QUY CHẾ CHỨNG THỰC

DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG BKAVCA

MỤC LỤC

1. GIỚI THIỆU

1.1 Tổng quan

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 31/2020/TT-BTTTT của Bộ Thông Tin và Truyền Thông (TTTT) ban hành ngày 20 tháng 10 năm 2020.

Bản Quy chế chứng thực này hoàn toàn phù hợp với "QUY CHẾ CHỨNG THỰC MẪU CỦA TỔ CHỨC CUNG CẤP DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ" được quy định tại Phụ lục III trong Thông tư số 31/2020/TT-BTTTT của Bộ Thông Tin và Truyền Thông (TTTT) ban hành ngày 20 tháng 10 năm 2020.

- BkavCA là dịch vụ chứng thực chữ ký số công cộng của CÔNG TY CỔ PHẦN BKAV. Tài liệu này là Quy chế chứng thực do BkavCA ban hành.
- Quy chế chứng thực này chỉ rõ những thủ tục mà BkavCA 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 BkavCA 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.
- 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). BkavCA 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. BkavCA duy trì một chính sách chứng thư số mà mọi thành viên trong miền quản lý (BkavCA, các RA, thuê bao, người nhận) phải tuân theo.
- BkavCA 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, BkavCA 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, BkavCA 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, BkavCA 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, BkavCA ban hành các chứng thư số được liệt kê trong bảng dưới đây:

Loại chứng thư số	**Mức độ đảm bảo**	**Mô tả chức năng**
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 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 BkavCA. Quy chế này mô tả các điều sau:
    - Nghĩa vụ của BkavCA, RA, thuê bao, và người nhận trong miền quản lý của BkavCA.
    - 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 BkavCA.
    - Kiểm tra, giám sát an ninh mà các thành viên trong miền BkavCA phải thực hiện.
    - Các phương pháp mà BkavCA 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 BkavCA với các thành viên trong miền quản lý của BkavCA. 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.
- Tài liệu Quy chế chứng thực tuân thủ theo “Khung quy chế chứng thực và chính sách chứng thư” RFC 3647

1.2 Tên và dấu hiệu nhận diện tài liệu

- Tài liệu này là **Quy chế chứng thực BkavCA**.

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

1.3.1 BkavCA

- BkavCA là dịch vụ chứng thực chữ ký số công cộng của CÔNG TY CỔ PHẦN BKAV.

1.3.2 Registration Authority (RA)

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

1.3.3 Thuê bao

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

1.3.4 Người nhận

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

1.3.5 Các đối tượng khác

- Ngoài BkavCA, RA, thuê bao và người nhận, BkavCA 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 BkavCA và thỏa thuận của thuê bao với BkavCA.
- Hiện tại Bkav 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 BkavCA 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 BkavCA 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 BkavCA cấp không được sử dụng vào các mục đích vi phạm pháp luật.
- Chứng thư số của thuê bao BkavCA 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 Bkav
- Tầng 2, toà nhà HH1, khu đô thị Yên Hoà, phường Yên Hoà, quận Cầu Giấy, Hà Nội.

1.5.2 Liên hệ

- Địa chỉ: Công ty Cổ phần Bkav, Tầng 2, toà nhà HH1, khu đô thị Yên Hoà, phường Yên Hoà, quận Cầu Giấy, Hà Nội
- Email: bkavca@bkav.com
- Điện thoại: 84 - 24 - 3763 2552

1.5.3 Công nhận sự phù hợp của quy chế chứng thực

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

1.5.4 Thủ tục phê chuẩn quy chế chứng thực

- Sự phê chuẩn được thực hiện bởi BkavCA PMA.
- Các thay đổi, cập nhật của quy chế chứng thực được ghi lại, công bố tại https://bkavca.vn/cps_update.
- Quy chế chứng thực bản mới nhất được lưu trữ tại https://bkavca.vn/cps

1.6 Các định nghĩa và từ viết tắt

- Chi tiết trong phụ lục 1

2. TRÁCH NHIỆM LƯU TRỮ VÀ CÔNG BỐ THÔNG TIN

2.1 Lưu trữ

Tổ chức cung cấp dịch vụ chứng thực chữ ký số có trách nhiệm lưu trữ thông tin, bao gồm:

- Lưu trữ và sử dụng thông tin của thuê bao một cách bí mật, an toàn và chỉ được sử dụng thông tin này vào mục đích liên quan đến chứng thư số.
- Lưu trữ đầy đủ, chính xác và cập nhật thông tin của thuê bao phục vụ việc cấp chứng thư số trong suốt thời gian chứng thư số có hiệu lực và trong thời gian ít nhất 05 năm, kể từ khi chứng thư số hết hiệu lực.
- Lưu trữ đầy đủ, chính xác và cập nhật danh sách các chứng thư số có hiệu lực, đang tạm dừng và đã hết hiệu lực và cho phép, hướng dẫn người sử dụng Internet truy nhập trực tuyến 24 giờ trong ngày và 7 ngày trong tuần.
- Lưu trữ toàn bộ thông tin liên quan đến việc tạm đình chỉ hoặc thu hồi giấy phép và các cơ sở dữ liệu về thuê bao, chứng thư số trong thời gian ít nhất 05 (năm) năm, kể từ khi giấy phép bị tạm đình chỉ hoặc thu hồi.
- Thực hiện nghiêm quy định đối với việc lưu trữ, cập nhật và sử dụng thông tin thuê bao dịch vụ chứng thực chữ ký số tuân thủ theo Nghị định 130/2018/NĐ-CP ngày 27/09/2018 của Chính phủ quy định Chi tiết thi hành Luật giao dịch điện tử về chữ ký số và Nghị định 13/2023/NĐ-CP ngày 17/04/2023 của Chính phủ về

bảo vệ dữ liệu cá nhân.

2.2 Công bố thông tin

- BkavCA 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.
    - BkavCA công bố thông tin chứng thư số của khách hàng tại địa chỉ https://directory.bkavca.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. Chi tiết hướng dẫn tra cứu qua trang chủ https://bkavca.vn/chu-ky-so/huong-dan-tra-cuu-thong-tin-chung-thu-so/624
    - Thông tin chứng thư số SHA1 còn hạn bị thu hồi được công bố tại địa chỉ:

      http://crl.bkavca.vn/BkavCA.crl
    - Thông tin chứng thư số SHA2 còn hạn bị thu hồi được công bố tại địa chỉ:

      http://crl.bkavca.vn/BkavCA2.crl
- BkavCA 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:

  https://bkavca.vn
- BkavCA công bố thông tin CA tại:

  https://bkavca.vn
- Địa chỉ truy cập OCSP Responder của Bkav CA:

  http://ocsp.bkavca.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.
- **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

- BkavCA 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 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 BkavCA 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 BkavCA 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.
Tên thường gọi (CN)	Tên, các thông tin bổ sung cho đối tượng sở hữu chứng thư số, tên miền nếu là chứng thư số SSL
Đối tượng thay thế	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, số CCCD, số hộ chiếu. Đối với cơ quan tổ chức có Mã số thuế, Bkav sẽ sử dụng Mã số thuế làm Mã định danh. Đối với cơ quan tổ chức nhà nước không có Mã số thuế, Bkav sẽ sử dụng Mã ngân sách làm Mã định danh.

3.1.2 Quy định yêu cầu đối với tên

- Tên trong chứng thư số do BkavCA 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 BkavCA. Một thuê bao có thể có nhiều chứng thư số với cùng DN.
- 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 BkavCA 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

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. BkavCA 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 BkavCA 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. BkavCA 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 phép theo quy định tại 130/2018/NĐ-CP, 48/2024/NĐ-CP gồm có:
    - Đơn xin cấp chứng thư (theo mẫu của BkavCA)
    - Bản sao hợp lệ Đăng ký kinh doanh, Giấy đăng ký thuế hoặc Quyết định thành lập. (Trường hợp Đăng ký kinh doanh và Đăng ký thuế là một thì chỉ cần một loại)
    - Bản sao hợp lệ CMND/CCCD/Passport của người đại diện pháp luật.
    - ...
  - BkavCA, hoặc các RA của BkavCA 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 BkavCA.

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. BkavCA sẽ xác minh các thông tin bắt buộc sau:
  - BkavCA, hoặc các RA của BkavCA 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 phép theo quy định tại 130/2018/NĐ-CP, 48/2024/NĐ-CP gồm có:
    - Đơn xin cấp chứng thư (theo mẫu của BkavCA)
    - 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 BkavCA/RA.
    - BkavCA/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 Công nhận quyền

- Khi tên của cá nhân trong chứng thư số có liên quan tới một tổ chức, Bkav CA cần thực hiện:
    - Xác thực sự tồn tại của tổ chức thông qua ít nhất một bên thứ ba.
    - Xác thực các thông tin ghi trong Phiếu đăng ký cấp chữ ký số thông qua các tài liệu cần thiết và có thể thu thập.
    - Xác định danh tính và vị trí của cá nhân trong tổ chức tương ứng với các thông tin đã đăng ký hay không.

3.3 Xác minh đề nghị thay đổi cặp khóa

- Thuê bao phải có đơn xin thay đổi cặp khóa và các hồ sơ liên quan cần thiết theo quy định tại 130/2018/NĐ-CP, 48/2024/NĐ-CP tương tự như mục 3.2. BkavCA sẽ thực hiện thẩm định trực tiếp với thuê bao, hồ sơ thuê bao và phía yêu cầu thay đổi để đảm bảo đúng đối tượng và gắn trách nhiệm trước khi BkavCA thực hiện thu hồi chứng thư số của thuê bao xin thay đổi cặp khóa.

3.4 Xác minh đề nghị thu hồi chứng thư số

- Khi có một yêu cầu thu hồi chứng thư số từ thuê bao, BkavCA 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: BkavCA 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.
    - Bkav 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, BkavCA 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 BkavCA 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

4.1 Yêu cầu cấp chứng thư số

4.1.1 Đối tượng đề nghị cấp chứng thư số

  - Đại diện của các RA/CA của BkavCA.
  - Cá nhân, đại diện của tổ chức xin cấp chứng thư số.

4.1.2 Hồ sơ đề nghị cấp chứng thư số

- Chứng thư số của thuê bao cá nhân, tổ chức: Hồ sơ xin cấp theo quy định tại 130/2018/NĐ-CP, 48/2024/NĐ-CP như mục 3.2
- Chứng thư số của RA: Để đăng ký cấp chứng thư số từ BkavCA, RA phải thực hiện việc ký hợp đồng với BkavCA và tiến hành các thủ tục đăng ký cấp chứng thư số tương tự như các thuê bao.
- 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

- BkavCA/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

- BkavCA/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.
- BkavCA/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.
  - BkavCA 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 BkavCA.

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 BkavCA.

4.3 Cấp chứng thư số

4.3.1 Vai trò của BkavCA trong tiến trình tạo chứng thư số

- Chứng thư số được ban hành sau khi BkavCA/RA chấp nhận đơn xin cấp chứng thư số trực tiếp từ thuê bao hoặc thông qua RA. BkavCA ban hành cho thuê bao một chứng thư số dựa vào những thông tin trong đơn xin cấp chứng thư số: Thời hạn Chứng thư số cấp cho thuê bao bằng với thời hạn Chứng thư số BkavCA và có Hạn sử dụng (Hạn dùng) dịch vụ bằng thời hạn tương ứng với Gói dịch vụ Thuê bao đăng ký

4.3.2 Thông báo cho thuê bao khi BkavCA đã tạo xong chứng thư số

- BkavCA 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 BkavCA.

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 xác nhận thông tin trên chứng thư số phù hợp với thông tin thuê bao. Việc xác nhận này được BkavCA thực hiện qua email hoặc sử dụng USB Token lần đầu tiên. Thông tin xác nhận của thuê bao được lưu trữ trên hệ thống.

4.4.2 BkavCA công bố chứng thư số

- Sau khi thuê bao chấp nhận chứng thư số (4.4.1), BkavCA sẽ cập nhật chứng thư số cho thuê bao và 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 BkavCA và cơ sở dữ liệu LDAP.

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 BkavCA 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 BkavCA, với các điều khoản của chính sách chứng thư số, quy chế chứng thực của BkavCA. 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 BkavCA
- 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 thay đổi, còn lại các thông tin khác trong chứng thư số giữ nguyên không thay đổi, nếu trong trường hợp có thay đổi cặp khóa, thuê bao cần yêu cầu rõ.

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 Xử lý yêu cầu gia hạn chứng thư số

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

4.6.3 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.

4.6.4 Cập nhật, công bố chứng thư số mới

- Tương tự phần 4.4.1.

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

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

4.7.4 Thông báo, cập nhật chứng thư số sau khi thay đổi cặp khóa đến thuê bao

- Thông báo về sự tạo chứng thư số mới cho thuê bao giống mô tả trong phần 4.3.2

4.8 Thay đổi thông tin chứng thư số

4.8.1 Đối tượng được gửi yêu cầu thay đổi thông tin chứng thư số

- Chỉ chủ sở hữu chứng thư số mới có quyền gửi yêu cầu thay đổi thông tin chứng thư số

4.8.2 Các trường hợp thay đổi thông tin chứng thư số của thuê bao

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

4.8.3 Xử lý yêu cầu thay đổi chứng thư số

- BkavCA 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, cập nhật chứng thư số sau khi thay đổi thông tin đến thuê bao

- Xem phần 4.3.2

4.9 Tạm dừng và thu hồi chứng thư số

4.9.1 Đối tượng được phép 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.
    - BkavCA/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.

4.9.2 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 (BkavCA, 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, BkavCA 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 BkavCA.
    - 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 BkavCA.
- Khi xem xét việc sử dụng chứng thư số có gây ảnh hưởng không tốt đến BkavCA hay không, BkavCA/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.
- BkavCA 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 BkavCA.
- Khi BkavCA/Thuê bao xác định khóa thuê bao bị lộ thì BkavCA 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).

4.9.3 Quy trình, thủ tục thu hồi chứng thư số

- Trước khi thu hồi chứng thư số, BkavCA xác thực yêu cầu thu hồi từ thuê bao bằng cách:
    - Sử dụng chữ ký số: BkavCA 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, BkavCA 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.

- BkavCA 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 chuyển các yêu cầu thu hồi tới BkavCA. Mỗi yêu cầu được xác thực qua một chữ ký của RA.
- Sau khi tiếp nhận, xác minh và xử lý yêu cầu thành công, BkavCA sẽ tiến hành thu hồi và cập nhật lên hệ thống OCSP, CRL và thông báo chứng thư số đã bị thu hồi cho thuê bao. Thuê bao có thể kiểm tra thông tin trạng thái chứng thư số như mục 4.10
- 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.
- BkavCA tiến hành cập nhật CRL hàng ngày

4.9.4 Tạm dừng chứng thư số

- BkavCA không cung cấp dịch vụ này

4.10 Kiểm tra trạng thái chứng thư số

4.10.1 Các hình thức kiểm tra trạng thái chứng thư số của thuê bao

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

4.10.2 Khả năng sẵn sàng của dịch vụ kiểm tra trạng thái chứng thư số

- 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 Các tính năng khác

- OCSP là dịch vụ tùy chọn.

4.11 Chấm dứt dịch vụ của thuê bao

- Các trường hợp thuê bao chấm dứt dịch vụ
  - Thuê bao đã hết hạn mà không làm mới.
  - Thu hồi chứng thư số xảy ra mà không xin cấp một chứng thư số mới.
  - Thuê bao vi phạm thỏa thuận sử dụng với Bkav tại https://bkavca.vn/thoa-thuan-su-dung
- Thủ tục thu hồi chứng thư số:

  - Tham chiếu mục 4.9.3

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

- Hiện tại, BkavCA 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

5.1.1 Vị trí đặt và xây dựng hệ thống

- Hệ thống thiết bị BkavCA được đặt tại các trung tâm dữ liệu 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.
- Hệ thống DC được đặt tại: IDC Hòa Lạc - Khu Trung tâm, Khu Công nghệ cao Hòa Lạc Km 29, ĐCT08, Thạch Hoà, Thạch Thất, Hà Nội
- Hệ thống DR được đặt tại: VNPT IT - số 136 đường Nguyễn Phong Sắc, Làng Quốc tế Thăng Long, Cầu Giấy, Hà Nội

5.1.2 Truy cập truy cập vật lý

- Hệ thống BkavCA 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, điều hòa, chống nước, phòng chống cháy nổ

- BkavCA 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.

- BkavCA trang bị hệ thống điều hòa có điều khiển chính xác nhiệt độ. Hệ thống cảnh báo khi nhiệt độ vượt ngưỡng cho phép.
- Hệ thống thiết bị của BkavCA được bố trí hạn chế tối đa sự tiếp xúc với nước.
- Hệ thống thiết bị của BkavCA được bố trí giảm thiểu tối đa các nguy cơ về lửa. BkavCA 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.

5.1.4 Thiết bị lưu trữ dữ liệu

- Phương tiện lưu trữ dữ liệu của BkavCA được bảo vệ tương đương với mức độ quan trọng 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.

5.1.5 Hệ thống dự phòng

- BkavCA 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.

5.1.6 Quy trình xử lý rác, tiêu hủy thông tin nhạy cảm

- Các tài liệu và tài nguyên nhạy cảm cần được cắt thành từng miếng vụn trước khi hủy. Các phương tiện thu thập hay truyền các thông tin nhạy cảm cần được làm cho không thể truy cập được trước khi tiêu hủy. Các thiết bị dùng để mã hóa phải được phá hủy về mặt vật lý theo hướng dẫn của nhà sản xuất trước khi tiêu hủy. Các loại rác khác phải tiêu hủy đạt yêu cầu về tiêu chuẩn rác thải thông thường của Bkav CA
- Các tài liệu nhạy cảm liên quan đến thông tin của thuê bao được tiêu hủy bằng thiết bị hủy tài liệu. Các nội dung, tài liệu liên quan đến thông tin của thuê bao nếu tiêu hủy sẽ được tuân thủ theo Nghị định 13/2023/NĐ-CP ngày 17/04/2023 của Chính phủ về bảo vệ dữ liệu cá nhân.

5.2 Quy trình kiểm soát

5.2.1 Kiểm soát người có quyền truy cập, thao tác với hệ thống

- 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.
- BkavCA 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, sao lưu key trên HSM.
- Các chính sách và thủ tục kiểm soát này của BkavCA luôn đòi hỏi có ít nhất 2 người để thực hiện các công việc nhạy cảm.

5.2.2 Nhận dạng và xác thực từng thành viên

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

5.2.3 Phân chia nhân sự cho mỗi công việc, vai trì, trách nhiệm của từng thành viên

- 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, bằng cấp

- Những người tin cậy của BkavCA được xác minh dựa trên: khả năng và kinh nghiệm chuyên môn đáp ứng các nhu cầu công việc.

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, BkavCA 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 cho cán bộ vận hành, quản lý hệ thống

- BkavCA 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 BkavCA hướng tới trách nhiệm cụ thể của mỗi nhân viên, nội dung huấn luyện bao gồm:
    - Các khái niệm PKI cơ bản.
    - Trách nhiệm công việc.
    - Các chính sách và thủ tục an ninh của BkavCA.
    - 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.
- BkavCA 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.
- BkavCA 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.

5.3.4 Hình thức xử lý các trường hợp vi phạm

- BkavCA 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 BkavCA. 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.

5.4 Các quy trình ghi nhật ký hệ thống

5.4.1 Các loại sự kiện được ghi lại

- BkavCA 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, thời gian lưu trữ, bảo vệ 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.

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

5.5 Lưu trữ các bản ghi

5.5.1 Các loại bản ghi được lưu trữ, thông tin 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 bản ghi nhật ký

- 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 Quy trình lưu trữ bản ghi

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

5.6 Thay đổi khóa

- Trước khi chứng thư số của CA hết hạn, theo quy định, BkavCA 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 BkavCA ban hành có thời gian sử dụng không quá thời gian sử dụng chứng thư số của BkavCA được dùng để ký lên nó.
- Cặp khóa của BkavCA sẽ không được sử dụng quá thời gian có hiệu lực của nó được quy định trong quy chế này. Chứng thư số của BkavCA có thể được gia hạn (đổi khóa) khi trước khi cặp khóa cũ hết hạn.

- Trước khi hết hạn chứng thư số của BkavCA, 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 BkavCA. Quá trình chuyển tiếp khóa của BkavCA đảm bảo rằng:
    - BkavCA 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, BkavCA 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 BkavCA nghi ngờ bị mất/lộ, BkavCA sẽ thực hiện thủ tục xử lý khi khóa bị lộ. Đội xử lý sự cố ninh của BkavCA (người đứng đầu BkavCA, người phụ trách kỹ thuật và người phụ trách cấp phát chứng thư số.)chịu trách nhiệm điều phối thực hiện các bước trong thủ tục này.
- Nếu chứng thư số của BkavCA bị thu hồi, các thủ tục sau sẽ được thực hiện:
    - Trạng thái thu hồi chứng thư số của BkavCA sẽ được công bố bởi RootCA.
    - BkavCA cố gắng thông báo cho toàn bộ người nhận trong hệ thống BkavCA dừng sử dụng các chứng thư số do BkavCA ban hành.

  - BkavCA 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

- BkavCA 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.
- BkavCA 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 BkavCA 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 BkavCA được thiết kế có khả năng phục hồi hoạt động toàn bộ hệ thống trong vòng một tuần.
- BkavCA dự phòng các thiết bị phần cứng và phần mềm cung cấp dịch vụ. Khóa bí mật của BkavCA 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, BkavCA hoặc RA dùng mọi biện pháp cố gắng thông báo cho thuê bao, người nhận và các đối tượng trước khi dừng hoạt động. BkavCA, RA sẽ có kế hoạch kết thúc nhằm giảm thiểu thiệt hại nhất cho khách hàng. BkavCA 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 BkavCA 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 BkavCA 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, BkavCA 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 BkavCA 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 Tạo cặp khóa, kích thước cặp khóa

- Cặp khóa cho BkavCA được sinh ra trong thiết bị phần cứng đạt chuẩn FIPS 140-2 level 3. Cặp khóa được tạo bởi thuật toán RSA với độ dài khóa là 1024/2048 bit.
- Quy trình sinh khóa Thuê bao:
- Thuê bao hoàn thành đơn đăng ký chứng thư số và cung cấp tài liệu xác minh thông tin đã kê khai.
- Cặp khóa của thuê bao được tạo bên phía thuê bao hoặc trên USB Token đạt tiêu chuẩn theo quy định, trong trường hợp thuê bao có thỏa thuận cho phép tạo khóa phía BkavCA
- Cặp khóa thuê bao được tạo trong thiết bị đạt tiêu chuẩn theo quy định
- Cặp khóa được tạo bởi thuật toán RSA với độ dài khóa là 1024/2048 bit.
- Gửi khóa công khai trực tiếp cho BkavCA 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.

6.1.2 Quy trình phân phối cặp khóa

- Hệ thống phân phối khóa cho thuê bao của BkavCA đảm bảo sự toàn vẹn và bảo mật của cặp khoá.
- Các giải pháp phân phối khóa của BkavCA 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 BkavCA: Khóa bí mật được lưu trong USB Token. BkavCA 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 BkavCA.
- Bkav cung cấp dịch vụ chuyển USB Token đến tận nơi cho thuê bao thông qua dịch vụ chuyển phát của Bkav 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.

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

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

6.2 Kiểm soát và bảo vệ khóa bí mật

6.2.1 Tiêu chuẩn kỹ thuật đối với thiết bị mật mã

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

6.2.2 Cơ chế kiểm soát, bảo vệ khóa bí mật

- Cơ chế kiểm soát khóa bí mật được BkavCA 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 BkavCA, N = 4;

6.2.3 Dự phòng khóa bí mật

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

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

6.3.1 Lưu trữ cặp khóa

- Sau khi chứng thư số của BkavCA 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 BkavCA .
- BkavCA không lưu trữ khóa bí mật của RA, của thuê bao khi không có yêu cầu của pháp luật.
- BkavCA sẽ lưu trữ khóa công khai của mình, của RA và toàn bộ thuê bao.

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

- Thời hạn sử dụng chứng thư số là thời hạn gói dịch vụ của thuê bao đăng ký theo thỏa thuận với Bkav CA.
- Thời hạn sử dụng của chứng thư số cung cấp cho thuê bao sẽ kết thúc khi hết hạn gói dịch vụ khách hàng đăng ký hoặc chứng thư số bị thu hồi.
- Trong trường hợp thay đổi chứng thư số của Bkav CA thuê bao sẽ được cấp chứng thư số mới bằng thời hạn còn lại của gói dịch vụ khách hàng đã đăng ký
- Trước ít nhất 30 ngày hết hạn dịch vụ của thuê bao, Bkav sẽ liên hệ mời thuê bao gia hạn dịch vụ. Đến ngày hết hạn dịch vụ mà thuê bao chưa đồng ý gia hạn và thanh toán phí gói dịch vụ tiếp theo thì Bkav có quyền ngừng cung cấp dịch vụ cho thuê bao bằng cách khóa không cho thuê bao sử dụng thông qua phần mềm quản lý Chứng thư số của Thuê bao hoặc thu hồi chứng thư số của thuê bao.
- BkavCA không ban hành các chứng thư số có thời hạn sử dụng vượt quá thời hạn sử dụng chứng thư số của CA.

6.4 Kích hoạt dữ liệu

6.4.1 Khởi tạo và cài đặt dữ liệu kích hoạt khóa bí mật

- Dữ liệu kích hoạt khóa bí mật của BkavCA 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 BkavCA được yêu cầu bảo vệ an toàn mã chia sẻ của họ. Những người này phải ký một thỏa thuận với BkavCA về việc đảm bảo trách nhiệm trong việc bảo vệ mã chia sẻ mà họ giữ.
- Thuê bao của BkavCA được yêu cầu lưu trữ khóa bí mật dưới dạng mã hóa sử dụng USB Token và mật khẩu bảo vệ.

6.5 Kiểm soát an ninh máy tính

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

6.5.1 Các yêu cầu an ninh hệ thống máy tính

- BkavCA đảm bảo rằng các máy chủ cài đặt hệ thống CA và dữ liệu được bảo vệ trước các truy nhập không được phép. BkavCA 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 BkavCA 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 BkavCA. Các quản trị viên của BkavCA chỉ truy nhập và quản trị hệ thống thông qua một số giới hạn các máy tính quản trị được xác định sẵn.
- BkavCA 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 Định kỳ đánh giá an ninh của hệ thống máy tính

- Hệ thống máy chủ cung cấp dịch vụ của BkavCA đa được đánh giá định kỳ 1 năm 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 BkavCA tuân theo các tiêu chuẩn thiết kế, phát triển và triển khai phần mềm của BkavCA. BkavCA cũng cung cấp phần mềm cho các RA.
- Phần mềm được BkavCA 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

- BkavCA 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.

6.7 Giám sát an ninh hệ thống mạng

- Hệ thống BkavCA thực hiện các chức năng trong vùng mạng đảm bảo an ninh.
- Mọi hoạt động tác động tới hệ thống đều được ghi lại.

6.8 Dấu thời gian (Time-Stamping)

- BkavCA chưa triển khai dịch vụ dấu 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 dạng của chứng thư số

7.1.1 Quy định các trường thông tin cơ bản của chứng thư số

- Chứng thư số do BkavCA ban hành tuân theo chuẩn ITU-T X.509 và các quy định của RFC 5280.
- Chứng thư số do BkavCA ban hành theo X.509 Version 3.
- Tối thiểu, chứng thư số do BkavCA 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 BkavCA 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 BkavCA, được mã hóa phù hợp với RFC 5280

7.1.2 Quy định các trường thông tin mở rộng của chứng thư số

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 BkavCA 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

7.1.2.2 Certificate policies

- Chứng thư số do BkavCA 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 BkavCA 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 BkavCA, giá trị này trùng với trường Subject Key Identifier trong chứng thư của BkavCA do Root CA ban hành.

7.1.2.8 Subject Key Identifier

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

7.1.3 Các thuật toán ký

- BkavCA 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 BkavCA 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

- BkavCA 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 Organizational Unit.

7.1.5 Ràng buộc tên

- BkavCA 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 BkavCA ban hành không có trường mở rộng này.

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

- BkavCA 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

- BkavCA 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

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

Trường	Giá trị
Version	Xem phần 7.2.1
Signature Algorithm	Thuật toán được dùng để ký CRL. BkavCA 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 – BkavCA.

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

- BkavCA ban hành X.509 Version 2 CRL.

7.2.2 CRL và các trường mở rộng của CRL

- CRL do BkavCA 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

- BkavCA 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

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

8.3 Các nội dung kiểm tra kỹ thuật

Các nội dung kiểm tra kỹ thuật, bảo trì hệ thống bao gồm:

- Hạ tầng hệ thống.
- Các quy trình quản lý khóa.
- Quy trình vận hành hệ thống.
- Các nội dung khác theo yêu cầu của đơn vị kiểm tra kỹ thuật.

8.4 Xử lý khi phát hiện sai sót

- Sau khi có báo cáo kiểm toán kỹ thuật, BkavCA sẽ làm việc với RootCA về những nội dung chưa phù hợp.
- BkavCA 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 BkavCA 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 ninh của hệ thống BkavCA.
    - BkavCA thực hiện kế hoạch xử lý nhưng không có kết quả.

8.5 Công bố kết quả kiểm tra kỹ thuật

- Báo cáo kết quả kiểm toán kỹ thuật được BkavCA công bố tại https://bkavca.vn/

8.6 Tần suất và các trường hợp đánh giá

- Như 8.1

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

- Như 8.2

9. CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC

9.1 Phí/Giá

- Phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số theo quy định tại Thông tư số 17/2018/TT-BTC ngày 09/02/2018 của Bộ Tài chính sửa đổi, bổ sung một số điều của Thông tư số 305/2016/TT-BTC và Thông tư số 305/2016/TT-BTC ngày 15/11/2016 của Bộ Tài chính quy định mức thu, chế độ thu, nộp, quản lý và sử dụng phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số.
- Giá cấp, gia hạn, thu hồi chứng thư số.

- Các loại chi phí khác (nếu có).

9.2 Trách nhiệm tài chính

- Bkav duy trì một mức mức bảo hiểm hợp lý cho các lỗi BkavCA.
- Bkav 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 BkavCA 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 BkavCA.
  - Báo cáo kiểm tra BkavCA.
  - 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 BkavCA: phần cứng, phần mềm và quản trị của dịch vụ của BkavCA.

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 BkavCA 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

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

9.4 Bảo mật thông tin cá nhân

- Chính sách bảo mật được công bố trên trang Web của BkavCA tại https://bkavca.vn/dieu-khoan-bao-mat.

9.4.1 Phạm vi thông tin nghiệp vụ cần được bảo vệ

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

9.4.2 Trách nhiệm bảo mật thông tin cá nhân

- BkavCA 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.

9.5 Quyền sở hữu trí tuệ

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

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

- BkavCA 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 (doanh 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 BkavCA, 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 BkavCA

- BkavCA cam kết chịu hoàn toàn trách nhiệm về tính chính xác của thông tin nêu trong quy chế chứng thực này.
- BkavCA 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 BkavCA 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.
- BkavCA xác nhận trong quá trình cung cấp dịch vụ chứng thực chữ ký số công cộng cho khách hàng, BkavCA có thực hiện các hoạt động xử lý dữ liệu cá nhân để cung cấp dịch vụ cho khách hàng theo quy định tại Nghị định 130/2018/NĐ-CP ngày 27/09/2018 của Chính phủ quy định Chi tiết thi hành Luật giao dịch điện tử về chữ ký số và Nghị định 13/2023/NĐ-CP ngày 17/04/2023 của Chính phủ về bảo vệ dữ liệu cá nhân.

9.6.2 Tuyên bố và cam kết của RA

- RA có trách nhiệm ký hợp đồng với Bkav. 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 BkavCA đã nhận đầy đủ hồ sơ của thuê bao, và thông tin thuê bao được thẩm định.
  - Cam kết của RA với BkavCA 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.
- RA có trách nhiệm :
  - Thực hiện các quyền, nghĩa vụ của đại lý theo quy định của pháp luật về thương mại.
  - Hướng dẫn đầy đủ hồ sơ, thủ tục cấp chứng thư số cho thuê bao.
  - Đảm bảo thông tin đăng ký cấp chứng thư số không sai lệch, Không có lỗi trong quá trình duyệt hồ sơ xin cấp chứng thư số và quá trình gửi thông tin cho BkavCA.
  - Niêm yết công khai quy trình cấp chứng thư số tại trụ sở của đại lý
  - Đảm bảo kênh thông tin 24 giờ trong ngày và 7 ngày trong tuần để tiếp nhận yêu cầu từ thuê bao.

  - Chịu trách nhiệm báo cáo khi có yêu cầu của cơ quan chức năng nhằm phục vụ công tác quản lý nhà nước về dịch vụ chứng thực chữ ký số.

- RA cam kết chỉ cung cấp yêu cầu của thuê bao đề nghị cấp chứng thư số cho BkavCA, RA không thực hiện lưu trữ thông tin thuê bao, việc lưu trữ, sử dụng thông tin thuê bao thuộc trách nhiệm của BkavCA

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

9.7 Từ chối trách nhiệm

- BkavCA 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 BkavCA. Trong mọi trường hợp, khoản tiền mà BkavCA 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	10.000 USD
Chứng thư số Web Server	20.000 USD
Chứng thư số ký phần mềm	20.000 USD

- 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 BkavCA 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 BkavCA 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 BkavCA
- 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 BkavCA. 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 với các bên tham gia

- Trừ khi được quy định rõ ràng, các thành viên BkavCA 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 Các trường hợp được sửa đổi, bổ sung quy chế

- Khi quy chế nội dung không còn phù hợp với thực tế, quy chế được bổ sung, sửa đổi

- Quy chế này được bổ sung, sửa đổi bởi BkavCA PMA. Nội dung sửa đổi được lưu tại https://bkavca.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 Quy trình sửa đổi, bổ sung quy chế

- Đối với các thay đổi không quan trọng như thay đổi URL, thông tin liên hệ, lỗi in ấn… BkavCA 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, BkavCA PMA sẽ xem xét yêu cầu thay đổi. Nếu quy chế cần thay đổi, BkavCA 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, BkavCA PMA sẽ thực hiện sự thay đổi quy chế này lập tức, sau đó sẽ thông báo cho các thành viên.

9.13 Thủ tục giải quyết tranh chấp

9.13.1 Tranh chấp giữa BkavCA với RA

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

9.13.2 Tranh chấp giữa BkavCA 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 pháp lý 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 bao trùm mọi thành viên

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

9.16.2 Sự chuyển nhượng

- Không có quy định nào cho phép chuyển nhượng quyền sử dụng chứng thư số. BkavCA 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 BkavCA.

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 BkavCA.

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.

10. PHỤ LỤC

Bảng các thuật ngữ

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.	BkavCA	Nhà chứng thực chữ ký số do Công ty Cổ phần Bkav quản lý, được Bộ Thông Tin và Truyền Thông cấp phép hoạt động.
5.	BkavCA 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 BkavCA.

STT	Thuật ngữ / Từ viết tắt	Ngữ nghĩa
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 BkavCA, 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.

STT	Thuật ngữ / Từ viết tắt	Ngữ nghĩa
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 BkavCA 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 BkavCA 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 BkavCA 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.