M.S.D.N: 0401486901 - C.T.C.P
CÔNG TY CỔ PHẦN THƯƠNG MẠI VISNAM
THÀNH PHỐ ĐÀ NẴNG

visnam
save time save money

CÔNG TY CỔ PHẦN THƯƠNG MẠI VISNAM

ONE-CA

QUY CHẾ CHỨNG THỰC
DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG
ONE-CA

Đà Nẵng – Tháng 10/2024

MỤC LỤC

Lời nói đầu

Bản Quy chế chứng thực này được viết dựa theo RFC 3647 về "Khung quy chế chứng thực và chính sách chứng thư số", đáp ứng theo tiêu chuẩn trong Thông tư số 6/2015/TT-BTTTT của Bộ Thông Tin và Truyền Thông (TTTT) ban hành ngày 23 tháng 3 năm 2015. 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.

1. Giới thiệu

ONE-CA là dịch vụ chứng thực chữ ký số công cộng của CÔNG TY CỔ PHẦN THƯƠNG MẠI VISNAM. Tài liệu này là Quy chế chứng thực do ONE-CA ban hành.
Quy chế chứng thực này chỉ rõ những thủ tục mà ONE-CA sử dụng trong việc cung cấp dịch vụ chứng thực chữ ký số như: ban hành, quản lý, thu hồi, làm mới chứng thư số...
Quy chế chứng thực mà ONE-CA 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

- Trong kiến trúc hệ thống cung cấp chứng thực chữ ký số công cộng Việt Nam, đứng đầu là CA do Trung tâm Chứng thực chữ ký số Quốc gia Việt Nam quản lý (sau đây gọi tắt là RootCA). ONE-CA là nhà cung cấp dịch vụ chứng thực chữ ký số công cộng được RootCA cấp chứng thư số và được Bộ TTTT cấp phép hoạt động. ONE-CA duy trì một chính sách chứng thư số mà mọi thành viên trong miền quản lý (ONE-CA, ONE-RA, thuê bao, người nhận) phải tuân theo.
- ONE-CA ban 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, ONE-CA 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, ONE-CA 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, BONE-CA xác minh quyền sở hữu tên miền mà thuê bao đã ghi trong đơn xin cấp chứng thư số.
- Chứng thư số được cấp tổ chức, cá nhân có thể sử dụng vào mục đính xác thực (Authentication); đảm bảo sự toàn vẹn của dữ liệu (Intergrity); tính bí mật (Confidentiality) và tính không chối bỏ (Non-repudiation)
- Với mức độ đảm bảo cao, ONE-CA ban hành các chứng thư số được liệt kê trong bảng dưới đây:

Loại chứng thư số	Mức độ	Mô tả chức năng

	đảm bảo	
Chứng thư số SSL	Cao	Xác thực Web Server, mã hóa 256 bit phiên giao dịch SSL giữa Server và Client.
Chứng thư số cho CodeSigning	Cao	Đảm bảo an ninh cho mã nguồn, nội dung được phân phối qua Internet.
Chứng thư số cá nhân cho cơ quan, tổ chức, cá nhân	Cao	Xác thực nhận dạng của client trong phiên giao dịch SSL với Server ứng dụng, xác thực chữ ký, mã hóa trong trao đổi email. Client ở đây có thể là một cơ quan, tổ chức hay một cá nhân.

- Quy chế chứng thực này mô tả quyền và nghĩa vụ của các bên liên quan, vấn đề pháp luật và đặc điểm hạ tầng kỹ thuật của hệ thống ONE-CA. Quy chế này mô tả các điều sau:
  - Nghĩa vụ của ONE-CA, RA, thuê bao, và người nhận trong miền quản lý của ONE-CA.
  - Các yếu tố liên quan đến pháp luật được đề cập trong thỏa thuận thuê bao, thỏa thuận người nhận trong miền quản lý của ONE-CA.
  - Kiểm tra, giám sát an ninh mà các thành viên trong miền ONE-CA phải thực hiện.
  - Các phương pháp mà ONE-CA sử dụng để xác minh nhận dạng thuê bao, cá nhân được ủy quyền, thực thể giữ khóa trong quá trình ban 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 và làm mới 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 đề cập đến các thỏa thuận giữa ONE-CA với các thành viên trong miền quản lý của ONE-CA. 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 là Quy chế chứng thực ONE-CA.

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

1.3.1. ONE-CA

- ONE-CA là dịch vụ chứng thực chữ ký số công cộng của CÔNG TY CỔ PHẦN THƯƠNG MẠI VISNAM.

1.3.2. ONE-RA

- RA (Registration Authority) là thành viên của ONE-CA, có nhiệm vụ quản lý thuê bao, nhận và duyệt các đơn đăng ký sử dụng chứng thư số.
- Bản thân ONE-CA cũng là một RA.

1.3.3. Thuê bao

- Thuê bao của ONE-CA là các đối tượng sở hữu chứng thư số do ONE-CA ban hành

1.3.4. Người nhận

- Là đối tượng tin tưởng chứng thư số hay một chữ ký số được cung cấp bởi ONE-CA. Người nhận có thể hoặc không là một thuê bao của ONE-CA.

1.3.5. Các đối tượng khác

- Ngoài ONE-CA, RA, thuê bao và người nhận, ONE-CA 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

- Thuê bao được sử dụng chứng thư số vào các mục đích được quy định bởi trường "Mục đích sử dụng" (KeyUsage) trong chứng thư số.
- Mục đích sử dụng không bị cấm bởi pháp luật, chính sách chứng thư số của RootCA, chính sách chứng thư số và quy chế chứng thực của ONE-CA và thỏa thuận của thuê bao với ONE-CA.
- Hiện tại ONE-CA cung cấp các gói dịch vụ tương ứng với KeyUsage được trình bày trong mục 7.1.2.1

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

- Chứng thư số chỉ được sử dụng đúng với mục đích mà chứng thư số đó được cấp phát.
- Chứng thư số do ONE-CA cấp không được sử dụng vào các mục đích như đảm bảo an ninh cho lĩnh vực hạt nhân, hệ thống điều khiển vũ khí...

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

1.5. Quản lý quy chế chứng thực

1.5.1. Tổ chức quản lý

- CÔNG TY CỔ PHẦN THƯƠNG MẠI VISNAM
- 33 Hải Hồ, P. Thanh Bình, Q. Hải Châu, TP. Đà Nẵng.

1.5.2. Liên hệ

- Người đứng đầu hệ thống
  - Giám Đốc: Nguyễn Văn Hùng
  - Email: hung@visnam.com
- CÔNG TY CỔ PHẦN THƯƠNG MẠI VISNAM
  - 33 Hải Hồ, P. Thanh Bình, Q. Hải Châu, TP. Đà Nẵng
  - Email: info@visnam.com
  - Điện thoại: +84 236 730 7666

1.5.3. Công nhận sự phù hợp của quy chế chứng thực

- ONE-CA PMA (Policy Management Authority) xác nhận sự phù hợp của quy chế chứng thực này.
- ONE-CA PMA là người đứng đầu hệ thống ONE-CA.

1.5.4. Thủ tục phê chuẩn quy chế chứng thực

- Sự phê chuẩn được thực hiện bởi ONE-CA PMA.
- Các thay đổi, cập nhật của quy chế chứng thực được ghi lại, công bố tại
  - http://one-ca.net/cps_update
- Quy chế chứng thực bản mới nhất được lưu trữ tại
  - http://one-ca.net/cps

1.6. Các định nghĩa và từ viết tắt

- Chi tiết trong phần từ ngữ 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. Chứng thư số của đối tượng đứng trước trong danh sách được dùng để ký lên chứng thư số của đối tượng đứng sau trong danh sách.
2	CA	Certificate Authority - Nhà chứng thực chữ ký số, có chức năng ban hành gia hạn, thu hồi và quản lý chứng thư 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.
4	ONE-CA	Nhà chứng thực chữ ký số do CÔNG TY CỔ PHẦN THƯƠNG MẠI VISNAM quản lý, được Bộ Thông Tin và Truyền Thông cấp phép hoạt động.
5	ONE-CA PMA	Nhóm các cá nhân có nhiệm vụ soạn thảo, bổ sung sửa đổi và ban hành chính sách chứng thư số, quy chế chứng thực và. các chính sách thỏa thuận khác của ONE-CA.
6	Chính sách bảo mật	Văn bản quy định về thông tin được coi là bí mật và trách nhiệm giữ bí mật thông tin của các đối tượng liên quan.
7	Chính sách hoàn phí	Văn bản quy định các điều khoản về hoàn phí cho thuê bao của ONE-CA, chính sách hoàn phí đi kèm trong thỏa thuận thuê bao.
8	Chủ thể chứng thư số	Chủ sở hữu của chứng thư số, chủ thể chứng thư số có thể là thuê bao chứng thư số hoặc các thiết bị như máy chủ Web.
9	CN	Common Name – một thuột tính trong trường DN của chứng thư số, CN biểu diễn tên thường gọi của đối tượng là chủ thể của chứng thư số.
10	CRL	Danh sách chứng thư số thu hồi.
11	DN	Distinguished Names – một trường trong chứng thư số, DN chưa thông tin nhận dạng đối tượng là chủ thể chứng thư số.
12	ISO/IEC 15408-3:1999	Tiêu chuẩn đánh giá an ninh hệ thống phần mềm.
13	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.
14	Khóa bí mật	Thành phần bí mật của cặp khóa được sử dụng trong hạ tầng khóa công khai (PKI – Public Key Infrastructure).

15	Khóa công khai	Thành phần công khai của cặp khóa được sử dụng trong hạn tầng khóa công khai.
16	Người nhận	Là đối tượng tin tưởng chứng thư số hay một chữ ký số được cung cấp bởi CA.
17	RA	Registration Authority – Nhà thẩm quyền có chức năng giúp đỡ CA duyệt đơn đăng ký chứng thư số, đơn gia hạn chứng thư số, đơn thu hồi chứng thư số và quản lý thông tin thuê bao.
18	Root CA	CA có chứng thư số được ký bởi chính khóa bí mật của CA. Root CA công cộng của Việt Nam được quản lý bởi Trung Tâm Chứng Thực Chữ Ký Số Quốc Gia – Bộ Thông Tin và Truyền Thông.
19	Thỏa thuận người nhận	Thỏa thuận giữa ONE-CA và người nhận, quy định rõ các điều khoản về quyền và trách nhiệm của mỗi bên trong quản lý thông tin và sử chứng thư số.
20	Thỏa thuận RA	Thỏa thuận giữa ONE-CA và RA, quy định rõ các điều khoản về quyền và nghĩa vụ của các bên trong cung cấp dịch vụ chứng thực chữ ký số.
21	Thỏa thuận thuê bao	Thỏa thuận giữa ONE-CA và thuê bao, quy định các điều khoản về quyền và nghĩa vụ của các bên trong ban hành, quản lý và sử dụng chứng thư số.
22	Thuê bao	Đối tượng đăng ký sử dụng chứng thư số.
23	USB token	Thiết bị phần cứng được sử dụng để bảo quản và sử dụng cặp khóa trong hạ tầng khóa công khai.

2. Trách nhiệm công bố thông tin và địa chỉ lưu trữ

2.1. Lưu trữ

- ONE-CA chịu trách nhiệm duy trì các địa chỉ lưu trữ (repository) cho phép truy nhập từ internet. ONE-CA 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

- ONE-CA 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.
    - ONE-CA công bố thông tin chứng thư số của khách hàng tại địa chỉ
        - ldap://ldap.one-ca.net:389
    - Thông tin chứng thư số bị thu hồi được công bố tại địa chỉ
        - http://crl.one-ca.net/one-ca.crl
- ONE-CA 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:
    - http://one-ca.net/cps
- ONE-CA công bố thông tin CA tại:
    - http://one-ca.net/download
- Địa chỉ truy cập OCSP Responder của ONE-CA:
    - http://ocsp.one-ca.net

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.
- **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

- ONE-CA không giới hạn việc truy xuất chính sách chứng thư số, quy chế chứng thực, chứng thư số, 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. 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 ONE-CA cấp phải được kiểm tra tính xác thực.

3.1.1. Quy định các kiểu 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 ONE-CA 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 mà đối tượng sở hữu chứng thư số thuộc.
Bộ phận tổ chức (OU)	Bộ phận thuộc tổ chức (O) mà đối tượng sở hữu chứng thư số thuộc
Tỉnh/Thành Phố (S)	Tên Tỉnh, Thành phố trực thuộc trung ương mà đối tượng sở hữu chứng thư số thuộc.
Quận/Huyện (L)	Tên Quận, Huyện mà đối tượng sở hữu chứng thư số thuộc
Tên thường gọi (CN)	Tên đối tượng sở hữu chứng thư số, tên miền nếu là chứng thư số SSL
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. • Đối với cơ quan tổ chức có Mã số thuế, ONE-CA sẽ sử dụng Mã số thuế làm Mã định danh. • Đối với cơ quan tổ chức nhà nước không có Mã số thuế, ONE-CA sẽ sử dụng Mã ngân sách làm Mã định danh.

DN trong chứng thư số có một thành phần là CN (Common Name - tên thường gọi).

- CN trong chứng thư số của các tổ chức có thể là tên miền, tên pháp lý của tổ chức hay tên của đại diện được ủy quyền của tổ chức đó.
- CN trong chứng thư số của người dùng cá nhân là họ tên trong chứng minh thư nhân dân/Căn cước công dân của người dùng đó.

CN được kiểm tra tính xác thực trong quá trình cấp chứng thư số.

3.1.2. Quy định yêu cầu đối với tên

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

3.1.3. Quy định cú pháp định dạng tên

- 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. Khi này, nội dung tên sẽ không phải kiểm tra.

3.1.4. Quy định tính duy nhất của tên

Tên (DN) của thuê bao là duy nhất trong ONE-CA. Một thuê bao có thể có nhiều chứng thư số với cùng DN.

3.1.5. Chấp nhận, xác thực và vai trò của nhãn hiệu đăng ký (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 ONE-CA 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 ph10áp lý.

3.2. Xác minh đề nghị cấp chứng thư số

Xác minh nhận dạng đối tượng đăng ký 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 trong chứng thư số. ONE-CA sử dụng PKCS#10 chứng minh quyền sở hữu khóa bí mật. Việc chứng minh sự sở hữu khóa bí mật không phải thực hiện khi cặp khóa được ONE-CA sinh ra trên USB token.

3.2.2. Xác thực nhận dạng của tổ chức

- Khi có một yêu cầu đăng ký chứng thư số nhận dạng cho tổ chức, thông tin nhận dạng của tổ chức đó được xác minh. ONE-CA 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 nhận đăng ký kinh doanh hoặc giấy phép hoạt động, địa chỉ.
    - Hồ sơ xin cấp gồm có:
        - Đơn xin cấp chứng thư (theo mẫu của ONE-CA)
        - Giấy tờ xác thực nhận dạng tổ chức
        - Giấy tờ cá nhân đại diện tổ chức (hoặc giấy ủy quyền)
        - Các giấy tờ liên quan (nếu có)

- ONE-CA, hoặc các RA của ONE-CA thực hiện xác thực nhận dạng của tổ chức theo các thông tin nêu trên.
- Khi chứng thư số của tổ chức có chứa tên cá nhân làm đại diện, cần thực hiện các thủ tục xác thực sự ủy quyền như 3.2.5.
- 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 ONE-CA.

3.2.3. Xác thực nhận dạng của cá nhân

- Khi có một yêu cầu đăng ký chứng thư số nhận dạng cho cá nhân, thông tin nhận dạng của cá nhân đó được xác minh. ONE-CA sẽ xác minh các thông tin bắt buộc sau:
  - ONE-CA, hoặc các RA của ONE-CA để thực hiện xác thực nhận dạng 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 ONE-CA)
    - Giấy tờ xác thực nhận dạng cá nhân
    - Các giấy tờ liên quan (nếu có)
  - Quy trình xác thực nhận dạng của cá nhân đăng ký chứng thư số như sau:
    - Người đăng ký nộp hồ sơ cho ONE-CA/RA.
    - ONE-CA/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:
  - Bộ phận 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 sự ủy quyền

- 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, 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, ONE-CA 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 đổi cặp khóa

- Trước khi một chứng thư số hết hạn, thuê bao cần có một chứng thư số mới. Thay đổi cặp khóa có thể có 2 trường hợp:
    - Thông thường: Sinh một cặp khóa mới thay thế cặp khóa trong chứng thư số đã hết hạn (đổi khóa - rekey) hoặc có yêu cầu gia hạn chứng thư số.
    - Thay đổi cặp khóa sau khi cặp khóa trong chứng thư số cũ bị thu hồi.

3.3.1. Nhận dạng và xác thực yêu cầu thay đổi cặp khóa thông thường

- Thời hạn xin thay đổi cặp khóa của thuê bao: từ 90 ngày trước đến ngày cuối cùng khi chứng thư số hết hạn yêu cầu gia hạn thay đổi cặp khóa sẽ được chấp nhận.
- Đối với trường hợp chứng thư số hết hạn, các yêu cầu được chuyển qua thực hiện cấp mới quy định trong 3.2 của tài liệu này
- ONE-CA hoặc RA có trách nhiệm xác thực yêu cầu thay đổi cặp khóa của thuê bao sau khi nhận đơn xin làm mới. ONE-CA sử dụng phương pháp xác thực làm căn cứ để chấp nhận một yêu cầu làm mới.
    - Sử dụng phương pháp xác thực: Thuê bao phải gửi các giấy tờ xác thực yêu cầu thay đổi khóa trong yêu cầu gia hạn chứng thư số cho ONE-CA. Bao gồm các thông tin tương ứng: Thông tin thuê bao, các giấy tờ kèm theo (nếu có thay đổi), đơn đăng ký, các giấy tờ khác nếu có.
- Sau khi xác thực, ONE-CA ban hành ngay chứng thư số mới cho thuê bao tương ứng với cặp khóa mới.
- Sau khi ban hành chứng thư số mới cho thuê bao, ONE-CA hoặc RA xác minh lại nhận dạng của đối tượng yêu cầu làm mới chứng thư số và các thông tin liên quan:
    - ONE-CA 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. ONE-CA 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, ONE-CA kiểm tra thông tin tên miền thông qua dữ liệu của các nhà cung cấp tên miền tương ứng.
    - ONE-CA 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 đổi cặp khóa sau khi thu hồi

- Nhận dạng và xác thực được thực hiện thông qua việc sử dụng bộ câu hỏi xác thực.
- Thuê bao không được phép làm mới cặp khóa (và chứng thư số) sau khi bị thu hồi nếu lý do thu hồi chứng thư số là một trong các nguyên nhân sau:
    - ONE-CA 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 ONE-CA.

3.4. Xác minh đề nghị thu hồi chứng thư số

- Khi có một yêu cầu thu hồi chứng thư số từ thuê bao, ONE-CA 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: ONE-CA 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.
  - ONE-CA 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, ONE-CA 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 ONE-CA một lúc. Mỗi yêu cầu sẽ được xác thực thông qua chữ ký số của RA.

3.5. Nhận dạng và xác thực yêu cầu gian hạn chứng thư số

- Trước khi một chứng thư số hết hạn, thuê bao cần có một chứng thư số mới. Làm mới chứng thư số có thể có 2 trường hợp:
  - Sinh một cặp khóa mới hoặc giữ nguyên thay thế cặp khóa trong chứng thư số đã còn thời hạn từ 0 đến 90 ngày.
- Thời hạn xin làm mới của thuê bao: từ 90 ngày trước khi chứng thư số hết hạn cho tới 30 ngày sau thời điểm chứng thư số hết hạn. Sau 30 ngày hết hạn chứng thư số, yêu cầu làm mới chứng thư số sẽ không được chấp nhận, thuê bao phải thực hiện lại các bước như đăng ký mới.
- ONE-CA hoặc RA có trách nhiệm xác thực yêu cầu làm mới của thuê bao sau khi nhận đơn xin làm mới. ONE-CA sử dụng một trong hai phương pháp xác thực làm căn cứ để chấp nhận một yêu cầu làm mới.
  - Chứng minh quyền sở hữu khóa bí mật: thuê bao sử dụng chứng thư số của mình để gửi yêu cầu gia hạn lên ONE-CA, khi thuê bao yêu cầu làm mới chứng thư số yêu cầu này ngay lập tức được ONE-CA chấp nhận.
  - Sử dụng phương pháp xác thực: Thuê bao phải trả lời đúng toàn bộ các câu hỏi xác thực để được ONE-CA chấp nhận yêu cầu làm mới chứng thư số.
- Sau khi xác thực, ONE-CA ban hành ngay chứng thư số mới cho thuê bao.
- Sau khi ban hành chứng thư số mới cho thuê bao, ONE-CA hoặc RA xác minh lại nhận dạng của đối tượng yêu cầu làm mới chứng thư số và các thông tin liên quan:

- ONE-CA 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. ONE-CA 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, ONE-CA kiểm tra thông tin tên miền thông qua dữ liệu của các nhà cung cấp tên miền tương ứng.
- ONE-CA 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).

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

4.1. Yêu cầu cấp chứng thư số

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

- Các đối tượng sau có thể gửi đăng ký cấp chứng thư số:
  - Đại diện của các RA/CA của ONE-CA.
  - Cá nhân, đại diện của tổ chức xin cấp chứng thư số.

4.1.2. Đăng ký cấp chứng thư số và trách nhiệm của các bên

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

- Thuê bao làm thủ tục và ký một thỏa thuận với ONE-CA, 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 ONE-CA: 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 ONE-CA hoặc thông qua RA
    - Chứng minh quyền sở hữu và tính duy nhất của khóa bí mật tương ứng với khóa công khai vừa gửi theo 3.2.1.

4.1.2.2. Chứng thư số của RA

- Để đăng ký cấp chứng thư số từ ONE-CA, RA phải thực hiện việc ký hợp đồng với ONE-CA và tiến hành các thủ tục đăng ký cấp chứng thư số tương tự như các thuê bao.
- ONE-CA sẽ tổ chức nghi lễ sinh khóa cho RA.
- Trách nhiệm của RA được làm rõ trong phần 9.6.2.

4.2. Xử lý yêu cầu cấp chứng thư số

4.2.1. Nhận dạng và xác thực

- ONE-CA/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 đăng ký cấp chứng thư số

- ONE-CA/RA chấp nhận một đơn đăng ký nếu các điều kiện sau đây thỏa mãn:

- Mọi thông tin cần xác thực được nhận dạng và xác thực đúng.
- Các khoản phí cần thiết đã nhận được từ đối tượng đăng ký.

- ONE-CA/RA không chấp nhận đơn đơn đăng ký nếu:
  - Một trong các thông tin cần xác thực được nhận dạng và xác thực sai.
  - Người đăng ký không cung cấp đủ tài liệu xác minh thông tin đã kê khai trong đơn đăng ký.
  - ONE-CA/RA chưa nhận được đầy đủ phí từ người đăng ký
  - 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 ONE-CA.

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

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

4.3. Cấp chứng thư số

4.3.1. Vai trò của ONE-CA trong tiến trình tạo chứng thư số

- Chứng thư số được ban hành sau khi ONE-CA/RA chấp nhận đơn xin cấp chứng thư số trực tiếp từ thuê bao hoặc thông qua RA. ONE-CA ban hành cho thuê bao một chứng thư số dựa vào những thông tin trong đơn xin cấp chứng thư số.

4.3.2. Thông báo cho thuê bao khi ONE-CA đã tạo xong chứng thư số

- ONE-CA sau khi ban hành chứng thư số cho sẽ thông báo cho thuê bao (trực tiếp hoặc gián tiếp thông qua RA). Thuê bao có thể lấy được chứng thư số bằng cách:
  - Nhận qua USB token.
  - Tải về từ trang Web của ONE-CA.

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 ONE-CA. 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 ONE-CA lưu trữ.

4.4.2. ONE-CA công bố chứng thư số

- Sau khi thuê bao chấp nhận chứng thư số (4.4.1), ONE-CA 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 ONE-CA và cơ sở dữ liệu LDAP.

4.4.3. Thông báo sự ban hành chứng thư số cho các đối tượng khác

- ONE-CA sẽ thông báo về việc chứng thư số được ban hành cho RA đã chấp nhận đơn xin cấp chứng thư số tương ứng.

4.5. Sử dụng cặp khóa và chứng thư số

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

- Chứng thư số và khóa bí mật tương ứng được phép sử dụng nếu thuê bao đã đồng ý thỏa thuận với ONE-CA 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 ONE-CA, với các điều khoản của chính sách chứng thư số, quy chế chứng thực của ONE-CA. Mục đích sử dụng chứng thư số phải nhất quán với phạm vi sử dụng được phép của chứng thư số đó (quy định trong trường KeyUsage trong chứng thư số). Ví dụ, nếu không có chức năng "Digital Signature" thì chứng thư số đó không được sử dụng để ký điện tử.
- 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. Khóa công khai và phạm vi sử dụng

- Để tin tưởng vào chứng thư số, người nhận cần đồng ý với các điều khoản của thỏa thuận với ONE-CA
- Người nhận cần dựa vào các thông tin sau để đánh giá sự tin cậy của chứng thư số:
    - Mục đích sử dụng của chứng thư số thể hiện trên chứng thư số (trong trường KeyUsage).
    - Mục đích sử dụng của chứng thư số thể hiện trong các tài liệu: thỏa thuận thuê bao, quy chế chứng thực, chính sách 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.

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

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

- Chỉ đối tượng đăng ký chứng thư số mới có quyền yêu cầu gia hạn chứng thư số đó.

4.6.3. Xử lý yêu cầu gia hạn chứng thư số

- ONE-CA/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 ONE-CA nhận được yêu cầu mà không cần có sự hiện diện vật lý của thuê bao tại ONE-CA 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

- Tương tự phần 4.4.1.

4.6.6. Công bố chứng thư số mới được tạo bởi CA

- Tương tự phần 4.4.2.

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

- Tương tự phần 4.4.3.

4.7. Thay đổi cặp khóa của thuê bao

- Đổi khóa là quá trình ban hành chứng thư số mới với một cặp khóa mới, thông tin khác trong chứng thư số không bị thay đổi. Đổi khóa được hỗ trợ cho mọi loại chứng thư số.

4.7.1. Các tình huống đổi khóa

- Trước khi hết hạn một chứng thư số, thuê bao đổi khóa chứng thư số để tiếp tục duy trì giá trị sử dụng của chứng thư số. Một chứng thư số có thể được đổi khóa sau khi đã hết hạn.
- Trong trường thuê bao nghi ngờ bị lộ khóa bí mật, thuê bao cần yêu cầu thu hồi khóa cũ và đổi khóa mới để duy trì giá trị sử dụng của chứng thư số.

4.7.2. Ai có thể yêu cầu đổi khóa

- Chỉ đối tượng đăng ký chứng thư số mới có quyền yêu cầu đổi khóa của chứng thư số đó.

4.7.3. Xử lý yêu cầu đổi khóa

- ONE-CA/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 ONE-CA nhận được yêu cầu mà không cần có sự hiện diện vật lý của thuê bao tại ONE-CA hoặc RA.

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

- Thông báo về sự tạo 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 đổi khóa cho các đối tượng khác

- Tương tự phần 4.4.3.

4.8. Thay đổi thông tin của chứng thư số

4.8.1. Các tình huống 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. Yêu cầu thay đổi chứng thư số

- Xem phần 4.1

4.8.3. Xử lý yêu cầu thay đổi chứng thư số

- ONE-CA 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 tình huống 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 (ONE-CA, 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, ONE-CA 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 ONE-CA.
    - 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 gây ảnh hưởng không tốt tới ONE-CA.
- Khi xem xét việc sử dụng chứng thư số có gây ảnh hưởng không tốt đến ONE-CA hay không, ONE-CA/RA sẽ xem xét dựa trên những yếu tố sau:
    - Số lượng phàn nàn nhận được.
    - Mức độ tin cậy của thông tin phàn nàn.
    - Các phàn nàn liên quan nhiều đến các yếu tố pháp luật (ví dụ: lừa đảo).
    - Có phàn nàn về thiệt hại gây ra do việc sử dụng chứng thư số của thuê bao.
    - ONE-CA 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 ONE-CA.
- Khi ONE-CA/Thuê bao xác định khóa thuê bao bị lộ thì ONE-CA 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.
  - ONE-CA/RA có quyền yêu cầu thu hồi chứng thư số mà nó đã duyệt cho thuê bao đó.
- Bộ Thông tin và Truyền thông có thể yêu cầu thu hồi chứng thư số nếu như hồ sơ không đầy đủ.

4.9.3. Thủ tục thu hồi chứng thư số

- Trước khi thu hồi chứng thư số, ONE-CA xác thực yêu cầu thu hồi từ thuê bao bằng cách:
  - Sử dụng chữ ký số: ONE-CA 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.
  - Sử dụng bộ câu hỏi xác thực: nếu thuê bao trả lời đúng các câu hỏi xác thực, quá trình thu hồi chứng thư số sẽ được thực hiện.
- Ngoài ra, ONE-CA xác thực bổ sung bằng cách liên lạc với thuê bao để chắc chắn rằng chính thuê bao đó 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 khác.
- ONE-CA sẽ xác thực nhận dạng của quản trị hệ thống thông qua xác thực chữ ký số trước khi cho phép thực hiện chức năng thu hồi.
- RA sử dụng hệ thống quản lý chứng thư số để chuyển các yêu cầu thu hồi tới ONE-CA. Mỗi yêu cầu được xác thực qua một chữ ký của RA.

4.9.4. Thời hạn gửi yêu cầu thu hồi chứng thư số

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

4.9.5. Thời gian bắt đầu xử lý yêu cầu thu hồi chứng thư số của CA

- ONE-CA sẽ xử lý ngay khi nhận được yêu cầu thu hồi chứng thư số.

4.9.6. Tần suất công bố CRL mới

- CRL cho chứng thư số của thuê bao được cập nhật ít nhất một ngày một lần. Chứng thư số hết hạn sẽ bị loại khỏi CRL.

4.9.7. Giới hạn trễ cho CRL

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

4.9.8. Kiểm tra trạng thái chứng thư số trực tuyến

- Thông tin thu hồi và trạng thái chứng thư số được công bố qua trang Web và OCSP như trong 2.2.

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

- 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 OCSP Responder.

4.9.10. Các dạng thông tin trạng thái thu hồi khác

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

4.9.11. Yêu cầu đặc biệt khi khóa CA bị mất hoặc lộ

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

4.9.12. Các tình huống tạm dừng chứng thư số

- ONE-CA không cung cấp dịch vụ này

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

- Không đối tượng nào có thể yêu cầu tạm dừng chứng thư số

4.9.14. Thủ tục tạm dừng chứng thư số

- Không có thủ tục tạm dừng chứng thư số

4.9.15. Giới hạn xử lý tạm dừng chứng thư số

- ONE-CA không cung cấp dịch vụ tạm dừng chứng thư số, không có quy định về giới hạn xử lý tạm dừng chứng thư số.

4.10. Kiểm tra trạng thái chứng thư số

4.10.1. Đặc điểm

- Trạng thái của chứng thư số được công bố qua CRL (Web hoặc LDAP) và OCSP responder

4.10.2. Tính sẵn sàng của dịch vụ

- Dịch vụ trạng thái chứng thư số được duy trì 24/7. Nếu có gián đoạn sẽ có thông báo trước 24 giờ.

4.10.3. Tùy chọn đặc biệt

- OCSP là dịch vụ tùy chọn, có phí.

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.

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

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

5. Kiểm soát, quản lý và vận hành

5.1. Kiểm soát an toàn, an ninh vật lý

- ONE-CA thực hiện các biện pháp kiểm soát và các thủ tục kiểm soát nhằm đảm bảo an ninh vật lý cho toàn bộ hệ thống. Được thể hiện theo các nội dung dưới đây.

5.1.1. Vị trí đặt và xây dựng hệ thống

- Hệ thống thiết bị ONE-CA được đặt tại hai trung tâm dữ liệu của công ty ONE-CA.
- 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 ONE-CA được bảo vệ nhất 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 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

- ONE-CA sử dụng nguồn điện ổn định, được thực hiện theo:
    - Sử dụng hệ thống UPS.
    - Có máy phát điện dự phòng, tự động chuyển từ điện lưới sang điện máy phát, hệ thống máy phát điện được kiểm tra bảo dưỡng định kỳ để đảm bảo tính sẵn sàng cao nhất.
- ONE-CA trang bị hệ thống điều hòa có điều khiển chính xác nhiệt độ. Hệ thống cảnh báo khi nhiệt độ vượt ngưỡng cho phép.

5.1.4. Chống nước

- Hệ thống thiết bị của ONE-CA được bố trí hạn chế tối đa sự tiếp xúc với nước.

5.1.5. Chống và bảo vệ trước các nguy cơ về lửa

- Hệ thống thiết bị của ONE-CA được bố trí giảm thiểu tối đa các nguy cơ về lửa. ONE-CA có quy định về phòng chống cháy nổ. Các biện pháp phòng cháy chữa cháy và thiết bị chữa cháy được chuẩn bị đầy đủ.

5.1.6. Phương tiện lưu trữ dữ liệu

- Phương tiện lưu trữ dữ liệu của ONE-CA được bảo vệ tương đương với mức độ quan trong của dữ liệu mà hệ thống đó lưu trữ.
- Phương tiện lưu trữ dữ liệu backup cũng được bảo vệ tương tự như hệ thống chính.

5.1.7. Xử lý rác thải

- Rác thải là tài liệu nhạy cảm, phương tiện lưu trữ dữ liệu được hủy bằng các biện pháp phù hợp trước khi được bỏ đi. Đảm bảo các thông tin trên các rác thải này không thể đọc được.

5.1.8. Hệ thống dự phòng ở địa điểm khác

- ONE-CA thực hiện việc lưu trữ dữ liệu dự phòng tại địa điểm dự phòng. Các biện pháp kiểm soát an ninh đối với hệ thống dự phòng cũng tương tự như hệ thống chính.

5.2. Quy trình kiểm soát

5.2.1. Những vai trò được tin tưởng

- Người được tin tưởng là những người có thể truy cập hay điều khiển các thao tác xác thực, mã hóa, liên quan đến:
  - Việc xác minh các thông tin trong đơn xin cấp chứng thư số.
  - Việc 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.
  - Việc ban hành, thu hồi chứng thư số.
  - Việc quản lý thông tin thuê bao, thông tin yêu cầu từ thuê bao.
- Người được tin tưởng bao gồm nhưng không giới hạn các đối tượng sau:
  - Người đứng đầu hệ thống.
  - Người quản trị hệ thống và bộ phận quản trị hệ thống.
  - Người phụ trách cấp phát chứng thư số và bộ phận phụ trách cấp phát chứng thư số.
- Những người được tin tưởng đều được xác minh về nhân thân, khả năng đảm bảo đáp ứng yêu cầu công việc trước khi được giao nhiệm vụ.

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

- ONE-CA thiết lập các chính sách và thủ tục kiểm soát đảm bảo có nhiều người tin tưởng thực hiện một công việc nhạy cảm như truy cập, điều khiển module phần cứng mã hóa.
- Các chính sách và thủ tục kiểm soát này của ONE-CA luôn đòi hỏi có ít nhất 2 người để thực hiện các công việc nhạy cảm.

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 ONE-CA đề phải được xác minh nhân thân, nhận dạng và trình độ. Quá trình nhận dạng được trình bày trong phần 5.3.1.
- ONE-CA đảm bảo rằng các cá nhân hoàn toàn được tin tưởng trước khi thực hiện các công việc nhạy cảm.

5.2.4. Những vai trò yêu cầu phải phân tách nhiệm vụ

- Các vai trò cần phải có sự phân tách nhiệm vụ, bao gồm nhưng không giới hạn:
  - Xác minh thông tin trong đơn xin cấp chứng thư số,
  - Chấp nhận, từ chối hay các xử lý khác với đơn xin cấp chứng thư số, yêu cầu thu hồi, làm mới chứng thư số
  - Ban hành, thu hồi chứng thư số.
  - Quản lý thông tin, yêu cầu của 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 ONE-CA được xác minh dựa trên: khả năng và kinh nghiệm chuyên môn đáp ứng các nhu cầu công việc, các bằng chứng chứng minh sự trong sạch về lý lịch.

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, ONE-CA kiểm tra các thông tin sau:
  - Kiểm tra, xác minh thông tin theo sơ yếu lý lịch.
  - Xác minh trình độ học vấn cao nhất đạt được.
  - Xem xét các thông tin tiền án/tiền sự (nếu có).

5.3.3. Yêu cầu đào tạo

- ONE-CA thực hiện các chương trình đào tạo nội bộ cho đội ngũ nhân viên, quá trình đào tạo được thực hiện theo quy trình, có ghi lại nhật ký đào tạo cho từng cá nhân.
- Chương trình huấn luyện của ONE-CA hướng tới trách nhiệm cụ thể của mỗi nhân viên, nội dụng huấn luyện bao gồm:
  - Các khái niệm PKI cơ bản.
  - Trách nhiệm công việc.
  - Các chính sách và thủ tục an ninh của ONE-CA.
  - Sử dụng và vận hành các thiết bị phần cứng và phần mềm.
  - Xử lý các sự cố.
  - Các thủ tục duy trì tính liên tục của dịch vụ khi có thảm họa.

5.3.4. Tần suất đào tạo và đào tạo lại

- ONE-CA 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.

5.3.5. Tần suất luân chuyển công việc

- ONE-CA thực hiện chính sách luân chuyển cán bộ trong phạm vi nội bộ của mình. ONE-CA không quy định cụ thể về tần suất luân chuyển công việc.

5.3.6. Hình phạt đối với các hành động không được phép

- ONE-CA 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 ONE-CA. Hình thức kỷ luật có thể gồm khiển trách, đình chỉ công việc tạm thời hoặc cho thôi việc, tùy thuộc vào mức độ nghiêm trọng của vi phạm.

5.3.7. Hợp đồng với các cố vấn độc lập

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

5.3.8. Cung cấp tài liệu cho nhân viên

- ONE-CA 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

- ONE-CA 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 ban hành chứng thư số, CRL.
  - Các sự kiện liên quan đến an ninh:
    - 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.

- 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
- 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

5.4.2. Tần suất xử lý nhật ký

- Nhật ký kiểm tra được kiểm tra, xử lý hàng tuần và khi có sự kiện không bình thường xảy ra.
- Tổng kết nhật ký được tài liệu hóa bằng văn bản.

5.4.3. Thời hạn giữ lại các nhật ký

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

5.4.4. Bảo vệ các nhật ký

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

5.4.5. Các thủ tục dự phòng nhật ký kiểm toán

- Nhật ký được backup theo chế độ backup chung của ONE-CA

5.4.6. Hệ thống ghi nhật ký

- Các log ứng dụng, hệ điều hành và mạng được ghi lại tự động
- Một số log được ghi bằng tay bởi nhân viên.
- Chi tiết về nơi lưu nhật ký và cơ chế lưu được mô tả trong Phương án kỹ thuật.

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.
- Thông tin đơn xin cấp chứng thư số.
- Các thông tin bổ sung của đơn xin cấp chứng thư số.
- Thông tin vòng đời chứng thư số như: thu hồi, đổi khóa, làm mới...

5.5.2. Thời hạn giữ lại các lưu trữ

- Thời gian lưu trữ các bản ghi ít nhất là 5 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

- Dữ liệu lưu trữ được backup theo chế độ backup chung của ONE-CA.

5.5.5. Nhãn thời gian của các bản ghi

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

5.5.6. Hệ thống lưu trữ

- Hệ thống lưu trữ của ONE-CA 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, ONE-CA 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 ONE-CA ban hành có thời gian sử dụng không quá thời gian sử dụng chứng thư số của ONE-CA được dùng để ký lên nó.

- Cặp khóa của ONE-CA sẽ không được sử dụng quá thời gian có hiệu lực của nó được quy định trong quy chế này. Chứng thư số của ONE-CA có thể được gia hạn (đổi khóa) khi trước khi cặp khóa cũ hết hạn.
- Trước khi hết hạn chứng thư số của ONE-CA, 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 ONE-CA. Quá trình chuyển tiếp khóa của ONE-CA đảm bảo rằng:
    - ONE-CA 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, ONE-CA 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 kiểm soát sự cố và thảm họa

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

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

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

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

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

5.7.4. Khả năng phục hồi hoạt động sau thảm họa

- ONE-CA thực hiện các kế hoạch dự phòng, đảm bảo hoạt động liên tục kể cả có thảm họa. Kế hoạch này được xây dựng thành các BCP (Business Continuity Planning). Các BCP này được kiểm tra, thử nghiệm và xem xét định kỳ.
- ONE-CA có khả năng phục hồi những hoạt động quan trọng trong vòng 24 giờ sau khi một thảm họa xảy ra. Ít nhất các hoạt động sau sẽ được phục hồi:
    - Ban hành chứng thư số.
    - Thu hồi chứng thư số.
    - Công bố thông tin thu hồi chứng thư số.
- Cơ sở dữ liệu của ONE-CA 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 ONE-CA được thiết kế có khả năng phục hồi hoạt động toàn bộ hệ thống trong vòng một tuần.
- ONE-CA dự phòng các thiết bị phần cứng và phần mềm cung cấp dịch vụ. Khóa bí mật của ONE-CA 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

- Khi không còn hoạt động, ONE-CA hoặc RA dùng mọi biện pháp cố gắng thông báo cho thuê bao, người nhận và các đối tượng trước khi dừng hoạt động. ONE-CA, RA sẽ có kế hoạch kết thúc nhằm giảm thiểu thiệt hại nhất cho khách hàng. ONE-CA 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 ONE-CA ban hành hết hạn.
    - Tiếp tục dịch vụ thu hồi như ban hành CRL và duy trì OCSP tới khi các chứng thư số do ONE-CA 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, ONE-CA 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 ONE-CA đảm nhiệm.
    - Thực hiện các thủ tục chuẩn bị trước khi chuyển các dịch vụ chứng thực sang cho CA khác.

6. Đảm bảo an toàn an ninh về kỹ thuật

6.1. Tạo và phân phối cặp khóa

6.1.1. Sự sinh cặp khóa

- Cặp khóa cho ONE-CA được sinh ra trong thiết bị phần cứng đạt chuẩn FIPS 140-2 level 3.
- Cặp khóa của thuê bao được tạo bên phía thuê bao hoặc trên USB Token trong trường hợp thuê bao có thỏa thuận cho phép tạo khóa phía ONE-CA.

6.1.2. Gửi khóa bí mật cho thuê bao

- Hệ thống phân phối khóa cho thuê bao của ONE-CA đảm bảo sự toàn vẹn và bảo mật của cặp khoá.
- Các giải pháp phân phối khóa của ONE-CA như sau:
    - Trường hợp cặp khóa được tạo ở phía thuê bao: không cần phải gửi khóa bí mật cho thuê bao.
    - Trường hợp cặp khóa được tạo trên ONE-CA: Khóa bí mật được lưu trong USB Token. ONE-CA 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 ONE-CA.
        - ONE-CA cung cấp dịch vụ chuyển USB Token đến tận nơi cho thuê bao thông qua dịch vụ chuyển phát của ONE-CA 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 ONE-CA

- Khóa công khai được thuê bao gửi cho ONE-CA thông qua thông điệp dạng PKCS#10. Nếu cặp khóa được tạo bên phía ONE-CA, việc gửi khóa cho CA là không cần thiết.

6.1.4. Gửi khóa công khai của ONE-CA cho người nhận

Người nhận có thể tải về khóa công khai của ONE-CA và RootCA từ trang Web của ONE-CA.

- Việc gửi khóa này cũng thông qua một phiên SSL để đảm bảo an ninh

6.1.5. Độ dài khóa

- ONE-CA chỉ chấp nhận cặp khóa có độ dài tối thiểu tương đương 1024 bit RSA cho các chứng thư số.

6.1.6. Các tham số sinh khóa công khai và kiểm tra chất lượng

- Quá trình sinh khóa công khai tuân theo chuẩn PKCS #1, đáp ứng theo các tiêu chuẩn trong Thông tư số 6/2015/TT-BTTTT ban hành ngày 23 tháng 3 năm 2015.

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

- Xem phần 7.1.2.1.

6.2. Kiểm soát và bảo vệ khóa bí mật

6.2.1. Tiêu chuẩn module mã hóa

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

6.2.2. Cơ chế kiểm soát khóa bí mật

- Cơ chế kiểm soát khóa bí mật được ONE-CA 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 nhất định, cần có M phần (M nhỏ hơn hoặc bằng N) mã chia sẻ để kích hoạt chứng năng đó.
- Tại ONE-CA, N = 4;

6.2.3. Lưu giữ ngoài khóa bí mật của thuê bao

- Lưu giữ ngoài khóa bí mật (key escrow) của thuê bao được trình bày trong phần 4.12.

6.2.4. Dự phòng khóa bí mật

- ONE-CA sẽ dự phòng (backup) khóa bí mật của mình để đề phòng thảm họa và trục trặc thiết bị. Khóa bí mật của ONE-CA được lưu trữ dự phòng trong các thiết bị HSM.
- ONE-CA không dự phòng khóa bí mật cho RA. Khóa bí mật của thuê bao được dự phòng như 6.2.3. Khóa bí mật được lưu trữ trong các thiết bị như USB Token sẽ không được dự phòng.

6.2.5. Lưu trữ khóa bí mật

- Sau khi chứng thư số của ONE-CA 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 ONE-CA.
- ONE-CA không lưu trữ khóa bí mật của RA, của thuê bao khi không có yêu cầu của pháp luật.

6.2.6. Chuyển khóa bí mật vào/ra HSM

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

6.2.7. Lưu trữ khóa bí mật trong HSM

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

6.2.8. Phương thức kích hoạt khóa bí mật

- Các thành viên ONE-CA sẽ có các biện pháp bảo vệ kích hoạt khóa bí mật phù hợp, cụ thể:
    - Đối với thuê bao: khóa bí mật được lưu trong USB token, việc kích hoạt khóa bí mật yêu cầu mật khẩu bảo vệ. Khi không sử dụng, khóa bí mật tồn tại ở dạng mã hóa.
    - Đối với quản trị hệ thống ONE-CA/RA: khóa bí mật được lưu trong USB token, việc kích hoạt khóa bí mật yêu cầu mật khẩu bảo vệ. Khi không sử dụng, khóa bí mật tồn tại ở dạng mã hóa.
    - Đối với RA: khóa bí mật được lưu trong USB token, việc kích hoạt khóa bí mật yêu cầu mật khẩu bảo vệ và phải xác thực được ít nhất 2 người quản trị. Khi không sử dụng, khóa bí mật tồn tại ở dạng mã hóa.
    - Đối với ONE-CA: 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 của ONE-CA/RA bị ngừng kích hoạt khi không chứa trong Token Reader (HSM). RA của ONE-CA được yêu cầu phải đăng xuất khỏi hệ thống khi rời chỗ làm việc.
- Khóa bí mật của quản trị hệ thống, của RA và của thuê bao có thể bị ngừng kích hoạt sau mỗi nhiệm vụ, sau khi đăng xuất hệ thống hoặc sau khi loại bỏ USB Token khỏi máy tính. Trong mọi trường hợp, thuê bao phải có nghĩa vụ thực hiện các biện pháp bảo vệ khóa bí mật của mình.

6.2.10. Thiết bị 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 mã hóa

- 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

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

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

- Thời hạn sử dụng của chứng thư số sẽ kết thúc khi chứng thư số đó hết hạn hoặc bị thu hồi.
- Thời hạn sử dụng cặp khóa của thuê bao giống như thời hạn sử dụng của chứng thư số, ngoại trừ chức năng giải mã và kiểm tra chữ ký sau khi chứng thư số hết hạn.
- ONE-CA 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 ONE-CA cung cấp cho thuê bao tùy thuộc vào thỏa thuận với thuê bao, thông thường là 1 năm. Chứng thư số cũng có thể kéo dài đến 2 năm hoặc hơn với các điều kiện sau:
    - Thuê bao được yêu cầu thực hiện lại các thủ tục xác thực ít nhất 12 tháng một lần (phần 3.2.3).
    - Thuê bao phải chứng minh quyền sở hữu khóa bí mật ít nhất 12 tháng một lần.
- Nếu điều kiện trên không được thực hiện, ONE-CA sẽ tự động thu hồi chứng thư số thuê bao.

6.4. Kích hoạt dữ liệu

6.4.1. Tạo và cài đặt dữ liệu kích hoạt

- Dữ liệu kích hoạt khóa bí mật của ONE-CA 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 9 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 ONE-CA được yêu cầu bảo vệ an toàn mã chia sẻ của họ. Những người này phải ký một thỏa thuận với ONE-CA 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 ONE-CA 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

6.4.3.1. Truyền, gửi dữ liệu kích hoạt

- Dữ liệu kích hoạt khi được truyền, gửi đi sẽ được bảo vệ chống lại việc mất, lộ, truy nhập không được phép.

6.4.3.2. Hủy bỏ dữ liệu kích hoạt

- Sau khi hết hạn sử dụng được quy định trong phần 5.5.2, ONE-CA sẽ loại bỏ dữ liệu kích hoạt khóa bí mật bằng cách ghi đè và/hoặc hủy bỏ vật lý.

6.5. Kiểm soát an ninh máy tính

- Hệ thống ONE-CA được vận hành trên hệ thống đảm bảo an ninh theo các chính sách của ONE-CA

6.5.1. Các yêu cầu an ninh hệ thống máy tính

- ONE-CA đảm bảo rằng các máy chủ cài đặt hệ thống CA và dữ liệu được bảo vệ trước các truy nhập không được phép. ONE-CA 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 ONE-CA 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 ONE-CA . Các quản trị viên của ONE-CA chỉ truy nhập và quản trị hệ thống thông qua một số giới hạn các máy tính quản trị được xác định sẵn.
- ONE-CA 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 nhiệp vụ phù hợp.

6.5.2. Đánh giá an ninh của hệ thống máy tính

- Hệ thống máy chủ cung cấp dịch vụ của ONE-CA đang hoạt động theo chuẩn ISO 27001, và được đánh giá định kỳ 6 tháng một lần.

6.6. Kiểm soát an ninh quy trình sử dụng

6.6.1. Giám sát triển khai triển khai hệ thống

- Các ứng dụng được phát triển và triển khai sử dụng trong ONE-CA tuân theo các tiêu chuẩn thiết kế, phát triển và triển khai phần mềm của ONE-CA. ONE-CA cũng cung cấp phần mềm cho các RA.
- Phần mềm được ONE-CA 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. Giám sát quản lý an ninh

- ONE-CA có các thủ tục và biện pháp kiểm soát an ninh trong quá trình thiết lập hệ thống. Các thủ tục và biện pháp này tuân theo tiêu chuẩn quản lý an ninh thông tin ISO 27001.

6.6.3. Giám sát an ninh vòng đời

- ONE-CA không quy định cụ thể quy trình giám sát an ninh vòng đời phát triển, triển khai và vận hành hệ thống cung cấp dịch vụ của ONE-CA.

6.7. Giám sát an ninh hệ thống mạng

- Hệ thống ONE-CA 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 (Time-Stamping)

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

6.9. Kiểm soát vòng đời khóa CA

6.9.1. Tạo và phân phối khóa

6.9.1.1. Sự sinh cặp khóa

- Cặp khóa cho ONE-CA được sinh ra trong thiết bị phần cứng đạt chuẩn FIPS 140-2 level 3.

6.9.1.2. Gửi khóa công khai của ONE-CA cho người nhận

- Người nhận có thể tải về khóa công khai của ONE-CA và RootCA từ trang Web của ONE-CA.
- Việc gửi khóa này cũng thông qua một phiên SSL để đảm bảo an ninh.

6.9.1.3. Độ dài khóa

- ONE-CA chỉ tạo cặp khóa có độ dài tối thiểu tương đương 2048 bit RSA để gửi lên bộ Thông Tin Truyền Thông.

6.9.1.4. Các tham số sinh khóa công khai và kiểm tra chất lượng

- Quá trình sinh khóa công khai tuân theo chuẩn PKCS #1, đáp ứng theo các tiêu chuẩn trong Thông tư số 6/2015/TT-BTTTT ban hành ngày 23 tháng 3 năm 2015.

6.9.2. Bảo vệ khóa bí mật và kiểm soát module mã hóa

6.9.2.1. Tiêu chuẩn module mã hóa

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

6.9.2.2. Cơ chế kiểm soát khóa bí mật

- Cơ chế kiểm soát khóa bí mật được ONE-CA 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 nhất định, cần có M phần (M nhỏ hơn hoặc bằng N) mã chia sẻ để kích hoạt chứng năng đó.
- Tại ONE-CA, N = 3;

6.9.2.3. Lưu giữ ngoài khóa bí mật của thuê bao

- Lưu giữ ngoài khóa bí mật (key escrow) của thuê bao được trình bày trong phần 4.12.

6.9.2.4. Dự phòng khóa bí mật

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

6.9.2.5. Lưu trữ khóa bí mật

- Sau khi chứng thư số của ONE-CA 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 ONE-CA.

6.9.2.6. Chuyển khóa bí mật vào/ra HSM

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

6.9.2.7. Lưu trữ khóa bí mật trong HSM

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

6.9.2.8. Phương thức kích hoạt khóa bí mật

- Các thành viên ONE-CA sẽ có các biện pháp bảo vệ kích hoạt khóa bí mật phù hợp, cụ thể:
    - Đối với ONE-CA: 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.

6.9.2.9. Phương pháp ngừng kích hoạt khóa bí mật

- Khóa bí mật của ONE-CA bị ngừng kích hoạt khi không chứa trong Token Reader (HSM).

6.9.2.10. 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 HSM được xóa bằng chứng năng xóa khóa của HSM
- Các hoạt động hủy bỏ khóa bí mật được ghi nhật ký.

6.9.2.11. Đánh giá module mã hóa

- Xem phần 6.2.1

6.9.3. Thời gian sử dụng cặp khóa CA

- Thời hạn sử dụng cặp khóa của ONE-CA 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.

6.9.4. Đổi khóa chứng thư số CA

- Đổi khóa là quá trình xin chứng thư số mới với một cặp khóa mới, thông tin khác trong chứng thư số ONE-CA không bị thay đổi.

6.9.4.1. Các tình huống đổi khóa

- Trước khi hết hạn một chứng thư số, thuê bao đổi khóa chứng thư số để tiếp tục duy trì giá trị sử dụng của chứng thư số. Một chứng thư số có thể được đổi khóa sau khi đã hết hạn.
- Trong trường thuê bao nghi ngờ bị lộ khóa bí mật, thuê bao cần yêu cầu thu hồi khóa cũ và đổi khóa mới để duy trì giá trị sử dụng của chứng thư số.

6.9.4.2. Ai có thể yêu cầu đổi khóa

- Chỉ đối tượng đăng ký chứng thư số mới có quyền yêu cầu đổi khóa của chứng thư số đó.

6.9.4.3. Xử lý yêu cầu đổi khóa

- ONE-CA tiến hành gửi hồ sơ xin phép lên bộ Thông Tin Truyền Thông.
- Sau khi được cấp phép, ONE-CA thực hiện sinh khóa và gửi PKCS#10 lên cho trung tâm chứng thực số quốc gia
- Khi trung tâm chứng thực chữ ký số quốc gia phê duyệt, cấp chứng thư, gửi lại cho ONE-CA thi thực hiện thông báo và cài đặt chứng thư vào hệ thống

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

- Thông báo về sự tạo chứng thư số mới trong phần 6.9.1.2.

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

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

7. Định dạng chứng thư số, CRL và OCSP

7.1. Định dạng của chứng thư số

- Chứng thư số do ONE-CA ban hành tuân theo chuẩn ITU-T X.509 và các quy định của RFC 5280. Tối thiểu, chứng thư số do ONE-CA 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 ONE-CA 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 5280
Signature	Chữ ký của ONE-CA, được mã hóa phù hợp với RFC 5280

7.1.1. Phiên bản

- Chứng thư số do ONE-CA ban hành theo X.509 Version 3.

7.1.2. Trường mở rộng

- ONE-CA ban hành chứng thư số X.509 phiên bản 3 với phần mở rộng được quy định từ 7.1.2 đến 7.1.2.8.

7.1.2.1. Key Usage

- Chứng thư số X.509 phiên bản 3 được ban hành theo RFC 5280. Phần mở rộng KeyUsage trong chứng thư số theo bảng sau.
- Chứng thư số do ONE-CA 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	dataEnciphermen t	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

7.1.2.2. Certificate policies

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

7.1.2.3. Subject Alternative Name

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

7.1.2.4. Basic Constraints

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

7.1.2.5. Extended Key Usage

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

	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

7.1.2.6. CRL Distribution Points

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

7.1.2.7. Authority Key Identifier

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

7.1.2.8. Subject Key Identifier

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

7.1.3. Các thuật toán ký

- ONE-CA ký lên các chứng thư số, sử dụng một trong các thuật toán sau:
  - sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
  - sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- Thủ tục ký chứng thư số áp dụng lược đồ RSASSA-PSS được quy định trong PKCS #1 phiên bản 2.1
- Phiên bản của ONE-CA hỗ trợ sử dụng thuật toán mã hóa SHA-256, SHA-384 và SHA-512 trong chứng thư số.

7.1.4. Khuôn dạng tên

- ONE-CA 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

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

7.1.6. Định danh chính sách và quy chế chứng thư số

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

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

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

7.1.8. Cú pháp và ngữ nghĩa của chính sách phân loại

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

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

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

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

- CRL do ONE-CA công bố tuân theo chuẩn ITU-T X.509 và các quy định của RFC 5280. Tối thiểu, CRL do ONE-CA 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. ONE-CA 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 – ONE-CA.
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

- ONE-CA ban hành X.509 Version 2 CRL.

7.2.2. CRL và các trường mở rộng của CRL

- CRL do ONE-CA ban hành không có quy định về các trường mở rộng.

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

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

7.3.2. Phần mở rộng OCSP

- Không quy định.

8. Kiểm định tính tuân thủ và các đánh giá khác

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

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

- Kiểm toán kỹ thuật được thực hiện ít nhất một năm một lần, phí tổn thuộc về phía bị kiểm toán.

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

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

8.3. Các nội dung kiểm toán kỹ thuật

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

8.4. Xử lý khi phát hiện sai sót

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

8.5. Công bố kết quả kiểm toán kỹ thuật

- Báo cáo kết quả kiểm toán kỹ thuật được ONE-CA công bố tại https://one-ca.net/

8.6. Tần suất và các trường hợp đánh giá

- Việc kiểm toán kỹ thuật các hoạt động ONE-CA được thực hiện định kỳ hàng năm hoặc theo yêu cầu từ RootCA.

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

- Kiểm toán kỹ thuật được thực hiện bởi những người không phụ thuộc vào ONE-CA.

9. Vấn đề nghiệp vụ và luật pháp

9.1. Phí/Giá

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

- ONE-CA có quyền yêu cầu tiền thù lao từ thuê bao cho việc ban hành, quản lý, và gia hạn chứng thư số. Mức phí sẽ tùy thuộc vào hợp đồng với từng thuê bao.

9.1.2. Phí truy nhập chứng thư số

- ONE-CA sẽ không thu phí cho việc truy nhập chứng thư số.

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

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

9.1.4. Phí dịch vụ khác

- ONE-CA không thu phí truy cập vào quy chế chứng thực của mình. ONE-CA giữ bản quyền với các tài liệu khác do ONE-CA công bố.

9.1.5. Chính sách hoàn phí

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

9.2. Trách nhiệm tài chính.

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

9.3. Bảo mật các 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:
  - Các thông tin được yêu cầu bởi pháp luật.
  - Hồ sơ đăng ký cấp chứng thư số.
  - Biên bản giao dịch.
  - Nhật ký kiểm tra ONE-CA.
  - Báo cáo kiểm tra ONE-CA.
  - 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 ONE-CA: phần cứng, phần mềm và quản trị của dịch vụ của ONE-CA.

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 ONE-CA và thông tin trên đó.
  - Không được chỉ rõ trong phần 9.3.1 được coi là không bí mật.

9.3.3. Trách nhiệm bảo vệ các thông tin bí mật

- ONE-CA thực hiện các biện pháp đảm bảo an ninh cho các thông tin bí mật.

9.4. Bảo mật thông tin cá nhân

9.4.1. Kế hoạch bảo mật thông tin cá nhân

- Chính sách bảo mật được công bố trên trang Web của ONE-CA. Nội dung chính sách bảo mật có trong phần phụ lục.

9.4.2. Phạm vi các thông tin bí mật

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

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

- Mọi thông tin được công bố trong một chứng thư số được coi là không bí mật.

9.4.4. Trách nhiệm bảo vệ các thông tin bí mật

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

9.4.5. Thông báo và sự đồng thuận sử dụng thông tin mật

- Thông tin bí mật sẽ không được sử dụng mà không có sự cho phép của người sở hữu thông tin hoặc đại diện 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

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

9.4.7. Các tình huống cung cấp thông tin khác

- ONE-CA 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

- ONE-CA giữ mọi quyền sở hữu chứng thư số và thông tin thu hồi mà nó tạo ra.
- ONE-CA 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

- ONE-CA 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 ONE-CA, 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 ONE-CA

- ONE-CA 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 ONE-CA 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 ONE-CA.
  - Tuân thủ theo quy trình quản lý vòng đời chứng thư số của ONE-CA.
- RA có trách nhiệm ký hợp đồng với ONE-CA. 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 ONE-CA đã nhận đầy đủ hồ sơ của thuê bao, và thông tin thuê bao được thẩm định.
  - Cam kết của RA với ONE-CA 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. Nội dung thỏa thuận thuê bao được trình bày trong phần phụ lục.

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 thư số, trong thỏa thuận người nhận trước khi quyết định tin tưởng chứng thư số do ONE-CA ban 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. Nội dung thỏa thuận thuê bao được trình bày trong phần phụ lục.

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

- Ngoài ONE-CA, RA, thuê bao và người nhận; không có tuyên bố và cam kết của đối tượng nào khác được ONE-CA quy định.

9.7. Từ chối trách nhiệm

- ONE-CA không quy định cụ thể về việc từ chối trách nhiệm.

9.8. Giới hạn trách nhiệm

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

Loại chứng thư số	Khoản tiền giới hạn phải trả
Chứng thư số cá nhân	250.000.000 VNĐ
Chứng thư số Web Server	500.000.000 VNĐ
Chứng thư số ký phần mềm	500.000.000 VNĐ

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

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 trả tiền cho ONE-CA 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 hoặc thuê bao sử dụng tên thuộc quyền sở hữu trí tuệ của người khác.
- Thỏa thuận thuê bao tương ứng có thêm các điều khoản bồi thường khác.

9.9.2. Bồi thường của người nhận

- Trong phạm vi cho phép của pháp luật, thỏa thuận người nhận sẽ yêu cầu người nhận trả tiền cho ONE-CA 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 ONE-CA
- Thỏa thuận người nhận tương ứng có thêm các điều khoản bồi thường khác.

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

9.10.2. Thời hạn hết hiệu lực

- Quy chế này được còn hiệu lực đến khi nó được thay thế bằng một phiên bản mới.

9.10.3. Ảnh hưởng của quy chế chứng thư số hết hiệu lực

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

9.11. Thông báo và trao đổi thông tin giữa các bên tham gia

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

9.12. Bổ sung và sửa đổi

9.12.1. Thủ tục bổ sung

- Quy chế này được bổ sung, sửa đổi bởi ONE-CA PMA. Nội dung sửa đổi được lưu tại https://one-ca.net/
- 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

- Đối với các thay đổi không quan trong như thay đổi URL, thông tin liên hệ, lỗi in ấn... ONE-CA PMA có quyền thay đổi quy chế mà không cần thông báo về sự thay đổi.

- Đối với các thay đổi theo đề xuất từ các thành viên, ONE-CA PMA sẽ xem xét yêu cầu thay đổi. Nếu quy chế cần thay đổi, ONE-CA PMA sẽ đưa ra thông báo về sự thay đổi này.
- Trong một số trường hợp đặc biệt, liên quan tới an ninh của hệ thống, ONE-CA PMA sẽ thực hiện sự thay đổi quy chế này lập tức, sau đó sẽ thông báo cho các thành viên.

9.12.2.1. Kỳ hạn góp ý

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

9.12.2.2. Cơ chế quản lý góp ý

- ONE-CA PMA sẽ xem xét mọi góp ý sửa đổi. ONE-CA PMA sẽ thực hiện một trong các tình huống sau:
    - Không thay đổi gì góp ý ban đầu; hoặc
    - Sửa đổi những góp ý sửa đổi và công bố lại chúng; hoặc
    - Hủy bỏ góp ý sửa đổi.

9.12.3. 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 ONE-CA PMA.

9.13. Thủ tục giải quyết tranh chấp

9.13.1. Tranh chấp giữa ONE-CA với RA

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

9.13.2. Tranh chấp giữa ONE-CA với người dùng cuối, người nhận

- Thỏa thuận thuê bao và thỏa thuận người nhận sẽ có một điều khoản về giải quyết tranh chấp.

9.14. Hệ thống giải quyết tranh chấp

- 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 bao trùm mọi thành viên

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

9.16.2. Sự chuyển nhượng

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

9.16.3. Tính độc lập của các điều khoản

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

9.16.4. Sự ép buộc

- Không có sự ép buộc nào đưa đến việc ban hành chứng thư của ONE-CA.

9.16.5. Trường hợp bất khả kháng

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

9.17. Các điều khoản khác

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