QUY CHẾ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG
LCS-CA

Certificate Practices Statement (CPS)

L.C.S Co., Ltd

Head Office: 102A Bui Minh Truc St., Dist. 8, HCMC

Branch: 210/16A CMT8 St, Dist 3, HCMC

Email: sales@lcs.com.vn

Website: www.lcs.com.vn

Tel: (84-28) 0844569999

MỤC LỤC

1 GIỚI THIỆU CHUNG

1.1 Tổng quan

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

Các quy định về quy chế chứng thực (CPS) của dịch vụ LCS-CA được trình bày trong tài liệu này, hướng dẫn chi tiết quy chế thực hiện chính sách cấp phát chứng thư số đối với LCS-CA, và quy trình đăng ký, sử dụng chứng thư số của thuê bao và bên nhận.

Bản CPS này là một chính sách quan trọng trong quá trình cung cấp dịch vụ chứng thực chữ ký số công cộng. CPS cung cấp nội dung các yêu cầu về kinh doanh, luật pháp, kỹ thuật cho quá trình chấp nhận, cấp phát, quản lý, thu hồi và cấp lại chứng thư số. Các yêu cầu của CPS được gọi là các "chuẩn LCS-CA", có nhiệm vụ cung cấp tính bảo mật và toàn vẹn cho dịch vụ LCS-CA, được áp dụng cho tất cả các thành phần tham gia dịch vụ chứng thực chữ ký số LCS-CA. Các thành phần tham gia dịch vụ LCS-CA phải tuân thủ các yêu cầu được đề ra trong CPS này.

Bản CPS này sẽ phải chịu sự quản lý của luật pháp Việt Nam cũng như tuân theo các chính sách, quy chế, văn bản và thủ tục ban hành bởi RootCA Việt Nam và các đơn vị chức năng có liên quan khác. Bản CPS của dịch vụ LCS-CA được xây dựng tuân theo khuyến nghị RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework).

Với thế mạnh về công nghệ thông tin và hạ tầng viễn thông, công ty TNHH LCS xây dựng dịch vụ này để hướng mục tiêu:

- Xây dựng dịch vụ chứng thực chữ ký số tin cậy trên toàn lãnh thổ Việt Nam
- Góp phần chuyển đổi các doanh nghiệp trong nước đi theo định hướng công nghệ mới của chính phủ.

- Ứng dụng cho các dịch vụ thương mại điện tử, giao dịch trực tuyến, chính phủ điện tử.

1.2 Tên tài liệu và nhận dạng

- Tên tài liệu: Quy chế chứng thực chữ ký số LCS-CA
- Phiên bản: v1.6
- Ngày tạo: 22/05/2019

1.3 Các bên tham gia

Các bên tham gia vào hạ tầng khóa công khai LCS-CA (Publick Key Infrastructure -PKI) bao gồm:

- Trung tâm Chứng thực điện tử quốc gia
- Tổ chức chứng thực chữ ký số công cộng LCS-CA
- Đại lý của LCS-CA (RA)
- Thuê bao chứng thư số LCS-CA
- Bên nhận

1.3.1 Trung tâm chứng thực điện tử quốc gia

Trung tâm chứng thực điện tử quốc gia có các đặc điểm sau:

- Trung tâm Chứng thực điện tử quốc gia là tổ chức trực thuộc Bộ Thông tin và Truyền thông có chức năng khai thác hạ tầng an toàn thông tin phục vụ hoạt động giao dịch điện tử, bao gồm dịch vụ chứng thực chữ ký số và xác thực điện tử
- Là cấp cao nhất trong hạ tầng chứng thực chữ ký số công cộng Việt Nam
- Thẩm tra hồ sơ và cấp chứng thư số cho các hệ thống chứng thực chữ ký số công cộng theo giấy phép của Bộ Thông tin và Truyền thông.
- Thiết lập các thông số kỹ thuật để vận hành cơ sở hạ tầng khóa công khai cho xác thực chữ ký số công cộng.
- Kiểm tra kỹ thuật, điều phối các hoạt động xử lý sự cố liên quan đến dịch vụ chứng thực chữ ký số công cộng.
- Thu thập, tổ chức, phân tích, thống kê và tổng hợp số liệu về dịch vụ chứng thực chữ ký số công cộng.

1.3.2 Tổ chức chứng thực chữ ký số công cộng LCS-CA

LCS-CA là tổ chức chứng thực chữ ký số công cộng được Trung tâm chứng thực điện tử quốc gia cấp chứng thư số theo giấy phép của Bộ Thông tin và Truyền thông.

LCS-CA cung cấp dịch vụ chứng thực chữ ký số công cộng cho các tổ chức, doanh nghiệp và cá nhân để thực hiện giao dịch trong môi trường mạng mở an toàn và có giá trị pháp lý theo quy định của pháp luật Việt Nam.

LCS-CA xây dựng một mô hình PKI có mức độ tin cậy cao trong việc sử dụng chữ ký số phục vụ chống chối bỏ, xác thực và toàn vẹn các dữ liệu và giao dịch điện tử.

Dịch vụ chứng thực chữ ký số công cộng LCS-CA vận hành tuân thủ theo Qui chế Chứng thư số LCS-CA, bao gồm:

- Tạo cặp khóa mật mã bao gồm khóa công khai và khóa bí mật LCS-CA;
- Cấp phát, gia hạn và thu hồi chứng thư số của thuê bao LCS-CA theo quy định của pháp luật
- Duy trì trực tuyến cơ sở dữ liệu về trạng thái của toàn bộ chứng thư số LCS-CA đảm bảo đảm bảo các bên tham gia truy xuất 24 giờ / ngày, 7 ngày / tuần;
- Những dịch vụ phát sinh sau khác có liên quan theo quy định

1.3.3 Đại lý của LCS-CA (RA)

Đại lý LCS-CA là đơn vị ký với LCS-CA một hợp đồng ủy quyền tham gia thẩm định đăng ký và cung cấp dịch vụ chứng thực chữ ký số theo quy định của pháp luật. Quyền và nghĩa vụ của hai bên được quy định trong hợp đồng hợp tác giữa hai bên.

1.3.4 Thuê bao chứng thư số LCS-CA

Là các tổ chức, cá nhân, doanh nghiệp sử dụng dịch vụ chứng thực chữ ký số công cộng LCS-CA. Quyền và nghĩa vụ của hai bên được quy định trong hợp đồng cung cấp dịch vụ giữa hai bên.

1.3.5 Bên nhận

Là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký là thuê bao LCS-CA, sử dụng chứng thư số LCS-CA của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.

1.4 Sử dụng chứng thư số LCS-CA

1.4.1 Phạm vi sử dụng chứng thư số LCS-CA

Chứng thư số LCS-CA chỉ được sử dụng theo đúng phạm vi quy định trong hợp đồng giữa LCS-CA và thuê bao.

1.4.2 Cấm sử dụng

Nghiêm cấm việc sử dụng chứng thư số LCS-CA trái với quy định trong hợp đồng giữa LCS-CA và thuê bao và trái với quy định của pháp luật.

1.5 Quản trị Quy chế chứng thực chữ ký số LCS-CA

1.5.1 Tổ chức

- Công Ty TNHH L.C.S
- Trung tâm chứng thư số công cộng LCS-CA
- Địa chỉ: 102 A, Bùi Minh Trực, Phường 6, Quận 8, Tp. HCM
- Website: http://lcs-ca.vn

1.5.2 Người liên hệ

Mọi thông tin liên hệ, phản hồi về bản quy chế chứng thực có thể liên hệ với:
Công Ty TNHH L.C.S

- Điện thoại: (84-28) 4456 999
- Đường dây nóng: 1900 555569
- Email: kythuat@lcs.com.vn
- Địa chỉ: 102 A, Bùi Minh Trực, Phường 6, Quận 8, Tp. HCM
- Website: http://lcs-ca.vn Các thông tin cập nhật, bổ sung bản quy chế chứng thực sẽ được thông báo qua trang

1.5.3 Người quyết định sự phù hợp của Quy chế chứng thực chữ ký số LCS-CA

- Ông Nguyễn Thanh Giang
- Mobile: 0982198227 / 0911992235
- Email: giangnguyen@lcs.com.vn

1.5.4 Tổ chức xác định Quy chế chứng thực chữ ký số LCS-CA phù hợp với chính sách

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

1.5.5 Thủ tục phê chuẩn Quy chế chứng thực chữ ký số LCS-CA

Công ty TNHH LCS sẽ phê chuẩn Quy chế chứng thực LCS-CA và những thay đổi kế tiếp. Các thay đổi được ghi trong một tài liệu chứa các sửa đổi mẫu (dạng) của CPS hay các thông về quá trình cập nhật.

LCS-CA quy định cụ thể về việc cập nhật, sửa đổi và ban hành Quy chế chứng thực chữ ký số LCS-CA.

1.6 Định nghĩa và viết tắt

1.6.1 Định nghĩa các thuật ngữ, khái niệm

Các khái niệm, thuật ngữ được sử dụng trong Quy chế chứng thực chữ ký số LCS-CA được giải thích như dưới đây:

- **Chứng thư số**: Hay còn gọi là chứng thư khóa công khai, là một dạng chứng thư điện tử do Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng LCS-CA cấp cho một khóa công khai bằng cách, ràng buộc khóa công khai của thuê bao với các thông tin định danh của thuê bao có khóa riêng là một cặp với khóa công khai này.
- **Chữ ký số**: Là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng theo đó người có được thông điệp dữ liệu ban đầu và khoá công khai của người ký có thể xác định được chính xác:

  a) Việc biến đổi nêu trên được tạo ra bằng đúng khoá bí mật tương ứng với khoá công khai trong cùng một cặp khóa;

  b) Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.
- **Bên ký:** Là thuê bao LCS-CA dùng khoá bí mật của mình để ký số vào một thông điệp dữ liệu dưới tên của mình.

- **Bên nhận:** Là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng chứng thư số của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.
- **Thuê bao:** Là tổ chức, cá nhân được LCS-CA cấp chứng thư số, chấp nhận chứng thư số và giữ khoá bí mật tương ứng với khoá công khai ghi trên chứng thư số được cấp đó.
- **Tổ chức cung cấp dịch vụ chứng thực chữ ký số**: Là tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử thực hiện hoạt động cung cấp dịch vụ chứng thực chữ ký số.
- **Khóa riêng CA tạo chữ ký**: Khóa riêng cùng cặp với khoá công khai nằm trong chứng thực LCS-CA và được sử dụng để ký số.
- **Danh sách thu hồi chứng thư số (Certificate Revocation List - CRL)**: Một cơ sở dữ liệu hoặc một danh sách các chứng thư số do LCS-CA thu hồi hay hủy bỏ trước thời hạn so với thời hạn hiệu lực của chứng thư số.
- **Tạo khóa (Key Generation):** là quá trình tạo một cặp khóa phi đối xứng bao gồm khóa riêng và khóa công khai
- **Cặp khóa (Key Pair):** Hai khóa liên kết với nhau một cách chính xác (một khóa riêng và tương ứng với nó là một khóa công khai), có đặc điểm là: (i) một khóa có thể được sử dụng để mã hóa các thông tin và chỉ có thể được giải mã bằng chiếc khóa cùng cặp còn lại; (ii) Nếu biết một khóa cũng không thể có khả năng biết được một khóa còn lại.
- **Kiểm tra trạng thái trực tuyến (Online Certificate Status Protocol):** trạng thái thời gian thực được kiểm tra trực tuyến về thời hạn hiệu lực của chứng thư số. Kiểm tra trạng thái trực tuyến liên quan tới một CRL bao gồm việc kiểm tra CRL công bố mới nhất.
- **Khóa riêng (Private Key):** Một khóa bí mật của người giữ chứng thư số, được sử dụng để ký chữ ký số và giải mã thông tin hoặc tài liệu được mã hóa bởi khóa công khai tương ứng.
- **Khóa công khai (Public Key):** Một khoá công khai thuộc sở hữu của người giữ khoá riêng cùng cặp với khoá công khai này. Khoá công khai được phát tán để người nhận

xác thực người "ký" điện tử (người giữ khoá bí mật cùng cặp với khoá công khai này) và người gửi sử dụng khoá công khai này để mã hoá dữ liệu trước khi gửi đi, chỉ có người nhận giữ khoá bí mật cùng cặp với khoá công khai này mới giải mã được.

- **Cơ sở hạ tầng khóa công khai (Public Key Infrastructure - PKI):** Tập hợp các kiến trúc, tổ chức, kỹ thuật, nguyên tắc thực hiện, thủ tục để hỗ trợ trong việc thực hiện và điều hành chứng thư số dựa trên hệ thống mã hóa khóa công khai.
- **Tổ chức đăng ký (Registration Authority - RA):** là một tổ chức được LCS-CA ký hợp đồng đại diện có quyền tiếp nhận và giải quyết các đơn xin cấp chứng thư số và xác minh nhận dạng các chủ thể cuối cùng cũng như chứng thực các thông tin có trong đơn xin chứng thư số tuân theo những điều khoản theo Quy chế này và các thỏa thuận có liên quan.
- **Danh bạ chứng thư số (Repository):** Hệ thống trực tuyến do LCS-CA phát hành duy trì để lưu trữ và phục hồi các chứng thư số hoặc các thông tin liên quan tới thuê bao chứng thư số, bao gồm các thông tin về thời hạn hiệu lực và sự thu hồi chứng thư số.
- **Thu hồi chứng thư số:** Là làm mất hiệu lực của chứng thư số một cách vĩnh viễn từ một thời điểm xác định.

1.6.2 Từ viết tắt

CA	Certification Authority Tổ chức cấp chứng thư số
CRL	Certificate Revocation List Danh sách chứng thư số bị thu hồi
HTTPS	Hypertext Transfer Protocol with SSL Giao thức web với bảo mật đường truyền SSL
PIN	Personal Identification Number Mã số cá nhân
PKCS	Public Key Cryptography Standard Chuẩn khoá công khai
PKI	Public Key Infrastructure Hạ tầng kỹ thuật mã hóa công khai

LDAP	Lightweight Directory Access Protocol Giao thức truy cập danh bạ chứng thư số
RA	Registration Authority Đại lý đăng ký thẩm định thuê bao
SSL	Secure Socket Layer Giao thức bảo mật giao dịch trên Internet
X.509	ITU-T standard for Certificates format Chuẩn về định dạng chứng thư số
HSM	Hardware Security Module Khối bảo mật phần cứng (HSM), là thiết bị có mức bao mật cao nhất trong hạ tầng chứng thư số.
PKI Token PKI SmartCard PKI Virtual Token	Khối bảo mật đầu cuối quản lý khóa thuê bao tuân theo chuẩn FIPS 140-2 level 2 trở lên hoặc tương đương.
Smart card chuyên dụng	Bộ thẻ nghiệp vụ chuyên dụng dùng trong hệ thống thiết bị HSM chuẩn FIPS 140-2 Level3.
FIPS 140-2	Chuẩn đánh giá an ninh an toàn cho hệ thống mật mã theo 4 mức từ Level 1 đến Level 4
FIPS 140-2 Level 2	Yêu cầu an ninh an toàn mức 2 trong hệ thống 4 mức tiêu chuẩn FIPS 140-2.
FIPS 140-2 Level 3	Yêu cầu an ninh an toàn mức 3 trong hệ thống 4 mức tiêu chuẩn FIPS 140-2.
Cơ chế 2 x 3	Cơ chế xác thực, sao lưu, dự phòng và phục hồi sử dụng Smart Card chuyên dụng. Mỗi bộ gồm 3 thẻ do 3 người giữ, mỗi nhiệm vụ phải có 2 trong 3 người tham gia, người còn lại dự phòng cho 2 người kia.
CP	Certificate Policy

	Chính sách chứng thực
CPS	Certification Practices Statement Quy chế chứng thực

1.7 Các loại chứng thư của dịch vụ LCS-CA

Mô hình ứng dụng PKI của hệ thống LCS-CA sẽ đóng vai trò:

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

Hệ thống cung cấp dịch vụ chứng thực chữ ký số LCS-CA cung cấp các sản phẩm trong đất nước Việt Nam như bên dưới:

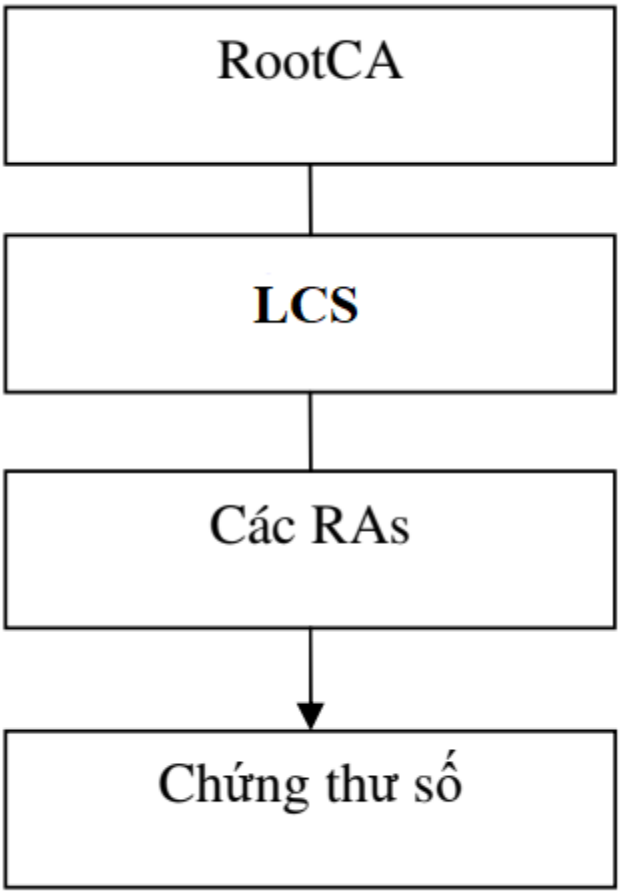
1. Chứng thư số dành cho khách hàng cá nhân.
2. Chứng thư số dành cho khách hàng doanh nghiệp.
3. Chứng thư số Code Signing cho cá nhân hoặc tổ chức phát triển phần mềm, đảm bảo an ninh cho mã nguồn, nội dung được phân phối qua internet.
4. Chứng thư số SSL bảo mật và chứng nhận hệ thống website, mã hóa 256 bit phiên giao dịch SSL giữa server và client.
5. Chứng thư số cho hệ thống bảo mật Managed PKI.

Các định dạng chứng thư số cụ thể tại mục 7 của tài liệu này.

1.8 Quy trình hoạt động LCS-CA

1.8.1 Mô hình tổ chức hoạt động của LCS-CA

LCS-CA hoạt động theo mô hình tổ chức sau:



Trong đó:

- RootCA: là đơn vị cấp phép cho LCS trở thành nhà cung cấp dịch vụ chứng thực chữ ký số. RootCA đồng thời cũng là đơn vị điều tiết và quản lý nội dung chính sách và quy chế chứng thực của dịch vụ phải tuân theo.
- LCS : là trung tâm xử lý duy nhất, dưới quyền quản lý công ty TNHH LCS được phép cung cấp dịch vụ trực tiếp cho người dùng cuối trong mạng tin cậy này.

- Các RAs: Registration Authorities(RAs) là những thực thể có nhiệm vụ xác thực thông tin và thẩm định các yêu cầu trong dịch vụ LCS-CA. Các RA của dịch vụ LCS-CA chịu trách nhiệm xác thực thông tin về các đối tượng muốn đăng ký sử dụng dịch vụ chứng thực. Chứng thư của thuê bao có thể cấp từ LCS hoặc qua các đơn vị RA quản lý.

1.8.2 Định nghĩa chức năng hoạt động

1.8.2.1 Certification Authority – CA

CA là thành phần quan trọng nhất trong hệ thống PKI. CA xác thực tính chính xác của những đối tượng tham gia trong quá trình trao đổi thông tin. CA là tập hợp gồm phần cứng, phần mềm, và những quản trị viên nhằm thực hiện các chức năng chính sau:

- Nhận các yêu cầu cấp chứng thư số và phát hành các chứng thư số mới:
  - Chấp nhận các yêu cầu cấp chứng thư số từ các đối tượng yêu cầu thông qua các thủ tục đăng ký chứa trong bản chính sách này.
  - Xác thực các đối tượng yêu cầu chứng thư số, có thể bởi sự giúp đỡ của các RA được chỉ định.
  - Phát hành các chứng thư số dựa trên các yêu cầu đã được xác thực.
  - Gửi thông báo về thông điệp phát hành đến đối tượng yêu cầu.
  - Đưa các chứng thư số được phát hành có thể sử dụng chung.
- Nhận các yêu cầu thu hồi chứng thư số và tiến hành thu hồi chứng thư số
  - Chấp nhận các yêu cầu thu hồi chứng thư số từ các đối tượng có yêu cầu thông qua các thủ tục có trong bản hướng dẫn thi hành các chính sách này.
  - Xác thực yêu cầu thu hồi chứng thư số của đối tượng tương ứng.
  - Đưa danh sách thu hồi chứng thư số có thể sử dụng chung.

CA có thể thực hiện các chứng năng trên một cách trực tiếp hoặc ủy quyền cho đối tượng khác tiến hành.

Quan hệ giữa các CA trong hệ thống PKI có thể tạo nên các mô hình tin cậy (Trust model) gồm: mô hình phân cấp, mô hình cầu và mô hình mạng lưới.

1.8.2.2 Registration Authority – RA

RA là một đối tượng được CA tin cậy uỷ quyền để đăng ký và đảm bảo tính đúng đắn nội dung thông tin trong chứng thư số của những thuê bao thuộc hệ thống. RA sẽ thu thập thông tin trên và cung cấp cho CA trực thuộc. RA bao gồm một tập hợp phần cứng máy tính, phần mềm, và những người vận hành. Mỗi RA sẽ thường xuyên vận hành bởi một người, và mỗi CA sẽ quản lý một nhóm RA tin cậy.

Các nhiệm vụ của RA bao gồm:

- Xác thực nhận dạng đối tượng.
- Xác nhận liên kết giữa khóa công khai và đặc điểm nhận dạng của đối tượng yêu cầu gồm phương thức chứng minh sở hữu phù hợp

1.8.2.3 Đối tượng sử dụng hệ thống LCS-CA

Các đối tượng sử dụng trong hệ thống LCS-CA là tất cả các tổ chức hay cá nhân sử dụng hệ thống LCS-CA nhưng không phát hành chứng thư số. Những đối tượng này dựa trên các chức năng của hệ thống LCS-CA để nhận được các chứng thư số của mình và xác thực các đối tượng khác trong quá trình trao đổi thông tin.

1.8.3 Quy trình hoạt động của LCS-CA

Hoạt động của hệ thống LCS-CA bao gồm các chức năng sau đây:

- Đăng ký một chứng thư số.
- Phát hành chứng thư số.
- Công bố chứng thư số.
- Gia hạn chứng thư số
- Thu hồi chứng thư số và thông báo chứng thư số bị thu hồi.

1.8.3.1 Đăng ký một chứng thư số

Khi người dùng có nhu cầu sử dụng một chứng thư số, người dùng này cần tạo một yêu cầu xin cấp một chứng thư số cho bộ phận quản lý đăng ký (LCS-RA). RA sẽ chịu tránh nhiệm kiểm tra tính hợp lệ của yêu cầu này. Nếu yêu cầu không hợp lệ RA sẽ trả lại yêu cầu cho người dùng đó và từ chối cấp chứng thư số. Trong trường hợp yêu cầu hợp lệ RA tiếp tục

chuyển yêu cầu tới LCS- CA. Nội dung một yêu cầu xin cấp phát phải tuân theo chuẩn PKCS#10 yêu cầu nội dung một yêu cầu phải có các thông tin sau:

- Tên của CA
- Khóa công khai của thuê bao
- Thuật toán tương ứng
- Chữ ký số của thuê bao được tạo ra từ khóa bí mật.

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

1.8.3.2 Phát hành chứng thư số

Phát hành chứng thư mới tiến hành theo các bước sau:

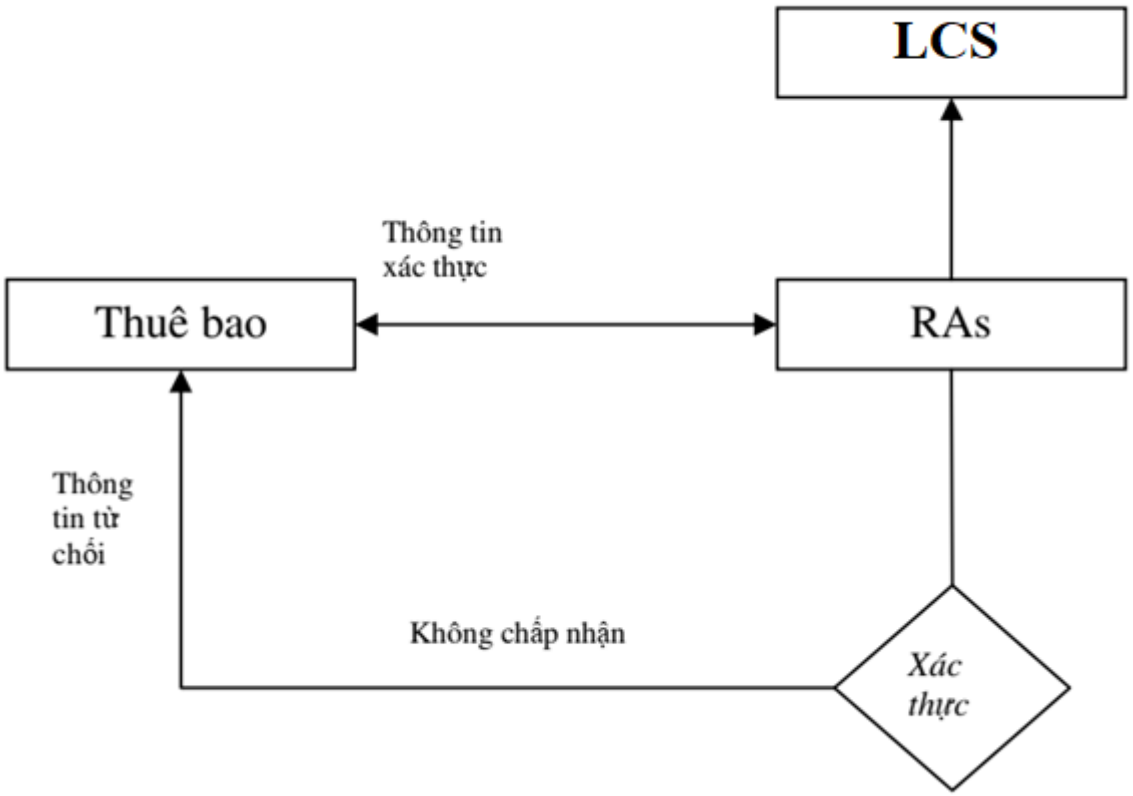
1.8.3.2.1 Nội dung xác thực thông tin thuê bao

Nội dung xác thực thông tin thuê bao gồm có:

- Đối với tổ chức
  - Tên tổ chức:
  - Địa chỉ:
  - Ngành nghề: (giấy phép kinh doanh, Giấy phép thành lập (bản chính hoặc bản sao có công chứng thư số),fax…)
  - Thông tin về website, tên miền của tổ chức(sử dụng cho chứng thư SSL)
  - Thông tin về người đăng ký sử dụng chứng thư
- Đối với cá nhân
  - Tên cá nhân
  - Địa chỉ:
  - Số CMTND :
  - Bản sao hộ khẩu(hoặc hợp đồng điện thoại cố định, hợp đồng điện thoại di
  - động trả sau…)
  - Hộ chiếu

- Thông tin sở hữu tên miền(sử dụng cho chứng thư SSL)

1.8.3.2.2 Quy trình xác thực thông tin thuê bao



Quy trình xác thực thông tin thuê bao được bắt đầu từ nội dung thông tin mà thuê bao kê khai cung cấp. Nếu các thông tin được xác thực là phù hợp sẽ được chấp nhận và chuyển thông báo về LCS nhằm tiến hành các bước tiếp theo của việc cấp chứng thư. Trong trường hợp thông tin thuê bao cung cấp được xác thực là không phù hợp, thuê bao sẽ được thông báo từ chối chấp nhận thông tin.

1.8.3.2.3 Thủ tục xác thực thông tin thuê bao

Thuê bao muốn đăng ký sử dụng chứng thư số cần đến trực tiếp giao dịch đăng ký tại trụ sở và các chi nhánh của LCS.

Thuê bao buộc phải khai báo thông tin thuê bao đã kê khai và tiến hành xác thực thông tin thuê bao. Trong trường hợp xác thực thông tin được chấp nhận hay không chấp nhận thì

các RAs có trách nhiệm gửi phiếu kết quả thông báo về việc xác thực thông tin thuê bao đăng ký.

RAs có trách nhiệm tiến hành làm hợp đồng đăng ký sử dụng chứng thư số với thuê bao đăng ký trong trường hợp thông tin xác thực được chấp nhận.

1.8.3.3 Công bố chứng thư số.

Nguyên tắc cơ bản của hệ thống LCS-CA là công bố rộng rãi chứng thư số sao cho mọi người đều truy cập được. LCS-CA sử dụng một số phương pháp công bố chứng thư số như sau:

- Dịch vụ thư mục (LDAP): Phương pháp này dành cho các chứng thư số theo chuẩn X.509. Dịch vụ thư mục dành cho PKI phổ biến là X.500/LDAP theo chuẩn của IETF.
- Trang web hoặc máy chủ FTP: Các chứng thư số được đưa lên trang web để mọi người có thể truy cập thông qua giao thức HTTP, FTP.

1.8.3.4 Gia hạn chứng thư số

Trước khi hết hạn chứng thư thuê bao cần phải đăng kí với LCS để có một chứng thư số thư số mới nhằm duy trì sự liên tục của việc sử dụng chứng thư. Gia hạn chứng thư tiến hành theo các bước sau:

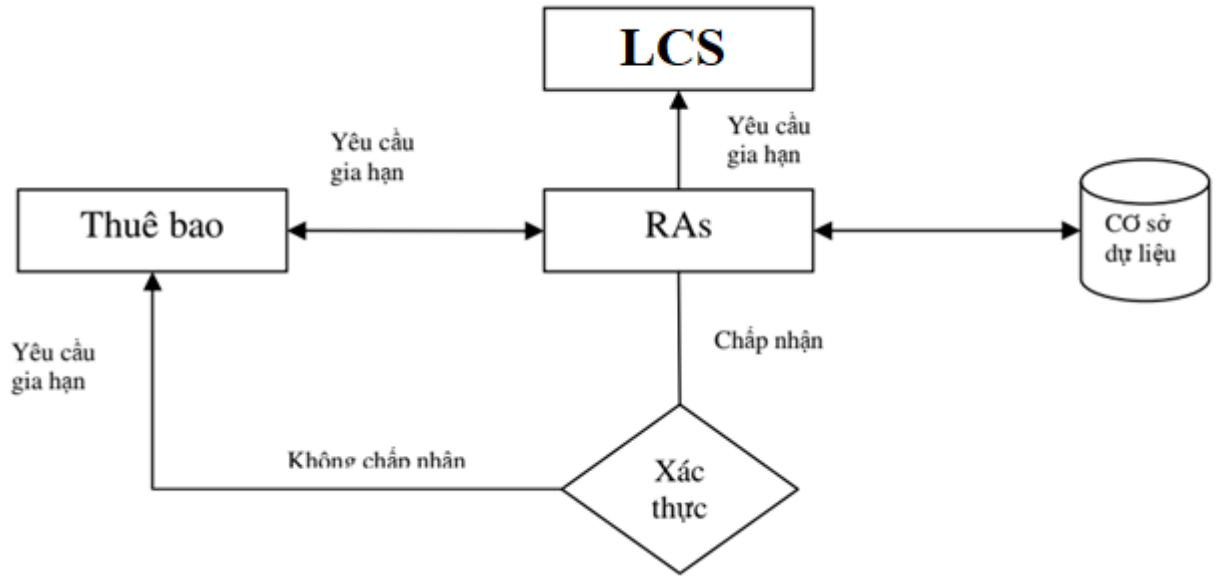
1.8.3.4.1 Nội dung xác thực gia hạn chứng thư

Thuê bao muốn gia hạn chứng thư phải đưa ra hợp đồng đăng ký sử dụng chứng thư số đã ký nhằm chứng minh quyền gia hạn. Trong trường hợp mất hợp đồng, thuê bao phải cung cấp đầy đủ các thông tin cần thiết sao cho khớp với thông tin đã đăng ký sử dụng chứng thư số gốc bao gồm:

- Đối với tổ chức
    - Tên tổ chức:
    - Địa chỉ:
    - Ngành nghề: (giấy phép kinh doanh, Giấy phép thành lập (bản chính hoặc bản sao có công chứng thư số),fax…)
    - Thông tin về website, tên miền của tổ chức(sử dụng cho chứng thư SSL)
    - Thông tin về người đăng ký sử dụng chứng thư
- Đối với cá nhân

- Tên cá nhân
- Địa chỉ:
- Số CMTND :
- Bản sao hộ khẩu(hoặc hợp đồng điện thoại cố định, hợp đồng điện thoại di
- động trả sau…)
- Hộ chiếu
- Thông tin sở hữu tên miền(sử dụng cho chứng thư SSL)

1.8.3.4.2 Qua trình xác thực việc gia hạn chứng thư



Sau khi nhận yêu cầu gia hạn chứng thư từ phía Thuê bao, các RA sẽ có trách nhiệm đối chiếu và xác thực thông tin từ phía thuê bao đã cung cấp với dữ liệu của chứng thư gốc được lưu giữ trong cơ sở dữ liệu chứng thư. Trong trường hợp khớp thông tin(thông tin được chấp nhận) yêu cầu gia hạn sẽ được chuyển về LCS xử lý. Ngược lại, nếu thông tin sai lệch yêu cầu gia hạn chứng thư của thuê bao bị hủy bỏ.

1.8.3.5 Thu hồi chứng thư số và thông báo các chứng thư số bị thu hồi

Thu hồi chứng thư số thực hiện theo các bước sau:

1.8.3.5.1 Nội dung xác thực đối với trường hợp thu hồi chứng thư số

Chỉ trong các tình huống được liệt kê dưới đây, chứng chỉ thuê bao dùng cuối sẽ bị LCS thu hồi(hoặc người đăng ký) và được công bố trên một CRL.

Một chứng thư của thuê bao sẽ bị thu hồi nếu rơi vào trong một trong số các tình huống sau:

- LCS, hay một thuê bao có lý do để tin rằng hoặc nghi ngờ lớn về sự tổn hại của khóa riêng người đăng ký.
- LCS hoặc thuê bao có lý do để tin rằng Thuê bao vi phạm nghĩa vụ, trách nhiệm, hoặc sự bảo đảm dưới các thỏa thuận thuê bao thích hợp.
- Hợp đồng thuê bao kết thúc.
- LCS hoặc một thuê bao có lý do để tin rằng Chứng thư số được ban hành không phù hợp với quy trình được yêu cầu bởi CPS.
- LCS hoặc thuê bao có lý do để tin rằng các tài liệu trong Đơn xin cấp chứng thư số sai.
- LCS hoặc thuê bao xác định được tài liệu đầu tiên để cấp chứng thư số không thỏa mãn cũng không khước từ.
- Trong trường hợp chứng thư số tổ chức mức 3, tên của tổ chức của thuê bao thay đổi.
- Thông tin trong Chứng thư, khác với thông tin thuê bao không thẩm tra, là không đúng hoặc có thay đổi.
- Việc tiếp tục sử dụng chứng thư số này gây nguy hại cho LCS.

Khi xem xét việc sử dụng chứng thư số có gây nguy hại cho LCS hay không. LCS xem xét giữa các yếu tố sau:

- Nguồn gốc và tên của các khiếu nại nhận được
- Xác nhận người khiếu nại
- Cưỡng chế theo pháp luật
- Trả lời cho việc sử dụng gây nguy hại cho người đăng ký

Khi xem xét việc sử dụng chứng thư số chữ ký mật mã là nguy hiểm cho LCS, LCS xem xét thêm các điều sau:

- Tên của mật mã được ký
- Hành vi của mật mã
- Phương pháp phân biệt mật mã
- Các nghi vấn khác về mật mã
- LCS có thể thu hồi Chứng thư số quản trị nếu thẩm quyền của người quản trị kết thúc.

1.8.3.5.2 Quy trình xác thực thu hồi chứng thư số

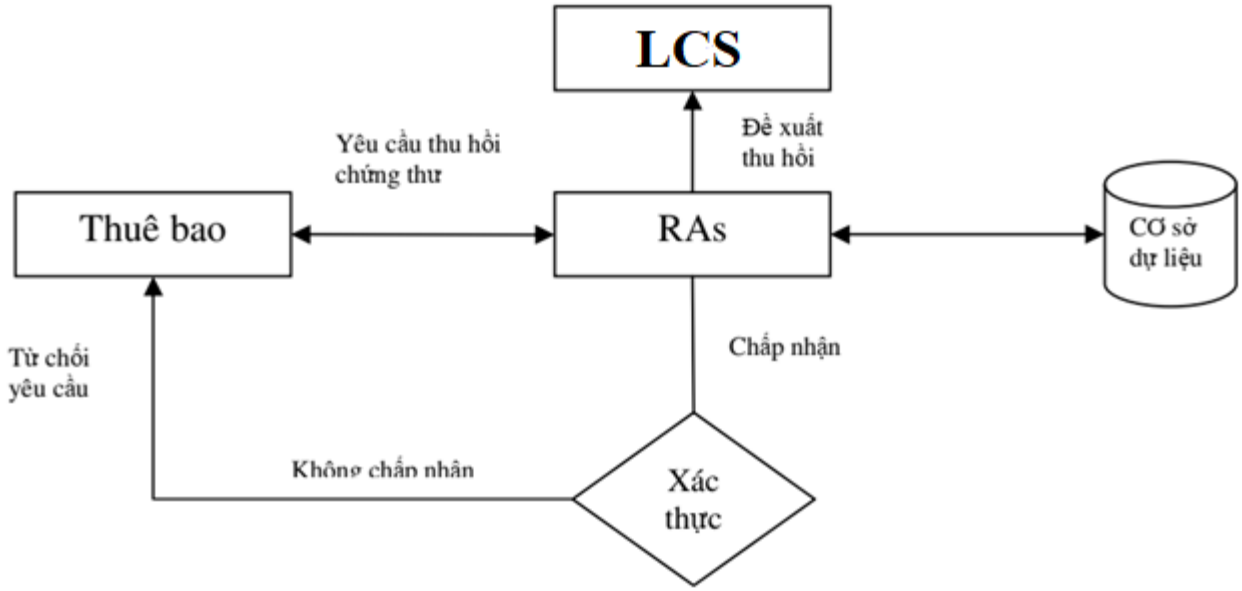
Nhận yêu cầu thu hồi

Kiểm tra nội tính đúng đắn của nội dung yêu cầu thu hồi

Nếu yêu cầu thu hồi đưa ra chưa hợp lý và phù hợp → hủy bỏ yêu cầu vào gửi thông báo cho người yêu cầu lý do không hợp lệ.

Nếu thông tin thu hồi đưa ra được xác thực là đúng đắn và hợp lý → RA có trách nhiệm gửi thông tin đã xác thực cho LCS-CA và yêu cầu LCS-CA tiến hành thu hồi chứng thư sớm nhất có thể.

Gửi yêu cầu thông báo thu hồi và lý do thu hồi tới thuê bao, RA phê chuẩn chứng thư đó.



1.8.3.6 Tạm dừng chứng thư số (không hỗ trợ)

LCS-CA không hỗ trợ tạm dừng chứng thư số

1.8.3.7 Khôi phục chứng thư số (không hỗ trợ)

LCS-CA không hỗ trợ khôi phục chứng thư số

1.8.3.8 Các mức độ đảm bảo tin cậy của chứng thư

Chứng thư có mức độ bảo đảm tin cậy thấp: không nên sử dụng với mục đích chứng thực hoặc hỗ trợ tính chống từ chối. Chữ ký số đảm bảo rằng thư điện tử đó bắt nguồn từ người gửi với một địa chỉ thư điện tử nhất định. Tuy nhiên, chứng thư này không hỗ trợ chứng

thực thuê bao. Ứng dụng mã hóa cho phép đối tác tin cậy sử dụng chứng thư của khách hàng để mã hóa các bản tin gửi tới khách hàng.

Chứng thư có mức độ bảo đảm tin cậy trung bình: thích hợp đảm bảo an ninh cho thư điện tử cá nhân, thư điện tử của một tổ chức hay giữa các tổ chức, thư điện tử thương mại, có yêu cầu mức bảo đảm trung bình.

1.8.3.9 Sử dụng chứng thư bất hợp pháp

Các chứng thư được sử dụng trong phạm vi phù hợp với quy định của pháp luật. Các chứng thư của LCS không được phép sử dụng như công cụ điều khiển trong các trường hợp nguy hiểm hoặc sử dụng cho các mục đích không an toàn ví dụ như hoạt động của các phương tiện hạt nhân, các hệ thống định vị và thông tin liên lạc máy bay, hệ thống điều khiển giao thông đường không, hay hệ thống điều khiển vũ khí gây tử vong hoặt sát thương con người hoặc phá hủy môi trường.

2 CÔNG BỐ VÀ LƯU TRỮ DANH BẠ CHỨNG THƯ SỐ

2.1 Hệ thống danh bạ

Công bố sẽ thực hiện tại website LCS-CA http://lcs-ca.vn và có phương án tốt nhất để thông báo thành công đến các bên liên quan đảm bảo yêu cầu về an toàn và bảo mật.

2.2 Công bố thông tin chứng thư

LCS-CA sẽ thực hiện công bố công khai và quản lý hệ thống danh bạ về chứng thư số của thuê bao ngay sau khi hoàn thành thủ tục cấp chứng thư số cho thuê bao.
Các thông tin cần được công bố bao gồm:

- CP/CPS trên toàn hệ thống
- CPS của từng CA
- Chứng thư của Trung tâm chứng thực điện tử quốc gia
- Chứng thư số của LCS-CA
- Danh sách chứng thư số bị thu hồi (CRL)
- Danh sách CA bị thu hồi (ARL)

Kho lưu trữ chứng thư của LCS sử dụng giao diện web, cho phép đối tác tin cậy thực hiện các yêu cầu truy vấn trực tuyến về thu hồi chứng thư hay truy vấn thông tin trạng thái các chứng thư. Các trường hợp khác phải có sự phê duyệt của LCS và phải dựa vào tài liệu trong CPS tương ứng. Trong hợp đồng với trung tâm dịch vụ, một trung tâm xử lý sẽ thực hiện việc lưu trữ cho trung tâm dịch vụ. LCS cung cấp cho đối tác tin cậy các thông tin chứng thư và cách thức kiểm tra trạng thái chứng thư, nếu có thể LCS sẽ cung cấp dịch vụ kiểm tra trạng thái chứng thư trực tuyến (OCSP). Trung tâm xử lý công khai danh sách các chứng thư đã được cấp phát. Ngoài ra, trung tâm xử lý còn cung cấp các danh sách chứng thư bị thu hồi (CRL – Certificate Revocation Lists) một cách rõ ràng, thuận tiện cho người tra cứu thông tin. Trung tâm xử lý đồng thời cung cấp dịch vụ OCSP cho các khách hàng sử dụng dịch vụ.
LCS sẽ liên tục phát hành phiên bản cập nhật của:

- Chính sách chứng thư (CP) của dịch vụ LCS-CA.
- Quy chế chứng thực (CPS) của dịch vụ LCS-CA.

- Các thỏa thuận với khách hàng.
- Các thỏa thuận với các relying party.

2.3 Chu kỳ phát hành thông tin chứng thư

Để đảm bảo tính an toàn cho hệ thống, bên cạnh việc công bố nhanh chóng chứng thư số đã cấp, cần phải kịp thời công bố những chứng thư số bị hủy, đặc biệt là khi khoá CA, RA bị sự cố (lộ, hỏng, mất token…) và nhanh chóng phục hồi để đáp ứng nhu cầu giao dịch của hệ thống.

- Chứng thư số cho người dùng sẽ được công bố ngay sau khi cấp.
- Danh sách chứng thư số bị hủy của người dùng được công bố ngay sau khi đã kiểm định thông tin yêu cầu hủy.
- Khi thấy có đủ dấu hiệu khóa RA bị sự cố, cần phải nhanh chóng thông báo lên CA để CA kịp thời ngừng các giao dịch liên quan tới RA đó và cấp lại chứng thư số cho RA.
- Khi thấy có đủ dấu hiệu khóa CA mức root bị lộ, trong vòng 15 phút cần thông báo được cho toàn bộ các CA các mức (nếu có), để ngừng mọi giao dịch trong hệ thống. Phải tạo chứng thư số CA mới, cập nhật chứng thư số này trong toàn bộ hệ thống, thông báo cho người dùng để họ kịp thời cập nhật lại chứng thư số Root mới. Dùng chứng thư số này bắt đầu lại các hoạt động cấp chứng thư số.
- LCS đưa ra danh sách chứng thư bị thu hồi và đưa ra dịch vụ kiểm tra trạng thái thông chứng thư qua kho lưu trữ của dịch vụ LCS-CA. Danh sách thu hồi chứng thư sẽ được cập nhật tối thiểu một lần trong ngày. Nếu một chứng thư nằm trong CRLs, khi hết hạn, chứng thư sẽ được xóa bỏ trong CRLs trong những lần cập nhật tiếp theo.
- Trong một số điều kiện, khi băng thông hạn chế, số lượng truy cập nhiều, người dùng có thể cache lại CRL. Tuy nhiên phải áp dụng giải thuật update phù hợp, tùy vào từng ứng dụng và điều kiện cụ thể, đảm bảo cập nhật kịp thời, không tốn tài nguyên băng thông, không tốn nhiều tài nguyên bộ nhớ nhưng vẫn đảm bảo được tính an toàn, chính xác.

2.4 Lưu trữ

Trung tâm xử lý của dịch vụ LCS-CA có tránh nhiệm duy trì việc phát hành, lưu trữ trực tuyến. Trung tâm xử lý này có trách nhiệm công bố chứng thư và các thông tin về chứng thư trong kho lưu trữ của trung tâm dịch vụ (Service Centers) dựa trên các đơn xin cấp chứng thư đã được trung tâm dịch vụ chấp thuận.

Thông tin về chứng thư số và danh sách chứng thư số bị thu hồi được lưu trữ trên các máy chủ Directory theo chuẩn LDAP X509 v3.

2.5 Quyền truy cập kho lưu trữ chứng thư

- CP: chỉ root CA mới được quyền thay đổi, cập nhật.
- CPS: chỉ SubCA (nếu có) mới được quyền thay đổi, cập nhật các CPS của riêng nó.
- Các thông tin được quy hoạch, thông tin cho người dùng phải được đặt trên các Directory riêng, CRL được quy hoạch theo cấu trúc của LCS để giảm kích thước CRL phải tải về.
- Đối với thuê bao, LCS không giới hạn truy cập tới CPS, CPS, chứng thư, thông tin chứng thư, hay CRLs. LCS 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. LCS triển khai các kiểm soát nhằm ngăn chặn việc truy cập bất hợp pháp vào kho lưu trữ nhằm thêm, xóa hay sửa đổi các mục trong kho lưu trữ.

3 ĐỊNH DANH VÀ THẨM ĐỊNH XÁC THỰC THÔNG TIN THUÊ BAO

3.1 Đặt tên

Tên xuất hiện trong chứng thư được cấp phát phải được LCS xác thực.

3.1.1 Kiểu tên

- Tên trong trường Subject name của chứng thư thuê bao cuối được đặt theo chuẩn X.501. Tên của chứng thư thuê bao cuối chứa thành phần tên chung (CN=). Thành phần tên chung có thể là tên miền, địa chỉ thư điện tử của tổ chức, tên hợp pháp của tổ chức hoặc tên đại diện hợp pháp của tổ chức. Thành phần tên chung của chứng thư các nhân đại diện cho cá nhân đó.
- Chứng thư chứa tên với nghĩa dễ hiểu cho phép nhận dạng được cá nhân hay tổ chức sở hữu chứng thư đó.
- Các chứng thư số do hệ thống LCS-CA cấp phát không được phép sử dụng bút danh (đặt theo tên của thuê bao hoặc tổ chức khác).
- Khi có yêu cầu của pháp luật bảo vệ sự nhận dạng của thuê bao, một chứng thư được cấp phát chỉ ra rằng danh tính này đã được xác minh đúng và được bảo vệ.
- Mỗi yêu cầu nặc danh trong chứng thư sẽ được LCS xem xét và đánh giá dựa theo các điều kiện hợp lý.

3.1.2 Tính duy nhất của tên thuê bao

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

3.1.3 Nhận dạng, xác thực và vai trò của thương hiệu

Người xin cấp chứng thư tuyệt đối không được sửa tên trong những đơn xin cấp chứng thư của người khác đã được bảo hộ quyền sở hữu. Tuy nhiên, LCS không xác định liệu một người xin cấp chứng thư có quyền sở hữu đối với tên xuất hiện trong đơn xin cấp chứng thư hay phân xử bất kỳ một cuộc tranh chấp nào liên quan đến quyền sở hữu một tên miền, tên thương mại, nhãn hiệu, hoặc nhãn hiệu dịch vụ. LCS được phép tạm dừng hoặc từ chối đơn xin cấp chứng thư nếu xảy ra tranh chấp.

3.2 Xác định danh tính thuê bao

3.2.1 Xác thực danh tính cá nhân

Chứng thực của các chứng thư số dựa trên sự có mặt của người xin cấp chứng thư trước khi RA hay một nhà chức trách có thể kiểm định được tính hợp pháp. RA kiểm tra nhận dạng của người xin cấp chứng thư dựa trên thủ tục để nhận dạng của chính phủ, như hộ chiếu, hoặc giấy phép lái xe...

Trên thực tế, để đảm bảo tính bảo mật và tránh các trường hợp giả mạo, thuê bao cần xuất trình các giấy tờ sau đây khi xin cấp chứng thư số từ LCS-CA:

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

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

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

3.2.2 Xác thực danh tính tổ chức, doanh nghiệp

Bất kỳ chứng thư nào cũng bao gồm tên của tổ chức, nhân dạng của tổ chức và thông tin được người xin cấp chứng thư cung cấp. Các thông tin này được xác minh theo những thủ tục được ghi trong tài liệu của dịch vụ LCS-CA.

Tối thiểu, dịch vụ LCS-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 kiểm lỗi của đối tác thứ ba, hoặc tài liệu xác nhận sự tồn tại của tổ chức

được cấp bởi cơ quan hợp pháp của chính phủ hay nhà chức trách. Ví dụ giấy phép đăng ký kinh doanh.

- Xác nhận bằng điện thoại, thư tín… các thông tin của tổ chức mà người xin cấp 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

3.2.3 Chứng minh quyền sở hữu khóa bí mật

Đối tượng sử dụng chứng thư phải chứng minh rằng họ sở hữu hợp pháp khóa bí mật tương ứng với khóa công khai được liệt kê trong chứng thư.

3.2.4 Những thông tin của thuê bao không được xác thực

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

- Đơn vị nhỏ thuộc tổ chức (Organization Unit)
- Bất kì một thông tin nào được coi là không cần xác thực trong chứng thư.

3.2.5 Các tiêu chí hoạt động

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

3.3 Nhận diện và xác thực đối với yêu cầu cấp lại khóa (Re-key)

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 RA yêu cầu thuê bao phải xin cấp một cặp khóa mới để thay thế cặp khóa đã hết hạn (gọi là “Rekey”), tuy nhiên trong một trường hợp nào đó (ví dụ như với các chứng thư cho máy chủ web) có thể yêu cầu một chứng thư mới thay thế cho một cặp khóa đã tồn tại (gọi là “Renewal”).

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

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

Thông thường, khi thuê bao có yêu cầu tiếp tục sử dụng chứng thư số thì chứng thư mới sẽ được tự động cấp phát. Sau khi cấp lại khoá, CA hoặc RA của dịch vụ LCS-CA sẽ xác nhận lại việc định danh của thuê bao sao cho phù hợp với các yêu cầu xác thực và định danh của đơn xin cấp chứng thư ban đầu.

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

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

- Chứng thư có thể gây hại cho các nhà cung cấp dịch vụ LCS.
- 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 đã được sử dụng vào các mục đích trái pháp luật…

3.4 Nhận diện và xác thực với các yêu cầu thu hồi chứng thư.

Trước thời điểm thu hồi một chứng thư, LCS phải kiểm tra và xác thực đúng nếu có yêu cầu sự huỷ bỏ chứng thư từ thuê bao của dịch vụ LCS-CA. Các thủ tục được dùng để nhận biết một thuê bao đã hết hạn gồm:

- Nhận các thông báo từ thuê bao về yêu cầu thu hồi, bao gồm cả việc xác thực chữ ký số có liên quan tới chứng thư bị thu hồi.
- 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 khách 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.

Quản trị CA/RA của dịch vụ LCS-CA được phép yêu cầu thu hồi chứng thư thuê bao trong miền con của RA, LCS xác thực việc nhận dạng của người quản trị thông qua điều khiển truy nhập sử dụng SSL và khách hàng xác nhận trước khi cho phép họ thực thi chức năng thu hồi chứng thư hoặc các quy trình khách đã được LCS phê chuẩn.

RA của dịch vụ LCS-CA sử dụng phần mềm quản lý tự động để xác minh yêu cầu thu hồi đối với dịch vụ LCS-CA. Các yêu cầu sẽ được xác thực thông qua việc chữ ký số được ký bằng khoá bí mật phần cứng tự động quản lý của RA.

4 CÁC THỦ TỤC, QUY TRÌNH LIÊN QUAN CHỨNG THƯ SỐ

4.1 Thủ tục xin cấp chứng thư số

4.1.1 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 bảo mật giao dịch.
- Đại diện của các tổ chức, doanh nghiệp, cá nhân.
- Các thành phần của CA hoặc RA trong hệ thống PKI.

4.1.2 Hồ sơ xin cấp mới chứng thư số.

- Đối với doanh nghiệp
    - Đơn xin cấp Chứng thư số LCS-CA
    - Sao y bản chính Giấy phép Đăng ký kinh doanh (có xác nhận của Doanh nghiệp)
    - Sao y bản chính Giấy đăng ký thuế (có xác nhận của Doanh nghiệp)
    - Photo CMND hoặc Hộ chiếu của người đại diện theo pháp lý
- Đối với cá nhân
    - Bảo sao có công chứng CMND hoặc hộ chiếu

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

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

- Hoàn thành bảng kê khai và cung cấp các thông tin đúng, chính xác.
- Tự tạo khoá hoặc yêu cầu tạo cặp khoá.
- Cung cấp khoá công khai đến RA, đến trung tâm xử lý trong trường hợp thuê bao tự tạo cặp khóa.
- Chứng minh sự tương thích giữa khoá bí mật và khoá công khai cho trung tâm xử lý.

4.2 Xứ lý đơn xin cấp chứng thư số

4.2.1 Chức năng nhận biết và xác thực

Một RA sẽ nhận biết và chứng thực các thông tin khách hàng theo mục 3.2

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

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

- Nhận biết và xác thực các thông tin về khách hàng theo mục 3.2.
- Phí dịch vụ đã thanh toán.

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

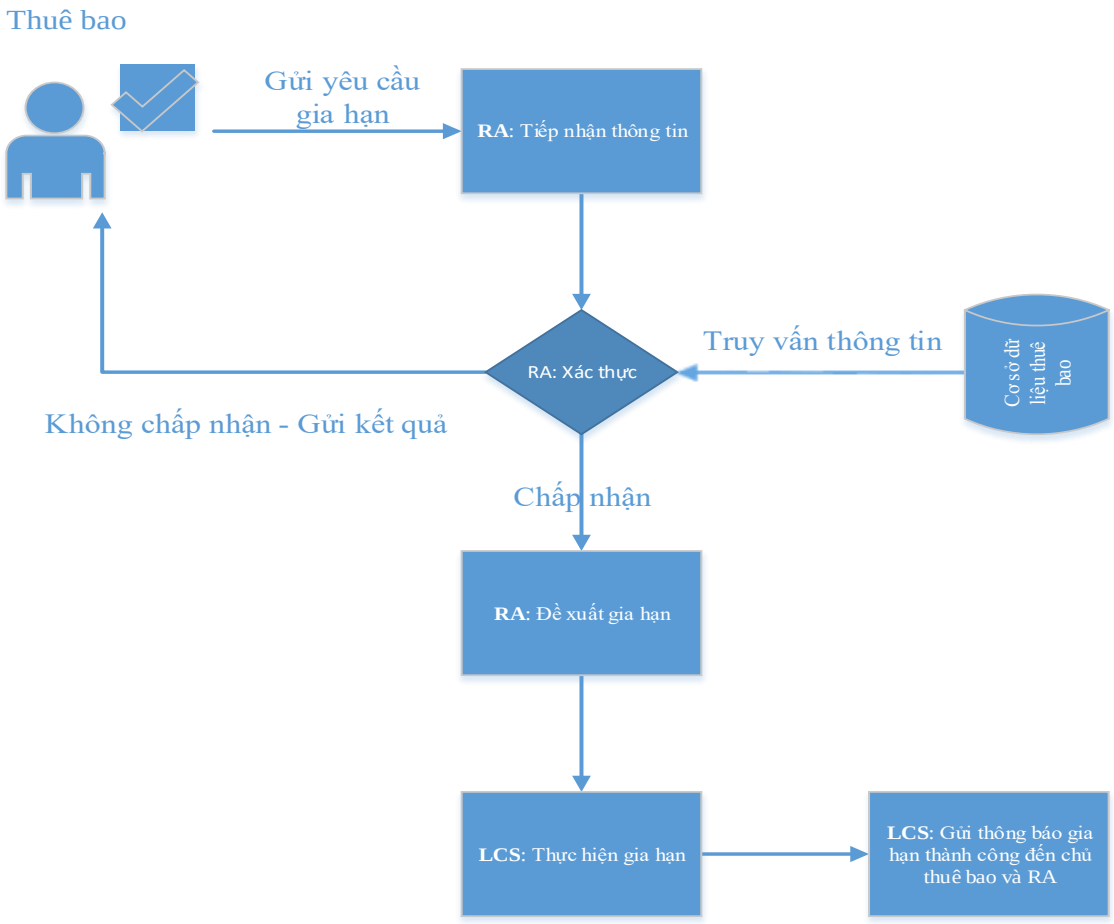
- Nhận biết và xác thực các thông tin về thuê bao không thành công.
- Thuê bao không cung cấp tài liệu hỗ trợ theo yêu cầu.
- Thuê bao không trả lời yêu cầu trong thời gian quy định.
- Phí dịch vụ chưa thanh toán.
- RA có lý do tin rằng việc cung cấp chứng thư cho thuê bao có thể gây bất lợi cho LCS.

4.2.3 Thời gian xử lý các đơn xin cấp chứng thư

RA có trách nhiệm xử lý các đơn xin cấp, gia hạn chứng thư trong khoảng thời gian phù hợp. Không quy định thời gian hoàn thành quá trình xử lý một đơn xin cấp, gia hạn chứng thư trừ khi được đưa ra trong hợp đồng với thuê bao, trong CPS hoặc thoả thuận giữa các bên của dịch vụ LCS-CA. Thông thường, nếu không có vướng mắc, hệ thống cung cấp dịch vụ LCS-CA có thể khởi tạo một chứng thư mới tối đa trong 05 ngày làm việc, thời gian xử lý gia hạn xong cho thuê bao đã hoàn tất cả thủ tục trong khoảng 1 buổi làm việc.

4.3 Thủ tục xin gia hạn chứng thư số

Quy trình gia hạn chứng thư số:



4.3.1 Các đối tượng có thể xin gia hạn chứng thư số

Những người sau đây có thể đệ trình đơn gia hạn chứng thư số:

- Các thuê bao có nhu cầu xin chứng thư cho mục đích bảo mật giao dịch.
- Đại diện của các tổ chức, doanh nghiệp, cá nhân.
- Các thành phần của CA hoặc RA trong hệ thống PKI.

4.3.2 Hồ sơ xin gia hạn chứng thư số.

- Đối với doanh nghiệp
    - Đơn xin gia hạn Chứng thư số LCS-CA
    - Sao y bản chính Giấy phép Đăng ký kinh doanh (có xác nhận của Doanh nghiệp)
    - Sao y bản chính Giấy đăng ký thuế (có xác nhận của Doanh nghiệp)

- Photo CMND hoặc Hộ chiếu của người đại diện theo pháp lý

- Đối với cá nhân
  - Bảo sao có công chứng CMND hoặc hộ chiếu

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

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

- Hoàn thành bảng kê khai và cung cấp các thông tin đúng, chính xác.
- Tự tạo khoá hoặc yêu cầu tạo cặp khoá.
- Cung cấp khoá công khai đến RA, đến trung tâm xử lý trong trường hợp thuê bao tự tạo cặp khóa.
- Chứng minh sự tương thích giữa khoá bí mật và khoá công khai cho trung tâm xử lý.

4.4 Xứ lý đơn xin gia hạn chứng thư

4.4.1 Chức năng nhận biết và xác thực

Một RA sẽ nhận biết và chứng thực các thông tin khách hàng theo mục 3.2

4.4.2 Phê duyệt hoặc từ chối các đơn xin gia hạn chứng thư

RA sẽ phê chuẩn đơn xin gia hạn chứng thư khi tuân theo các tiêu chuẩn sau đây:

- Nhận biết và xác thực các thông tin về khách hàng theo mục 3.2.
- Phí dịch vụ đã thanh toán.

RA sẽ từ chối đơn xin gia hạn chứng thư theo tiêu chí sau đây:

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

4.4.3 Thời gian xử lý các đơn xin gia hạn chứng thư

RA có trách nhiệm xử lý các đơn xin cấp, gia hạn chứng thư trong khoảng thời gian phù hợp. Không quy định thời gian hoàn thành quá trình xử lý một đơn xin cấp, gia hạn chứng thư trừ

khi được đưa ra trong hợp đồng với thuê bao, trong CPS hoặc thoả thuận giữa các bên của dịch vụ LCS-CA. Thông thường, nếu không có vướng mắc, hệ thống cung cấp dịch vụ LCS-CA có thể khởi tạo một chứng thư mới tối đa trong 05 ngày làm việc, thời gian xử lý gia hạn xong cho thuê bao đã hoàn tất cả thủ tục trong khoảng 1 buổi làm việc.

4.5 Công bố phát hành chứng thư

4.5.1 Hoạt động LCS trong suốt quá trình phát hành chứng thư

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

Sau khi nhận được yêu cầu xin cấp chứng thư số từ phía RA, CA tiến hành tạo chứng thư số dựa trên các thông tin có trong yêu cầu này. Sau đó CA dùng khóa cá nhân ký lên chứng thư số đảm bảo tính toàn vẹn nội dung và khẳng định sự tin cậy của CA đối với chứng thư số vừa tạo.

Chứng thư số sau khi phát hành sẽ chứng thực khóa công khai gửi kèm theo yêu cầu xin cấp chứng thư số là của thuê bao đã gửi yêu cầu lên RA. Nó được công bố rộng rãi cho bất kỳ ai có nhu cầu trao đổi thông tin với chủ thể của chứng thư số đó.

4.5.2 Thông báo của LCS đến thuê bao về việc cấp chứng thư

LCS cấp phát các chứng thư trực tiếp tới thuê bao hoặc thông qua RA. LCS thông báo cho thuê bao rằng chứng thư của họ đã được tạo đồng thời cung cấp cho thuê bao quyền truy cập tới chứng thư đó để kiểm tra tính sẵn sàng của chứng thư.

Nguyên tắc cơ bản của hệ thống LCS-CA là công bố rộng rãi chứng thư số sao cho mọi người đều truy cập được. LCS-CA sử dụng một số phương pháp công bố chứng thư số như sau:

- Dịch vụ thư mục (LDAP): Phương pháp này dành cho các chứng thư số theo chuẩn X.509. Dịch vụ thư mục dành cho PKI phổ biến là X.500/LDAP theo chuẩn của IETF.
- Trang web hoặc máy chủ FTP: Các chứng thư số được đưa lên trang web để mọi người có thể truy cập thông qua giao thức HTTP, FTP.

- Website http://lcs-ca.vn

4.6 Chấp nhận chứng thư

4.6.1 Điều kiện chứng minh việc chấp thuận chứng thư

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

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

4.6.2 Công khai chứng thư của LCS

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

4.6.3 Thông báo sự phát hành chứng thư đến các đối tượng khác

LCS có trách nhiệm gửi thông báo cho RA về sự phát hành chứng thư.

4.7 Cách sử dụng cặp khoá và chứng thư

4.7.1 Cách sử dụng chứng thư và khoá bí mật của thuê bao

Việc sử dụng khoá bí mật tương ứng với khoá công khai trong chứng thư chỉ được cho phép khi thuê bao đồng ý với bản thoả thuận thuê bao và thuê bao chấp nhận chứng thư. Chứng thư sẽ được sử dụng hợp pháp dựa theo bản thoả thuận thuê bao với các điều khoản có trong CP và CPS của nhà cung cấp chứng thư. Chứng thư sử dụng phải khớp với đuôi mở rộng của trường KeyUsage có trong chứng thư (ví dụ: nếu chữ ký số không có hiệu lực thì chứng thư không được sử dụng để ký).

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

4.7.2 Cách sử dụng chứng thư và khoá công khai của các đối tác tin cậy

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

Tính tin cậy của chứng thư phải phù hợp với từng hoàn cảnh cụ thể. Nếu hoàn cảnh chỉ ra rằng phải cần thêm sự đảm bảo, thì đối tác tin cậy phải đạt được sự bảo đảm cần thiết. Trước khi tin cậy, các đối tác tin cậy sẽ đánh giá một cách một cách độc lập:

- Sử dụng chứng thư một cách phù 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, LCS, 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 (ví dụ: chữ ký số mà không có hiệu lực thì chứng thư không được tin cậy cho tính xác thực chữ ký thuê bao)
- Trạng thái của chứng thư và tất cả các CA trong mắt xích chịu trách nhiệm phát hành chứng thư. 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 hoặc phần cứng tương ứng thực hiện việc xác thực chữ ký số hoặc các thao tác hoá khác họ mong muốn như một điều kiện để tin cậy. Các thao tác này bao gồm việc định danh một mắt xích chứng thư và xác thực các chữ ký số trên tất cả các chứng thư trong chuỗi chứng thư.

4.8 Sửa đổi cập nhật chứng thư

4.8.1 Các trường hợp sửa đổi chứng thư

Việc sửa đổi chứng thư ưu tiên cho những ứng dụng cấp phát chứng thư mới để thay đổi các thông tin trong chứng thư đang tồn tại.

Việc sửa đổi chứng thư tuân theo mục 4.1

4.8.2 Đối tượng yêu cầu sửa đổi chứng thư

Xem trong mục 4.1.1

4.8.3 Quá trình xử lý yêu cầu sửa đổi chứng thư

RA sẽ nhận biết và xác thực các thông tin từ thuê bao theo mục 3.2

Thông báo phát hành chứng thư mới tới thuê bao

Xem mục 4.5.2

4.8.4 Điều kiện chấp nhận sửa đổi thuê bao

Xem mục 4.6.1

4.8.5 Việc phát hành chứng thư đã được sửa đổi từ LCS

Xem mục 4.6.2

4.8.6 Thông báo phát hành chứng thư của LCS tới các đối tượng khác

Xem mục 4.6.3

4.9 Thu hồi chứng thư số

4.9.1 Các trường hợp thu hồi

Chỉ trong các tình huống được liệt kê dưới đây, chứng thư thuê bao dùng cuối sẽ bị LCS thu hồi và được công bố trên một CRL. Dựa vào yêu cầu không sử dụng của thuê bao với lý do không nằm trong các lý do liệt kê bên dưới. LCS sẽ đánh dấu chứng thư là không hoạt động trong cơ sở dữ liệu nhưng sẽ không công bố chứng thư trên một CRL.

Một chứng thư sẽ bị thu hồi nếu:

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

Khi xem xét việc sử dụng chứng thư có hại cho LCS hay không, các RA xem xét các yếu tố sau:

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

Ngoài ra, khi xem xét việc sử dụng chứng thư Code Signing Certificate là nguy hiểm cho LCS, các RA xem xét thêm các điều sau:

- Tên mã nguồn được ký
- Cách xử lý mã nguồn
- Phương thức phân phối mã nguồn
- Vấn đề để lộ mã nguồn
- Bất kì luận điểm khác về mã nguồn

LCS có thể thu hồi chứng tư quản trị nếu thẩm quyền của người quản trị kết thúc.

Thoả thuận với thuê bao yêu cầu thuê bao thông báo cho LCS ngay lập tức về những thông tin và nghi ngờ về việc lộ khoá bí mật.

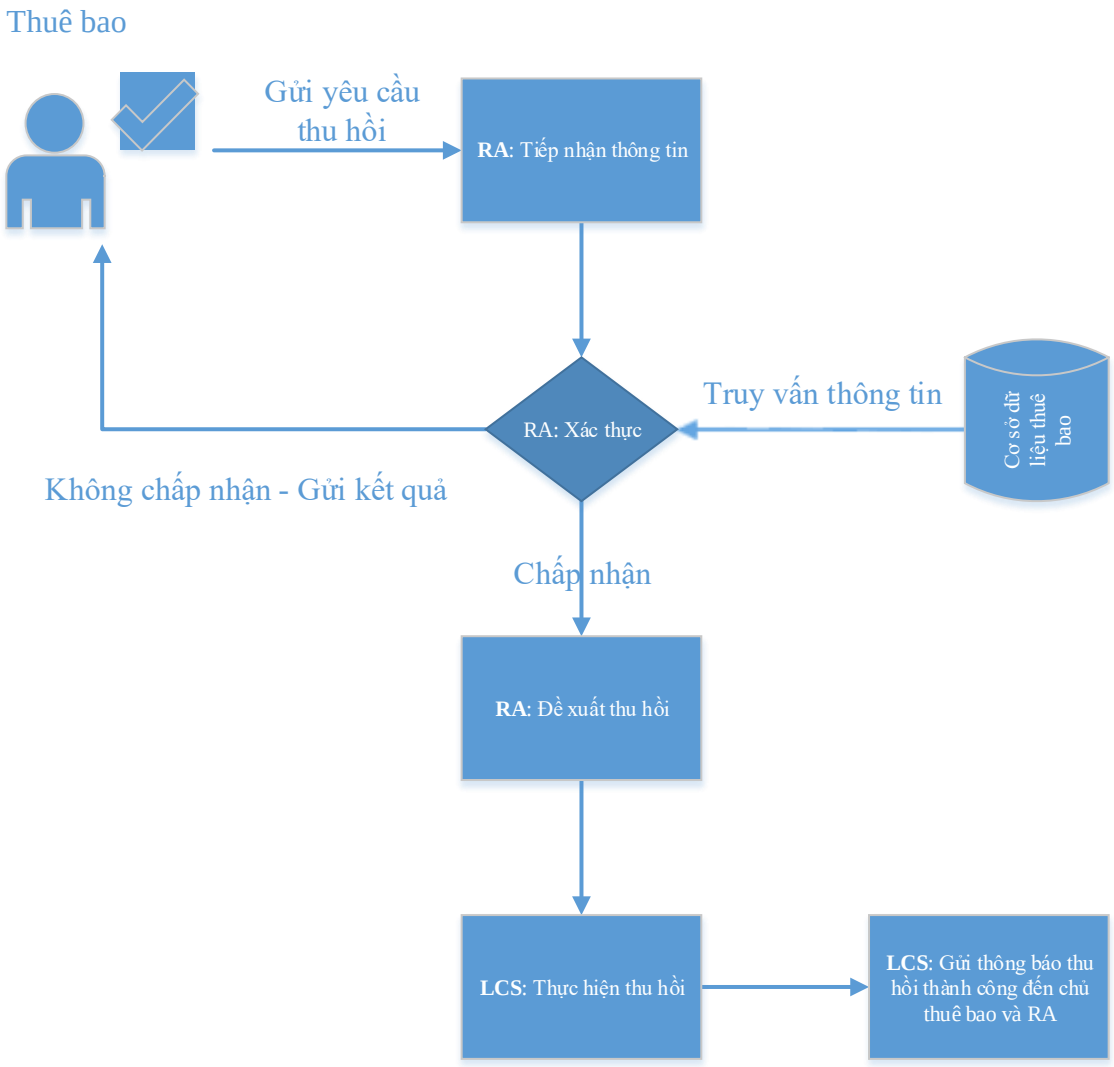
Thoả thuận yêu cầu thuê bao ngay lập tức thông báo với trung tâm xử lý khi có nghi ngờ về việc lộ khoá bí mật.

4.9.2 Đối tượng có thể yêu cầu thu hồi

Những thuê bao cá nhân có thể yêu cầu thu hồi chứng thư cá nhân của chính họ. Trong trường hợp chứng thư của tổ chức, một đại diện được uỷ quyền hợp pháp của tổ chức được quyền yêu cầu thu hồi chứng thư đã ban hành cho tổ chức. Đại diện được uỷ quyền hợp pháp của LCS hoặc RA sẽ được quyền yêu cầu thu hồi chứng thư quản trị của RA. Đơn vị phê chuẩn đơn xin cấp chứng thư của người đăng ký cũng sẽ được quyền thu hồi hoặc yêu cầu thu hồi chứng nhận của thuê bao.

4.9.3 Thủ tục yêu cầu thu hồi chứng thư

Quy trình thu hồi chứng thư số:



Theo trình tự thu hồi chứng thư, CA xác nhận thuê bao yêu cầu thu hồi chứng thư là cá nhân hay tổ chức được chấp nhận đơn xin cấp chứng thư. Trình tự xác nhận yêu cầu thu hồi của thuê bao bao gồm:

- Thuê bao thông báo nội dung yêu cầu chứng thư, chữ ký và chữ ký số liên quan với chứng thư thu hồi
- Thông báo cho các 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.

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

4.9.4 Thời gian cho một yêu cầu thu hồi chứng thư

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

4.9.5 Chu kỳ cấp phát CRL

Các CRL đối với chứng thư thuê bao được đưa ra ít nhất mỗi lần một ngày.
Nếu một chứng thư hết hạn được liệt kê trong CRL, nó có thể bị xoá khỏi CRLs trong lần phát hành CRL tiếp theo. Đối tác tin cậy có thể tải về danh sách chứng thư số bị thu hồi CRL tự động từ LCS. LCS cung cấp miễn phí phát hành CRL cho đối tác.

4.9.6 Thời gian trễ tối đa cho các CRL

Các CRL được gửi đến nơi lưu trữ trong một khoảng thời gian thương mại hợp lý sau khi phát hành. Điều này thường được cấp phát tự động.

4.9.7 Dịch vụ kiểm tra trạng thái chứng thư số trực tuyến OCSP

Thông tin trạng thái chứng thư và thông tin thu hồi chứng thư trực tuyến được công bố trên kho lưu trữ của Website và có thể truy cập qua OCSP. Trung tâm xử lý sẽ cho phép đối tác tin cậy truy vấn trực tuyến các thông tin thu về thu hồi và trạng thái chứng thư. Trong hợp đồng với trung tâm dịch vụ. LCS cung cấp cho đối tác tin cậy các thông tin chứng thư và cách thức kiểm tra trạng thái chứng thư, nếu có thể LCS sẽ cung cấp dịch vụ kiểm tra trạng thái chứng thư trực tuyến (OCSP)

Một đối tác tin cậy phải kiểm tra tình trạng của một chứng thư mà đối tượng đó mong muốn tin cậy. Nếu đối tác tin cậy không kiểm tra bằng cách tham khảo nhiều CRL liên quan gần đây nhất, thì các đối tác tin cậy sẽ kiểm tra trạng thái chứng thư bằng cách tham khảo kho lưu trữ thích hợp hay bằng việc yêu cầu sử dụng OCSP phù hợp.
Tùy theo trường hợp và loại hợp đồng cụ thể, LCS sẽ thu phí dịch vụ kiểm tra trạng thái chứng thư số trực tuyến OCSP để đảm bảo duy trì băng thông và các tài nguyên khác của LCS.

4.9.8 Những yêu cầu đặc biệt liên quan đến vấn đề bị lộ khoá

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

4.10 Tạm dừng chứng thư số (không hỗ trợ)

LCS-CA không hỗ trợ tạm dừng sử dụng chứng thư số

4.11 Khôi phục chứng thư số (không hỗ trợ)

LCS-CA không hỗ trợ khôi phục chứng thư số

4.12 Dịch vụ kiểm tra trạng thái chứng thư số

4.12.1 Dịch vụ hỗ trợ

Trạng thái của chứng thư công cộng luôn được báo cáo sẵn sàng qua CRL tại website dịch vụ LCS-CA, thư mục LDAP và qua phản hồi OCSP.
Dịch vụ cung cấp trạng thái hoạt động của chứng thư luôn sẵn sàng trực 24/7 (24giờ/ngày, 7ngày/tuần).

4.12.2 Các đặc tính tuỳ chọn

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

4.13 Kết thúc hợp đồng

Một thuê bao có thể kết thúc đăng ký sử dụng dịch vụ chứng thư của LCS khi:

- Để chứng thư hết hạn mà không làm mới hay gia hạn chứng thư đó .
- Thu hồi chứng thư trước khi chứng thư hết hạn mà không thay thế bằng một chứng thư khác.

4.14 Cam kết và nghĩa vụ của thuê.

4.14.1 Cam kết và nghĩa vụ của thuê bao khi đăng ký chứng thư số

- Phải chắc chắn rằng bất kỳ thông tin nào được trình lên CA (RA) khi cấp, cập nhật hay yêu cầu thu hồi chứng thư số phải đầy đủ và chính xác
- Những khách hàng cá nhân hay doanh nghiệp sử dụng dịch vụ Quản lý khóa PKI có thể lưu trữ các bản sao của khoá bí mật cho thuê bao có đơn xin cấp chứng thư đã được chấp nhận.
- Khi đăng ký sử dụng dịch vụ chứng thư số, thuê bao cần chỉ rõ có sử dụng dịch vụ lưu trữ khóa cá nhân tại LCS-CA hay không. Việc lưu trữ khóa cá nhân trên máy chủ LCS đảm bảo rằng nếu thuê bao mất khóa bí mật thì có thể phục hồi lại các tài liệu mà đối tác đã mã hóa bằng cách sử dụng khóa công khai của thuê bao. Khóa bí mật được lưu trữ với công nghệ mã hóa tiên tiến trên hệ thống máy chủ được bảo mật kỹ lưỡng của hệ thống LCS-CA
- Tuy nhiên, LCS cam kết không lưu trữ khóa bí mật của thuê bao nếu không có yêu cầu.
- Bảo vệ khóa bí mật và các thiết bị khóa (nếu có) và tuân thủ tất các các yêu cầu nhằm tránh bị mất, bị lộ, thay đổi hay bị sửa dụng bất hợp phát chứng thư số của thuê bao đó.

4.14.2 Lưu trữ khoá, chính sách phục hồi khoá riêng và cách thức thực hiện.

Khách hàng doanh nghiệp sử dụng dịch vụ quản lý hạ tầng khoá công khai PKI (hay một dịch vụ tương đương được phê chuẩn bởi LCS) được phép sao lưu khóa bí mật của thuê bao cuối. Khóa bí mật sẽ được lưu giữ dưới dạng mã hoá sử dụng phần mềm quản lý công khai. Ngoại trừ khách hàng doanh nghiệp đang sử dụng dịch vụ quản lý khoá công khai (hay dịch vụ tương đương được phê chuẩn bởi LCS), khoá bí mật của CA hoặc thuê bao cuối sẽ không được lưu trữ dự phòng.

Khoá bí mật của thuê bao cuối sẽ chỉ được phục hồi trong các trường hợp được cho phép bởi hướng dẫn dưới đây:

- Khách hàng doanh nghiệp sử dụng chương trình quản lý khóa công khai sẽ kiểm tra lại tính xác thực của các khách hàng để đảm bảo những yêu cầu về khoá bí mật là của chính khách hàng, không phải là giả mạo.
- Khách hàng doanh nghiệp sẽ phục hồi lại khoá bí mật của khách hàng với mục đích hợp pháp mà không cần sự cho phép của khách hàng, chẳng hạn như để tuân theo pháp luật hoặc phục vụ mục đích quản trị hay tìm chứng nhận, không vì mục đích bất hợp pháp, lừa đảo hay mục đích xấu nào khác. Khách hàng doanh nghiệp sẽ có các điều chỉnh về tổ chức để ngăn chặn người quản trị dịch vụ quản lý khoá và những cá nhân khác truy cập bất hợp pháp tới các khoá bí mật riêng.

Khách hàng doanh nghiệp sử dụng dịch vụ quản lý khoá (KMS) được khuyến cáo:

- Thông báo cho khách hàng biết rằng khoá bí mật của họ đã được lưu giữ.
- Bảo vệ khoá bí mật của khách hàng đã được lưu giữ không bị lộ.
- Gữi bí mật các thông tin bao gồm: khoá của người quản trị được sử dụng để phục hồi khoá bí mật đã lưu trữ của khách hàng
- Ban hành các khoá đã sao lưu chỉ cho các yêu cầu đã được xác thực và có thẩm quyền hợp lý.
- Thu hồi các cặp khoá của khách hàng trước khi phục hồi các khoá đã mã hoá.
- Không cần thiết phải trao đổi thông tin liên quan đến việc phục hồi khoá trừ phi chính khách hàng yêu cầu khôi phục khoá.
- Không để lộ hoặc cho phép để lộ các khoá đã sao lưu hay các thông tin liên quan đến khóa đã sao lưu với bất cứ bên thứ 3 nào trừ khi có yêu cầu bởi luật pháp, chính phủ hay sự điều chỉnh, theo chính sách của công ty hay theo yêu cầu có thẩm quyền từ toà án.

5 KIỂM SOÁT BẢO MẬT HỆ THỐNG LCS-CA

5.1 Tạo cặp khoá và cài đặt

5.1.1 Tạo cặp khoá

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

- Đối với khóa của nhà cung cấp dịch vụ (LCS-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 LCS-CA hoàn toàn tương thích với những nhà cung cấp HSM hàng đầu thế giới hiện tại như AEP, Luna SA, nCipher, Thales…
- Đối với khóa của thuê bao, LCS-CA có thể cung cấp phần mềm sinh khóa hoặc thuê bao có thể cung cấp cặp khóa được sinh ra từ trước. Đương nhiên cặp khóa này phải được sinh theo thuật toán mã hóa RSA, phù hợp với các tiêu chuẩn bảo mật mã hóa về tính duy nhất, độ mật được nêu ra trong thông tư 06/2015/TT-BTTTT

5.1.2 Chuyển giao khoá bí mật cho thuê bao

Thuê bao có thể tự tạo khoá bí mật cho mình. Trong trường hợp LCS-CA tạo cặp khóa cho thuê bao, khóa bí mật được lưu trữ dưới định dạng PKCS # 12 hoặc các phương thức chuyển giao tương đương (Ví dụ mã hoá) để ngăn chặn sự mất mát, bị tiết lộ, sửa đổi và sử dụng bất hợp pháp khoá bí mật. Nếu cặp khoá được tạo ra trên thẻ cứng, việc phân phối thẻ sẽ áp dụng những chính sách thương mại hợp lý để cung cấp bảo mật phần cứng của thẻ nhằm ngăn chặn sự mất mát, bị tiết lộ, sửa đổi và sử dụng bất hợp pháp khoá bí mật.

5.1.3 Chuyển giao khoá công khai tới tổ chức ban hành chứng thư

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

5.1.4 Chuyển giao khoá công khai của CA tới các đối tác tin cậy

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

5.1.5 Kích thước khoá

Các cặp khoá cần có chiều dài thích hợp để ngăn việc lộ khoá bí mật trong thời gian sử dụng cặp khóa. Chuẩn hiện tại của dịch vụ LCS-CA yêu cầu chiều dài tối thiểu của cặp khoá để đảm bảo mức độ mã hoá đủ mạnh là 1024 bit RSA cho PCAs.
LCS khuyến khích sử dụng cặp khoá có chiều dài tối thiểu là 1024 bit RSA. LCS không chấp thuận các chứng thư được tạo ra có chiều dài cặp khoá nhỏ hơn hoặc bằng 512 bit.

5.1.6 Tạo các tham số cho các khoá công khai và kiểm tra chất lượng

Những người tham gia dịch vụ LCS-CA (LCS-CA Participants) sử dụng chuẩn chữ ký số sẽ phải đưa ra thông số khoá (key Parameters) tuân theo chuẩn FIPS 186-2 hoặc một chuẩn tương đương khác được LCS chấp thuận. Khi những người tham gia dịch vụ LCS-CA sử dụng chuẩn chữ ký số (Digital Signature Standard), các thông số khoá được tạo ra sẽ kiểm tra tuân theo chuẩn FIPS 186-2 hoặc một chuẩn tương đương khác được LCS-CA chấp thuận.

5.2 Bảo vệ khoá bí mật và kiểm soát phương thức mã hoá

5.2.1 Kiểm soát và chuẩn hoá mô đun mã hoá

Khóa bí mật nằm trong hệ thống LCS-CA sẽ được bảo vệ bởi hệ thống tin cậy và người nắm giữ khoá bí mật sẽ giữ chức năng phòng ngừa để ngăn chặn sự mất mát, bị tiết lộ, sửa đổi và sử dụng bất hợp pháp khoá bí mật phù hợp với CPS này, nghĩa vụ hợp đồng và yêu cầu được cung cấp nằm trong văn kiện bảo mật riêng của LCS-CA. Thuê bao cuối có quyền lựa chọn bảo vệ khoá bí mật của họ bằng thẻ thông minh hoặc thẻ cứng khác.
Trung tâm xử lý sẽ mã hoá trên các mô đun mã hoá tối thiểu theo FIPS 139-1 mức độ 3. Trung tâm dịch vụ sẽ thực hiện tất cả các chức năng mã hoá RA trên các module mã hoá theo FIPS 139-1 mức độ 2. LCS khuyến cáo các thuê bao doanh nghiệp RA sẽ thực hiện tất cả chức

năng mã hoá RA quản trị tự động tối thiểu theo FIPS 139-1 mức độ 2. Những điều kiện đánh giá trong mục này có thể áp dụng cho các điều kiện đánh giá cục bộ hoặc cao hơn.

5.2.2 Đa kiểm soát khoá bí mật (m out of n)

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

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

5.2.3 Sao lưu dự phòng khoá bí mật

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

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

5.2.4 Lưu trữ khoá bí mật

Khi một chứng thư của LCS hết hạn, những cặp khóa gắn với chứng thư ấy sẽ đảm bảo được lưu trữ trong khoảng thời gian ít nhất là 5 năm trong các mô đun phần cứng có cơ chế mã hoá đáp ứng được các yêu cầu của CPS. Những cặp khoá 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 của CPS.

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

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

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

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

5.2.6 Cách thức lưu trữ khoá bí mật trên mô đun mã hoá

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

5.2.7 Mô đun mã hoá của RA

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

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

- Sử dụng mô đun mã hoá cùng với một mật khẩu có cấu trúc sẽ được đề cập trong mục 6.4.1 để xác thực người quản trị trước khi kích hoạt khoá bí mật
- Cân nhắc một giải pháp hợp lý cho việc bảo vệ về mặt vật lý đối với máy trạm có chứa đầu đọc mô đun mã hoá để ngăn chặn việc sử dụng may trạm và khoá bí mật cùng với mô đun mã hoá trái phép.

Thuê bao có nghĩa vụ bảo vệ khoá bí mật của họ. Nghĩa vụ mở rộng là để bảo vệ các khoá bí mật sau khi khoá bí mật được lấy ra. Các khoá bí mật có thể tạm ngưng hiệu lực sau khi mỗi

hoạt động lúc hệ thống của họ log-off hoặc lúc di chuyển thẻ thông minh ra khỏi đầu đọc thẻ tuỳ thuộc vào cơ chế xác thực được áp dụng bởi người sử dụng.

5.2.8 Huỷ khóa bí mật

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

5.3 Một số vấn đề khác của việc quản lý cặp khoá

Thời gian hoạt động của chứng thư và của cặp khoá

Các chứng thư thuê bao (end user) được tạo mới có thể có giá trị trong khoảng thời gian lâu hơn (tối đa tới 3 tháng)

Thời gian sử dụng cặp khoá của thuê bao cuối sẽ bằng thời gian hiệu lực của chứng thư, ngoại trừ khoá bí mật của họ, các khoá bí mật này được sử dụng sau thời gian có hiệu lực để giải mã để kiểm tra chữ ký. Thời gian hoạt động của chứng thư sẽ phụ thuộc vào hạn kết thúc chứng thư hoặc thời gian bị thu hồi chứng thư. Một CA sẽ không được cấp phát chứng thư nếu thời gian hiệu lực của chứng thư dài hơn thời gian sử dụng của cặp khoá CA. Đặc biệt, thời gian sử dụng bằng thời gian hiệu lực của chứng thư CA trừ đi thời gian hiệu lực của chứng thư mà CA phát hành. Lúc kết thúc thời gian sử dụng cặp khoá của thuê bao hoặc CA, thuê bao hoặc CA sau đó sẽ bị tạm ngừng tất cả các hoạt động sử dụng cặp khóa, loại trừ trường hợp CA được mở rộng cần phải đánh dấu thông tin bị huỷ bỏ cho đến khi hết thời gian hiệu lực của chứng thư cuối cùng được phát hành.

Thêm vào đó, dịch vụ LCS-CA ngưng cấp phát các chứng thư mới trước ngày chứng thư của các CA hết hạn nhằm đảm bảo rằng không có một chứng thư nào được cấp phát bởi một CA cấp dưới sẽ bị hết hạn sau khi các chứng thư của các CA cấp dưới đó hết hạn sử dụng.

Các thư được cấp phát bởi các CA cho thuê bao đầu cuối sẽ có thùoi gian hiệu lực lâu hơn 2 năm, tối đa là 5 năm nếu đáp ứng được các yêu cầu:

- Các chứng thư cấp phát cho các thuê bao riêng lẻ.
- Các cặp khóa cho thuê bao đầu cuối lưu trên các thẻ phần cứng, ví dụ như thẻ thông minh.
- Thuê bao phải chứng minh được là người sở hữu của khoá bí mật tương ứng với khoá công khai của chứng nhận.
- Nếu thuê bao không thể thực hiện thành công quy trình xác thực lại hoặc không chứng minh được quyền sở hữu đối với khoá bí mật khi được yêu cầu như ở trên thì CA sẽ thực hiện thu hồi chứng thư của thuê bao.

Các chứng thư cá nhân của Chứng thư cung cấp dịch vụ chia sẻ LCS sẽ cấp phát cho thực thể không liên kết có thể có giá trị 3 năm.

Ngoài các thủ tục này ra bất kỳ các yêu cầu nào cũng phải được sự chấp thuận từ LCS và phải được chứng minh tron CPS có liên quan.

5.4 Dữ liệu kích hoạt

5.4.1 Quá trình tạo và cài đặt dữ liệu kích hoạt

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

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

5.4.2 Bảo vệ dữ liệu kích hoạt

Các thành viên trong dịch vụ LCS-CA sẽ bảo vệ dữ liệu kích hoạt cho những khoá bí mật của họ bằng các phương pháp nhằm để tránh sự mất mát, sự ăn cắp, sự cải biến, sự tiết lộ trái phép, hoặc sử dụng trái phép các khoá bí mật.

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

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

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

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

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

5.4.3 Các vấn đề khác của dữ liệu kích hoạt

5.4.3.1 Vấn đề chuyển tải dữ liệu kích hoạt

Để chuyển giao các dữ liệu kích hoạt cho các khoá bí mật, các thành viên thuộc dịch vụ LCS-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.

5.4.3.2 Huỷ dữ liệu kích hoạt

Dữ liệu kích hoạt khóa bí mật của CA sẽ bị vô hiệu hoá bằng cách sử dụng biện pháp nhằm chống lại nguy cơ mất mát, bị đánh cắp, bị sửa đổi, bị tiết lộ hoặc bị sử dụng trái phép đối với các khoá bí mật mà dữ liệu kích hoạt đó bảo vệ. Sau khi hết thời gian lưu trữ được đề cập trong mục 5.5.2, dịch vụ LCS-CA sẽ vô hiệu hoá dữ liệu kích hoạt bằng cách ghi đè hoặc tiến hành huỷ vật lý.

5.5 Kiểm soát bảo mật máy tính

Dịch vụ LCS-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 LCS-CA. Các thuê bao tổ chức phải sử dụng hệ thống đáng tin cậy.

Trung tâm xử lý sẽ phải đảm bảo chắc chắn rằng các hệ thống chứa phần mềm CA và các tệp dữ liệu phải là hệ thống đáng tin cậy chống lại được các truy cập trái phép, điều này có thể được giải thích theo yêu cầu và tiêu chuẩn kiểm định 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 sự truy cập mạng trái phép ngoại trừ các tiến hành ứng dụng đã được định nghĩa. Trung tâm xử lý sẽ xử dụng tường lửa để bảo vệ hệ thống mạng trước nguy cơ xâm nhậm từ bên trong lẫn bên ngoài. Trung tâm xử lý sẽ yêu cầu sử dụng mật khẩu có đội dài tối thiểu và kết hợp giữa chữ cái với các ký tự đặc biệt, và yêu cầu mật khẩu phải được thay đổi trong một khoảng thời gian nhất định và những khi cần thiết. Việc truy cập trực tiếp dữ liệu của trung tâm xử lý được duy trì trong vùng nhớ của trung tâm xử lý sẽ bị giới hạn đối với những người được tin tưởng trong nhóm hoạt động của trung tâm xử lý có những lý do hợp lệ để truy cập

5.6 Kiểm soát chu kỳ kỹ thuật

Kiểm soát vấn đề quản lý bảo mật

Giải pháp An ninh mạng cho LCS-CA được thiết lập dựa trên các thành phần sau:

- Chính sách an ninh mạng được triển khai.
- Kiến trúc Module hóa các thành phần như: Core, Distribution, Edge, Access.
- Tường lửa Firwall: gồm Firewall Internet GW, Campus Firewall, Egde Firewall, Internal FW.
- Hệ thống phát hiện và chống thâm nhập mạng IPS/IPS Network Sensor
- Hệ thống phát hiện và chống thâm nhập các máy chủ ứng dụng IPS Host sensor.

- Hệ thống phòng chống Antivirus nhiều điểm: Internet Gateway, Mail server, spam mail, Client/server, quản lý tập trung.
- Hệ thống cập nhật bản vá cho máy chủ/máy trạm.
- Hệ thống quản trị an ninh : thành phần quản lý và giám sát an ninh tập trung, các thành phần dò tìm các lỗ hổng, thành phần thiết lập chính sách an ninh mạng, thành phần phân tích an ninh và báo cáo, thành phần cập nhật các bản vá cho HĐH mạng, thành phần quản lý và phân tích băng thông của mạng.

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

5.7 Bảo mật mạng cho hệ thống LCS-CA

Hệ thống tường lửa dành cho LCS-CA (Firewall)

Firewall sử dụng trong hệ thống LCS-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.

Firewall cho LCS-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 LCS-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

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

Ngoài các hệ thống Firwall để điều khiển truy cập, một trong những xu thế an ninh mạng rất phổ biến trên thế giới tập trung vào tấn công các hệ thống Website của các cơ quan, các tổ chức, các doanh nghiệp và các thiết bị bảo mật thông thường rất khó phát hiện các cuộc tấn

công vào cổng dịch vụ TCP 80 này. Chính vì thế giải pháp bảo mật cho hệ thống mạng của LCS-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.

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

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

6 KIỂM SOÁT QUẢN LÝ VÀ ĐIỀU HÀNH HOẠT ĐỘNG

6.1 Kiểm soát bảo mật mức vật lý

LCS có tài liệu chi tiết điều khiển vật lý và có những chính sách đảm bảo an toàn cho các RA và CA. Những chính sách này bao gồm yêu cầu kiểm tra độc lập, được mô tả ở mục 8. Những tài liệu chứa thông tin nhạy cảm chỉ sẵn sàng khi có sự đồng ý của LCS. Khái quát về yêu cầu mô tả dưới đây.

6.1.1 Cấu trúc và khoanh vùng

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

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

6.1.2 Truy cập vật lý

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

Phòng đặt hệ thống CA, RA của hệ thống chứng thực chữ ký số LCS 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 LCS-CA đáp ứng mô hình 4 lớp về bảo mật truy cập vật lý với hệ thống pulic CA.

1. Hệ thống nhân viên an ninh kiểm soát vật lý (TIER 1).

2. Hệ thống truy nhập bằng thẻ từ vào/ra của hệ thống Public CA, có sự hỗ trợ của Camera giám sát (TIER 2).
3. Hệ thống truy nhập bằng sinh trắc học, Camera giám sát 24/24 tại phòng đặt máy chủ 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 (off –line).
4. Để thực hiện các thao tác với hệ thống CA (TIER 4) (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 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.

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

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

Thiết bị an toàn của LCS-CA và các RA được trang bị, bổ sung phương án phòng ngừa để ngăn chặn và dập tắt lửa hay các thảm họa khác có thể gây ra như cháy hay khói. Hệ thống thiết kế để phù hợp với tiêu chuẩn phòng cháy chữa cháy của bộ công an.

6.1.4 Phương tiện lưu trữ

Thông tin LCS và RA 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 hủy hoại và bảo vệ tránh sử dụng truy cập trái phép hay phá hủy.

6.1.5 Bảo mật thông tin và tiêu hủy rác

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

6.1.6 Dự phòng từ xa

LCS và các RA bảo dưỡng 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 LCS-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 back up đầy đủ của hệ thống chính. Ngay khi xảy ra sự cố, hệ thống này sẽ được sử dụng để truy trì hoạt động mà không làm ảnh hưởng đến giao dịch hiện tại.

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

6.2 Các kiểm soát thủ tục

6.2.1 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, các kỹ sư, các tư vấn viên 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

6.2.2 Số lượng thành viên cho mỗi công việc

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

Chính sách và thủ tục được thực hiện để đảm bảo sự phân công nhiệm vụ dựa trên khả năng làm việc. Những công việc mang tính nhạy cảm cao, chẳng hạn truy cập và quản lý hệ thống phần cứng mã hóa (đơn vị mã hóa chữ ký CSU) 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 hóa 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 hủy về logic hoặc về vật lý. Mỗi một 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 thàng phần riêng biệt có chứa các thành phần riêng biệt của khóa bí mật hoặc dữ liệu kích hoạt và ngược lại).

6.2.3 Nhận dạng và xác thực cho từng thành viên

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

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

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.

6.2.4 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 hủy một chứng thư số.
- Quá trình tải CA.

6.3 Kiểm soát nhân sự

LCS ban hành những tài liệu về kiểm soát nhân sự và chính sách bảo mật cho CA và RA. Việc tuân thủ những chính sách bao gồm các yêu cầu kiểm tra độc lập được mô tả ở mục 8. Những tài liệu này chứa thông tin bảo mật nhạy cảm và chỉ dành riêng cho bên tham gia dịch vụ LCS-CA dưới sự đồng ý của LCS.

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

6.3.1 Quy trình kiểm tra lai lịch

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

Những nhân tố phát hiện trong lai lịch là cơ sở để xem xét việc loại trừ những ứng viên khỏi vị trí tin cậy như được đề cập trong bản hướng dẫn về yêu cầu kiểm tra và bảo mật của LCS, bao gồm 4 điểm sau:

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

Bản báo cáo chứa thông tin đánh giá của bộ phận nhân sự và bộ phận an ninh, bộ phận này sẽ thực hiện các hoạt động kiểm tra khách quan thông tin 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 quy định.

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

6.3.2 Yêu cầu về đào tạo

LCS 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 LCS.
- 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.

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

6.3.3 Kỷ luật đối với các hoạt động không hợp pháp

LCS 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.

6.3.4 Yêu cầu đối với các nhà thầu độc lập

LCS 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.

6.3.5 Cung cấp tài liệu cho nhân viên

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

6.4 Kiểm tra truy cập

6.4.1 Các loại bản ghi sự kiện

Các sự kiện có thể kiểm định phải được ghi lại bởi CA và các RA của LCS. 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

Các dạng sự kiện có thể kiểm định bao gồm:

- Các sự kiện:
    1. Tạo khóa CA,
    2. Bật tắt các hệ thống và ứng dụng,
    3. Thay đổi khóa CA,
    4. Sự kiện có liên quan đến quản lý chu kỳ mã hóa,
    5. Quá trình xử lý dữ liệu kích hoạt cho khóa bí mật của CA, các bản ghi truy cập vật lý,
    6. Bảo trì và thay đổi cấu hình hệ thống,
    7. Bản ghi hủy bỏ các phương tiện chứa khóa, dữ liệu kích hoạt, hoặc thông tin thuê bao. Các sự kiện về chu kỳ sống của chứng thư (bao gồm phát hành, cấp lại, cấp mới, thu hồi),
- Sự kiện liên quan tới nhân viên tin cậy (bao gồm (1) hành động truy cập hay thoát ra, (2) tạo và xóa bỏ mật khẩu hay thay đổi đặc quyền của người sử dụng, (3) thay đổi nhân sự).
- Báo cáo về việc truy nhập vào mạng và các hệ thống không được cấp quyền.
- Lỗi trong việc đọc và ghi của chứng thư và kho lưu trữ.
- Thay đổi chính sách tạo chứng thư, thời gian hợp lệ.

6.4.2 Xử lý bản ghi sự kiện

Bản ghi kiểm định được xem lại tương ứng với các cảnh báo không định kỳ và có liên quan trong hệ thống CA/RA. Các trung tâm xử lý so sánh bản ghi với sự hỗ trợ bản ghi bằng tay hay điện tử từ khách hàng của LCS và Trung tâm dịch vụ khi có bất kỳ hoạt động nghi ngờ nào.

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

6.4.3 Thời gian duy trì lưu trữ cho bản ghi kiểm định

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

6.4.4 Bảo vệ các bản ghi kiểm định

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

6.4.5 Thủ tục sao lưu dự phòng cho các bản ghi kiểm định

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

6.4.6 Đánh giá điểm yếu

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

6.5 Lưu trữ các bản ghi

6.5.1 Những kiểu bản ghi được lưu trữ cho dịch vụ LCS-CA:

- Dữ liệu kiểm toán.
- Thông tin về đơn xin cấp chứng thư số.
- Tài liệu hỗ trợ những đơn xin cấp chứng thư.
- Thông tin về chu kỳ làm việc của chứng thư số, ví dụ: các thông tin thu hồi, cáp phát chứng thư.

6.5.2 Thời gian duy trì tài liệu lưu trữ

Các dữ liệu sẽ được lưu trong một khoảng thời gian nhất định trước ngày chứng thư hết hạn hoặc bị hủy bỏ.
Các thông tin về chứng thư của hệ thống LCS được lưu trữ tối thiểu là 5 năm.

6.5.3 Bảo mật tài liệu lưu trữ

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

6.5.4 Thủ tục sao lưu dự phòng dữ liệu

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

6.5.5 Yêu cầu thời gian cho dữ liệu

Chứng thư, CRLs, và toàn bộ cơ sở dữ liệu về việc thu hồi sẽ chứa thông tin về ngày tháng. Những thông tin này cần ở dạng không mã hóa.

6.5.6 Hệ thống thu nhập dữ liệu và lưu trữ

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

6.5.7 Thủ tục thu nhập và kiểm tra thông tin lưu trữ

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

6.6 Thay đổi khóa

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

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

6.7 Thỏa thuận và khôi phục sau thảm họa

6.7.1 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. Bản sao lưu dự phòng của các khóa bí mật CA sẽ được tạo ra và duy trì theo mục 6.2.4 có trong CPS. 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.

6.7.2 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 LCS được nêu trong tài liệu CPS này.

6.7.3 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 LCS.

6.7.4 Khả năng duy trì liên tục trong kinh doanh sau thảm họa

LCS tiến hành bảo mật cho các hoạt động phát triển, kiểm tra, bảo trì của CA và RA. LCS sẽ triển khai 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 LCS 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 sau thảm họa của Trung tâm xử lý được đồng bộ hóa thường xuyên với cơ sở dữ liệu sản xuất trong một khoảng thời gian giới hạn theo chỉ dẫn về yêu cầu an ninh và kiểm toán (Security and Audit Requirements Guide). Các thiết bị để khôi phục sau thảm 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 LCS.

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

Kế hoạch khôi phục sau thảm 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. 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.

6.8 Kết thúc sự hoạt động của CA hay RA

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

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

7 MẪU TRÍCH NGANG CỦA CHỨNG THƯ, CRT, VÀ OCSP

7.1 Khuôn dạng của chứng thư

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

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

Tên Trường	Giá Trị
Serial Number	Duy nhất cho một lssuer DN
Signature Algorithm	Định danh thuật toán được sử dụng để ký chứng thư (Xem phần CPS mục 7.1.3)
Issuer DN	Xem mục 7.1.4
Valid From	Thời điểm chứng thư bắt đầu có hiệu lực. Được đồng bộ với Master Clock của U.S Naval Observatory. Được mã hóa theo tiêu chuẩn RFC 5280
Valid To	Thời điểm chứng thư hết hiệu lực. Được đồng bộ với Master Clock của U.S Naval Observatory. Được mã hóa theo tiêu chuẩn RFC 5280
Subject DN	Xem mục 7.1.4
Subject Public Key	Được mã hóa theo tiêu chuẩn RFC 5280
Signature	Được sinh và mã hóa phù hợp với tiêu chuẩn RFC 5280

7.1.1 Phiên bản

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

7.1.2 Phần mở rộng của chứng thư

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

7.1.2.1 Sử dụng khóa

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

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

7.1.2.2 Phần mở rộng của các chính sách chứng thư

Phần mở rộng của các chính sách chứng thư của X.509 phiên bản 3 được biết đến là việc nhận biết đối tượng của CPS theo mục 7.1.6 và hạn định chính sách tuân theo mục 7.1.8.

7.1.2.3 Tên thay thế của chủ thể (subjectAltName)

Trường mở rộng subjectAltName của chứng thư LCS-CA X.509 phiên bản 3 tuân theo chuẩn RFC 5280.

7.1.2.4 Ràng buộc cơ bản (BasicConstraints)

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

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

7.1.2.5 Việc sử dụng khóa mở rộng

Với chứng thư thuê bao cuối X.509 phiên bản 3 của dịch vụ LCS-CA, trường mở rộng ExtendedKeyUsage được cấu hình bao gồm các khóa OID (object identifiers). Mặc định, trường này được đánh dấu là không quan trọng. Các chứng thư của CA trong dịch vụ LCS-CA không chứa trường mở rộng này.

7.1.2.6 Điểm phân bố CRL

Trong chứng thư LCS-CA X.509 phiên bản 3, trường mở rộng CRLDistributionPoints chứa các URL để đối tác tin cậy có thể lấy được CRL để kiểm tra trạng thái chứng thư.

7.1.2.7 Định danh khóa cho đơn vị cấp chứng thư

Trong chứng thư LCS-CA X.509 phiên bản 3, phương pháp nhận dạng khóa dựa vào khóa công khai do CA phát hành tuân theo phương thức được mô tả trong RFC 3208.

7.1.2.8 Định danh khóa cho chủ thể chứng thư

Nếu xuất hiện trong chứng thư LCS-CA X.509 phiên bản 3, trường mở rộng criticality sẽ được thiết lập là FALSE và phương thức nhận dạng khóa dựa trên khóa công khai của chủ thể chứng thư sẽ tuân theo phương thức được mô tả trong RFC 5280.

7.1.3 Thuật toán nhận biết đối tượng

Dịch vụ LCS-CA sử dụng các thuật toán sau:

- SHA-256

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

Phiên bản hiện tại của trung tâm xử lý sử dụng thuật mã hóa SHA-256 cho chứng thư thuê bao cuối.

7.1.4 Cấu trúc tên

Tên của chứng thư LCS-CA tuân theo mục 3.1.1

Ngoài ra, chứng thư thuê bao cuối còn có trường Organizational Unit chứa các thông báo về giới hạn sử dụng của chứng thư được thiết lập trong URL và URL trỏ đến bản thỏa thuận với đối tác tin cậy. Ngoại trừ những nhu cầu nêu trên sẽ được cho phép khi giới hạn không gian

định dạng, hoặc giới hạn thao tác bên trong chứng thư giống như không thể có một đơn vị thuộc tổ chức để dùng chung một đơn xin cấp chứng thư mong đợi. Hoặc một pointer có thể dùng được bản thỏa thuận với đối tác tin cậy bao gồm các chính sách mở rộng của chứng thư.

7.1.5 Ràng buộc tên

Không có sự ràng buộc nào về tên.

7.1.6 Chính sách nhận biết đối tượng

Việc nhận biết đối tượng cho chính sách chứng thư tương ứng với mỗi cấp được thiết lập trong mục 1.2. Mở rộng chính sách chứng thư trong mỗi chứng thư LCS-CA X.509 phiên bản 3 tuân theo mục 1.2.

7.1.7 Cách dùng của sự mở rộng chính sách ràng buộc

Không có ràng buộc nào.

7.1.8 Chính sách hạn định cấu trúc và ngữ nghĩa

Chứng thư LCS-CA X.509 phiên bản 3 chứa hạn định chính sách trong phần mở rộng chính sách chứng thư. Nói chung, chứng thư bao gồm một CPS pointer qualifier trỏ đến bản thỏa thuận với đối tác tin cậy hoặc CPS của LCS. Ngoài ra, một vài chứng thư còn bao gồm một User Qualifier chỉ đến bản thỏa thuận với đối tác tin cậy.

7.2 Khuôn dạng danh sách thu hồi chứng thư CRL

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

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

- Version – Phiên bản: Trường này miêu tả cú pháp của CRL (Thông thường trường phiên bản sẽ là 2).
- Signature - Chữ ký: Trường này chứa thông tin về kỹ thuật nhận diện cho chữ ký số mà CA sử dụng để ký vào CRL.
- Issuer – Phát hành: Trường này chứa tên theo chuẩn X.509 của CA phát hành CRL.
- This Update - Cập nhật hiện tại: Trường này chứa thông tin ngày phát hành (cập nhật) CRL.
- Next update - Cập nhật sắp tới: Trường này chứa thông tin ngày sẽ cập nhật tiếp theo gần nhất.
- Revoked certificates – Chứng thư số bị thu hồi: Trường này chứa thông tin về các chứng thư bị thu hồi (bao gồm Serial number, time of revoke certification - Thời gian chứng thư bắt đầu bị thu hồi, và một số thông tin mở rộng khác). Các thông tin mở rộng khác được sử dụng để cung cấp thông tin bổ sung. Trường này chỉ xuất hiện trong các CRL phiên bản 2.

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

- CRL number: Số phát hành của CRL.
- Authority key identifier: Chúng ta đã biết mỗi CA có thể có nhiều cặp khóa khác nhau vì vậy trường này giúp người dùng biết cần chọn lựa khóa công khai nào để xác thực chữ ký số của CA đã ký trên CRL để có thể xác định độ tin cậy của CRL.
- Issuer alternative name: Trường Issuer ở trên đã chứa thông tin tên chuẩn X.509 của CA phát hành CRL, tuy nhiên một số ứng dụng đặc biệt không thể hiểu chuẩn đặt tên này. Do đó trường Issuer alternative name chứa thông tin về CA phát hành CRL theo một cú pháp thích hợp khác. Ví dụ: dạng DNS hay e-mail chẳng hạn: CA1@xyz.vn.
- Issuing distribution points: Trường này để kết hợp cùng với trường mở rộng CRL distribution point trong chứng thư X.509.
- Reason code: Trường này được dùng để đưa ra lý do vì sao một chứng thư cụ thể bị thu hồi. (Nhằm giúp người dùng xử lý mềm dẻo hơn).

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

8 TUÂN THỦ KIỂM TOÁN, KIỂM ĐỊNH VÀ CÁC ĐÁNH GIÁ KHÁC

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

Bên cạnh đó, các tiêu chuẩn của dịch vụ LCS-CA sẽ được dùng để tiến hành đánh giá và thanh tra nhằm đảm bảo tính trung thực của LCS, bao gồm những điều sau: Các tiêu chuẩn của dịch vụ LCS-CA sẽ được dùng để thanh tra hay đánh giá LCS, hay thuê bao là các doanh nghiệp. Trong trường hợp LCS hoặc Superior Entity được kiểm tra và kết quả cho thấy các thực thể không đạt các tiêu chuẩn của dịch vụ LCS-CA, sẽ được tiếp tục hoạt động hoặc không được hoạt động tùy thuộc vào mức độ và hậu quả của tổn thất gây ra. Những lỗi hay những tổn thất, cho thấy mối đe dọa tiềm ẩn và thực sự đối với an ninh hay tính toàn vẹn của LCS-CA.

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

8.1 Tần suất và các trường hợp đánh giá

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

8.2 Danh tính và khả năng của người kiểm toán

Hãng kiểm toán đóng vai trò là bên thứ 3 sẽ tiến hành kiểm toán quá trình tuân thủ của LCS. Việc đánh giá và kiểm toán trên lại được kiểm tra bởi một công ty kế toán nhà nước đã được cấp chứng thư trong sự giám định của an ninh máy tính hoặc bởi các chuyên gia có uy tín về

an ninh máy tính do ban cố vấn an ninh chỉ định. Công ty này cũng sẽ phải giám định về an ninh công nghệ thông tin và việc thực hiện PKI.

8.3 Mối quan hệ giữa kiểm toán viên và thực thể được kiểm toán

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

8.4 Những đối tượng trong quá trình đánh giá

Chủ thể kiểm toán của mỗi loại thực thể sẽ được đưa ra như dưới đây. Thực thể được kiểm tra có thể tiến hành kiểm toán việc thực hiện theo một mô mình là một phần của cuộc kiểm tra tổng thể hàng năm về hệ thống thông tin của thực thể.
LCS sẽ được kiểm toán dựa theo những hướng dẫn có trong các tuyên bố số 70 về chuẩn kiểm toán (SAS) do viện kế toán công chứng Hoa Kỳ (American Institule of Certificate Public Accounts) đưa ra và các báo cáo về quá trình giao dịch của các tổ chức dịch vụ.

8.5 Giải quyết khi kết quả bị đánh giá là thiếu sót

Sau khi nhận được báo cáo kiểm toán, SE của thực thể được kiểm toán sẽ liên lạc với bên kiểm toán để thảo luận về những trường hợp ngoại lệ và những thiếu sót mà kết quả cuộc kiểm toán chỉ ra. Các tiêu chuẩn của dịch vụ LCS-CA sẽ được sử dụng để thảo luận về những trường hợp ngoại lệ và những thiết sót với bên kiểm toán. Thực thể đuợc kiểm toán và SE sẽ dùng những nỗ lực thương mại để thỏa thuận kế hoạch hành động đúng đắn để giải quyết các vấn đề do các trường hợp ngoại lệ và thiếu sót gây ra và để thực hiện kế hoạch đó.
Trong trường hợp bên thực thể được kiểm toán thất bại trong việc đưa ra một kế hoạch hành động hoặc thất bại trong việc thực hiện nó, hoặc nếu bản báo cáo chỉ ra những ngoại lệ và những thiếu sót mà LCS và SE tin rằng chúng là mối đe dọa tức thì tới an ninh và tính thống nhất của LCS:

(a) LCS và SE sẽ khẳng định có cần thiết phải thu hồi hay thỏa hiệp báo cáo hay không.
(b) LCS và SE sẽ được phép tạm dừng dịch vụ để tiến hành kiểm toán.

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

8.6 Thông báo kết quả

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

9 CÁC VẤN ĐỀ THƯƠNG MẠI VÀ PHÁP LÝ KHÁC

9.1 Lệ phí

9.1.1 Lệ phí cấp Chứng thư hoặc gia hạn Chứng thư

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

9.1.2 Lệ phí sử dụng Chứng thư

Các thuê bao của dịch vụ LCS-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.

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

Các thành phần tham gia dịch vụ LCS-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.

9.1.4 Lệ phí sử dụng cho các dịch vụ khác

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

9.1.5 Chính sách hoàn trả phí

LCS 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 thỏa thuận với khách hàng hay đưa vào trong bản CPS.

9.2 Trách nhiệm tài chính

9.2.1 Bảo hiểm

LCS 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.

9.2.1.1 Các trường hợp LCS tiến hành đền bù bảo hiểm và mức đền bù bảo hiểm

LCS 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.
- LCS 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.

9.2.1.2 Các trường hợp không được hưởng đền bù bảo hiểm

LCS 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 hủy 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.

9.2.2 Các tài sản khác

LCS 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.

9.2.3 Thông tin bảo đảm mở rộng

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

9.3 Tính bảo mật của thông tin kinh doanh

9.3.1 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 bảo 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 LCS hoặc một thuê bao.
- Các báo cáo kiểm toán tạo bởi LCS 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.

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

Chứng thư, thu hồi chứng thư và các thông tin về trạng thái của chứng thư, nơi lưu giữ của LCS 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.

9.3.3 Trách nhiệm bảo vệ thông tin mật

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

9.4 Tính bí mật của thông tin cá nhân

9.4.1 Kế hoạch đảm bảo tính riêng tư

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

9.4.2 Thông tin riêng tư

Tất cả những thông tin về thuê bao không được công bố công khai, bao gồm chứng thư ban hành, danh mục chứng thư và các CRL trực tuyến được coi là thông tin riêng tư.

9.4.3 Thông tin không riêng tư

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

9.4.4 Trách nhiệm bảo vệ thông tin riêng tư

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

9.4.5 Thông báo và cho phép sử dụng thông tin mật

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

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

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

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

9.4.7 Những trường hợp làm lộ thông tin khác

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

9.5 Quyền sở hữu trí tuệ

9.5.1 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. LCS 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 thỏa thuận với đối tác tin cậy. LCS 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 thỏa thuận sử dụng CRL, thỏa thuận với đối tác tin cậy hay các thỏa thuận thích hợp khác.

9.5.2 Quyền sở hữu trong CPS

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

9.5.3 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.

9.5.4 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.

9.6 Vấn đề đại diện và bảo lãnh

9.6.1 Đại diện của CA và vấn đề bảo lãnh

Dịch vụ LCS-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 và CPS.

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

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

9.6.2 Đại diện của RA và vấn đề bảo lãnh

Các RA của dịch vụ LCS-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.

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

9.6.3 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.
- 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.

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

9.6.4 Đại diện cho các đối tác tin cậy và vấn đề bảo lãnh

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

Thỏa 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.

9.7 Vấn đề bồi thường

9.7.1 Vấn đề bồi thường của khách hàng

Khi pháp luật yêu cầu, khách hàng phải bồi thường cho LCS 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.

9.7.2 Vấn đề bồi thường của các đối tác tin cậy

Khi được pháp luật cho phép, bản thỏa thuận với đối tác tin cậy sẽ yêu cầu đối tác tin cậy bồi thường cho LCS hay các thành phần tham gia dịch vụ LCS-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 dịnh 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.

9.8 Thời hạn và sự kết thúc

9.8.1 Thời hạn

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

9.8.2 Sự kết thúc

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

9.8.3 Ảnh hưởng của sự kết thúc và những tồn tại

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

9.9 Thông báo riêng và thỏa thuận giữa các bên

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

9.10 Sự sửa đổi

9.10.1 Các thủ tục sửa đổi

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

9.10.2 Các trường hợp cần sửa đổi nhận diện đối tượng (OID)

Nếu cần thiết, LCS 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.

9.10.3 Cách thức và thời hạn thông báo

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

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

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

9.10.3.1 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 LCS-CA. Bất kỳ ai tham gia vào dịch vụ LCS-CA cũng có quyền đề xuất ý kiến tới LCS cho đến lúc hết thời gian sửa đổi.

9.10.3.2 Cơ chế xử lý các sửa đổi

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

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

9.11 Thủ tục tranh chấp

9.11.1 Thủ tục tranh chấp giữa LCS, các bên cộng tác và thuê bao

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

9.11.2 Thủ tục tranh chấp giữa thuê bao và đối tác tin cậy

Những cuộc tranh chấp có liên quan đến dịch vụ LCS-CA yêu cầu thời gian đàm phán là 60 ngày (2 tháng), sau đó có thể được đưa lên tòa án có đủ thẩm quyền để xử lý.

9.12 Luật quản trị

Tuân theo luật pháp của nhà nước CHXHCN Việt Nam và luật Thương Mại Điện Tử của Việt Nam, các đối tượng sẽ bị cưỡng chế thực hiện, xây dựng, giải thích và hợp lệ hóa CPS này, không quan tâm tới sự lựa chọn các văn bản luật khác, và không yêu cầu thiết lập mối quan hệ thương mại ở Việt Nam. Việc lựa chọn luật này nhằm đảm bảo tính thống nhất của các thủ tục và giải thích cho những người tham gia dịch vụ LCS-CA, bất kể họ ở đâu.
CPS này tùy thuộc vào hệ thống các điều luật, quy tắc, các điều chỉnh, quy định, các sắc lệnh và mệnh lệnh thuộc phạm vi địa phương, vùng miền, quốc gia, nhưng không giới hạn hay hạn chế trong lĩnh vực xuất khẩu hay nhập khẩu phần mềm, phần cứng và các thông tin kỹ thuật liên quan.

9.13 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, vùng miền, quốc gia, nhưng không giới hạn hay hạn chế cho lĩnh vực xuất khẩu phần mềm, phần cứng và các thông tin kỹ thuật liên quan.

9.13.1 Trách nhiệm

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

9.13.2 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.

9.13.3 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.

9.13.4 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 LCS-CA.

10 Phụ lục

10.1 Chi tiết các loại chứng thư số do hệ thống LCS-CA cung cấp

10.1.1 Chứng thư số dành cho khách hàng cá nhân

Chứng thư số cá nhân cơ bản (LCS-CA Basic Certificate)

Gói chứng thư cá nhân cơ bản cho phép thuê bao sử dụng chứng thư để ký số và mã hóa nội dung gửi đi khi sử dụng địa chỉ Email đã đăng ký với nhà cung cấp dịch vụ.

Khi sử dụng gói dịch vụ này, người nhận email của thuê bao sẽ nhận biết rằng, nội dung thư họ vừa nhận từ đúng địa chỉ email của thuê bao và duy trì được tính bảo mật đường truyền. Thuê bao có thể sử dụng chứng thư cho các hoạt động giao dịch điện tử khác xác thực (client authentication), mã hóa giao dịch.

Đặc điểm gói dịch vụ:

- Mã hóa với chiều dài khóa 1024 bit
- Mức bảo hiểm 500.000 VND
- Hạn đăng ký sử dụng cho thuê bao từ 06 tháng trở lên

Chứng thư số cá nhân chuyên nghiệp (LCS-CA Professional Certificate)

Gói này cho phép thuê bao sử dụng chứng thư để ký số và mã hóa nội dung gửi đi khi sử dụng địa chỉ Email đã đăng ký với nhà cung cấp dịch vụ. Chứng thư số cá nhân chuyên nghiệp cung cấp cho thuê bao chất lượng mã hóa bảo mật cao hơn với chiều dài khóa là 2048 bit. Khi sử dụng gói dịch vụ này, người nhận email của thuê bao sẽ nhận biết rằng, nội dung thư họ vừa nhận từ đúng địa chỉ email của thuê bao và duy trì được tính bảo mật đường truyền. Thuê bao có thể sử dụng chứng thư cho các hoạt động giao dịch điện tử khác xác thực (client authentication), mã hóa giao dịch.

Đặc điểm gói dịch vụ:

- Mã hóa với chiều dài khóa 2048 bit
- Mức bảo hiểm 1.000.000 VND
- Hạn đăng ký sử dụng cho thuê bao từ 12 tháng trở lên

10.1.2 Chứng thư số cho khách hàng doanh nghiệp (Enterprise Certificate)

Doanh nghiệp sử dụng chứng thư số có thể phục vụ cho rất nhiều giao dịch điện tử đòi hỏi đảm bảo tính xác thực và toàn vẹn của dữ liệu như: Thanh toán hóa đơn, E-Tax, xuất xứ điện tử… Việc sử dụng chữ ký số làm giảm những thủ tục giấy tờ không cần thiết, tăng năng suất lao động hướng đến hệ thống chính phủ điện tử. Phù hợp với quy định của luật pháp Việt Nam.

Đặc điểm gói dịch vụ:

- Mã hóa với chiều dài khóa 2048 bit
- Mức bảo hiểm 50.000.000 VND
- Dịch vụ hỗ trợ 24/7 miễn phí
- Áp dụng cho doanh nghiệp đăng ký sử dụng từ 12 tháng trở lên

10.1.3 Chứng thư số Code Signing

Chứng thư số LCS-CA Code Signing Professional

Gói dịch vụ LCS-CA Code Signing cho phép thuê bao có thể ký số lên các sản phẩm phần mềm và macro tự phát triển. Điều này cho phép người dùng có thể tải các phần mềm từ trên mạng từ các nhà cung cấp mà không cần phải lo lắng về xuất xứ cũng như tính toàn vẹn của phần mềm đó.

Đặc điểm gói dịch vụ:

- Mã hóa với chiều dài khóa 2048 bit
- Mức bảo hiểm cho loại chứng thư ở mức cao
- Thời gian ưu tiên xử lý cao
- Dịch vụ hỗ trợ 24/7 miễn phí.
- Hạn đăng hạn ký sử dụng cho thuê bao từ 12 tháng trở lên

Chứng thư số LCS-CA Code Signing Special

Gói dịch vụ chứng thư Code Signing Special cho phép thuê bao có thể ký số lên các sản phẩm phần mềm và macro tự phát triển. Loại chứng thư số này có độ dài khóa cũng như mức bảo hiểm cao hơn chứng thư số Professional.

Đặc điểm gói dịch vụ:

- Mã hóa với chiều dài khóa 4096 bit

- Mức bảo hiểm cho loại chứng thư ở mức cao
- Thời gian ưu tiên xử lý cao
- Dịch vụ hỗ trợ 24/7 miễn phí.
- Hạn đăng hạn ký sử dụng cho thuê bao từ 12 tháng trở lên

10.1.4 Chứng thư số SSL cho web server (LCS-CA SSL Server)

Chứng thư số LCS-CA SSL Basic

Dịch vụ LCS-CA cung cấp chứng thư SSL nhằm đảm bảo tính bảo mật đường truyền đối với các dữ liệu mật, nhạy cảm trên các trang web, mạng Internet và các mạng Intranet sử dụng mã hóa tối thiểu chiều dài khóa từ 1024 bit.

Đặc tính gói dịch vụ:

- Xác thực thông tin đầy đủ trong hoạt động kinh doanh
- Mã hóa với chiều dài khóa từ 1024 bit
- Mức bảo hiểm 100.000.000 VND
- Dịch vụ hỗ trợ 24/7 miễn phí

Chứng thư số LCS-CA SSL Professional

Gói chứng thư cho Server SSL Professional của LCS tạo điều kiện thuận lợi cho khách hàng thuê bao thực hiện mọi bước giao dịch trực tuyến trong sự bảo mật thông tin tuyệt đối với công nghệ mã hóa mạnh nhất. Với đặc tính mã hóa 2048 bit SSL giúp khách hàng có thể yên tâm tuyệt đối khi truy cập website cũng như tin tưởng hoàn toàn vào đối tượng doanh nghiệp khi giao dịch thương mại.

Đặc tính gói dịch vụ:

- Mã hóa với chiều dài khóa tối thiểu từ 2048 bit
- Xác thực thông tin đầy đủ trong hoạt động kinh doanh
- Mức bảo hiểm 200.000.000 VND
- Thời gian ưu tiên xử lý cao
- Dịch vụ hỗ trợ cài đặt và hỗ trợ sử dụng miễn phí trong quá trình đăng ký sử dụng Chứng thư số LCS-CA SSL Special

Gói LCS-CA SSL Special tạo cho khách hàng của thuê bao đăng ký sử dụng dịch vụ OIC-CA sự yêu tâm và tin tưởng khi tham gia giao dịch trực tuyến trên website của thuê bao. Đảm

bảo độ bảo mật cao khi truy cập trên Website. Việc đăng ký sử dụng gói SSL Domain Protection không chỉ làm gia tăng hiệu quả bảo mật trực tuyến mà còn tạo cho doanh nghiệp có được lòng tin từ phía khách hàng.

Đặc điểm gói dịch vụ:

- Mã hóa với chiều dài khóa tối thiểu từ 2048 bit
- Xác thực thông tin đầy đủ trong hoạt động kinh doanh
- Mức bảo hiểm 500.000.000 VND
- Thời gian ưu tiên xử lý cao
- Dịch vụ hỗ trợ cài đặt và hỗ trợ sử dụng miễn phí trong quá trình đăng ký sử dụng

10.1.5 Chứng thư số hệ thống bảo mật Managed PKI

Ngoài các gói chứng thư số cho các khách hàng cá nhân và doanh nghiệp, hệ thống LCS-CA còn cung cấp dịch vụ chứng thực Managed PKI. Đặc điểm của dịch vụ này là các tổ chức vẫn toàn quyền đăng ký, thu hồi chứng thư số của người sử dụng mà không cần quan tâm đến việc cài đặt, vận hành và duy trì hệ thống. Cơ sở hạ tầng sẽ được đặt tại LCS-CA. Với hình thức này, các tổ chức không cần đầu tư quá nhiều tiền cho việc xây dựng một hệ thống PKI mới và vẫn hoàn toàn có thể tự mình vận hành hệ thống PKI thực sự.

Đặc điểm gói dịch vụ:

- Mã hóa với chiều dài khóa ít nhất 2048 bit
- Hỗ trợ kỹ thuật 24/7
- Ưu tiên mức cao
- Bảo hiểm 500.000.000 VND

10.2 Cấu trúc tổng quát các thông điệp trong hệ thống LCS-CA

Tất cả các quá trình trao đổi thông tin giữa các đối tượng trong hệ thống PKI đều được thực hiện thông qua việc trao đổi các thông điệp được định nghĩa riêng cho hệ thống. Các thông điệp này được tạo ra trên cơ sở các chức năng hoạt động cơ bản của hệ thống PKI đã được nêu trong phần trước. Phần sau đây sẽ mô tả về các thông điệp được sử dụng trong hệ thống PKI.

Một thông điệp sẽ có hai trường cơ bản và hai trường tùy chọn.

Hai trường cơ bản là:

- Trường **header**: Trường này cho biết các thông tin liên quan đến các đối tượng truyền và nhận trong hệ thống PKI. Trong hầu hết các thông điệp PKI, trường header có định dạng giống nhau. Trường này bắt buộc phải tồn tại trong mọi thông điệp PKI và không được phép là rỗng.
- Trường **body**: Trường này chứa nội dung mà thông điệp PKI cần truyền tải. Phần này của thông điệp có cấu trúc không xác định. Định dạng của trường body trong thông điệp sẽ tùy thuộc vào đối tượng tạo ra nó, vào thông tin nó truyền tải và nó được tạo ra bởi chức năng nào của hệ thống. Trong những trường hợp đặc biệt, trường body có thể là rỗng.

Hai trường tùy chọn là:

- Trường protection: Trường này đóng vai trò bảo vệ cho thông tin được truyền đi. Về nguyên tắc, các thông tin cần được bảo vệ thường được mã hóa và chứa trong phần thân của thông điệp. Trường protection có vai trò bảo vệ ở lớp ngoài cho cả thông điệp PKI. Thông thường, đây là những bit được tạo ra nhờ một số thuật toán mã hóa bảo mật được hệ thống PKI hỗ trợ. Tuy nhiên, đây là một trường tùy chọn và trong thực tế ít sử dụng đến trường này.
- Trường extraCerts: Đây là trường chứa mảng các chứng thực bổ sung. Các chứng thực này thường có tác dụng giúp cho đối tượng nhận kiểm chứng thông tin nhận được và xác thực đối tượng.

Các thông điệp

- Thông điệp yêu cầu khởi tạo (Initialization Request – IR): chỉ ra chứng thực được yêu cầu. Thông điệp này được sử dụng khi một EE lần đầu tiên được khởi tạo trong hệ thống PKI.
- Thông điệp trả lời yêu cầu khởi tạo (Initialization Response - IP) được dùng để trả lời các thông điệp yêu cầu thông tin về trạng thái của hệ thống PKI, về các đối tượng sử dụng hoặc có thể là một khóa riêng. Thông thường, các thông tin trả về được mã hóa với một khóa phiên đã định. Chính khóa phiên này lại được mã hóa bởi khóa được sử dụng trong giao thức quản lý PKI (protocolEncKey).

- Thông điệp yêu cầu đăng ký/yêu cầu chứng thư (Registration Request - RR và Certificate Request - CR) xác định những chứng thư được yêu cầu và được sử dụng khi một đối tượng sử dụng muốn có thêm các chứng thư.
- Thông điệp trả lời yêu cầu đăng ký/yêu cầu chứng thư (Registration Reply - RR) mang một giá trị trạng thái của mỗi chứng thư được yêu cầu. Ngoài ra, có thể có khóa công khai của CA, các thông tin về yêu cầu không được chấp nhận, một chứng thư của đối tượng hoặc một khóa riêng đã được mã hóa.
- Thông điệp yêu cầu cập nhật khóa (Key Update Request - KUR) được sử dụng để cập nhật thông tin cho các chứng thư đã tồn tại.
- Thông điệp trả lời yêu cầu cập nhật khóa (Key Update Response - KUP) tương tự thông điệp trả lời yêu cầu khởi tạo.
- Thông điệp yêu cầu khôi phục khóa (Key Recovery Request - KRR) tương tự thông điệp yêu cầu khởi tạo.
- Thông điệp trả lời yêu cầu khôi phục khóa (Key Recovery Response - KRP) (ngoại trừ một số giá trị trạng thái, không còn trường tùy chọn nào được sử dụng)
- Thông điệp yêu cầu hủy bỏ (Revocation Request - RR)
- Thông điệp yêu cầu chứng thực ngang hàng (Cross-Cert. Request - CCR) các CA cũng sử dụng cùng một kiểu thông điệp như khi các đối tượng sử dụng yêu cầu chứng thư từ CA. Tuy nhiên, có một điểm ràng buộc là cặp khóa sử dụng để mã hóa thông điệp chứa chứng thực phải do phía CA yêu cầu chứng thư tạo ra từ trước. Đồng thời, khóa riêng trong cặp khóa này bắt buộc phải không được gửi đến cho CA trả lời.
- Thông điệp trả lời yêu cầu xác nhận ngang hàng (Cross-Cert. Response - CCP) cũng giống với thông điệp trả lời yêu cầu xác nhận. Tuy nhiên, có một ràng buộc là không được phép gửi khóa riêng (kể cả đã được mã hóa) cho CA yêu cầu. Điều này xuất phát từ nguyên tắc: chỉ thành phần off-line mới biết được khóa riêng của đối tượng.
- Thông điệp công bố cập nhật khóa CA (CA Key Update Announcement - CKUANN) được sử dụng khi CA cập nhật cặp khóa của chính mình.
- Thông điệp công bố chứng thư (Certificate Announcement - CANN) được sử dụng để thông báo về sự tồn tại của một chứng thư. Cần lưu ý là phương pháp sử dụng thông

điệp này chỉ được sử dụng trong trường hợp không tồn tại một phương pháp phát hành chứng thư nào khác. Ví dụ: nếu có một phương thức phát hành thẻ theo chuẩn X.500 thì phương pháp này sẽ không được sử dụng.

- Thông điệp thông báo thu hồi chứng thư (Revocation Announcement - RANN) được dùng khi một chứng thư bị thu hồi hoặc sắp bị thu hồi bởi CA, nó sẽ đưa ra thông báo về sự kiện này.

CA có thể sử dụng thông báo kiểu này để báo với thuê bao sở hữu chứng thư biết rằng chứng thư mà đối tượng ấy nắm giữ sẽ hoặc đã bị thu hồi. Nó chủ yếu được sử dụng trong trường hợp thuê bao nắm giữ chứng thư không gửi yêu cầu hủy bỏ. Nghĩa là CA chủ động hủy bỏ một chứng thư. Trường willBeRevokedAt được dùng để xác định thời điểm mà một chỉ mục mới ứng với chứng thư này được bổ sung vào danh sách những chứng thư bị hủy bỏ.

- Thông điệp thông báo CRL (CRL Announcement - CRLANN) được sử dụng khi một CA phát hành một hoặc một tập các CRL mới.
- Thông điệp xác nhận (Confirmation - CONF) được sử dụng trong các hoạt động của giao thức quản lý PKI theo kiểu yêu cầu - trả lời - xác nhận. Nội dung của thông điệp này giống nhau trong tất cả các trường hợp vì bản thân phần header của thông điệp đã mang tất cả các thông tin cần thiết.
- Thông điệp PKI đa mục đích (General Message - GENM) được sử dụng trong một số trường hợp truyền thông tin cho các thiết bị hoặc các trình ứng dụng của các đối tượng sử dụng trong hệ thống.
- Thông điệp trả lời tổng quát (General Response - GENP).
- Thông điệp thông báo lỗi (Error Message - ERROR) được sử dụng trong trường hợp khi có lỗi nào đó trong các hoạt động của giao thức PKI. Đi kèm với thông tin về lỗi là những thông tin về trạng thái của hệ thống.

10.3 Hiệu lực của quy chế chứng thực chữ ký số

10.3.1 Thời điểm có hiệu lực của quy chế chứng thực chữ ký số

Quy chế chứng thực chữ ký số có hiệu lực kể từ khi ban hành, phải công bố công khai giữa các bên để thi hành quy chế.

Chỉ trong trường hợp thật cần thiết, quy chế chứng thực chữ ký số mới quy định hiệu lực trở về trước.

Quyết định ngừng việc thi hành quy chế, quyết định xử lý quy chế phải được công bố công khai.

10.3.2 Ngưng hiệu lực quy chế chứng thực chữ ký số

Khi có quyết định ngừng thi hành quy chế thì quy chế cũng bị ngưng hiệu lực.

Thời điểm ngưng hiệu lực phải được ghi rõ tại quyết định đình chỉ hay quyết định xử lý quy chế chứng thực chữ ký số.

10.3.3 Các trường hợp hết hiệu lực của quy chế chứng thực chữ ký số

- Hết thời hạn hiệu lực của quy chế đã được ghi trong văn bản
- Được sửa đổi hoặc bổ sung bằng một quy chế chứng thực mới
- Quy chế chứng thực chữ ký số bị hủy bỏ hoặc bãi bỏ.

10.3.4 Thông báo đến thuê bao

Mọi thay đổi về quy chế chứng thực chữ ký số được thông báo trên website