CÔNG TY CỔ PHẦN ĐẦU TƯ CÔNG NGHỆ VÀ THƯƠNG MẠI SOFTDREAMS

QUY CHẾ CHỨNG THỰC

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

Phiên bản: 1.1

Hà nội, năm 12.2021

MỤC LỤC

1. Giới thiệu

Dịch vụ chứng thực chữ ký số công cộng EasyCA của Công ty cổ phần đầu tư công nghệ và thương mại Softdreams (SDS). Bản Quy chế chứng thực do EasyCA ban hành.

Bản Quy chế chứng thực EasyCA này được viết tuân thủ RFC 3647 về "Khung quy chế chứng thực và chính sách chứng thư số", đáp ứng theo tiêu chuẩn trong quyết định số 59/2008/QĐ – BTTTT của Bộ Thông Tin và Truyền Thông ban hành ngày 31 tháng 12 năm 2008.

Bản Quy chế chứng thực này hoàn toàn phù hợp với "Mẫu quy chế chứng thực chữ ký số" được quy định trong quyết định 20/2007/QĐ – BBCVT của Bộ Bưu Chính Viễn Thông ban hành ngày 19 tháng 06 năm 2007.

Bản Quy chế chứng thực này chỉ rõ những thủ tục mà EasyCA sử dụng trong việc cung cấp dịch vụ chứng thực chữ ký số như: Phát hành, quản lý, thu hồi, gia hạn, thay đổi cặp khóa chứng thư số… Quy chế chứng thực mà EasyCA áp dụng tuân theo những ràng buộc được chỉ rõ trong Chính sách chứng thư số do Trung tâm Chứng thực chữ ký số Quốc gia Việt Nam quản lý.

1.1. Tổng quan

Tại Việt Nam kiến trúc hệ thống cung cấp dịch vụ chứng thực chữ ký số công cộng đứng đầu là CA do Trung tâm chứng thực điện tử quốc gia Việt Nam quản lý gọi là RootCA. EasyCA là nhà cung cấp dịch vụ chứng thực chữ ký số công cộng được RootCA cấp chứng thư số và được Bộ TT&TT cấp phép hoạt động.

EasyCA phát hành chứng thư số với mức đảm bảo cao về nhận dạng các thuê bao (tổ chức, cá nhân). Để đảm bảo cao về nhận dạng các thuê bao, EasyCA thực hiện các thủ tục xác minh nhận dạng của thuê bao:

- Với thuê bao là cá nhân: thực hiện các thủ tục xác minh sự tồn tại của thuê bao.
- Với đối tượng tổ chức, ngoài xác minh tồn tại của tổ chức, EasyCA xác minh nhận dạng của cá nhân là đại điện được ủy quyền gửi đơn xin cấp chứng thư số cho tổ chức đó.
- Với chứng thư số cho Web Server, EasyCA xác minh quyền sở hữu tên miền mà thuê bao đã ghi trong đơn xin cấp chứng thư số.

EasyCA cấp chứng thư số cho tổ chức, cá nhân để xác thực (Authentication); đảm bảo sự toàn vẹn của dữ liệu (Intergrity); bí mật (Confidentiality) và chống chối bỏ (Non-

repudiation)

EasyCA ban hành các chứng thư số dưới đây:

Loại chứng thư số	**Mức độ đảm bảo**	**Mô tả chức năng**
Chứng thư số SSL	Cao	Xác thực Web Server
Chứng thư số CodeSigning	Cao	Xác thực, toàn vẹn trong quá trình phân phối trên mạng
Chứng thư số cá nhân cho cơ quan, tổ chức, cá nhân	Cao	Xác thự, đảm bảo toàn vẹn, chống chối bỏ, và bí mật

Quy chế chứng thực này mô tả quyền và nghĩa vụ của các bên liên quan, vấn đề pháp lý và đặc điểm hạ tầng kỹ thuật của hệ thống EasyCA. Quy chế này mô tả:

- Nghĩa vụ của EasyCA, RA, thuê bao, và người nhận.
- Các yếu tố liên quan đến pháp luật được đề cập trong thỏa thuận thuê bao, thỏa thuận người nhận với EasyCA.
- Kiểm tra, giám sát an ninh mà các thành viên của EasyCA phải thực hiện.
- Các phương pháp mà EasyCA sử dụng để xác minh nhận dạng thuê bao, cá nhân được ủy quyền, thực thể giữ khóa trong quá trình phát hành, quản lý chứng thư số.
- Các thủ tục quản lý vòng đời chứng thư số bao gồm: cấp chứng thư số, ban hành chứng thư số, nhận chứng thư số, thu hồi, thay đổi cặp khóa và gia hạn chứng thư số.
- Các thủ tục an ninh như việc ghi nhật ký kiểm tra (audit), việc lưu giữ bản ghi vận hành hệ thống, và việc phục hồi sự cố, thảm họa.
- Quản lý các thiết bị vật lý, con người, quản lý khóa; các quy trình, biện pháp đảm bảo an ninh.
- Nội dung của chứng thư số, nội dung của danh sách chứng thư số bị thu hồi.
- Các phương pháp sửa đổi bổ sung quy chế chứng thực.

Ngoài ra, quy chế chứng thực này còn đề cập đến các thỏa thuận giữa EasyCA với các thành viên của EasyCA. Những thỏa thuận này áp dụng cho RA, thuê bao, người nhận. Các thỏa thuận này chỉ rõ các thành viên phải làm gì để phù hợp với các yêu cầu trong quy chế chứng thực này.

1.2. Tên và dấu hiệu nhận diện của tài liệu

- Tài liệu này: Quy chế chứng thực chữ ký số EasyCA.
- Phiên bản: v1.1
- Ngày tạo 12/2021
- OID: Không có quy định.

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

- Trung tâm Chứng thực điện tử quốc gia - MIC National RootCA
- Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng EasyCA
- RA (RA của EasyCA và các đại lý EasyCA)
- Thuê bao chứng thư số của EasyCA
- Người nhận

1.3.1. Các tổ chức cung cấp dịch vụ chứng thực chữ ký số

- MIC National RootCA
    - MIC National RootCA là cấp cao nhất trong hạ tầng chứng thực chữ ký số công cộng Việt Nam.
    - 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 tại Việt Nam.
    - 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.

- EasyCA
    - EasyCA là dịch vụ chứng thực chữ ký số công cộng của Công ty cổ phần đầu tư công nghệ và thương mại Softdreams.
    - EasyCA 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.

- EasyCA xây dựng một mô hình PKI có mức độ tin cậy cao trong việc sử dụng chữ ký số phục vụ xác thực, chống chối bỏ, toàn vẹn và bảo mật các dữ liệu và giao dịch điện tử.
- Dịch vụ chứng thực chữ ký số công cộng EasyCA vận hành tuân thủ theo Quy chế chứng thực số này.

1.3.2. Tổ chức đăng ký (RA)

- RA là thành viên của EasyCA (Bao gồm bản thân EasyCA và các đại lý của EasyCA) là các tổ chức được EasyCA tin cậy giao nhiệm vụ quản lý thuê bao, nhận và duyệt các đơn đăng ký liên quan đến chứng thư số.

1.3.3. Thuê bao chứng thư số EasyCA

- Thuê bao của EasyCA là các tổ chức, cá nhân sử dụng dịch vụ chứng thực chữ ký số công cộng EasyCA. Quyền và nghĩa vụ của hai bên được quy định trong hợp đồng cung cấp dịch vụ giữa hai bên.

1.3.4. Người nhận

- Người nhận là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi thuê bao của EasyCA, người nhận sử dụng chứng thư số được cấp cho người ký để xác thực giao dịch.

1.3.5. Các đối tượng khác

- Ngoài EasyCA, RA, thuê bao và người nhận, EasyCA không quản lý đối tượng nào khác.

1.4. Mục đích sử dụng chứng thư số

1.4.1. Mục đích sử dụng chứng thư số EasyCA

- Mục đích sử dụng được quy định trong hợp đồng giữa EasyCA và thuê bao mà không bị cấm bởi pháp luật, chính sách và quy chế chứng thực của RootCA và EasyCA.
- Mục đích được quy định bởi trường "Mục đích sử dụng" (KeyUsage) trong chứng thư số.
- Hiện tại EasyCA cung cấp các gói dịch vụ tương ứng với KeyUsage được trình

bày trong mục 7.1.2

1.4.2. Cấm sử dụng chứng thư số EasyCA vào những mục đích sau

- Ngoài mục đích mà chứng thư số đó được cấp phát.
- Đảm bảo an ninh cho lĩnh vực hạt nhân, hệ thống điều khiển vũ khí…
- Ngoài mục đích dân sự như trong lĩnh vực an ninh, quân sự, đảm bảo an ninh quốc gia.
- Vi phạm pháp luật.
- Cấp phép CA cấp dưới.

1.4.3. Thời gian có hiệu lực của chứng thư số

- Thời gian sử dụng của chứng thư số do EasyCA cấp tối đa là 3 năm. Thời gian sử dụng không được vượt quá thời gian của chứng thư số SubCA tức là chứng thư số EasyCA do RootCA quốc gia cấp.

1.4.4. Phạm vi sử dụng của chữ ký số chứng thư số

STT	Loại chữ ký số và chứng thư số	Phạm vi sử dụng	Thời gian sử dụng
1	Cho tổ chức, doanh nghiệp	Ký số, chống chối bỏ, mã hóa khóa, bảo vệ Email	1-3 năm
2	Chứng thư số cho cá nhân	Ký số, chống chối bỏ, mã hóa khóa, bảo vệ Email	1-3 năm
3	Chứng thư số Web Server	Ký số, chống chối bỏ, mã hóa khóa.	1-3 năm
4	Chứng thư số Codesigning	Ký số, xác thực, chống chối bỏ.	1-3 năm

1.5. Quản lý quy chế chứng thực

1.5.1. Tổ chức quản lý

- Công ty cổ phần đầu tư công nghệ và thương mại Softdreams
- Số 7, Ngách 97/1, Ngõ 97 Chính Kinh, Phường Nhân Chính, Quận Thanh Xuân, Thành phố Hà Nội, Việt Nam.

1.5.2. Liên hệ

- Công ty Cổ phần đầu tư công nghệ và thương mại Softdreams
    - Trụ sở chính: Nhà khách ATS, số 8 Phạm Hùng, Phường Mễ Trì, Quận Nam Từ Liêm, Hà Nội.

- Chi nhánh:
  - Số H.46 đường Dương Thị Giang, Phường Tân Thới Nhất, Quận 12, TP HCM.
- Điện thoại: 0914 969 009
- Email: easyca@easyca.vn
- Website: https://easyca.vn

1.5.3. Công nhận sự phù hợp của Quy chế chứng thực chữ ký số EasyCA

- EasyCA xác nhận sự phù hợp của quy chế chứng thực này.

1.5.4. Thủ tục phê chuẩn Quy chế chứng thực chữ ký số EasyCA

- EasyCA quy định cụ thể thủ tục phê chuẩn ban hành, cập nhật, sửa đổi và ban hành Quy chế chứng thực chữ ký số EasyCA.
- Các thay đổi, cập nhật của quy chế chứng thực được ghi lại, công bố tại https://easyca.vn/cps_update.
- Quy chế chứng thực bản mới nhất được lưu trữ tại https://easyca.vn/cps

1.6. Các định nghĩa và từ viết tắt

STT	Thuật ngữ / Từ viết tắt	Ngữ nghĩa
1	Chuỗi chứng thư số	Danh sách có thứ tự các chứng thư số, bắt đầu từ chứng thư số của Root CA đến chứng thư số của người dùng cuối, theo trình tự chứng thư đứng trước ký xác thực xác nhận cho chứng thư số đứng sau.
2	CA	Certificate Authority – Tổ chức cung cấp dịch vụ chứng thực chữ ký số.
3	Chứng thư số	Một thông điệp điện tử, chứa thông tin CA, thông tin về khóa công khai, thông tin về chủ thể, thông tin về hạn sử dụng chứng thư số, thông tin về thuật toán ký và chữ ký của CA, các thông tin kênh kiểm tra trạng thái. Chứng thư số tuân theo chuẩn X509 v3.

4	EasyCA	Dịch vụ chứng thực chữ ký số công cộng do Công ty cổ phần đầu tư công nghệ và thương mại Softdreams xin cấp phép và quản lý, được Bộ Thông Tin và Truyền Thông cấp phép hoạt động.
5	Chủ thể chứng thư số	Chủ thể chứng thư số có thể là thuê bao chứng thư số hoặc các thiết bị như máy chủ Web.
6	CN	CommonName – CN là tên thường gọi của đối tượng là chủ thể của chứng thư số.
7	CRL	Danh sách chứng thư số thu hồi.
8	DN	Distinguished Names – DN chưa thông tin nhận dạng đối tượng là chủ thể chứng thư số.
9	ITU-T X.509	Tiêu chuẩn về chứng thư số và danh sách thu hồi chứng thư số do tổ chức viễn thông quốc tế quy định.
10	Khóa bí mật	Là khóa trong cặp khóa bất đối xứng dùng để tạo chữ ký số, và được lưu trữ bí mất chỉ có thuê bao nắm giữ.
11	Khóa công khai	Là khóa trong cặp khóa bất đối xứng dùng để xác thực khóa bí mật, và được công bố trong chứng thư số để cho mọi người có thể truy cập.
12	Người nhận	Là đối tượng tin tưởng chứng thư số hay một chữ ký số được cung cấp bởi CA.
13	RA	Registration Authority – Tổ chức tiếp nhận duyệt đơn đăng ký chứng thư số, đơn gia hạn chứng thư số, đơn thay đổi cặp khóa, đơn thu hồi chứng thư số và quản lý thông tin thuê bao.

14	Root CA	RootCA là CA có chứng thư số được ký bởi chính khóa bí mật của CA đó. Root CA công cộng của Việt Nam được quản lý bởi Trung tâm Chứng thực điện tử quốc gia – Bộ Thông Tin và Truyền Thông.
15	Thuê bao	Đối tượng đăng ký sử dụng chứng thư số.
16	USB token	Thiết bị phần cứng được sử dụng để bảo quản và sử dụng cặp khóa trong hạ tầng khóa công khai.
17	PKI	Public key infrastructure - Hạ tầng mã khóa công khai.
18	OCSP	Online Certificate Status Protocol - giao thức cho phép kiểm tra trạng thái chứng thư số trực tuyến.

2. Trách nhiệm lưu trữ và công bố

2.1. Lưu trữ

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

2.2. Công bố thông tin

- EasyCA duy trì công bố địa chỉ lưu trữ cho phép người nhận truy nhập các thông tin về trạng thái và các thông tin khác của chứng thư số.
    - EasyCA công bố thông tin chứng thư số của khách hàng tại địa chỉ: https://directory.easyca.vn. Việc tra cứu thông tin tại địa chỉ này được thực hiện thông qua cổng kết nối trung gian để đảm bảo an toàn. EasyCA cho phép download chứng thư số của thuê bao theo chuẩn X.509, đảm bảo tính toàn vẹn.
    - Thông tin chứng thư số bị thu hồi được công bố tại địa chỉ: https://crl.easyca.vn/EasyCA.crl

- EasyCA luôn công bố phiên bản hiện tại của chính sách chứng thư số, quy chế chứng thực, thỏa thuận thuê bao, thỏa thuận người nhận và chính sách bảo mật tại địa chỉ: https://easyca.vn/
- EasyCA công bố thông tin CA tại địa chỉ: https://easyca.vn/
- Địa chỉ truy cập OCSP Responder của EasyCA tại địa chỉ: https://ocsp.easyca.vn

2.3. Thời gian, tần suất công bố thông tin

- Quy chế chứng thực: được cập nhật theo phần 9.12.
- Thỏa thuận thuê bao, thỏa thuận người nhận: được cập nhật khi cần thiết.
- Chứng thư số: được công bố khi chứng thư số được ban hành và xác nhận của thuê bao.
- Trạng thái chứng thư số: được công bố ngay lập tức lên OCSP Responder.
- Danh sách chứng thư số bị thu hồi: được cập nhật hằng ngày.

2.4. Kiểm soát truy nhập thông tin

- EasyCA không giới hạn việc truy xuất Quy chế chứng thực chữ ký số EasyCA, chứng thư số EasyCA, thông tin trạng thái chứng thư số hay danh sách chứng thư số bị thu hồi.

3. Nhận dạng và xác thực yêu cầu xin cấp chứng thư số

3.1. Đặt tên trong chứng thư số

- Ngoài những trường hợp ngoại lệ được chỉ ra trong chính sách chứng thư số, quy chế chứng thực, tên trong chứng thư số do EasyCA cấp phải được kiểm tra tính xác thực.

3.1.1. Các loại tên

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

Thuộc tính	Giá trị
Quốc gia (C)	Hai chữ cái chỉ tên quốc gia theo ISO, Việt Nam được ký hiệu là "VN"
Tổ chức (O)	Tên tổ chức được cấp chứng thư số hoặc tên miền đối với chứng thư số được cấp cho tên miền

Bộ phận tổ chức (OU)	Tên đơn vị nằm trong tổ chức.
Tỉnh/Thành Phố (S)	Tên Tỉnh, Thành phố là nơi cứ trú hoặc đặt trụ sở của thuê bao.
Quận/Huyện (L)	Tên Quận, Huyện là nơi cư trú hoặc đặt trụ sở của thuê bao.
Tên thường gọi (CN)	Các loại giá trị của thuộc tính này: - Tên miền. - Tên tổ chức. - Tên cá nhân
Địa chỉ email (E)	Địa chỉ email của đối tượng sở hữu chứng thư số
Mã duy nhất (UID)	Mã định danh của đối tượng sở hữu chứng thư số. Đối với cá nhân Mã số định danh sẽ là số CMND hoặc số thẻ căn cước công dân. Đối với cơ quan tổ chức có Mã số thuế, EasyCA sẽ sử dụng Mã số thuế làm Mã định danh. Đối với cơ quan tổ chức nhà nước không có Mã số thuế, EasyCA sẽ sử dụng Mã ngân sách làm Mã định danh.

3.1.2. Tên có ý nghĩa

- Tên trong chứng thư số do EasyCA ban hành cho phép xác định được nhận dạng của đối tượng sở hữu của chứng thư số.

3.1.3. Biệt hiệu hay nặc danh của thuê bao

- Chứng thư số không được sử dụng biệt hiệu hoặc nặc danh cho tên.
- Việc sử dụng biệt hiệu hoặc nặc danh cho tên trong chứng thư số chỉ được thực hiện khi có yêu cầu của pháp luật.

3.1.4. Tính duy nhất của tên

- Tên (DN) của thuê bao là duy nhất trong EasyCA, một thuê bao có thể có nhiều chứng thư số có thể có cùng DN.

3.1.5. Chấp nhận, xác thực và vai trò của các nhãn hiệu (TradeMarks)

- Người gửi đơn xin cấp chứng thư số không được sử dụng những tên vi phạm quyền sở hữu trí tuệ. Nếu có sự tranh chấp xảy ra về sở hữu thì EasyCA sẽ có quyền thu hồi, tạm dừng chứng thư số hay loại bỏ đơn xin cấp chứng thư số mà không phải chịu trách nhiệm pháp lý.

3.2. Xác minh đề nghị cấp chứng thư số lần đầu

3.2.1. Phương thức chứng minh sự sở hữu khóa bí mật

- Người gửi yêu cầu xin cấp chứng thư số phải chứng minh quyền sở hữu khóa bí mật tương ứng với khóa công khai được đề nghị cấp chứng thư số.
- Các phương pháp chứng minh thuê bao thực sự sở hữu khóa riêng:
  - Tệp tin đề nghị cấp chứng thư số EasyCA mã hóa theo chuẩn PKCS#10 sinh từ PKI Smartcard, PKI Token đạt chuẩn FIPS 140-2 Level 2 trở lên, hoặc tương đương do thuê bao thực hiện.
  - Hoặc thuê bao ủy quyền cho EasyCA, EasyCA sinh khóa theo ủy quyền của thuê bảo sử dụng PKI Smartcard, PKI Token đạt chuẩn FIPS 140-2 Level 2 trở lên. Theo quy trình, EasyCA đảm bảo quyền sở hữu khóa riêng của thuê bao và bàn giao an toàn tránh các rủi ro trong quá trình giao nhận.

3.2.2. Xác thực định danh của tổ chức

- Khi có một yêu cầu đăng ký chứng thư số cho tổ chức, thông tin định danh của tổ chức đó được xác minh. EasyCA sẽ xác minh các thông tin bắt buộc sau:
  - Thông tin xác định sự tồn tại của tổ chức, gồm có: tên tổ chức, giấy chứng minh định danh – đăng ký kinh doanh hoặc giấy phép hoạt động, địa chỉ.
  - EasyCA, hoặc các RA của EasyCA thực hiện xác thực định danh của tổ chức theo các thông tin nêu trên.
  - Khi chứng thư số của tổ chức có chứa tên cá nhân làm đại diện, cần thực hiện các thủ tục xác thực sự ủy quyền như 3.2.5.
  - Tên miền hay email chứa trong chứng thư số khi cần xác thực cũng được xác minh về quyền sở hữu của tổ chức với tên miền, email đó. Tên miền được xác thực dựa vào giấy đăng ký tên miền hoặc thông qua cơ sở dữ liệu của nhà cung cấp tên miền. Địa chỉ email được xác thực bằng cách yêu cầu trả lời lại email đã được gửi từ EasyCA.

3.2.3. Xác thực định danh của cá nhân

- Khi có một yêu cầu đăng ký chứng thư số cho cá nhân, thông tin định danh của cá nhân đó được xác minh. EasyCA sẽ xác minh các thông tin bắt buộc sau:
  - EasyCA, hoặc các RA của EasyCA để thực hiện xác thực định danh của cá nhân thông qua một trong các giấy tờ sau: chứng minh thư, hộ chiếu, sơ yếu lý lịch có xác minh của chính quyền.
  - Hồ sơ xin cấp gồm có:

- Đơn xin cấp chứng thư (theo mẫu của EasyCA)
- Giấy tờ xác thực nhận dạng cá nhân
- Các giấy tờ liên quan (nếu có)

- Địa chỉ email khi cần xác thực được xác minh bằng cách yêu cầu trả lời lại email đã được gửi từ EasyCA.
- Quản trị viên của EasyCA cũng phải được cấp chứng thư số, tuy nhiên việc xác thực định danh cá nhân khi cấp chứng thư số không phải thực hiện lại, do đã có xác thực trước khi tham gia quản trị hệ thống.
- Quy trình xác thực định danh của cá nhân đăng ký chứng thư số như sau:
  - Người đăng nộp hồ sơ cho EasyCA/RA.
  - EasyCA/RA xác minh thông tin trên hồ sơ với các thông tin trên Giấy tờ xác thực nhận dạng cá nhân.

3.2.4. Thông tin thuê bao không được kiểm tra

- Thông tin thuê bao không được kiểm tra gồm:
  - Đơn vị nằm trong tổ chức - Organization Unit (OU).
  - Những thông tin khác được chỉ định là không được kiểm tra trong chứng thư số.

3.2.5. Xác thực ủy quyền

- Khi chứng thư số được cấp cho cá nhân của tổ chức hoặc người đại diện của tổ chức, cần thực hiện các thủ tục xác thực ủy quyền, các thủ tục xác thực này bao gồm:
  - Xác thực sự tồn tại của tổ chức như 3.2.2.
  - Xác thực cá nhân như 3.2.3 và xác thực sự ủy quyền của tổ chức đối với cá nhân đó bằng giấy ủy quyền. Trong một số trường hợp cần làm rõ, EasyCA sẽ xác thực bổ sung bằng cách gọi điện hoặc xác thực trực tiếp tại tổ chức về cá nhân đó.

3.3. Xác minh đề nghị thay cặp khóa hoặc gia hạn

3.3.1. Nhận dạng, xác thực yêu cầu thay cặp khóa hoặc gia hạn thông thường

- Khi có đơn yêu cầu thay cặp khóa hoặc gia hạn ít nhất là 30 ngày trước khi chứng thư số hết hạn.

- EasyCA hoặc RA có trách nhiệm xác thực yêu cầu thay cặp khóa hoặc gia hạn sau khi nhận đơn. EasyCA sử dụng một trong hai phương pháp xác thực làm căn cứ để chấp nhận một yêu cầu.
    - Chứng minh quyền sở hữu khóa bí mật: thuê bao sử dụng chứng thư số để đăng nhập vào tài khoản của mình, sau khi đăng nhập thuê bao yêu cầu thay cặp khóa hoặc gia hạn chứng thư số và yêu cầu này ngay lập tức được EasyCA chấp nhận.
    - Sử dụng phương pháp xác thực: Thuê bao phải trả lời đúng toàn bộ các câu hỏi xác thực để được EasyCA chấp nhận yêu cầu.
- Sau khi xác thực, EasyCA ban hành ngay chứng thư số mới cho thuê bao.
- Sau khi ban hành chứng thư số mới cho thuê bao, EasyCA hoặc RA xác minh lại định danh của đối tượng yêu cầu thay cặp khóa hoặc gia hạn chứng thư số và các thông tin liên quan:
    - EasyCA hoặc RA liên lạc với thuê bao hoặc đại diện được ủy quyền nếu là tổ chức thông qua điện thoại, email, thư tín hay các phương tiện khác để khẳng định lại chính thuê bao đã yêu cầu làm mới chứng thư số. EasyCA cũng xác minh lại đối tượng yêu cầu làm mới có phải là thành viên của tổ chức như trong thông tin đăng ký ban đầu hay không.
    - Nếu tên đặc trưng (DN) trong chứng thư số chứa tên miền, EasyCA kiểm tra thông tin tên miền thông qua dữ liệu của các nhà cung cấp tên miền tương ứng.
    - EasyCA kiểm tra lại sự tồn tại của tổ chức thông qua cơ sở dữ liệu của các đơn vị quản lý nhà nước (Cơ quan thuế, Sở Kế hoạch Đầu tư).

3.3.2. Nhận dạng và xác thực yêu cầu thay cặp khóa hoặc gia hạn

- Thuê bao không được phép thay cặp khóa hoặc gia hạn sau khi bị thu hồi nếu lý do thu hồi chứng thư số là một trong các nguyên nhân sau:
    - EasyCA phát hiện ít nhất 1 thông tin cần xác minh trong chứng thư số không đúng.
    - Chứng thư số được sử dụng trong các hoạt động phạm pháp, các hoạt động có thể ảnh hưởng tới uy tín của EasyCA.

3.4. Xác minh đề nghị thu hồi chứng thư số

- Khi có một yêu cầu thu hồi chứng thư số từ thuê bao, EasyCA hoặc RA sẽ tiến

hành xác thực thuê bao gửi yêu cầu thu hồi. Thủ tục xác thực yêu cầu có thể sử dụng một trong hai phương pháp sau:

- Sử dụng chữ ký số: EasyCA nhận một thông điệp từ thuê bao yêu cầu thu hồi chứng thư số, yêu cầu thu hồi này được ký bằng chứng thư số đã được cấp. Nếu chữ ký đúng, chứng thư số sẽ bị thu hồi tự động.
- EasyCA sẽ xác nhận lại yêu cầu thu hồi chứng thư số của khách hàng, qua thông tin liên hệ khách hàng đã cung cấp, khi đăng ký cấp chứng thư số.

- Sau khi xác thực, EasyCA sẽ tiến hành xác thực bổ sung bằng cách liên lạc với đối tượng yêu cầu thu hồi để đảm bảo chắc chắn rằng chính thuê bao đã yêu cầu thu hồi chứng thư số. Tùy từng hoàn cảnh, việc liên lạc này có thể thông qua điện thoại, email, thư tín hay thông qua các phương tiện truyền thông.
- RA sử dụng hệ thống quản lý chứng thư số có thể đệ trình nhiều yêu cầu thu hồi tới EasyCA một lúc. Mỗi yêu cầu sẽ được xác thực thông qua chữ ký số của RA.

4. Các yêu cầu đối với vòng đời hoạt động của chứng thư số thuê bao EasyCA

4.1. Yêu cầu cấp chứng thư số

4.1.1. Hồ sơ cấp chứng thư số của thuê bao

- Đơn cấp chứng thư số theo mẫu của EasyCA.
- Giấy tờ kèm theo bao gồm:
  - Đối với cá nhân: Chứng minh nhân dân hoặc căn cước công dân hoặc hộ chiếu;
  - Đối với tổ chức: Quyết định thành lập hoặc quyết định quy định về chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức hoặc giấy chứng nhận đăng ký doanh nghiệp hoặc giấy chứng nhận đầu tư; chứng minh nhân dân, hoặc căn cước công dân hoặc hộ chiếu của người đại diện theo pháp luật của tổ chức.
- Cá nhân, tổ chức có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc nộp bản sao xuất trình kèm bản chính để đối chiếu.

4.1.2. Ai có thể gửi đăng ký cấp chứng thư số

- Đại diện của các RA/CA của EasyCA.
- Bất cứ cá nhân, tổ chức đều có quyền đăng ký yêu cầu EasyCA cung cấp dich vụ.

4.1.3. Quy trình đăng ký và trách nhiệm của các bên

- Chứng thư số của RA
  - Để đăng ký cấp chứng thư số từ EasyCA, RA phải thực hiện việc ký hợp đồng với EasyCA và tiến hành các thủ tục đăng ký cấp chứng thư số tương tự như các thuê bao.
  - EasyCA sẽ tổ chức nghi lễ sinh khóa cho RA.
  - Trách nhiệm của RA được làm rõ trong phần 9.6.2.
- Chứng thư số của thuê bao cá nhân, tổ chức
  - Thuê bao làm thủ tục và ký một thỏa thuận với EasyCA, các điều khoản và cam kết trong thỏa thuận được mô tả trong phần 9.6.3.
  - Thuê bao có thể lựa chọn một trong 2 hình thức sau:
    - Tạo khóa phía EasyCA: Thuê bao hoàn thành đơn đăng ký chứng thư số và cung cấp tài liệu xác minh thông tin đã kê khai.
    - Tạo khóa phía thuê bao: thuê bao đăng ký thực hiện các bước sau:
      - Thuê bao hoàn thành đơn đăng ký chứng thư số và cung cấp tài liệu xác minh thông tin đã kê khai.
      - Tạo hoặc chuẩn bị cặp khóa
      - Gửi khóa công khai trực tiếp cho EasyCA hoặc thông qua RA
      - Chứng minh quyền sở hữu và tính duy nhất của khóa bí mật tương ứng với khóa công khai vừa gửi theo 3.2.1.

4.2. Xử yêu cầu cấp chứng thư số EasyCA

4.2.1. Nhận dạng và xác thực

- EasyCA/RA sẽ thực hiện nhận dạng và xác thực mọi thông tin trong yêu cầu cấp chứng thư số được chỉ rõ trong phần 3.2.

4.2.2. Duyệt hoặc từ chối đăng ký cấp chứng thư số

- EasyCA/RA chấp nhận một đơn đăng ký nếu các điều kiện sau đây thỏa mãn:
  - Mọi thông tin cần được định danh và xác thực đúng theo quy định tại mục 3.2.
  - Người đăng ký thanh toán các khoản phí cần thiết theo quy định chính sách dịch vụ.
- EasyCA/RA từ chối đơn đăng ký nếu:

- Một trong các thông tin cần được đinh danh và xác thực sai.
- Người đăng ký không cung cấp hồ sơ theo yêu cầu.
- Chứng thư số có khả năng được sử dụng trong các hoạt động phạm pháp và các hoạt động có thể ảnh hưởng tới uy tín của EasyCA.
- EasyCA/CA chưa nhận được đầy đủ phí từ người đăng ký

4.2.3. Thời gian xử lý đăng ký cấp chứng thư số EasyCA

- Trong vòng 3 ngày làm việc EasyCA sẽ trả lời về việc chấp nhận đơn yêu cầu cấp chứng thư số và phát hành chứng thư số EasyCA.
- Trong một số tình huống phức tạp, đặc biệt, thời gian xử lý một yêu cầu cấp chứng thư số được quy định trong bản thỏa thuận giữa thuê bao với EasyCA.

4.3. Cấp chứng thư số EasyCA

4.3.1. Quy trình phát hành chứng thư số EasyCA

- Tiếp nhận yêu cầu: Bộ phận thẩm định tiếp nhận đăng ký và yêu cầu cấp chứng thư số từ thuê bao, RA. Xác nhận với khách hàng gói đăng ký, tình trạng bảo hiểm và thời gian đăng ký chứng thư số...
- Thẩm định: Bộ phận thẩm định tiến hành kiểm tra xác nhận thông tin hồ sơ theo quy định và chuyển yêu cầu cấp đến bộ phận cấp.
- Cấp chứng thư số: Bộ phận cấp chứng thư số tiến hành cấp, quản lý chứng thư số và cập nhật cơ sở dữ liệu ngay khi có phát sinh từ hệ thống.
- Thông báo: Bộ phận thẩm định thông báo với khách hàng. Khách hàng xác nhận thông tin chứng thư số đã được cấp theo biểu mẫu xác nhận EasyCA ban hành.
- Bàn giao và công bố: Bộ phận thẩm định, bộ phận cấp tiến hành làm thủ tục bàn giao chứng thư số và công bố trên https://directory.easyca.vn. Sau đó, lưu trữ chứng thư số và hồ sơ.
- Đối soát & thanh toán: Bộ phận đối soát đảm bảo việc phát sinh từ hệ thống được xác nhận bởi các cá nhân, các bộ phận nghiệp vụ có liên quan và chuyển qua bộ phận kế toán làm thủ tục thanh toán.
- Đối soát số Serial phát sinh và yêu cầu cấp CTS từ khách hàng hàng ngày.
- Chi tiết quy trình kỹ thuật cấp chứng thư số:
  - B1: Thuê bao/RA cắm USB Token vào máy, mở hệ thống RA lên, đăng nhập vào hệ thống sử dụng chứng thư số, hoặc Username/Password với thuê bao,

hệ thống sẽ xác thực đúng quyền đăng nhập và USB Token được cấp.

- B2: Thuê bao/RA yêu cầu cấp chứng thư số trên hệ thống RA.
- B3: Hệ thống RA sẽ kết nối với USB Token qua Token Tool để yêu cầu sinh cặp khóa trong thiết bị USB Token đảm bảo tính bảo mật và toàn vẹn vì cặp khóa được sinh trong thiết bị nên khóa bí mật chỉ tồn tại trong thiết bị không thể lấy ra.
- B4: Hệ thống RA sẽ đóng gói yêu cầu cấp chứng thư số bao gồm: thông tin chủ thể, khóa công khai, các thuộc tính yêu cầu của chứng thư số. RA gửi dữ liệu yêu cầu đến USB Token để ký tạo ra yêu cầu cấp chứng thư số chuẩn dưới dạng PKCS#10 và gửi đến hệ thống RA.
- B5: RA sẽ phê duyệt yêu cầu và gửi yêu cầu đến EasyCA.
- B6: EasyCA đăng nhập hệ thống EasyCA sử dụng USB Token chứa chữ ký số với quyền đăng nhập, kiểm tra yêu cầu cấp, so sánh với các thông tin được xác thực, xác thực khóa bí mật của thuê bao yêu cầu cấp chứng thư số, EasyCA sẽ phê duyệt yêu cầu cấp.
- B7: Hệ thống EasyCA tạo dữ liệu chứng thư số dưới dạng chuẩn X509 v3. Hệ thống EasyCA gửi yêu cầu ký chứng thư số tới HSM, HSM sẽ thực hiện ký chứng thư số cho thuê bao tạo ra chứng số chuẩn X509.
- B8: Hệ thống EasyCA sẽ lưu trữ vào cơ sở dữ liệu của EasyCA các thông tin của thuê bao: Hồ sơ thông tin thuê bao; Request yêu cầu cấp phát chứng thư PKCS#10; Chứng thư số của thuê bao. Hệ thống cập nhật dữ liệu chứng thư số vào Master LDAP. Hệ thống cập nhật trạng thái chứng thư số vừa được cấp phát vào Database OCSP của EasyCA.
- B9: Gửi chứng thư số lại cho RA.
- B10: Hệ thống RA tiến hành cài đặt chứng thư số vào trong Token cho thuê bao.

4.3.2. Thông báo cho thuê bao EasyCA

- EasyCA sau khi phát hành chứng thư số:
  - B1: EasyCA sẽ tiến hành phân phối khóa cho thuê bao.
  - B2: Thuê bao xác nhận đúng tính chính xác thông tin trên chứng thư số của thuê bao, ký biên bản bàn giao và nghiệm thu.
  - B3: EasyCA sinh mã PIN cho token ngẫu nhiên theo tiêu chuẩn tối thiểu 8 ký

tự (bao gồm chữ hoa, chữ hường, số, và ký tự đặc biệt). EasyCA gửi mã PIN qua Email hoặc SMS để kích hoạt thuê bao.

- B4: Hệ thống EasyCA sẽ công bố trên kênh LDAP và được công khai trên địa chỉ https://directory.easyca.vn.

4.4. Xác nhận và công bố công khai chứng thư số

4.4.1. Cách thức thể hiện sự chấp nhận một chứng thư số của thuê bao

- Thuê bao thể hiện sự chấp nhận một chứng thư số khi ký vào biên bản giao nhận chứng thư số của EasyCA. Biên bản giao nhận có sự xác nhận thông tin trên chứng thư số phù hợp với thông tin thuê bao. Biên bản giao nhận này được EasyCA lưu trữ.

4.4.2. EasyCA công bố chứng thư số

- Sau khi thuê bao chấp nhận chứng thư số (4.4.1), EasyCA sẽ công bố chứng thư số khi thuê bao sử dụng USB Token lần đầu tiên.
- Chứng thư số sau khi được ban hành sẽ được công bố trên Web của EasyCA và cơ sở dữ liệu LDAP.

4.4.3. Thông báo việc phát hành chứng thư số cho đối tượng khác

- EasyCA thông báo việc cấp phát Chứng thư số thuê bao đến các tổ chức, cá nhân khác được thực hiện bằng cách công bố chứng thư số thuê bao trên hệ thống danh bạ trực tuyến về chứng thư số của EasyCA và trên giấy chứng nhận do EasyCA cấp cho thuê bao.

4.5. Sử dụng cặp khóa và chứng thư số

4.5.1. Sử dụng của khóa bí mật và chứng thư số của thuê bao

- Chứng thư số và khóa bí mật tương ứng được phép sử dụng nếu thuê bao đã đồng ý thỏa thuận với EasyCA và đã chấp nhận chứng thư số được ban hành.
- Chứng thư số cần được sử dụng hợp pháp, phù hợp với thỏa thuận với EasyCA, với các điều khoản của quy chế chứng thực của EasyCA. Mục đích sử dụng chứng thư số phải nhất quán với phạm vi sử dụng được phép của chứng thư số đó.
- Các thuê bao có trách nhiệm bảo vệ khóa bí mật của mình, không được sử dụng khóa bí mật nếu chứng thư số tương ứng hết hạn hay bị thu hồi.

4.5.2. Sử dụng chứng thư số và khóa công khai với bên nhận

- Khi đồng ý sử dụng chứng thư số và khóa công khai của EasyCA tức là bên nhận đã đồng ý với các điều khoản áp dụng cho bên nhận.
- Người nhận dựa vào các thông tin sau để xác thực sự tin cậy của chứng thư số:
  - Mục đích sử dụng của chứng thư số thể hiện trên chứng thư số.
  - Trạng thái của chứng thư số: kiểm tra trạng thái thu hồi của chứng thư số cũng như các chứng thư số khác trong chuỗi chứng thư số.
  - Chữ ký số: kiểm tra chữ ký số có hợp lệ hay không hợp lệ, tức là dữ liệu và thời gian trong tài liệu được ký có khớp với chữ ký số đã được tạo ra.

4.6. Gia hạn chứng thư số

- Gia hạn chứng thư số là quá trình ban hành một chứng thư số mới cho thuê bao mà ngoài thời hạn sử dụng chứng thư số, mọi thông tin khác trong chứng thư số đều không thay đổi.

4.6.1. Các tình huống gia hạn chứng thư số

- Trước khi hết hạn ít nhất 30 ngày, thuê bao cần phải gia hạn chứng thư số để duy trì sử dụng chứng thư số.

4.6.2. Ai có thể yêu cầu gia hạn chứng thư số

- Chỉ có thuê bao có quyền yêu cầu gia hạn chứng thư số đó.

4.6.3. Xử lý yêu cầu gia hạn chứng thư số

- EasyCA/RA tiến hành xác minh yêu cầu gia hạn chứng thư số như trong phần 3.3.
- Nếu thông tin thuê bao không thay đổi, chứng thư số mới của thuê bao sẽ được ban hành ngay sau khi EasyCA nhận được yêu cầu mà không cần có sự hiện diện vật lý của thuê bao tại EasyCA hoặc RA.

4.6.4. Thông báo sự tạo chứng thư số mới cho thuê bao

- Thông báo về việc ban hành chứng thư số mới khi gia hạn cho thuê bao cũng giống như thông báo khi chứng thư số được cấp mới 4.3.2.

4.6.5. Chấp nhận chứng thư số mới gia hạn

- Tương tự phần 4.4.1.

4.6.6. Công bố chứng thư số mới được gia hạn bởi CA

- Tương tự phần 4.4.2.

4.6.7. Thông báo phát hành chứng thư số mới cho các đối tượng khác

- Tương tự phần 4.4.3.

4.7. Thay đổi khóa của thuê bao

- Thuê bao có đơn xin thay đổi khóa chứng thư số.
- RA/EasyCA thẩm định và cấp chứng thư số mới chứng thực khóa công khai thay đổi.
- Đổi khóa hỗ trợ cho mọi loại chứng thư số.

4.7.1. Các trường hợp thay đổi khóa

- Trong trường hợp thuê bao nghi ngờ khóa bí mật bị lộ.
- Khi gia hạn chứng thư số, thuê bao mong muốn thay đổi cặp khóa.

4.7.2. Ai có thể yêu cầu đổi khóa

- Chỉ có thuê bao mới có quyền yêu cầu thay đổi khóa.

4.7.3. Xử lý yêu cầu đổi khóa

- EasyCA/RA tiến hành xác minh yêu cầu đổi khóa chứng thư số như trong phần 3.3.
- Nếu thông tin thuê bao không thay đổi, chứng thư số mới của thuê bao sẽ được ban hành ngay sau khi EasyCA nhận được yêu cầu mà không cần có sự hiện diện vật lý của thuê bao tại EasyCA hoặc RA.

4.7.4. Thông báo việc phát hành chứng thư số mới cho thuê bao

- Thông báo về việc phát hành chứng thư số mới cho thuê bao giống mô tả trong phần 4.3.2

4.7.5. Chấp nhận chứng thư số đổi khóa

- Tương tự phần 4.4.1

4.7.6. Công bố chứng thư số đổi khóa bởi CA

- Tương tự phần 4.4.2.

4.7.7. Thông báo phát hành chứng thư số cho các đối tượng khác

- Tương tự phần 4.4.3.

4.8. Thay đổi thông tin khác của chứng thư số

4.8.1. Các trường hợp thay đổi thông tin khác của chứng thư số

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

4.8.2. Ai có thể yêu cầu thay đổi chứng thư số

- Xem phần 4.1

4.8.3. Xử lý yêu cầu thay đổi chứng thư số

- EasyCA hoặc RA sẽ thực hiện nhận dạng và xác thực mọi thông tin thuê bao được yêu cầu trong phần 3.2.

4.8.4. Thông báo chứng thư số mới cho CA

- Xem phần 4.3.2

4.8.5. Chấp nhận chứng thư số mới được thay đổi

- Xem phần 4.4.1

4.8.6. Công bố chứng thư số mới thay đổi bởi CA

- Xem phần 4.4.2

4.8.7. Thông báo cho các đối tượng khác

- Xem phần 4.4.3

4.9. Tạm dừng và thu hồi chứng thư số

4.9.1. Các trường hợp thu hồi chứng thư số

- Yêu cầu thu hồi chứng thư số sẽ được xử lý khi thuê bao hay các đối tượng có thẩm quyền (EasyCA, RA) yêu cầu. Nếu chứng thư số bị thu hồi, thông tin chứng thư số bị thu hồi sẽ được công bố lên danh sách chứng thư số bị thu hồi (CRL) và OCSP. Khi nhận yêu cầu thu hồi từ một thuê bao cho chứng thư số của mình, EasyCA sẽ thu hồi chứng thư số sau khi xác minh.
- Chứng thư số bị thu hồi trong những trường hợp sau:
    - Khóa bí mật của thuê bao có chứng thư số bị lộ.

- Thỏa thuận với thuê bao kết thúc trước thời hạn.
- Thông tin trong chứng thư số sai khác so với thực tế.
- Thuê bao vi phạm thỏa thuận đã ký với EasyCA.
- Chứng thư số có tên mạo danh hoặc vi phạm quyền sỡ hữu trí tuệ.
- Người được cấp chứng thư số đại diện cho tổ chức không còn làm việc trong tổ chức đó nữa.
- Chứng thư số đã được tạo ra không tuân theo những thủ tục được yêu cầu bởi quy chế chứng thực này.
- Chứng thư số được sử dụng sai mục đích, với mục đích bị cấm hoặc với các mục đích làm mất uy tín EasyCA.
- Khi có yêu cầu của cơ quan quản lý nhà nước, các cơ quan thực thi pháp luật.
- EasyCA sẽ thu hồi một chứng thư số của quản trị viên khi kết thúc nhiệm vụ.

- Khi khóa bí mật của thuê bao bị mất/lộ hoặc nghi ngờ bị mất/lộ, thuê bao phải báo ngay lập tức cho EasyCA.
- Khi EasyCA/Thuê bao xác định khóa thuê bao bị lộ thì EasyCA sẽ thực hiện:
  - Xác minh với thuê bao về việc lộ khóa.
  - Thu hồi chứng thư số của thuê bao.
  - Kiểm tra xác minh ảnh hưởng đến các thuê bao khác (nếu có).

4.9.2. Ai có thể yêu cầu thu hồi chứng thư số

- Đối với chứng thư số của thuê bao:
  - Thuê bao đăng ký chứng thư số có quyền yêu cầu thu hồi chứng thư số.
  - EasyCA/RA có quyền yêu cầu thu hồi chứng thư số mà nó đã duyệt cho thuê bao đó.
- Các cơ quan quản lý nhà nước, các cơ quan thực thi pháp luật có thẩm quyền.

4.9.3. Thủ tục thu hồi chứng thư số

- Trước khi thu hồi chứng thư số, EasyCA xác thực yêu cầu thu hồi:
  - Từ thuê bao qua thông điệp ký số yêu cầu thu hổi, hoặc các bộ câu hỏi, Email, điện thoại.
  - Từ RA.
  - Từ các cơ quan quản lý nhà nước hoặc các cơ quan thực thi pháp luật.

- RA sử dụng hệ thống quản lý chứng thư số để chuyển các yêu cầu thu hồi tới EasyCA.
- EasyCA tiến hành thu hồi chứng thư số.
- EasyCA tiến hành cập nhật trang thái chứng thư số vào các cơ sở dữ liệu xác thực trực tuyến như CRL trong ngày và OCSP ngay lập tức.

4.9.4. Thời gian ân hạn yêu cầu thu hồi

- Thuê bao sẽ gửi yêu cầu thu hồi chứng thư số ngay lập tức khi phát hiện hay nghi ngờ khóa bí mật bị mất/lộ.
- Các cơ quan quản lý nhà nước hoặc các cơ quan thực thi pháp luật gửi sớm nhất yêu cầu.
- Quản trị hệ thống EasyCA/RA sẽ gửi yêu cầu thu hồi chứng thư số ngay khi nhận được yêu cầu.

4.9.5. Khoảng thời gian EasyCA phải xử lý yêu cầu thu hồi

- Tạm dừng chứng thư số đó ngay khi có yêu cầu thu hồi.
- EasyCA sẽ tiến hành thu hồi ngay sau khi thẩm tra xong yêu cầu thu hối.
- Cập nhật trạng thái thu hồi vào cơ sở dữ liệu trực tuyến phục vụ xác thực như CRL trong ngày và OCSP ngay lập tức.

4.9.6. Kiểm tra trạng thái thu hồi

- Người nhận sẽ kiểm tra thông tin trạng thái chứng thư số, thông qua CRL hoặc OCSP.
- EasyCA duy trì và công bố địa chỉ lưu trữ cho phép người nhận truy nhập các thông tin về trạng thái và các thông tin khác của chứng thư số như 2.2

4.9.7. Tần suất phát hành CRL

- CRL được phát hành hàng ngày và được phát hành ngay khi có phát sinh thu hồi chứng thư số của thuê bao bất kỳ.

4.9.8. Độ trễ tối đa cho CRL

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

4.9.9. Tính sẵn sàng kiểm tra trạng thái chứng thư số trực tuyến

- Chứng thư số và thông tin liên quan đến xác thực chứng thư số được cung cấp trừng tuyến 24/7 bằng các kênh danh bạ chứng thư số trực tuyến

https://easyca.vn, danh sách thu thồi CRL, giao thức kiểm tra trực tuyến về trạng thái chứng thư số OCSP.

4.9.10. Yêu cầu kiểm tra trạng thái thu hồi trực tuyến

- Khi nhận được thông điệp có ký số của thuê bao EasyCA, người nhận phải kiểm tra trạng thái của một chứng thư số nếu muốn tin tưởng.
- Việc kiểm tra trạng thái chứng thư số được thực hiện thông qua kênh xác thực trực tuyến OCSP Responder của EasyCA được gắn vào hầu hết các ứng dụng đọc dữ liệu phổ biến như PDF, Email, … hoặc bằng phát triển ứng dụng.

4.9.11. Các dạng thông tin trạng thái thu hồi khác

- EasyCA không có quy định.

4.9.12. Yêu cầu đặc biệt khi khóa bị mất hoặc lộ

- Lập tức báo cho EasyCA về việc bị mất/lộ hoặc nghi ngờ mất/lộ khóa.
- Tạm dừng chứng thư số cho tới khi kết quả được xác minh.
- EasyCA sẽ nỗ lực cao nhất để thông báo tới các bên.

4.9.13. Các trường hợp tạm dừng chứng thư số

- Khi thuê bao yêu cầu.
- Các cơ quan quản lý nhà nước, cơ quan thực thi pháp luật yêu cầu.
- EasyCA đang xử lý việc thu hồi chứng thư số.

4.9.14. Ai có thể yêu cầu tạm dừng chứng thư số

- Thuê bao.
- EasyCA/RA
- Các cơ quan quản lý nhà nước, các cơ quan thực thi pháp luật.

4.9.15. Thủ tục tạm dừng chứng thư số

- EasyCA sẽ quyết định tạm dừng khi nhận được các yêu cầu chính xác tư thuê bao, các cơ quan quản lý nhà nước, các cơ quan thực thi pháp luật về việc tạp dừng hoặc thu hồi.

4.9.16. Giới hạn thời gian xử lý tạm dừng chứng thư số

- Ngay sau khi kết thúc thẩm định yêu cầu thu hồi.

4.10. Kiểm tra trạng thái chứng thư số

4.10.1. Đặc điểm

- Kiểm tra trạng thái chứng thư số qua danh sách thu hồi CRL được công bố trên Website.
- Kiểm tra bằng việc tìm kiếm thông tin chứng thư số qua danh bạ chứng thứ số và CRL trong LDAP
- Kiểm tra trạng thái chứng thư số qua giao thức trực tuyến OCSP.

4.10.2. Tính sẵn sàng của dịch vụ

- Dịch vụ trạng thái chứng thư số được duy trì 24/7.

4.10.3. Tùy chọn đặc biệt

- OCSP là dịch vụ tùy chọn, vì không phải ứng dụng nào cũng có sẵn tình năng OCSP để hỗ trợ việc từ động xác thực trạng thái chứng thư số trực tuyến.

4.11. Chấm dứt dịch vụ của thuê bao

- Kết thúc thuê bao chứng thư số có hiệu lực trong các trường hợp sau:
    - Thuê bao đã hết hạn mà không làm mới.
    - Thu hồi chứng thư số xẩy ra mà không xin cấp một chứng thư số mới.
    - Hủy hợp đồng thuê bao.

4.12. Lưu trữ và phục hồi khóa

- EasyCA không có quy định.

4.12.1. Chính sách và thủ tục lưu trữ và phục hồi khóa

- EasyCA không có quy định.

4.12.2. Chính sách và thủ tục đóng gói và phục hồi khóa phiên

- EasyCA không có quy định.

5. Kiểm soát, quản lý, vận hành

5.1. Kiểm soát an toàn, an ninh vật lý

5.1.1. Vị trí đặt và xây dựng hệ thống

- Hệ thống thiết bị EasyCA được đặt tại trung tâm dữ liệu của hai nơi của nhà cung cấp dịch vụ IDC là VNPT và Viettel đáp ứng tiêu chuẩn Tier 3:
    - VNPT tại Lô B2-1-6, Khu công nghiệp Nam Thăng Long, quận Bắc Từ

Liêm, TP Hà Nội

- Viettel tại Khu công nghệ cao Láng Hòa Lạc - Km29 Đại lộ Thăng Long - Thạch Thất - Hà Nội

- Mỗi địa điểm đặt thiết bị được trang bị nhiều lớp bảo vệ khác nhau: bảo vệ vật lý vòng ngoài của tòa nhà, bảo vệ khu đặt thiết bị, bảo vệ tủ đặt thiết bị, bảo vệ chống cháy nổ.

5.1.2. Truy cập vật lý

- Hệ thống EasyCA được đặt trong Datacenter tiêu chuẩn Tier 3 nên đáp ứng được các yêu cầu bảo vệ bởi các lớp an ninh vật lý, phải vượt qua được lớp bảo vệ thấp trước khi có thể tiếp cận được lớp bảo vệ cao hơn. Hệ thống camera giám sát hoạt động 24/7 cho phép ghi lại toàn bộ các hoạt động.
  - Lớp bảo vệ vòng ngoài - bảo vệ tòa nhà
  - Lớp bảo vệ khu đặt thiết bị
- Việc truy nhập qua các lớp được kiểm soát chặt chẽ, chỉ những người có quyền truy cập mới được truy nhập vào các lớp tương ứng. Càng truy nhập vào các lớp quản lý yêu cầu an ninh cao, sự hạn chế càng tăng.
- Tất cả mọi truy nhập đều được ghi nhận.

5.1.3. Điều kiện về nguồn điện và không khí

- Hệ thống EasyCA được đặt tại Hạ tầng đáp ứng tiêu chuẩn Tier 3 nên đáp ứng các tiêu chuẩn:
  - Nguồn điện dự phòng.
  - Điều khiển vi xử lý tốc độ quạt và giám sát bộ lọc khí.
  - Kiểm soát nhiệt độ chính xác (+/-1oC)
  - Kiểm soát độ ẩm chính xác (+/-5%)

5.1.4. Chống nước

- Hệ thống thiết bị của EasyCA được đặt tại hạ tầng đáp ứng tiêu chuẩn Tier3 đảm bảo khả năng chống ngập lụt và mưa bão, trong phòng hệ thống còn được giám sát độ ẩm chính xác
- Toàn bộ hệ thống thiết bị đặt trong tủ Rack công nghiệp nên không có khả năng tiếp xúc nước.

5.1.5. Phòng cháy chữa cháy

- Hệ thống EasyCA được đặt trong Datacenter đạt tiêu chuẩn Tier 3 nên đảm bảo quản lý chặt chẽ về nguy cơ cháy nổ: Hệ thống giám sát chặt chẽ nhiệt độ, không khí, độ ẩm, hệ thống chữa cháy tự động.
- Hệ thống EasyCA cũng được đặt tại hai nơi DC ở VNPT và DR ở Viettel ở Hà Nội để đảm bảo khi có thảm họa dẫn đến cháy nổ thì hệ thống có phương án dự phòng.

5.1.6. Phương tiện lưu trữ

- Hệ thống lưu trữ dữ liệu, kiểm toán, sao lưu, dự phòng được đặt tại hai nơi là hai Datacenter của VNPT và Viettel ở Hà Nội.
- Hệ thống lưu trữ được thiết kế đảm bảo truy xuất ở mức phần mềm và phần cứng nhằm bảo vệ phương tiện lưu trữ với các rủi ro từ các sự cố hỏng vật lý, do nước, lửa, điện và điện từ trường.

5.1.7. Xử lý rác thải

- Các thiết bị và tài liệu nhạy cảm phải được xử lý trước khi bỏ đi.
- Các phương pháp phá hủy đảm bảo theo tiêu chuẩn nhà sản xuất trước khi vứt rác và đảm bảo thông tin trên rác thải không thể đọc bằng mọi phương pháp.

5.1.8. Hệ thống dự phòng cách lý

- Hệ thống EasyCA được thiết kế các trung tâm DC và DR được đặt tại hai nơi khác nhau đảm bảo cách lý và dự phòng rủi ro:
    - Hệ thống EasyCA DC được đặt tại Datacenter của VNPT: Lô B2-1-6, Khu công nghiệp Nam Thăng Long, quận Bắc Từ Liêm, TP Hà Nội.
    - Hệ thống EasyCA DR được đặt tại Datacenter của Viettel: Tòa nhà Viettel IDC Hòa Lạc, Khu công nghệ cao Hòa Lạc, Km 29 Đại lộ Thăng, Thạch Thất, Hà Nội

5.2. Các quy trình kiểm soát

5.2.1. Những vai trò được tin tưởng

- Các công việc cần phải có những những người tin tưởng để thực hiện:
    - Quản trị vận hành, khai thác hệ thống hạ tầng phần cứng, mạng máy tính của hệ thống EasyCA.
    - Xác minh các thông tin trong đơn xin cấp chứng thư số.
    - Chấp nhận, loại bỏ, hay các xử lý khác đối với đơn xin cấp chứng thư số, yêu cầu thu hồi, làm mới, hay thông tin đăng ký.

- Phát hành, thu hồi chứng thư số.
- Quản lý và vận hành thiết bị HSM.
- Quản lý thông tin thuê bao, thông tin yêu cầu từ thuê bao.

- Người được tin tưởng bao gồm:
  - Người đứng đầu hệ thống EasyCA.
  - Người quản lý vận hành hạ tầng phần cứng và thiết bị mạng EasyCA.
  - Những người quản trị hệ thống phần mềm trong hệ thống EasyCA.
  - Những người quản lý cấp phát, thu hồi, phát hành chứng thư, CRL.
  - Những người quản lý vận hành thiết bị HSM.
- Những người được tin tưởng đều được xác minh về nhân thân, khả năng đảm bảo đáp ứng yêu cầu công việc trước khi được giao nhiệm vụ.

5.2.2. Số lượng người được yêu cầu cho một nhiệm vụ

- EasyCA thiết lập các chính sách và thủ tục kiểm soát đảm bảo có nhiều người tin tưởng thực hiện một nhiệm vụ.
- Những chức năng nhiệm vụ sau bố trí tối thiểu hai cán bộ tin tưởng tham gia:
  - Quản trị vận hành hệ thống phần cứng và thiết bị mạng EasyCA.
  - Quản trị hệ thống phần mềm trong hệ thống EasyCA.
  - Cấp phát, thu hồi, phát hành chứng thư, CRL.
  - Quản lý vận hành thiết bị HSM.

5.2.3. Nhận dạng và xác thực trong mỗi vai trò

- Mọi cá nhân trước khi trở thành người được tin tưởng trong hệ thống EasyCA đề phải được xác minh nhân thân, nhận dạng và trình độ. Quá trình nhận dạng được trình bày trong phần 5.3.1.
- EasyCA đảm bảo rằng các cá nhân hoàn toàn được tin tưởng trước khi thực hiện các công việc nhạy cảm.
- EasyCA sẽ cấp các thẻ xác thực cho các vị trí tham gia hệ thống khác nhau

5.2.4. Những vai trò yêu cầu phân tách nhiệm vụ

- Các vai trò cần phải có sự phân tách nhiệm vụ:
  - Thẩm định yêu cầu cấp, thu hồi, gia hạn chứng thư số.

- Cấp, phát hành, thu hồi chứng thư số.
- Vận hành khai thác hệ thống phần mềm, hạ tầng, thiết bị mạng, HSM.
- Quản lý thông tin thuê bao.

5.3. Kiểm soát nhân sự

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

- Những người tin cậy của EasyCA được xác minh dựa trên:
  - Trình độ chuyên môn.
  - Kinh nghiệm phù hợp.
  - Lý lịch tốt.

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

- Trước khi bổ nhiệm nhân viên vào một nhiệm vụ cần được tin tưởng, EasyCA kiểm tra các thông tin sau:
  - Kiểm tra, xác minh thông tin theo sơ yếu lý lịch, thông tin tiền án/tiền sự (nếu có).
  - Xác minh trình độ học vấn cao nhất đạt được.
  - Xem xét các kinh nghiệm.

5.3.3. Yêu cầu đào tạo

- Chương trình đào tạo của EasyCA hướng tới trách nhiệm cụ thể của mỗi nhân viên, nội dụng đào tạo bao gồm:
  - Cơ sở pháp lý về dịch vụ chứng thực chữ ký số công cộng.
  - Trách nhiệm công việc.
  - Hiểu biết về cơ sở hạ tầng mã khóa công khai PKI.
  - Quy chế, chính sách, an ninh EasyCA.
  - Sử dụng và vận hành các thiết bị phần cứng và phần mềm.
  - Xử lý và báo cáo các sự cố.
  - Các thủ tục duy trì tính liên tục của dịch vụ khi có thảm họa.
  - Báo cáo về nguy cơ lộ khóa.

5.3.4. Tần suất đào tạo và đào tạo lại

- Tổ chức đào tạo cho các cán bộ mới, khi cập nhật, nâng cấp hệ thống.
- EasyCA duy trì và thực hiện chương trình đào tạo với tần suất đào tạo và thời gian đào tạo lại đảm bảo các nhân viên đều thành thạo và thực hiện tốt công việc được giao.
- Tổ chức đào tạo khi có khuyến nghị của kiểm tra kiểm toán.

5.3.5. Tần suất và trình tự luân chuyển công việc

- EasyCA không có quy định.

5.3.6. Xử phạt đối với các hành động trái phép

- EasyCA thực hiện các hình thức kỷ luật các nhân viên có những hành động không được phép, vi phạm các chính sách, thủ tục của EasyCA.
- Hình thức kỷ luật có thể gồm khiển trách, đình chỉ công việc tạm thời hoặc cho thôi việc, khởi kiện ra tòa tùy thuộc vào mức độ nghiêm trọng của vi phạm.

5.3.7. Yêu cầu nhà thầu độc lập

- EasyCA không có quy định.

5.3.8. Cung cấp tài liệu cho nhân viên

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

5.4. Các quy trình ghi nhật ký hệ thống

5.4.1. Các loại sự kiện được ghi lại

- EasyCA ghi nhật ký (log) các sự kiện sau, việc ghi log được thực hiện tự động hay và thủ công tùy vào từng trường hợp:
  - Các sự kiện vòng đời chứng thư số:
    - Đăng ký, làm mới, đổi khóa, thay đổi, và thu hồi chứng thư số.
    - Kết quả khi xử lý những yêu cầu.
    - Tạo khóa và phát hành chứng thư số, CRL.
  - Các sự kiện liên quan đến an ninh:
    - Hoạt động vận hành HSM.
    - Truy cập hệ thống (thành công/không thành công).

- Hành động đọc, ghi hoặc xóa các file, bản ghi an ninh nhạy cảm.
- Hồ sơ an ninh bị thay đổi
- Sự cố hệ thống và những hiện tượng bất thường.
- Hoạt động của tường lửa, router.
- Thiết bị giám sát vào ra.
- Các sự kiện sao lưu, dự phòng, phục hồi.

- RA ghi lại các thông tin đăng ký bao gồm:
  - Loại tài liệu nhận dạng được người đăng ký đưa ra.
  - Thông tin định danh như: số chứng minh thư, số hộ chiếu…
  - Nơi lưu trữ các bản sao đơn đăng ký và tài liệu nhận dạng.
  - Tên RA tiếp nhận đơn.
- Mỗi bản ghi nhật ký gồm các thông tin sau:
  - Thời gian của bản ghi
  - Thứ tự của bản ghi (đối với bản ghi được tạo tự động).
  - Đối tượng tạo ra bản ghi
  - Loại bản ghi

5.4.2. Tần suất xử lý nhật ký

- Nhật ký kiểm tra được kiểm tra, xử lý hàng ngày, tuần, tháng, năm và khi có sự kiện không bình thường xảy ra.

5.4.3. Thời hạn giữ lại các nhật ký kiểm toán

- Nhật ký sẽ được giữ tại hệ thống ít nhất 3 tháng sau khi xử lý và sau đó được chuyển sang khu vực lưu trữ (phần 5.5.2).
- Các bản ghi kiểm toán được lưu trữ trong vòng 5 năm.

5.4.4. Bảo vệ các nhật ký kiểm toán

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

5.4.5. Các thủ tục dự phòng nhật ký kiểm toán

- EasyCA sẽ tiến hành sao lưu gia tăng hàng ngày các bản ghi kiểm toán và thực hiện các bản sao lưu dự phòng đầy đủ hàng tuần.

5.4.6. Hệ thống thu thập nhật ký (Bên trong và bên ngoài)

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

5.4.7. Thông báo cho đối tượng gây ra sự kiện

- Khi một sự kiện được ghi nhật ký, không có thông báo cho đối tượng gây ra sự kiện đó.

5.4.8. Đánh giá lỗ hổng hệ thống

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

5.5. Lưu trữ các bản ghi

5.5.1. Các loại bản ghi được lưu trữ

- Mọi dữ liệu nhật ký trong phần 5.4.
- Hồ sơ của thuê bao cả giấy và hồ sơ điện tử.
- Dữ liệu thẩm định.
- Thông tin vòng đời chứng thư số như: thu hồi, đổi khóa, làm mới…

5.5.2. Thời hạn giữ lại các lưu trữ

- Thời gian lưu trữ theo quy định của pháp luật (ít nhất 10 năm).

5.5.3. Bảo vệ lưu trữ

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

5.5.4. Các thủ tục sao lưu lưu trữ

- EasyCA thực hiện sao lưu gia tăng hàng ngày các bản ghi kiểm toán và thực hiện các bản sao lưu dự phòng đầy đủ hàng tuần, hàng tháng và hàng năm theo cơ chế backup của EasyCA.

5.5.5. Yêu cầu về nhãn thời gian của các bản ghi

- Toàn bộ hồ sơ đều có chi tiết thông tin về thời gian.

5.5.6. Hệ thống tập hợp lưu trữ (Nội bộ hoặc bên ngoài)

- Hệ thống lưu trữ của EasyCA là tập trung, trừ trường hợp khách hàng doanh nghiệp với vai trò là RA.

5.5.7. Thủ tục lấy và kiểm tra thông tin lưu trữ

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

5.6. Thay đổi khóa

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

5.7. Xử lý sự cố, thảm họa và phục hồi

5.7.1. Các thủ tục xử lý lộ khóa và sự cố

- Các sự cố có thể xẩy ra:
  - Sự cố về tài nguyên máy tính, phần mềm và/hoặc dữ liệu.
  - Sự cố về mạng.
  - Sự cố về an ninh mạng, an ninh thông tin.
  - Sự cố về nguy cơ bị lộ khóa.
  - Thảm họa: Động đất, cháy nổ, chiến tranh.
- Khi có các sự cố xẩy ra, tùy theo từng mức độ EasyCA sẽ thực hiện tập hợp nhóm xử lý sự cố có thể là một thành phần hoặt một số hoặc tất cả để xử lý ngay lập tức: Lãnh đạo, Những người về quản trị hệ thống; Những người về vận hành hệ thống và cấp phát chứng thư số; Những người đảm bảo an toàn thông tin.
- Việc xử lý sự cố chi tiết được tiến hành theo thủ tục khôi phục đảm bảo duy trì hoạt động liên tục trong phục vụ dịch vụ cho khách hàng như các mục 5.7.2, 5.7.3, 5.7.4. Phương án xử lý chi tiết sự cố được lưu hành nội bộ đảm bảo xử lý chi tiết từng bước cho người thực thi và đảm bảo an ninh thông tin.

5.7.2. Sự cố về tài nguyên máy tính, phần mềm và/hoặc dữ liệu

- EasyCA có hệ thống chỉ dẫn chi tiết về việc quản lý phục hồi dịch vụ trong các trường hợp có sự cố hỏng hóc về tài nguyên máy tính, phần mềm, và/hoặc dữ liệu. Các tài liệu này được lưu hành nội bộ.

5.7.3. Thủ tục xử lý khi khóa bí mật bị làm mất/lộ

- Khi khóa bí mật của thuê bao EasyCA nghi ngờ bị mất/lộ, EasyCA sẽ thực hiện thủ tục xử lý khi khóa bị lộ. Đội xử lý sự cố an ninh của EasyCA: Lãnh đạo EasyCA, Người đứng đầu về quản trị hệ thống; Người đứng đầu về vận hành hệ thống và cấp phát chứng thư số; Người đứng đầu về đảm bảo an toàn thông tin.
- Các thủ tục được thực hiện:
  - Tạm dừng chứng thư số.
  - Tiến hành các thủ tục thu hồi chứng thư số như phần 4.9.
  - EasyCA cố gắng thông báo cho toàn bộ người nhận trong hệ thống EasyCA dừng sử dụng các chứng thư số do EasyCA ban hành.
  - EasyCA sinh cặp khóa mơi và cấp chứng thư mới cho thuê bao như phần 4.3.

5.7.4. Khả năng phục hồi hoạt động sau thảm họa

- Hệ thống EasyCA được triển khai đảm bảo tính sẵn sàng cao bao gồm một trung tâm DC được đặt tại VNPT ở Hà Nội và một trung tâm DR được đặt tại Viettel ở Hà Nội và cách nhau trên 40km đảm bảo hoạt động liên tục kể cả khi có những thảm họa tại một địa điểm mà hệ thống EasyCA đặt thì địa điểm kia vẫn hoạt động đảm bảo cung cấp dịch vụ cho khách hàng.
- EasyCA có khả năng phục hồi những hoạt động quan trọng trong vòng 8 giờ sau khi một thảm họa xảy ra. Ít nhất các hoạt động sau sẽ được phục hồi:
  - Ban hành chứng thư số.
  - Thu hồi chứng thư số.
  - Công bố thông tin thu hồi chứng thư số.
- Cơ sở dữ liệu của EasyCA phục hồi thảm họa sẽ được đồng bộ với cơ sở dữ liệu chính trong thời gian phù hợp, ít nhất là một ngày một lần đồng bộ.
- Kế hoạch phục hồi của EasyCA được thiết kế có khả năng phục hồi hoạt động toàn bộ hệ thống trong vòng 3 ngày.
- EasyCA dự phòng các thiết bị phần cứng và phần mềm cung cấp dịch vụ. Khóa bí mật của EasyCA cũng được dự phòng và duy trì phục vụ cho mục đích phục hồi hệ thống như phần 6.2.4.

5.8. Dừng hoạt động dịch vụ EasyCA/RA

- Khi không còn hoạt động, EasyCA dùng mọi biện pháp cố gắng thông báo cho thuê bao, người nhận và các đối tượng trước khi dừng hoạt động. EasyCA sẽ có kế hoạch kết thúc nhằm giảm thiểu thiệt hại nhất cho khách hàng. EasyCA thực hiện kế hoạch kết thúc như sau:
  - Chuẩn bị thông báo cho các thành viên bị ảnh hưởng (thuê bao, người nhận và RA nếu cần).
  - Chịu chi phí cho các thông báo.
  - Bảo quản dữ liệu lưu trữ và bản ghi của CA trong thời gian được quy định bởi quy chế này.
  - Tiếp tục dịch vụ hỗ trợ thuê bao và khách hàng tới khi các chứng thư số do EasyCA ban hành hết hạn.
  - Tiếp tục dịch vụ thu hồi như ban hành CRLs và duy trì OCSP tới khi các chứng thư số do EasyCA ban hành hết hạn.

- Thu hồi chứng thư số của thuê bao nếu cần thiết.
- Có chính sách trả lại tiền cho thuê bao bị thu hồi chứng thư số nếu chứng thư số của họ chưa hết hạn, chưa bị thu hồi nhưng phải thu hồi do kế hoạch dừng hoạt động. Trong trường hợp có thể, EasyCA thỏa thuận cùng thuê bao bị thu hồi chứng thư số về việc thuê bao chuyển sang sử dụng dịch vụ tại nhà cung cấp dịch vụ khác, chi phí và các thủ tục cần thiết sẽ do EasyCA đảm nhiệm.
- Thực hiện các thủ tục chuẩn bị trước khi chuyển các dịch vụ chứng thực sang cho CA khác.

- Ngừng dịch vụ một hoặc một số RA:
  - Thu hồi các chứng thư số thực hiện các quyền của RA.
  - Thông báo đến các bên liên quan về việc dừng RA.
  - Có các phương án xử lý chi tiết phù hợp để đảm bảo không ảnh hưởng đến hoạt động bình thường của toàn hệ thống EasyCA.

6. Đảm bảo an toàn an ninh về kỹ thuật

6.1. Tạo khóa và phân phối cặp khóa

6.1.1. Sự sinh cặp khóa

- Cặp khóa cho EasyCA được sinh ra trong thiết bị phần cứng HSM đạt chuẩn FIPS 140-2 level 3, khóa ký trong HSM được bảo vệ bởi bộ thẻ thông minh chuyên dụng và quy trình kiểm soát nhiều lớp.
- Cặp khóa của thuê bao được sinh ra tại PKI Smartcard, PKI token theo tiêu chuẩn FIPS 140-2 Level 2 trở lên, sử dụng sinh khóa ký số phải có Token và mã PIN xác thực truy xuất vào thiết bị.
- Trong một số trường hợp khách hàng có nhu cầu đặt biệt, khách hàng sử dụng thiết bị HSM đạt chuẩn FIPS 140-2 Level 3, cặp khóa được sinh ra trong thiết bị HSM của khách hàng

6.1.2. Gửi khóa bí mật cho thuê bao

- Hệ thống phân phối khóa cho thuê bao của EasyCA đảm bảo sự toàn vẹn và bảo mật của cặp khoá.
- Các giải pháp phân phối khóa của EasyCA như sau:
  - Trường hợp cặp khóa được tạo ở phía thuê bao: không phải gửi khóa bí mật

cho thuê bao.

- Trường hợp cặp khóa được tạo trên EasyCA: Khóa bí mật được lưu trong USB Token. EasyCA chịu trách nhiệm và đảm bảo giao USB Token và mật khẩu sử dụng đến tận tay thuê bao một cách an toàn theo quy trình chuyển giao khóa bí mật:
  - Mật khẩu sử dụng cho USB Token được tạo ngẫu nhiên cho từng thuê bao.
  - USB Token và mật khẩu sử dụng được đóng gói và niêm phong trong phong bì của EasyCA.
  - EasyCA cung cấp dịch vụ chuyển USB Token đến tận nơi cho thuê bao thông qua dịch vụ chuyển phát của EasyCA hoặc đối tác.
  - Thuê bao chỉ ký vào biên bản giao nhận khi USB Token và mật khẩu sử dụng nằm trong phong bì vẫn còn niêm phong.

6.1.3. Gửi khóa công khai cho EasyCA

- Khi thuê bao sinh cặp khóa tại phía thuê bao, thuê bao gửi yêu cầu phát hành chứng thư số tới nhà cung cấp dịch vụ chứng thực chữ ký số EasyCA.
- Thuê bao tiến hành gửi khóa công khai bằng cách gửi thông điệp đề nghị cấp chứng thư số ở định dạng PKCS#10 được sinh ra ở các thiết bị Token hoặc HSM đạt chuẩn gửi đến EasyCA.
- Việc gửi các thông điệp này trực tiếp qua các kênh của EasyCA, RA hoặc qua đường truyền có sử dụng SSL.

6.1.4. Gửi khóa công khai của EasyCA cho người nhận

- Người nhận có thể tải về khóa công khai của EasyCA và RootCA từ trang Web của EasyCA.
- Việc gửi khóa này cũng thông qua một phiên SSL để đảm bảo an ninh.
- EasyCA cũng cung cấp chứng thư số của EasyCA kèm với chứng thư số của thuê bao.

6.1.5. Độ dài khóa

- Đô dài khóa EasyCA: Khóa RSA có độ dài 2048 hoặc 4096 theo cấp phép của BTT&TT
- Độ dài khóa thuê bảo của EasyCA: Khóa RSA có độ dài từ 2048 trở lên.

6.1.6. Kiểm tra chất lượng và các tham số khóa công khai

- Tất cả các cặp khóa xin cấp phép dịch vụ chứng thực chữ ký số EasyCA đều được sinh ra trong thiết bị theo tiêu chuẩn FIPS 140-2 Level 2 và PKCS#1 v2.1 trở lên, nên đều đáp ứng về chất lượng và các tham số theo tiêu chuẩn quốc tế, đồng thời đáp ứng này theo đúng tiêu chuẩn trong quyết định số 59/2008/QĐ – BTTTT của Bộ Thông Tin và Truyền Thông ban hành ngày 31 tháng 12 năm 2008.

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

- Xem phần 7.1.2

6.2. Kiểm soát và bảo vệ khóa bí mật

6.2.1. Tiêu chuẩn và kiểm soát module mật mã

- Module mật mã EasyCA sử dụng thiết bị HSM đáp ứng chuẩn chuẩn FIPS 140-2 level 3. Việc vận hành thiết bị được kiểm soát hoạt động theo tiêu chuẩn của hạ tầng mã khóa công khai và tiêu chuẩn nhà cung cấp.
- Module mật mã của thuê bao: Sử dụng chuẩn FIPS 140-2 Level 2 trở lên. Việc vận hành thiết bị được kiểm soát hoạt động theo tiêu chuẩn của hạ tầng mã khóa công khai và tiêu chuẩn nhà cung cấp.

6.2.2. Cơ chế kiểm soát khóa bí mật CA (m out of n)

- Cơ chế kiểm soát khóa bí mật được EasyCA sử dụng là cơ chế chia sẻ mã. Cơ chế này tách dữ liệu kích hoạt khóa bí mật thành N phần khác nhau, các phần này được giữ bởi các đối tượng khác nhau.
- Với mỗi chức năng cần kích hoạt khóa bí mật CA của EasyCA, cần có M phần (M nhỏ hơn hoặc bằng N) mã chia sẻ để kích hoạt chứng năng đó.
- EasyCA áp dụng N = 3; M>=2;

6.2.3. Lưu giữ ngoài khóa bí mật của thuê bao

- EasyCA không có quy định.

6.2.4. Sao lưu dự phòng khóa bí mật

- EasyCA triển khai hạ tầng sẽ dự phòng (backup) khóa bí mật CA của mình để đề phòng khắc phục sự cố và thảm họa. EasyCA sử dụng 3 thiết bị HSM được đặt tại DC và một được đặt tại DR để đảm bảo sao lưu dự phòng cho khóa bí mật CA.

- EasyCA không dự phòng khóa bí mật cho RA, thuê bao.

6.2.5. Lưu trữ khóa bí mật

- EasyCA không lưu khóa riêng của thuê bao và RA.
- Sau khi chứng thư số CA của EasyCA hết hạn, cặp khóa tương ứng vẫn được lưu trữ (archive) an toàn với thời hạn ít nhất 5 năm trong HSM. Những cặp khóa đó sẽ không còn được sử dụng cho bất kỳ hoạt động của EasyCA .

6.2.6. Chuyển khóa bí mật vào/ra HSM

- EasyCA giữ khóa trên một HSM và một bản sao khóa sang một thiết bị HSM khác để dự phòng phục vụ cho trường hợp phục hồi khi có sự cố hoặc thảm họa.
- Việc sao một bản sao khóa từ thiết bị HSM sang thiết bị HSM khác chỉ áp dụng được với cùng một loại HSM của cùng một hãng.
- Quá trình sao này thường phải thực hiện theo quy trình quản lý hạ tầng mã khóa công khai và theo chỉ dẫn cụ thể của nhà cung cấp với các thiệt bị chuyên dùng đi kèm của nhà cung cấp.

6.2.7. Lưu trữ khóa bí mật trong HSM

- EasyCA giữ khóa bí mật CA trong các HSM, khóa bí mật được lưu trong dạng được mã hóa.

6.2.8. Phương thức kích hoạt khóa bí mật

- Việc kích hoạt khóa bí mật EasyCA được thực hiện:
  - Đối với thuê bao: Khóa bí mật được lưu trong USB token hoặc Smartcard, việc kích hoạt khóa bí mật yêu cầu mật khẩu bảo vệ. Khi không sử dụng, khóa bí mật tồn tại ở dạng mã hóa trong chip nhớ của thiết bị theo chuẩn FIPS 140-2 Level 2 trở lên.
  - Đối với quản trị hệ thống EasyCA/RA: Khóa bí mật được lưu trong USB token hoặc Smartcard, việc kích hoạt khóa bí mật yêu cầu mật khẩu bảo vệ. Khi không sử dụng, khóa bí mật tồn tại ở dạng mã hóa trong chip nhớ của thiết bị bị theo chuẩn FIPS 140-2 Level 2 trở lên.
  - Đối với RA: khóa bí mật được lưu trong USB token hoặc Smartcard, việc kích hoạt khóa bí mật yêu cầu mật khẩu bảo vệ. Khi không sử dụng, khóa bí mật tồn tại ở dạng mã hóa trong chip nhớ của thiết bị bị theo chuẩn FIPS 140-2 Level 2 trở lên.
  - Đối với EasyCA: sử dụng HSM để lưu trữ khóa bí mật, việc kích hoạt khóa

bí mật yêu cầu các mã chia sẻ theo cơ chế chia sẻ mã trong 6.2.2.

6.2.9. Phương pháp ngừng kích hoạt khóa bí mật

- Khóa bí mật CA của EasyCA bị ngừng kích hoạt khi rút CA token khỏi đầu đọc Token của HSM hoặc chúng ta chủ động ngừng kích hoạt bằng lệnh trên thiết bị HSM.
- Khóa bí mật của thuê bao và RA token sẽ tự đông ngừng kích hoạt sau mỗi giao dịch kích hoặc, hoặc người dùng đăng xuất hoặc rút Token ra khỏi đầu đọc.

6.2.10. Phương pháp hủy bỏ khóa bí mật

- Việc xóa khóa bí mật được thực hiện theo phương pháp an toàn, đảm bảo không thể phục hồi lại khóa đã xóa.
- Khóa bí mật lưu trên USB token được xóa bằng phần mềm quản trị USB token
- Khóa bí mật lưu trên HSM được xóa bằng chứng năng xóa khóa của HSM
- Các hoạt động hủy bỏ khóa bí mật được ghi nhật ký.

6.2.11. Đánh giá module mật mã

- Xem phần 6.2.1

6.3. Các vấn đề khác liên quan đến quản lý cặp khóa

6.3.1. Lưu trữ khóa công khai

- EasyCA sẽ lưu trữ khóa công khai của mình, của RA và toàn bộ thuê bao trên danh bạ EasyCA, và được lưu trữ theo quy định của pháp luật.

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

- Thời hạn sử dụng của chứng thư số sẽ kết thúc khi chứng thư số đó hết hạn hoặc bị thu hồi.
- Thời hạn sử dụng cặp khóa của thuê bao giống như thời hạn sử dụng của chứng thư số, ngoại trừ chức năng giải mã và kiểm tra chữ ký sau khi chứng thư số hết hạn.
- EasyCA không ban hành các chứng thư số có thời hạn sử dụng vượt quá thời hạn sử dụng chứng thư số của CA.
- Chứng thư số mà EasyCA cung cấp cho thuê bao tùy thuộc vào thỏa thuận với thuê bao, thông thường là 1-3 năm.

6.4. Dữ liệu kích hoạt khóa bí mật

6.4.1. Tạo và cài đặt dữ liệu kích hoạt

- Dữ liệu kích hoạt khóa bí mật CA của EasyCA được chia thành các mã chia sẻ, các mã chia sẻ này được tạo theo các yêu cầu trong phần 6.2.2 và tuân theo các thủ tục của nghi lễ sinh khóa. Quá trình tạo và phân phối mã chia sẻ được ghi nhật ký.
- Mật khẩu để bảo vệ kích hoạt khóa bí mật được đặt theo nguyên tắc mật khẩu mạnh:
  - Có ít nhất 8 ký tự.
  - Chứa từ 3 trong 4 loại ký tự sau: chữ hoa (A, B, C…), chữ thường (a, b, c), chữ số (0, 1, 2…) và các ký hiệu (!, @, $...)
  - Không chứa tất cả hoặc một phần tên tài khoản người dùng tương ứng.

6.4.2. Bảo vệ dữ liệu kích hoạt

- Người giữ mã chia sẻ của EasyCA được yêu cầu bảo vệ an toàn mã chia sẻ của họ. Những người này phải ký một thỏa thuận với EasyCA về việc đảm bảo trách nhiệm trong việc bảo vệ mã chia sẻ mà họ giữ.
- RA và quản trị hệ thống được yêu cầu phải giữ khóa bí mật ở dạng mã hóa sử dụng mật khẩu bảo vệ và chọn “high security” cho trình duyệt khi sử dụng.
- Thuê bao của EasyCA được yêu cầu lưu trữ khóa bí mật dưới dạng mã hóa sử dụng USB Token và mật khẩu bảo vệ.

6.4.3. Các vấn đề khác của dữ liệu khích hoạt

- EasyCA không có quy định.

6.5. Kiểm soát an ninh hệ thống máy tính

6.5.1. Các yêu cầu an ninh hệ thống máy tính

- EasyCA đảm bảo rằng các máy chủ cài đặt hệ thống CA và dữ liệu được bảo vệ trước các truy nhập không được phép. EasyCA giới hạn quyền truy nhập tới CA server theo vai trò của quản trị. Trên các máy chủ cài đặt hệ thống CA, không có ứng dụng nào khác được cài đặt thêm.
- Hệ thống mạng của EasyCA được cách ly với các thành phần khác, bảo vệ khỏi sự truy cập bất hợp pháp. Sự cách ly này được thực hiện bằng hệ thống tường lửa đa lớp. Lớp tường lửa bên ngoài bảo vệ cả hệ thống khỏi các truy nhập từ ngoài. Lớp tường lửa bên trong cách ly các server CA ra khỏi hệ thống mạng chung của EasyCA. Các quản trị viên của EasyCA chỉ truy nhập và quản trị hệ thống thông

qua một số giới hạn các máy tính quản trị được xác định sẵn.

- EasyCA yêu cầu sử dụng mật khẩu theo các tiêu chí trong phần 6.4.1, mật khẩu được định kỳ được thay đổi.
- Việc truy nhập trực tiếp dữ liệu của CA chỉ được giới hạn cho những người có quyền và nhiệm vụ phù hợp.

6.5.2. Đánh giá an ninh của hệ thống máy tính

- EasyCA áp dụng tuân theo chuẩn hệ thống máy tính ISO 27001, hệ thống máy tính được đánh giá định kỳ 6 tháng một lần hoặc khi có yêu cầu đột xuất cần phải đánh giá.

6.6. Kiểm soát an ninh quy trình sử dụng

6.6.1. Giám sát phát triển hệ thống

- Các ứng dụng được phát triển và triển khai sử dụng trong EasyCA tuân theo các tiêu chuẩn thiết kế, phát triển và triển khai phần mềm của EasyCA. EasyCA cũng cung cấp phần mềm cho các RA.
- Phần mềm được EasyCA phát triển sẽ được ký số đảm bảo trong quá trình phân phối không bị thay đổi nội dung hoặc phiên bản. Chữ ký trên phần mềm sẽ được kiểm tra khi phần mềm được cài đặt.

6.6.2. Kiểm soát quản lý an ninh

- EasyCA có các thủ tục biện pháp kiểm soát an ninh trong quá trình thiết lập hệ thống theo tiêu chuẩn ISO 27001

6.6.3. Kiểm soát an ninh vòng đời

- EasyCA không có quy đinh.

6.7. Giám sát an ninh hệ thống mạng

- Hệ thống EasyCA thực hiện các chức năng trong vùng mạng đảm bảo an ninh. Mọi thông tin nhạy cảm sẽ được mã hóa và ký số.

6.8. Dấu thời gian

- Chứng thư số, danh bạ chứng thư số, danh sách thu hồi chứng thư số có gắn thông tin thời gian.

7. Định dạng chứng thư số, danh sách thu hồi chứng thư số (CRL), giao thức kiểm tra trạng thái chứng thư số trực tuyến (OCSP)

7.1. Định dang chứng thư số

- Chứng thư số do EasyCA ban hành tuân theo chuẩn ITU-T X.509 và các quy định của RFC 3280. Tối thiểu, chứng thư số do EasyCA ban hành có các trường và giá trị theo bảng dưới đây.

Trường	Giá trị/Ý nghĩa
Serial Number	Giá trị là duy nhất đối với mỗi chứng thư số do EasyCA ban hành
Signature Algorithm	Định danh (OID) của thuật toán được sử dụng để ký lên chứng thư số (xem phần 7.1.3)
Issuer DN	Xem phần 7.1.4
Valid From	Thời điểm bắt đầu chứng thư số có hiệu lực, theo giờ UTC
Valid To	Thời điểm hết hiệu lực của chứng thư số, theo giờ UTC
Subject DN	Xem phần 7.1.4
Subject Public key	Khóa công khai, được mã hóa phù hợp với RFC 3280
Signature	Chữ ký của EasyCA, được mã hóa phù hợp với RFC 3280

7.1.1. Phiên bản

- Chứng thư số do EasyCA ban hành theo X.509 v3.

7.1.2. Trường mở rộng

EasyCA phát hành chứng thư số X.509 v3 với phần mở rộng được quy định như sau.

❖ **Key Usage**

- Chứng thư số X.509 phiên bản 3 được ban hành theo RFC 3280. Phần mở rộng KeyUsage trong chứng thư số theo bảng sau.
- Chứng thư số do EasyCA ban hành có sử dụng trường KeyUsage

Bit		Chứng thư số cá nhân thuộc cơ quan, tổ chức và cá nhân.	Chứng thư số Web Server (SSL)	Chứng thư số ký mã phần mềm (CodeSigning)
0	**digitalSignature**	Có	Có	Có
1	**nonRepudiation**	Có	Có	Có
2	**keyEncipherment**	Có	Có	Không
3	**dataEncipherment**	Không	Không	Không
4	**keyAgreement**	Không	Không	Không
5	**keyCertSign**	Không	Không	Không
6	**CRLSign**	Không	Không	Không
7	**encipherOnly**	Không	Không	Không
8	**decipherOnly**	Không	Không	Không

❖ **Certificate policies**

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

❖ **Subject Alternative Name**

- Phần mở rộng subjectAltName của chứng thư số được gán giá trị theo RFC 3280.

❖ **Basic Constraints**

- Phần mở rộng Basic Constraints của chứng thư số được gán giá trị theo RFC 3280.

❖ **Extended Key Usage**

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

	Chứng thư số của cá nhân	Chứng thư số ký số của Server	Chứng thư số ký phần mềm
ServerAuth	Không	Có	Không

ClientAuth	Có	Có	Không
CodeSigning	Không	Không	Có
EmailProtection	Có	Không	Không
TimeStamping	Không	Không	Không

❖ **CRL Distribution Points**

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

❖ **Authority Key Identifier**

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

❖ **Subject Key Identifier**

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

7.1.3. Các định danh đối tượng thuật toán

- Đáp ứng theo tiêu chuẩn RFC 3280

7.1.4. Định dạng tên

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

7.1.5. Ràng buộc tên

- EasyCA không có quy định.

7.1.6. Định danh đối tượng chính sách chứng thư

- EasyCA không có quy đinh.

7.1.7. Mở rộng những ràng buộc chính sách sử dụng

- EasyCA không có quy định.

7.1.8. Cú pháp và ngữ nghĩa của chính sách

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

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

- EasyCA không có quy định.

7.2. Định dạng danh sách thu hồi chứng thư số (CRL)

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

Trường	Giá trị
Version	Xem phần 7.2.1
Signture Algorithm	Thuật toán được dùng để ký CRL. EasyCA sử dụng một trong bốn hàm băm an toàn: SHA-1, SHA-256, SHA-384, SHA-512.
Issuer	Thực thể ký và ban hành CRL – EasyCA.
Effective Date	Ngày có hiệu lực của CRL.
Next Update	Thời gian mà CRL tiếp theo sẽ được công bố. Việc công bố CRL tuân theo các yêu cầu trong phần 4.4.7
Revoked Certificates	Danh sách các chứng thư số bị thu hồi, bao gồm Serial Number của các chứng thư số bị thu hồi và ngày thu hồi.

7.2.1. Phiên bản

- EasyCA ban hành X.509 v3 CRL.

7.2.2. Những mở rộng thực thể CRL

- EasyCA không quy định.

7.3. Định dạng giao thức kiểm tra trạng thái chứng thư số trực tuyến (OCSP)

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

7.3.1. Phiên bản

- EasyCA cung cấp dịch vụ OCSP Version 1 theo RFC 2560.

7.3.2. Phần mở rộng OCSP

- Easy CA không quy định.

8. Kiểm định tính tuân thủ và đánh giá khác

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

8.1. Tần suất và các tình huống kiểm tra kỹ thuật

- EasyCA tuân thủ chế độ kiểm tra quy định, ngoài ra EasyCA thực hiện tự đánh giá hoạt động của EasyCA, RA, đại lý ít nhất một năm một lần.

8.2. Đơn vị, người thực hiện kiểm tra kỹ thuật

- Người thực hiện kiểm tra kỹ thuật được chỉ định bởi RootCA để thực hiện các cuộc kiểm tra kỹ thuật EasyCA.

8.3. Các nội dụng kiểm tra kỹ thuật

- Kiểm tra kỹ thuật được thực hiện bởi những đơn vị độc lập.

8.4. Xử lý khi phát hiện sai sót

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

8.5. Công bố kết quả kiểm tra kỹ thuật

- Báo cáo kết quả kiểm tra kỹ thuật được EasyCA công bố tại https://easyca.vn/

8.6. Tần suất và các trường hợp đánh giá

- Đánh giá kiểm tra được thực hiện ít nhất định kỳ hàng năm hoặc theo thời hạn chứng chỉ của các thành phần hệ thống bởi đơn vị kiểm định đáp ứng yêu cầu theo quy định của pháp luật và yêu cầu của EasyCA.

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

- Đơn vị kiểm tra EasyCA phải là đơn vị độc lập có khả năng sau:
    - Có năng lực thành thạo về công nghệ hạ tầng khóa công khai, công cụ và kĩ thuật an toàn thông tin.

- Được chứng nhận bởi RootCA

9. Các vấn đề nghiệp vụ và pháp lý khác

9.1. Phí/Giá

9.1.1. Phí đăng ký mới và gia hạn chứng thư số

- EasyCA có quyền yêu cầu tiền thù lao từ thuê bao cho việc ban hành, quản lý, và gia hạn chứng thư số. Mức phí được niêm yết trên website https://easyca.vn, và có thể theo từng hợp đồng với thuê bao.

9.1.2. Phí truy nhập chứng thư số

- EasyCA không thu phí

9.1.3. Phí truy nhập thông tin trạng thái chứng thư số

- EasyCA không thu phí.

9.1.4. Phí dịch vụ khác

- EasyCA có thể thiết lập và tính một mức phí hợp lý cho dịch vụ khác.

9.1.5. Chính sách hoàn phí

- Thuê bao có thể yêu cầu EasyCA thu hồi chứng thư số và hoàn lại phí trong các trường hợp sau:
  - Nếu EasyCA vi phạm điều khoản trong hợp đồng với thuê bao
- Việc hoàn phí được thực hiện trên thỏa thuận trong hợp đồng với thuê bao.

9.2. Trách nhiệm tài chính

9.2.1. Bảo hiểm

- EasyCA sẽ cung cấp đa dạng các gói bảo hiểm dịch vụ chứng thực chữ ký số, khách hàng có thể tùy chọn theo mục đích sử dụng, chính sách bảo hiểm chỉ được áp dụng với thuê bao của EasyCA.
- Các mức đền bù bảo hiểm và trách nhiệm thực hiện bảo hiểm của EasyCA được thực hiện theo hợp đồng dịch vụ giữa EasyCA – Thuê bao.

9.2.2. Các tài sản khác

- EasyCA 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 người nhận.

9.2.3. Trách nhiệm bảo hiểm với các thực thể cuối khác

- EasyCA không có quy định.

9.3. Bảo mật thông tin nghiệp vụ

9.3.1. Phạm vi các thông tin bí mật

- Những thông tin sau sẽ được coi là thông tin bí mật và riêng tư:
  - Các dữ liệu ứng dụng CA.
  - Hồ sơ thuê bao.
  - Các dữ liệu kiểm toán EasyCA.
  - Quản lý các mức độ an ninh phần cứng, phần mềm, các quản trị viên của dịch vụ EasyCA.
  - Kế hoạch đối phó với sự cố và kế hoạch khôi phục lại sau thảm họa.
  - Phương pháp điều khiển hoạt động các thành phần EasyCA: phần cứng, phần mềm và quản trị của dịch vụ của EasyCA.
  - Các thông tin được yêu cầu bởi pháp luật.

9.3.2. Những thông tin ngoài phạm vi thông tin bí mật

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

9.3.3. Trách nhiệm bảo vệ các thông tin bí mật

- EasyCA thực hiện các biện pháp đảm bảo an ninh cho các thông tin bí mật và đảm bảo các thông tin riêng tư không bị lộ với bên thứ 3.

9.4. Tính riêng tư của thông tin cá nhân

9.4.1. Kế hoạch bảo vệ tính riêng tư

- EasyCA cam kết không tiết lộ thông tin của thuê bao cho bên thứ 3 trừ các yêu cầu của cơ quan quản lý nhà nước có thẩm quyền theo quy định của pháp luật.
- Chính sách bảo mật được công bố trên trang Web của EasyCA.

9.4.2. Những thông tin được coi là riêng tư.

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

9.4.3. Những thông tin không được coi bí mật

- Mọi thông tin được công bố trong một chứng thư số được coi là không phải riêng tư.

9.4.4. Trách nhiệm bảo vệ các thông tin riêng tư

- EasyCA thực hiện các biện pháp đảm bảo an ninh cho các thông tin bí mật của thuê bao không bị tiết lộ cho bên thứ 3 và phải tuân theo quy định của luật pháp.

9.4.5. Thông báo và sự cho phép sử dụng thông tin riêng tư

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

9.4.6. Cung cấp thông tin theo yêu cầu của cơ quan pháp luật hay cho xử lý quản trị

- EasyCA sẽ cung cấp thông tin bí mật nếu có yêu cầu của cơ quan pháp luật có thẩm quyền, quá trình quản trị và tuân thủ theo quy định của pháp luật.

9.4.7. Các tình huống cung cấp thông tin khác

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

9.5. Quyền sở hữu trí tuệ

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

- EasyCA giữ mọi quyền sở hữu trí tuệ liên quan đến chứng thư số và thông tin thu hồi mà nó phát hành.
- EasyCA cho phép sử dụng thông tin thu hồi khi thực hiện chức năng của người nhận. Việc sử dụng này tuân thủ theo thỏa thuận sử dụng CRL, thỏa thuận người nhận và những thỏa thuận khác nếu có.

9.5.2. Quyền sở hữu quy chế chứng thực

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

9.5.3. Quyền sở hữu tên

- Đối tượng đăng ký chứng thư số phải có quyền sở hữu về nhãn hiệu đăng ký,

nhãn hiệu dịch vụ, hoặc tên tổ chức (danh nghiệp) trong đơn xin cấp chứng thư số và tên đặc trưng trong chứng thư số.

9.5.4. Quyền sở hữu khóa

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

9.6. Tuyên bố và cam kết

9.6.1. Tuyên bố và cam kết của EasyCA

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

9.6.2. Tuyên bố và cam kết của RA

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

- Nhân viên RA trực tiếp tham gia vào quy trình cung cấp chứng thư số phải có hiểu biết pháp luật về chữ ký số và dịch vụ chứng thực chữ ký số.

9.6.3. Tuyên bố và cam kết của thuê bao

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

9.6.4. Tuyên bố và cam kết của người nhận

- Người nhận chịu trách nhiệm về việc tìm hiểu các thông tin trong quy chế chứng thực số, trong thỏa thuận người nhận trước khi quyết định tin tưởng chứng thư số do EasyCA phát hành.
- Người nhận phải chịu trách nhiệm cho những hành động của mình do không thực hiện theo các nội dung liên quan được quy định trong thỏa thuận người nhận hoặc quy chế chứng thực này.
- Thỏa thuận thuê bao có thể bao gồm thêm những điều khoản khác.

9.6.5. Tuyên bố và cam kết của các đối tượng khác

- EasyCA không có quy đinh.

9.7. Từ chối trách nhiệm

- EasyCA không quy định.

9.8. Giới hạn trách nhiệm pháp lý

- Trong giới hạn của luật pháp, hợp đồng thuê bao và người nhận có khả năng giới hạn trách nhiệm pháp lý của EasyCA. Việc giới hạn trách nhiệm pháp lý bao gồm các việc loại bỏ các thiệt hại ngẫu nhiên, gián tiếp hay những thiệt hại nghiêm trọng.
- Hợp đồng dịch vụ giữa thuê bao và EasyCA sẽ quy định cụ thể về trách nhiệm pháp lý của hai bên.

9.9. Bồi thường thiệt hại

9.9.1. Bồi thường của thuê bao

- Trong giới hạn được cho phép bởi pháp luật, thuê bao được yêu cầu bồi thường cho EasyCA nếu:
    - Cung cấp thông tin không đúng khi đăng ký cấp chứng thư số.
    - Thuê bao có lỗi trong việc bảo vệ khóa bí mật, sử dụng hệ thống không tin cậy, hoặc không thực hiện các biện pháp phòng ngừa cần thiết để gây ra hậu quả.
    - Để lộ những nhân tố xác thực, sự bỏ sót hay làm sai lệch do sự cẩu thả hoặc với mục đích lừa đảo.
    - Sử dụng tên của thuê bao vi phạm quyền sở hữu trí tuệ của bên thứ ba.
- Có thể có thêm các điều khoản khác trong hợp đồng dịch vụ.

9.9.2. Bồi thường của người nhận

- Trong phạm vi cho phép của pháp luật, EasyCA có quyền yêu cầu người nhận bồi trường thiệt hại nếu người nhận không thực hiện kiểm tra trạng thái của mỗi chứng thư số để xác định chứng thư số hết hạn hay bị thu hồi, gây ra các ảnh hưởng tới EasyCA

9.10. Hiệu lực của Quy chế chứng thực

9.10.1. Thời hạn bắt đầu có hiệu lực

- Quy chế chứng thư số này có hiệu lực EasyCA được cấp phép và chính thức đi vào hoạt động, CPS này được công bố trên Web của EasyCA.
- Các điều chỉnh bổ sung cho quy chế chứng thư số này có hiệu lực khi được công bố.

9.10.2. Thời hạn hết hiệu lực

- Hết hạn chứng thư số EasyCA
- Dịch vụ của EasyCA chấm dứt.
- Một phiên bản mới được phát hành.

9.10.3. Ảnh hưởng của hết hạn quy chế

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

thư số hết hạn hoặc bị thu hồi.

9.11. Thông báo cá nhân và các trao đổi với các bên tham gia

- EasyCA sẽ sử dụng các biện pháp thích hợp để thông báo cho các bên liên quan về nội dung thay đổi và công bố CPS.

9.12. Bổ sung và sửa đổi quy chế chứng thực

9.12.1. Thủ tục bổ sung sửa đổi

- Quy chế này được bổ sung, sửa đổi bởi EasyCA. Những nội dung bổ sung, sửa đổi có thể được công bố dưới dạng tài liệu chứa tất cả các những bổ sung sửa đội cho CPS hoặc ở dạng cập nhật. Nội dung được công bố trên https://easyca.vn/
- Nội dung sửa đổi sẽ thay thế các nội dung trong các điều khoản tương đương trong phiên bản quy chế chứng thực tương ứng và mọi tài liệu liên quan khác.

9.12.2. Cơ chế và thời hạn thông báo

- Một số thay đổi thông tin đơn giản như thay đổi URL, thông tin liên hệ, lỗi in ấn… EasyCA có quyền không phải thông báo về sự thay đổi.
- Các thành viên của EasyCA/RA đề xuất thay đổi, EasyCA sẽ xem xét yêu cầu thay đổi. Nếu thay đổi, EasyCA sẽ đưa ra thông báo về sự thay đổi này.
- Một số trường hợp đặc biệt liên quan tới an ninh của hệ thống, EasyCA sẽ thực hiện sự thay đổi quy chế này lập tức, sau đó sẽ thông báo cho các thành viên.
- Các thành viên EasyCA/RA có quyền góp ý.
- EasyCA sẽ xem xét mọi góp ý sửa đổi và thực hiện một trong các tính huống sau:
  - Không thay đổi gì.
  - Sửa đổi theo những góp đúng và công bố lại chúng.

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

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

9.13. Thủ tục giải quyết tranh chấp

- Tranh chấp giữa EasyCA với Ra, các thuê bao và người nhận dựa trên các điều khoản trong hợp đồng và trên cơ sở quy định của pháp luật.

9.14. Pháp luật điều chỉnh

- Pháp luật Việt Nam sẽ được sử dụng trong mọi trường hợp, kể cả có liên quan

đến các yếu tố nước ngoài.

9.15. Phù hợp với pháp luật hiện hành

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

9.16. Các điều khoản chung

9.16.1. Thỏa thuận chung

- EasyCA không có quy định.

9.16.2. Sự chuyển nhượng

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

9.16.3. Tính độc lập của các điều khoản

- Nếu trong trường hợp một số điều khoản trong quy chế chứng thực này không hợp pháp các điều khoản đó sẽ không có giá trị, phần còn lại của CPS vẫn có hiệu lực.

9.16.4. Bắt buộc thực thi

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

9.16.5. Trường hợp bất khả kháng

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

9.17. Những điều khoản khác

- EasyCA không quy định.