiện hành.

IX.4.6 Những trường hợp cung cấp thông tin khác

EFY-CA không cung cấp thông tin hoặc từ chối cung cấp thông tin cho các đối tượng khác nằm ngoài phạm vi cho phép, tuân thủ theo các quy định của pháp luật hiện hành.

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. EFY-CA 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. EFY-CA 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 EFY-CA chấp nhận rằng EFY-CA 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 khóa và các tài liệu của khóa

Cặp khóa 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 Tuyên bố và cam kết

IX.6.1 Cam kết và đảm bảo của CA/RA

EFY-CA đảm bảo rằng:

- Các thông tin trong chứng thư số là đúng với thông tin đăng ký hợp lệ.
- Kết quả xác minh tính chính xác của hồ sơ thuê bao được kiểm tra, xác nhận và chịu trách nhiệm.
- Chứng thư số tuân thủ các yêu cầu trong CPS này.
- Thỏa thuận thuê bao có thể chứa các cam kết và tuyên bố khác.
- Dịch vụ chứng thư số và sử dụng chứng thư đảm bảo thích hợp với yêu cầu trong CPS này.
- Các nhân sự và bên thứ 3 đáp ứng các mức độ đảm bảo an toàn thông tin trong hoạt động CA.
- Các nhân sự và bên thứ 3 được đào tạo và nắm được quy trình dịch vụ theo quy định.
- Hệ thống kỹ thuật đáp ứng các yêu cầu đối với hệ thống thông tin theo cấp độ.

IX.6.2 Cam kết và đảm bảo của thuê bao

- Cung cấp thông tin đăng ký dịch vụ và hồ sơ đầy đủ, hợp lệ.
- Sử dụng chứng thư tuân theo các mục đích hợp pháp và tuân thủ CPS này.
- Thuê bao có trách nhiệm bảo vệ mã PIN của mình.
- Tuân thủ các yêu cầu chính sách hợp đồng, cam kết và CPS.

IX.6.3 Đại diện của CA và vấn đề bảo lãnh

Dịch vụ EFY-CA 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/CPS.
- Dịch vụ thu hồi chứng thư và sử dụng kho lưu trữ phù hợp với tiêu chuẩn trong CP/CPS.

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

IX.6.4 Đại diện của RA và vấn đề bảo lãnh

Các RA của dịch vụ EFY-CA 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.6.5 Đại diện của khách hàng và sự bảo lãnh

Khách hàng cam kết rằng:

- Mỗi chữ ký số được tạo sử dụng khóa bí mật tương ứng với khóa 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.
- Khóa bí mật được bảo vệ và người không có thẩm quyền không thể truy cập vào khóa 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 EFY-CA.
- Khách hàng là thuê bao cuối và không phải là một CA, không được phép sử dụng khóa bí mật kết hợp với bất kì khóa 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.6.6 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.

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 Từ chối trách nhiệm

Trong phạm vi của quy định pháp luật, hợp đồng thuê bao và các cam kết, thỏa thuận, người dùng có thể bị EFY-CA từ chối bảo hành.

IX.8 Giới hạn trách nhiệm

Trong giới hạn của quy định pháp luật, hợp đồng thuê bao, hợp đồng với đối tác có thể giới hạn trách nhiệm pháp lý của EFY-CA.

IX.9 Bồi thường thiệt hại

IX.9.1 Vấn đề bồi thường của khách hàng

Khi pháp luật yêu cầu, khách hàng phải bồi thường cho EFY-CA 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.9.2 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 EFY-CA hay các thành phần tham gia dịch vụ EFY-CA 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.10 Hiệu lực của Quy chế chứng thực

IX.10.1 Thời hạn

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

IX.10.2 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.10.3 Ảnh hưởng của sự kết thúc và những tồn tại

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

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

EFY-CA 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.12 Bổ sung và sửa đổi

IX.12.1.1 *Các thủ tục sửa đổi*

Những sửa đổi của CPS sẽ được thực hiện bởi Cấp quản lý chính sách có thẩm quyền của EFY-CA. 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.12.1.2 *Các trường hợp cần sửa đổi nhận diện đối tượng (OID)*

Nếu cần thiết, EFY-CA 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.12.1.3 *Cách thức và thời hạn thông báo*

EFY-CA có quyền quyết định việc thay đổi là cần thiết hay không cần thiết.

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

Trái ngược với một số điều trong CPS, nếu EFY-CA cho rằng sự thay đổi CPS là cần thiết để ngăn chặn sự xâm phạm đến an toàn của dịch vụ EFY-CA, EFY-CA có quyền thay đổi CPS. Công bố về sự thay đổi sẽ ngay lập tức có hiệu lực. Sau khi công bố, EFY-CA 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 EFY-CA. Bất kỳ ai tham gia vào dịch vụ EFY-CA cũng có quyền đề xuất ý kiến tới EFY-CA cho đến lúc hết thời gian sửa đổi.

B. Cơ chế xử lý các sửa đổi

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

EFY-CA 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 EFY-CA. Những sửa đổi có hiệu lực sau khi hết hạn sửa đổi.

IX.13 Thủ tục tranh chấp

IX.13.1 Thủ tục tranh chấp giữa EFY-CA, cộng tác và thuê bao

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

IX.13.2 Thủ tục tranh chấp giữa thuê bao và đối tác tin cậy

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

IX.14 Hệ thống pháp lý điều chỉnh

Tài liệu Quy chế chứng thực của các tổ chức cung cấp dịch vụ chứng thực chữ ký số được điều chỉnh bởi các văn bản quy phạm pháp luật, bao gồm: Luật giao dịch điện tử 2005; Nghị định 130/2018/NĐ-CP quy định chi tiết thi hành luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số; và các văn bản quy phạm pháp luật khác có liên quan.

IX.14.1 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.14.1.1 *Trách nhiệm*

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

IX.14.1.2 *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.14.1.3 *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.14.1.4 *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 EFY-CA.

IX.15 Phù hợp với pháp luật hiện hành

Tuân thủ và phù hợp với các quy định hiện hành của pháp luật Việt Nam.

IX.16 Các điều khoản chung

Không có quy định.

IX.17 Các điều khoản khác

Không có quy định.