

QUY CHẾ CHỨNG THỰC

**DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ THEO MÔ HÌNH KÝ SỐ TỪ XA
BKAV REMOTE SIGNING**

Mục lục

1. GIỚI THIỆU	5
1.1 Tổng quan	5
1.2 Tên và dấu hiệu nhận diện tài liệu	6
1.3 Các thành phần trong hệ thống dịch vụ chứng thực chữ ký số	6
1.4 Mục đích sử dụng chứng thư số	7
1.5 Quản lý quy chế chứng thực	7
1.6 Các định nghĩa và từ viết tắt	8
2. TRÁCH NHIỆM LƯU TRỮ VÀ CÔNG BỐ THÔNG TIN	8
2.1 Lưu trữ	8
2.2 Công bố thông tin	8
2.3 Thời gian, tần suất công bố thông tin	9
2.4 Kiểm soát truy nhập thông tin	9
3. NHẬN DẠNG VÀ XÁC THỰC YÊU CẦU XIN CẤP CHỨNG THƯ SỐ	9
3.1 Đặt tên trong chứng thư số	9
3.2 Xác minh đề nghị cấp chứng thư số	10
3.3 Xác minh đề nghị thay đổi cặp khóa	12
3.4 Xác minh đề nghị thu hồi chứng thư số	12
4. CÁC YÊU CẦU ĐỐI VỚI VÒNG ĐỜI HOẠT ĐỘNG CỦA CHỨNG THƯ SỐ THUÊ BAO	13
4.1 Yêu cầu cấp chứng thư số	13
4.2 Xử lý yêu cầu cấp chứng thư số	13
4.3 Cấp chứng thư số	14
4.4 Xác nhận và công bố công khai chứng thư số	14
4.5 Sử dụng cặp khóa và chứng thư số	14
4.6 Gia hạn chứng thư số	15
4.7 Thay đổi cặp khóa của thuê bao	15
4.8 Thay đổi thông tin chứng thư số	16
4.9 Tạm dừng và thu hồi chứng thư số	16
4.10 Kiểm tra trạng thái chứng thư số	18
5. KIỂM SOÁT, QUẢN LÝ VÀ VẬN HÀNH	19
5.1 Kiểm soát an toàn, an ninh vật lý	19
5.2 Quy trình kiểm soát	21
5.3 Kiểm soát nhân sự	22
5.4 Các quy trình ghi nhật ký hệ thống	23
5.5 Thay đổi khóa	25
5.6 Xử lý sự cố, thảm họa và phục hồi	26
5.7 Dừng hoạt động	27
6. ĐẢM BẢO AN TOÀN AN NINH VỀ KỸ THUẬT	27
6.1 Tạo và phân phối cặp khóa	27
6.2 Kiểm soát và bảo vệ khóa bí mật	27
6.3 Các vấn đề khác liên quan đến quản lý cặp khóa	28
6.4 Kích hoạt dữ liệu	28
6.5 Kiểm soát an ninh máy tính	28
6.6 Kiểm soát an ninh quy trình sử dụng	29

6.7	Giám sát an ninh hệ thống mạng	29
6.8	Dấu thời gian (Time-Stamping).....	30
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)	30
7.1	Định dạng của chứng thư số.....	30
7.2	Định dạng danh sách thu hồi chứng thư số (CRL)	33
7.3	Định dạng giao thức kiểm tra trạng thái chứng thư số trực tuyến (OCSP)	33
8	KIỂM ĐỊNH TÍNH TUÂN THỦ VÀ CÁC ĐÁNH GIÁ KHÁC	34
8.1	Tần suất và các tình huống kiểm tra kỹ thuật	34
8.2	Đơn vị, người thực hiện kiểm tra kỹ thuật	34
8.3	Các nội dung kiểm tra kỹ thuật	34
8.4	Xử lý khi phát hiện sai sót	34
8.5	Bkav RS thực hiện kế hoạch xử lý nhưng không có kết quả. Công bố kết quả kiểm tra kỹ thuật	34
8.6	Tần suất và các trường hợp đánh giá	34
8.7	Danh tính và khả năng của đơn vị, người kiểm tra	34
9	CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC	35
9.1	Phí/Giá.....	35
9.2	Trách nhiệm tài chính	35
9.3	Bảo mật các thông tin nghiệp vụ	35
9.4	Bảo mật thông tin cá nhân.....	35
9.5	Quyền sở hữu trí tuệ	36
9.6	Tuyên bố và cam kết.....	36
9.7	Từ chối trách nhiệm.....	37
9.8	Giới hạn trách nhiệm	38
9.9	Bồi thường thiệt hại.....	38
9.10	Hiệu lực của Quy chế chứng thực.....	38
10	PHỤ LỤC.....	40

1. GIỚI THIỆU

1.1 Tổng quan

- Tài liệu bao gồm các chính sách bảo mật, thực tiễn và yêu cầu của Bkav Remote Signing, với tư cách là nhà cung cấp dịch vụ chứng nhận đủ điều kiện cung cấp dịch vụ chữ ký số từ xa. Quy chế chứng thực và chính sách đáp ứng các yêu cầu đặc tính kỹ thuật ETSI 119 431 – 1, ETSI 119 431 – 2 và các tiêu chuẩn CEN EN 419 241 -1. Các thành phần điều khiển thiết bị tạo chữ ký điện tử từ xa (QSCD / SCDev) và các thành phần hỗ trợ dịch vụ tạo chữ ký được sử dụng. Việc sử dụng các thành phần điều khiển QSCD tuân theo các quy định trong thông tư 16/2019 – BTTTT về việc tạo chữ ký số từ xa. Các yêu cầu dựa trên chính sách, quy trình được nêu trong ETSI 319 401, các yêu cầu chứng nhận liên quan trong ETSI EN 319 401, cũng như các yêu cầu được nêu trong CEN EN 419 241 – 1.
- Bkav RS cung cấp dịch vụ chữ ký điện tử từ xa, hoạt động như một nhà cung cấp dịch vụ cung cấp ứng dụng ký máy chủ / ký từ xa (SSASP) và nhà cung cấp dịch vụ cung cấp ứng dụng tạo chữ ký / tạo chữ ký từ xa (SCASP).
- Các yêu cầu được đáp ứng bởi thành phần dịch vụ ứng dụng ký máy chủ (SSASC) phù hợp với cơ cấu tổ chức, quy trình hoạt động, cơ sở vật chất và môi trường giao tiếp của Bkav Remote Signing. Ngoài các yêu cầu về chính sách bảo mật Bkav RS được áp dụng chung khi sử dụng SSASC kiểm soát thiết bị tạo chữ ký từ xa (SCDev), Bkav RS cũng áp dụng các yêu cầu cụ thể liên quan đến việc sử dụng thiết bị tuân thủ thông tư 16/2019 - BTTTT. Thành phần dịch vụ bao gồm ứng dụng ký (SSA) và QSCD/SCDev. Các yêu cầu về chính sách bảo mật được mô tả liên quan đến các yêu cầu đối với việc tạo, duy trì và quản lý vòng đời của các khóa ký được sử dụng để tạo chữ ký điện tử.
- Các yêu cầu được đáp ứng bởi thành phần dịch vụ ứng dụng tạo chữ ký điện tử (SCASC) phù hợp với các yêu cầu của chính sách bảo mật Bkav khi sử dụng thành phần hỗ trợ dịch vụ tạo chữ ký số AdES phục vụ ứng dụng tạo chữ ký. Trong trường hợp này, đó là Ứng dụng Tạo Chữ ký (SCA). SCASC có các kết nối với các dịch vụ (chứng nhận) bên ngoài mà thể kết nối mục đích cung cấp thông tin cần có trong chữ ký. SCASC kết nối với thành phần dịch vụ ứng dụng ký máy chủ (SSASC) bằng các giao thức truy cập. Bkav sử dụng các giao thức kết nối SCASC hoặc SSASC phù hợp với ETSI TS 119 432. Tài liệu này mô tả các biện pháp kiểm soát cụ thể được yêu cầu để giải quyết các rủi ro cụ thể liên quan đến việc cung cấp dịch vụ tạo chữ ký.
- Bkav RS cung cấp dịch vụ tạo chữ ký điện tử từ xa phù hợp với các yêu cầu của thông tư 16/2019-BTTTT về chữ ký điện tử, dựa trên chứng chỉ X.509. Điều quan trọng nhất là người dùng và các bên tin cậy phải làm quen với các mục tiêu và vai trò của Chính sách và Thực tiễn về khả năng áp dụng của dịch vụ này và để người dùng dịch vụ thêm tin tưởng. Các mối quan hệ giữa Bkav RS và người dùng sẽ được điều chỉnh bởi thỏa thuận và giá của dịch vụ được bao gồm trong biểu giá Bkav Remote Signing. Tài liệu này được cấu trúc phù hợp với khuôn khổ được xác định bởi IETF RFC Khuyến nghị 3647 Khung quy chế chứng thực và chính sách chứng thư” RFC 3647
- Tài liệu tham khảo

- CEN EN 419 241-1 “Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements”;
- CEN EN 419 241-2 “Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing”;
- ETSI TS 119 431-1 “Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD/SCDev (remote signing)”;
- ETSI TS 119 431-2 “Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation”;
- ETSI EN 319 411-1 “Policy and security requirements for Trust Service Providers issuing certificates. Part 1: General requirements”;
- ETSI EN 319 401 “Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers”;
- ETSI TS 119 101 “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation”;
- ETSI TS 119 102-1 “Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation”;
- IETF RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”

1.2 Tên và dấu hiệu nhận diện tài liệu

- Tài liệu này là Quy chế chứng thực Bkav Remote Signing.

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

1.3.1 Bkav RS

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

1.3.2 Bkav Remote Signing

- Bkav remote signing **Bkav RS** là dịch vụ tạo chữ ký từ xa theo chuẩn Châu Âu đáp ứng thông tư 16/2019 BT TT
- Tài liệu Quy chế chứng thực Bkav RS tập trung cho giải pháp tạo chữ ký số từ xa

1.3.3 Registration Authority (RA)

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

1.3.4 Thuê bao

- Thuê bao của Bkav RS là các đối tượng sở hữu chứng thư số do Bkav RS ban hành
- Bkav RS đảm bảo chỉ người ký có đủ điều kiện mới có quyền truy cập khóa cá nhân đảm bảo quyền kiểm soát truy cập duy nhất.

- Người ký có thể là: Cá nhân, tổ chức

1.3.5 Người nhận

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

1.3.6 Các đối tượng khác

- Ngoài Bkav RS, RA, thuê bao và người nhận, Bkav RS không quản lý đối tượng nào khác.
- Bkav sử dụng các nhà thầu phụ và nhà cung cấp dịch vụ như trung tâm dữ liệu chuyên biệt để đặt máy chủ và thiết bị mạng đáng tin cậy và an toàn, nhà cung cấp hệ thống và dịch vụ đám mây, dịch vụ CNTT và các nhà cung cấp khác. Khi làm việc với các nhà thầu phụ và nhà cung cấp, Bkav yêu cầu họ tuân thủ nghiêm ngặt các quy trình, phù hợp với quy định.

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 Bkav RS và thỏa thuận của thuê bao với Bkav RS

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 Bkav RS 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 Bkav RS 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 Bkav RS cấp không được sử dụng vào các mục đích vi phạm pháp luật.
- Chứng thư số của thuê bao Bkav RS 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: BkavRS@bkav.com

- Điện thoại: 1900 54 54 14

1.5.3 Công nhận sự phù hợp của quy chế chứng thực

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

1.5.4 Thủ tục phê chuẩn quy chế chứng thực

- Sự phê chuẩn được thực hiện bởi Bkav RS PMA.
- Các thay đổi, cập nhật của quy chế chứng thực được ghi lại, công bố tại: <https://remotesigning.bkav.com/update-cps>
- Quy chế chứng thực bản mới nhất được lưu trữ tại <https://remotesigning.bkavca.vn/documents/33134/52312/CPS.pdf>

1.6 Các định nghĩa và từ viết tắt

- Chi tiết trong Phụ lục

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

2.2 Công bố thông tin

- Bkav RS 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.

Bkav RS 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/huong-dan-lien-quan-den-CKS/-/view-content/92873/huong-dan-tra-cuu-thong-tin-chung-thu-so>

- Thông tin chứng thư số Bkav RS còn hạn bị thu hồi được công bố tại địa chỉ: <http://crl.bkavca.vn/BkavRemoteSigning.crl>
- Bkav RS 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://remotesigning.bkavca.vn/>
- Bkav RS công bố thông tin CA tại: <https://remotesigning.bkavca.vn/documents/33134/52312/CPS.pdf>
- Địa chỉ truy cập OCSP Responder của Bkav RS: <http://ocsprs.bkavca.vn>

2.3 Thời gian, tần suất công bố thông tin

Bkav RS công bố và duy trì thông tin 24 giờ trong ngày và 7 ngày trong tuần các thông tin quy định tại mục 2.2 và cập nhật các thông tin này trong vòng 24 giờ khi có sự thay đổi.

- **Quy chế chứng thực:** được cập nhật khi có thay đổi.
- **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

- Bkav RS 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 Bkav RS 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 Bkav RS 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 đối tượng sở hữu chứng thư số, tên miền nếu là chứng thư số SSL, thông tin khác theo thỏa thuận với thuê bao
Đối tượng thay thế	thông tin khác theo thỏa thuận với thuê bao
Mã duy nhất (UID)	Mã định danh của đối tượng sở hữu chứng thư số: a) Đối với cá nhân: Mã định danh là mã trên giấy tờ tùy thân của thẻ căn cước công dân hoặc thẻ căn cước hoặc căn cước điện tử hoặc giấy chứng nhận căn cước hoặc tài khoản định danh điện tử mức độ 2 hoặc hộ chiếu còn thời hạn; thị thực nhập cảnh còn thời hạn hoặc giấy tờ chứng minh được miễn thị thực nhập cảnh (đối với cá nhân là người nước ngoài); b) Đối với tổ chức: Mã định danh là mã quyết định thành lập hoặc quyết định quy định về chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức hoặc giấy chứng nhận đăng ký doanh nghiệp hoặc giấy chứng nhận đầu tư hoặc giấy chứng nhận đăng ký hộ kinh Trường hợp đặc thù khác: Mã định danh có thể là mã số khác được xác định trên cơ sở thỏa thuận giữa Bkav và thuê bao, với điều kiện mã số đó phải phù hợp và không trái với quy định pháp luật hiện hành tại thời điểm ký kết thỏa thuận.

3.1.2 Quy định yêu cầu đối với tên

3.1.3 Tên trong chứng thư số do Bkav RS ban hành cho phép xác định được nhận dạng của đối tượng sở hữu của chứng thư số. 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 Bkav RS. 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 Bkav RS 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. Bkav RS sử dụng PKCS#10 chứng minh quyền sở hữu khóa bí mật.
- Khóa bí mật của khách hàng được lưu tập trung trên server

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. Bkav RS sẽ xác minh các thông tin bắt buộc dựa trên hồ sơ đề nghị phát hành chứng thư chữ ký số công cộng theo quy định pháp luật như sau:
 - Giấy đề nghị phát hành chứng thư chữ ký số công cộng dưới dạng bản giấy hoặc điện tử theo mẫu của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.
 - Tài liệu kèm theo bao gồm: quyết định thành lập hoặc quyết định quy định về chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức hoặc giấy chứng nhận đăng ký doanh nghiệp hoặc giấy chứng nhận đầu tư hoặc giấy chứng nhận đăng ký hộ kinh doanh và giấy tờ tùy thân của người đại diện theo pháp luật của tổ chức, bao gồm thẻ căn cước công dân hoặc thẻ căn cước hoặc giấy chứng nhận căn cước hoặc tài khoản định danh điện tử mức độ 2 hoặc hộ chiếu; hoặc tài khoản định danh điện tử của tổ chức.
 - Tổ chức có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc bản sao điện tử hoặc nộp bản sao trình kèm bản chính để đối chiếu hoặc sử dụng tài khoản định danh điện tử mức độ 2 theo quy định của pháp luật về định danh và xác thực điện tử.
 - Bkav RS, hoặc các RA của Bkav RS 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 Bkav RS.

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. Bkav sẽ xác minh các thông tin bắt buộc dựa trên hồ sơ đề nghị phát hành chứng thư chữ ký số công cộng theo quy định pháp luật như sau:
 - Giấy đề nghị phát hành chứng thư chữ ký số công cộng dưới dạng bản giấy hoặc điện tử theo mẫu của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.

- Tài liệu kèm theo bao gồm: giấy tờ tùy thân bao gồm thẻ căn cước công dân hoặc thẻ căn cước hoặc căn cước điện tử hoặc giấy chứng nhận căn cước hoặc tài khoản định danh điện tử mức độ 2 hoặc hộ chiếu còn thời hạn; thị thực nhập cảnh còn thời hạn hoặc giấy tờ chứng minh được miễn thị thực nhập cảnh (đối với cá nhân là người nước ngoài).
- Cá nhân có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc bản sao điện tử hoặc nộp bản sao trình kèm bản chính để đối chiếu hoặc sử dụng tài khoản định danh điện tử mức độ 2 theo quy định của pháp luật về định danh và xác thực điện tử.
- Quy trình xác thực nhận dạng của cá nhân đăng ký chứng thư số như sau:
 - Người đăng ký nộp hồ sơ cho Bkav RS/RA.
 - Bkav RS/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, Bkav RS 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

- Bước 1: Thuê bao gửi đơn đề nghị thay đổi cặp khóa theo mẫu của Bkav RS.
- Bước 2: Bkav RS thực hiện việc xác minh theo quy trình mục 3.2

3.4 Xác minh đề nghị thu hồi chứng thư số

- Khi có một yêu cầu thu hồi chứng thư số từ thuê bao, Bkav RS 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: Bkav RS 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, Bkav RS 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 Bkav RS 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 Bkav RS.
- 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 đề nghị như mục 3.2
- Chứng thư số của RA: Để đăng ký cấp chứng thư số từ Bkav RS, RA phải thực hiện việc ký hợp đồng với Bkav RS 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

- Bkav RS/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

- Bkav RS/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.
- Bkav RS/RA không chấp nhận 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.
 - Bkav/CA 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 Bkav RS.

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 Bkav RS.

4.3 Cấp chứng thư số

4.3.1 Vai trò của Bkav RS trong tiến trình tạo chứng thư số

- Chứng thư số được ban hành sau khi Bkav RS/RA chấp nhận đơn xin cấp chứng thư số trực tiếp từ thuê bao hoặc thông qua RA. Bkav RS 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 Bkav RS 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 Bkav RS đã tạo xong chứng thư số

- Bkav RS sau khi ban hành chứng thư số 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:
 - Tải về từ trang Web của Bkav RS.
 - Trên các ứng dụng Bkav Remote Signing

4.4 Xác nhận và công bố công khai chứng thư số

- 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 Bkav RS thực hiện qua email hoặc trên ứng dụng Bkav RS. Trong một số trường hợp cụ thể, việc xác nhận có thể được thực hiện bổ sung bằng hình thức khác nhằm bảo đảm Chứng thư chữ ký số được cấp ra chính xác... Thông tin xác nhận của thuê bao được lưu trữ trên hệ thống.
- Bkav RS công bố chứng thư số
 - Sau khi thuê bao chấp nhận chứng thư số (4.4.1), Bkav RS sẽ công bố chứng thư số khi thuê bao sử dụng ứng dụng Bkav RS
 - Chứng thư số sau khi được ban hành sẽ được công bố trên Web của Bkav RS 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 Bkav RS 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 Bkav RS, với các điều khoản của chính sách chứng thư số, quy chế chứng thực của Bkav RS. 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 thiết bị xác thực. Chứng thư số không thể sử dụng khi thu hồi hoặc hết hạn.

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 Bkav RS
- 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 trường hợp được gia hạn chứng thư số của thuê bao.

- 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.

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

4.6.3 Thông báo, cập nhật, công bố chứng thư số được gia hạn của 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

- Chứng thư số hết hạn hoặc thu hồi
- Theo yêu cầu của người dùng hoặc cơ quan nhà nước

- 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

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

- Bkav RS 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

4.9 Tạm dừng và 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.
 - Bkav RS/RA có quyền yêu cầu thu hồi chứng thư số mà đã duyệt cho thuê bao.
- Bộ Thông tin và Truyền thông có thể yêu cầu thu hồi chứng thư số nếu như hồ sơ không đầy đủ.

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 (Bkav RS, 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, Bkav RS 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 Bkav RS.
 - Chứng thư số có tên mạo danh hoặc vi phạm quyền sở 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 Bkav RS.
- Khi xem xét việc sử dụng chứng thư số có gây ảnh hưởng không tốt đến Bkav RS hay không, Bkav RS/RA sẽ xem xét dựa trên những yếu tố sau:
 - Số lượng phản nản nhận được.
 - Mức độ tin cậy của thông tin phản nản.
 - Các phản nản liên quan nhiều đến các yếu tố pháp luật (ví dụ: lừa đảo).
 - Có phản nản về thiệt hại gây ra do việc sử dụng chứng thư số của thuê bao.
- Bkav RS 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 Bkav RS.
- Khi Bkav RS/Thuê bao xác định khóa thuê bao bị lộ thì Bkav RS 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 Quy trình, Thủ tục thu hồi chứng thư số

- Trước khi thu hồi chứng thư số, Bkav RS xác thực yêu cầu thu hồi từ thuê bao bằng cách:
 - Sử dụng chữ ký số: Bkav RS 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, Bkav RS 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.
- Bkav RS 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 Bkav RS.
- Sau khi tiếp nhận, xác minh và xử lý yêu cầu thành công, Bkav RS 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.
- Bkav RS tiến hành cập nhật CRL hàng ngày

4.9.3 Tạm dừng chứng thư số

- Bkav RS 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 trên web 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

4.10.4 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://remotesigning.bkavca.vn/thoa-thuan-su-dung>
- Thủ tục thu hồi chứng thư số:
 - Tham chiếu mục 4.9.2

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

- Hiện tại, Bkav RS 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

- Bkav 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 DC được đặt tại: Data Center Viettel 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: Colocation server tại IDC VNPT, DC tòa nhà Internet VDC – Nguyễn Phong Sắc
- 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 An ninh vật lý và môi trường

- Hệ thống Bkav RS 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 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. Danh sách nhân sự tham gia vào hệ thống được xác định và kèm theo các điều khoản trách nhiệm
- Các máy tính trong hệ thống CA được kiểm soát bảo mật. Các chương trình tiện ích được hạn chế và kiểm soát
- Áp dụng các biện pháp ngăn chặn mất mát, hủy hoại hoặc xâm phạm tài sản và gián đoạn hoạt động kinh doanh
- Tất cả mọi truy nhập đều được ghi nhận.

5.1.3 Kiểm soát truy cập

- Việc truy cập vào hệ thống bị hạn chế cho những người có trách nhiệm
- Áp dụng các biện pháp bảo vệ các domain mạng nội bộ khỏi truy cập trái phép, bao gồm quyền truy cập người dùng và các bên thứ 3
- Áp dụng tường lửa ngăn chặn toàn bộ giao thức và truy cập không được phép
- Quản trị viên hệ thống quản lý tài khoản người dùng và đảm bảo sửa đổi hoặc xóa quyền truy cập kịp thời
- Quyền truy cập vào thông tin và các ứng dụng bị hạn chế theo Chính sách kiểm soát truy cập;

- Hệ thống công nghệ của Bkav đảm bảo kiểm soát đủ an ninh máy tính đối với việc quản trị và hoạt động của nhân viên phù hợp với vai trò của họ;
- Bkav RS kiểm soát việc sử dụng phần mềm và nhân viên cần chứng minh danh tính của họ trước khi sử dụng các ứng dụng quan trọng liên quan đến dịch vụ;
- Các nhân viên của Bkav chịu trách nhiệm về các hành động của mình
- Bkav đảm bảo kiểm soát việc truy cập thông tin nhạy cảm. Dữ liệu nhạy cảm được bảo vệ khỏi bị tiết lộ bởi người dùng trái phép

5.1.4 Điều kiện về nguồn điện và không khí

- Bkav RS 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.
- Bkav RS trang bị hệ thống điều hòa có điều khiển chính xác nhiệt độ. Hệ thống cảnh báo khi nhiệt độ vượt ngưỡng cho phép.

5.1.5 Chống nước

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

5.1.6 Chống và bảo vệ trước các nguy cơ về lửa

- Hệ thống thiết bị của Bkav RS được bố trí giảm thiểu tối đa các nguy cơ về lửa. Bkav RS 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.

5.1.7 Phương tiện lưu trữ dữ liệu

- Phương tiện lưu trữ dữ liệu của Bkav RS 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.

5.1.8 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.
- Quy trình xử lý rác thải, tiêu hủy thông tin nhạy cảm:
 - Hủy tài liệu giấy
 - Bước 1: Chuẩn bị máy hủy tài liệu kiểu hủy vụn
 - Bước 2: Hủy tài liệu: Cho tài liệu vào máy hủy tài liệu. Tài liệu lần lượt được cho đến hết. Nếu số lượng tài liệu nhiều hơn so với sức chứa của máy, thì lấy các mảnh giấy đã cắt ra khỏi máy trước khi tiếp tục cho tài liệu vào hủy.

- Bước 3: Chia số giấy vụn ra các túi khác nhau. Lấy một phần vụn giấy từ mỗi loại tài liệu và cho chúng vào các túi khác nhau.
- Bước 4: Vứt bỏ tài liệu đã cắt vào ngày gom rác
- Hủy tài liệu điện tử
 - Cách 1: Xóa tài liệu
 - Cách 2: Ghi đè lên ổ cứng
 - Cách 3: Dùng bộ khử từ ổ cứng
 - Cách 4: Phá hủy ổ cứng bằng phương pháp vật lý

5.1.9 Hệ thống dự phòng ở địa điểm khác

- Bkav RS 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

- Bkav RS 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 Bkav RS 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 Bkav RS đều phải được xác minh nhân thân, nhận dạng và trình độ. Quá trình nhận dạng được trình bày trong phần 5.3.1

- Bkav RS 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 Bkav RS 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, Bkav RS 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

- Bkav RS 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 Bkav RS hướng tới trách nhiệm cụ thể của mỗi nhân viên, nội dung huấn luyện bao gồm:
 - Các khái niệm PKI cơ bản, giải pháp Bkav RS.
 - Trách nhiệm công việc ứng với từng vai trò bao gồm:
 - **Security Officers:** Có trách nhiệm chung cho việc quản lý ứng dụng về chính sách bảo mật, quyền truy cập thông tin. Là những người sử dụng thống đặc quyền
 - **System Administrator:** Cài đặt, cấu hình hệ thống. Có trách nhiệm khôi phục hệ thống
 - **System Operator:** Chịu trách nhiệm vận hành hệ thống. Có nhiệm vụ sao lưu, khôi phục. Là vai trò đặc quyền nhưng không có vai trò quản lý và cấu hình hệ thống
 - **System Auditor:** Ủy quyền xem các bản sao lưu và kiểm tra dữ liệu nhật ký. Không có vai trò quản lý và cấu hình

- Các chính sách và thủ tục an ninh của Bkav RS.
- 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

- Bkav RS 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

- Bkav RS thực hiện chính sách luân chuyển cán bộ trong phạm vi nội bộ của mình. Bkav RS 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

- Bkav RS 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 Bkav RS. 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 Bkav RS. Những người này cũng phải tuân theo các tiêu chuẩn an ninh như nhân viên của Bkav RS. 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 Bkav RS.

5.3.8 Cung cấp tài liệu cho nhân viên

- Bkav RS 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.

5.3.9 Xử lý vi phạm

- Bất kỳ hành vi vi phạm nào theo Quy chế, chính sách này sẽ bị áp dụng các hình thức kỷ luật theo quy định của Công ty, tùy theo mức độ vi phạm sẽ bị nhắc nhở, tick lỗi đến đình chỉ công việc theo quyết định của lãnh đạo đơn vị. Trường hợp gây thiệt hại thì sẽ phải bồi thường theo quy định của Công ty/hoặc pháp luật.

5.4 Các quy trình ghi nhật ký hệ thống

5.4.1 Các loại sự kiện được ghi lại

- Bkav RS 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 quan trọng về môi trường, quản lý khóa của TW4S (tạo khóa, sử dụng và hủy khóa)
 - Các sự kiện của người ký (ký thành công và quản lý DTBS/R)
 - Xác thực người dùng

- Quản lý SAD
- Bật/ Tắt mở hệ thống chức năng tạo nhật ký
- Thay đổi các tham số nhật ký
- Mỗi bản ghi nhật ký gồm các thông tin sau:
 - Thời gian của bản ghi
 - Loại sự kiện
 - Đối tượng thực hiện (admin, người dùng, quy trình, ...)
 - Kết quả thành công, thất bại của sự kiện

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 năm (tùy từng loại nhật ký) sau khi xử lý và sau đó được chuyển sang khu vực lưu trữ.

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.
- Nhật ký được Bkav RS đảm bảo tính toàn vẹn và cung cấp chức năng xác thực tính toàn vẹn của dữ liệu

5.4.5 Các thủ tục dự phòng, khôi phục và lưu trữ nhật ký kiểm toán

- Nhật ký được backup theo chế độ backup chung của Bkav RS.
- Mỗi mục trong nhật ký bao gồm thời gian khi quá trình lưu trữ diễn ra
- Dữ liệu nhật ký không có chứa bất kỳ thông tin nhạy cảm như mật khẩu người dùng. Các tham số nhạy cảm được lưu trữ dưới dạng được bảo vệ đảm bảo tính toàn vẹn và an toàn
- Quản trị viên đặc quyền mới có thể thực hiện chức năng khôi phục từ các bản sao lưu.

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, có thông báo cho đối tượng gây ra sự kiện đó.

5.4.8 Đánh giá hệ thống

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

5.4.9 Lưu trữ các bản ghi

- Các loại hình, thông tin bản ghi nhật ký được lưu trữ.
 - 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...
- Thời gian lưu trữ bản ghi nhật ký: 5 năm với các nhật ký liên quan tới vòng đời chứng thư số
- 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.
- Quy trình lưu trữ bản ghi.
 - 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 Thay đổi khóa

Trước khi chứng thư số của CA hết hạn, theo quy định, Bkav RS 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 Bkav RS ban hành có thời gian sử dụng không quá thời gian sử dụng chứng thư số của Bkav RS được dùng để ký lên nó

Cặp khóa của Bkav RS sẽ không được sử dụng quá thời gian có hiệu lực của nó được quy định trong quy chế này. Chứng thư số của Bkav RS có thể được gia hạn (đổi khóa) khi trước khi cặp khóa cũ hết hạn

Trước khi hết hạn chứng thư số của Bkav RS, 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 Bkav RS. Quá trình chuyển tiếp khóa của Bkav RS đảm bảo rằng:

- Bkav RS 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, Bkav RS sử dụng cặp khóa mới để ban hành chứng thư số cho thuê bao

5.6 Xử lý sự cố, thảm họa và phục hồi

5.6.1 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.

5.6.2 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

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

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

5.6.4 Đảm bảo tính liên tục, phục hồi hoạt động sau thảm họa

- Bkav RS 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.
- Cơ sở dữ liệu của Bkav RS 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. Có phương án quản lý, phân loại các thông tin nhạy cảm.
- Bkav RS dự phòng các thiết bị phần cứng và phần mềm cung cấp dịch vụ. Khóa bí mật của Bkav RS cũng được dự phòng và duy trì
- Bkav RS sử dụng hệ thống giám sát, thông báo (Bkav BNI, Bkav SOC) khi có sự kiện bất thường xảy ra trong vòng 24H, sử dụng hệ thống Bkav PAM giám sát truy cập, sử dụng hệ thống CNTT
- Bkav RS quy định chính sách, cơ chế khắc phục khi phát hiện ra lỗ hổng.
- Bkav RS quy định các thủ tục báo cáo và ứng phó để giảm thiểu thiệt hại

5.7 Dừng hoạt động

- Khi không còn hoạt động, Bkav RS hoặc RA dùng mọi biện pháp cố gắng thông báo cho thuê bao, người nhận và các đối tượng trước khi dừng hoạt động. Bkav RS, RA sẽ có kế hoạch kết thúc nhằm giảm thiểu thiệt hại nhất cho khách hàng. Bkav RS 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 Bkav RS 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 Bkav RS 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, Bkav RS 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 Bkav RS 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

- Cách thức tạo cặp khóa, kích thước cặp khóa.
- Quy trình phân phối cặp khóa.

6.2 Kiểm soát và bảo vệ khóa bí mật

6.2.1 Tiêu chuẩn kỹ thuật đối với thiết bị mật mã.

- Bkav RS sử dụng thiết bị mã hóa phần cứng chuyên dụng (Hardware Security Module) để lưu trữ khóa bí mật của Bkav RS. Thiết bị HSM của Bkav RS đáp ứng chuẩn chuẩn FIPS 140-2 level 3 và EAL 4+.

6.2.2 Cơ chế kiểm soát, bảo vệ các khóa bí mật.

- Cơ chế kiểm soát khóa bí mật được Bkav RS 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 Bkav RS, $N = 4$;

6.2.3 Dự phòng khóa bí mật

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

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

- Bkav RS giữ khóa bí mật trong các HSM, khóa bí mật được lưu trong dạng được mã hóa.
- Sau khi chứng thư số của Bkav RS 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 Bkav RS.

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 Bkav RS 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 nhận 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 toàn bộ hoặc một phần tên tài khoản người dùng tương ứng

6.5 Kiểm soát an ninh máy tính

- Hệ thống Bkav RS được vận hành trên hệ thống đảm bảo an ninh theo các chính sách của Bkav RS tuân thủ tiêu chuẩn EN 419 241 – 1.
- Hệ thống có cơ chế đưa ra cảnh báo phát hiện các sự kiện bất thường, thông báo cho nhân viên quản trị có liên quan
- Cơ chế quản lý các sự kiện bất thường liên quan đến hoạt động của người dùng.
- Bkav RS đảm bảo rằng các máy chủ cài đặt hệ thống CA và dữ liệu được bảo vệ trước các truy nhập không được phép. Bkav RS 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 Bkav RS 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 Bkav RS. Các quản trị viên của Bkav RS chỉ truy nhập và quản trị hệ thống thông qua một số giới hạn các máy tính quản trị được xác định sẵn.

- Bkav RS yêu cầu sử dụng mật khẩu mạnh, 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.
- Hệ thống áp dụng cơ chế cảnh báo cho các sự kiện bất thường, các sự kiện bất thường bao gồm nhưng không hạn chế:
 - Thời gian sử dụng vượt tiêu chuẩn
 - Hành động của người dùng được thực hiện với tốc độ bất thường
 - Hành động của người dùng bỏ qua các bước trong quy trình tiêu chuẩn
 - Phiên bị trùng lặp

6.6 Kiểm soát an ninh quy trình sử dụng

6.6.1.1 Giám sát triển khai hệ thống

- Các ứng dụng được phát triển và triển khai sử dụng trong Bkav RS tuân theo các tiêu chuẩn thiết kế, phát triển và triển khai phần mềm của Bkav RS. Bkav RS cũng cung cấp phần mềm cho các RA.
- Phần mềm được Bkav RS 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.

6.6.1.2 Giám sát quản lý an ninh

- Bkav RS 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.

6.6.2 Giám sát an ninh vòng đời

- Bkav RS 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 Bkav RS.

6.7 Giám sát an ninh hệ thống mạng

- Bkav RS sử dụng công nghệ hiện đại để trao đổi và bảo vệ thông tin đảm bảo an ninh mạng của hệ thống trước bất kỳ sự can thiệp hoặc mối đe dọa nào từ bên ngoài
- Bkav RS chia hệ thống thành các Zones chức năng, logic và vùng vật lý dựa trên nguy cơ và mối liên kết hệ thống và dịch vụ
- Tài liệu chi tiết về cấu hình mạng và các phương tiện bảo vệ được nêu trong tài liệu kỹ thuật nội bộ.

- Bkav RS áp dụng các biện pháp kiểm soát bảo mật giống nhau khi hệ thống nằm trong cùng zone
- Bkav RS giới hạn quyền truy cập và giao tiếp giữa các zone cần thiết để thực hiện các hoạt động liên quan. Mọi nỗ lực truy cập trái phép vào hệ thống đều được ghi lại
- Bkav RS cấm hoặc hủy kích hoạt các liên kết, dịch vụ không cần thiết
- Bkav RS thường xuyên xem xét thiết lập luật bảo vệ
- Bkav RS sử dụng mạng riêng để quản trị hệ thống VNTT mà mạng lưới hoạt động
- Hệ thống không được sử dụng để quản lý chính sách bảo mật cho các mục đích khác
- Hệ thống phục vụ phát triển, thử nghiệm tách biệt với hệ thống dịch vụ triển khai cho thuê bao.

6.8 Dấu thời gian (Time-Stamping)

- Không áp dụng

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

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

7.1.1 Phiên bản

- Chứng thư số do Bkav RS ban hành theo X.509 Version 3.

7.1.2 Trường mở rộng

- Bkav RS ban hành chứng thư số X.509 phiên bản 3 với phần mở rộng được quy định

7.1.3 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 Bkav RS 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

7.1.4 Certificate policies

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

7.1.5 Subject Alternative Name

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

7.1.6 Basic Constraints

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

7.1.7 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

7.1.8 CRL Distribution Points

- Chứng thư số do Bkav RS 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.

7.1.9 Authority Key Identifier

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

7.1.10 Subject Key Identifier

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

7.1.11 Các thuật toán ký

- Bkav RS ký lên các chứng thư số, sử dụng một trong các thuật toán sau:
 - sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsads(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 Bkav RS hỗ trợ sử dụng thuật toán mã hóa SHA-256, SHA-384 và SHA-512 trong chứng thư số.

7.1.12 Khuôn dạng tên

- Bkav RS 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.

7.1.13 Ràng buộc tên

- Bkav RS không quy định cụ thể các ràng buộc cho việc đặt tên.

7.1.14 Định danh chính sách và quy chế chứng thư số

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

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

- Bkav RS không quy định các ràng buộc sử dụng trường mở rộng chính sách chứng thư số.

7.1.16 Cú pháp và ngữ nghĩa của chính sách phân loại

- Bkav RS 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.

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

- Bkav RS 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 Bkav RS công bố tuân theo chuẩn ITU-T X.509 và các quy định của RFC 5280. Tối thiểu, CRL do Bkav RS 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. Bkav RS sử dụng một trong bốn hàm băm an toàn: SHA-256, SHA-384, SHA-512.
Issuer	Thực thể ký và ban hành CRL – Bkav RS.
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

- Bkav RS ban hành X.509 Version 2 CRL.

7.2.2 CRL và các trường mở rộng của CRL

- CRL do Bkav RS 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

- Bkav RS 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

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

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

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, Bkav RS sẽ làm việc với RootCA về những nội dung chưa phù hợp.
- Bkav RS 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 Bkav RS 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 Bkav RS.

8.5 Bkav RS thực hiện kế hoạch xử lý nhưng không có kết quả. Công bố kết quả kiểm tra kỹ thuật

- Báo cáo kết quả kiểm toán kỹ thuật được Bkav RS công bố với cơ quan có thẩm quyền

8.6 Tần suất và các trường hợp đánh giá

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

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 hiện hành của pháp luật phí và lệ phí cho đến khi cơ quan có thẩm quyền ban hành văn bản thay thế
- Giá cấp, gia hạn, thu hồi chứng thư số.
- Các loại chi phí khác (nếu có).

9.2 Trách nhiệm tài chính

- Nghĩa vụ nộp phí trong quá trình cung cấp dịch vụ.
- 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 Bkav RS 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 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 Bkav RS.
 - Báo cáo kiểm tra Bkav RS.
 - 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 Bkav RS: phần cứng, phần mềm và quản trị của dịch vụ của Bkav RS.

9.3.2 Những thông tin ngoài phạm vi thông tin 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 Bkav RS 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 mật thông tin nghiệp vụ.

- Bkav RS 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 Bkav RS tại <https://remotesigning.bkavca.vn/dieu-khoan-bao-mat>.
- Mọi thông tin thuê bao không được công bố qua nội dung của chứng thư số, dịch vụ Directory và CRL.
- Bkav RS thực hiện các biện pháp đảm bảo an ninh cho các thông tin bí mật của thuê bao, tuân thủ 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

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

- Bkav RS 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

- Cấp khoá tương ứng với chứng thư số của Bkav RS, 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 Bkav RS

- Bkav RS cam kết chịu hoàn toàn trách nhiệm về tính chính xác của thông tin nêu trong quy chế chứng thực này.
- Bkav RS 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 Bkav RS 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.
- Bkav RS xác nhận trong quá trình cung cấp dịch vụ chứng thực chữ ký số công cộng cho khách hàng, Bkav RS có thực hiện các hoạt động xử lý dữ liệu cá nhân để cung cấp dịch vụ cho khách hàng theo thỏa thuận tại <https://remotesigning.bkavca.vn/thoa-thuan-su-dung> và <https://remotesigning.bkavca.vn/dieu-khoan-bao-mat>

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 Bkav RS đã nhận đầy đủ hồ sơ của thuê bao, và thông tin thuê bao được thẩm định.
 - Cam kết của RA với Bkav RS 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 Bkav RS.
 - 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 Bkav RS, RA không thực hiện lưu trữ thông tin thuê bao, việc lưu trữ, sử dụng thông tin thuê bao thuộc trách nhiệm của Bkav RS

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

9.7 Từ chối trách nhiệm

- Bkav RS 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 Bkav RS. Trong mọi trường hợp, khoản tiền mà Bkav RS 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

- Thực hiện theo thỏa thuận sử dụng tại <https://remotesigning.bkavca.vn/toa-thuan-su-dung>

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 Bkav RS 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 Bkav RS
- 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 <https://remotesigning.bkavca.vn>. 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 Bkav RS 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 Bkav RS PMA. Nội dung sửa đổi được lưu tại <https://remotesigning.bkavca.vn/documents/33134/52312/CPS.pdf>
- 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 trọng như thay đổi URL, thông tin liên hệ, lỗi in ấn... Bkav RS 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, Bkav RS PMA sẽ xem xét yêu cầu thay đổi. Nếu quy chế cần thay đổi, Bkav RS 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, Bkav RS PMA sẽ thực hiện sự thay đổi quy chế này lập tức, sau đó sẽ thông báo cho các thành viên.

9.12.3 Kỳ hạn góp ý

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

9.12.4 Cơ chế quản lý góp ý

- Bkav RS PMA sẽ xem xét mọi góp ý sửa đổi. Bkav RS 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.

9.12.5 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 Bkav RS PMA.

9.13 Thủ tục giải quyết tranh chấp

9.13.1 Tranh chấp giữa Bkav RS với RA

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

9.13.2 Tranh chấp giữa Bkav RS 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

- Quy chế chứng thực này được điều chỉnh bởi pháp luật Việt Nam, bao gồm Luật Giao dịch điện tử và các văn bản hướng dẫn liên quan. Pháp luật Việt Nam được áp dụng trong mọi trường hợp, kể cả khi có 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 Bkav RS phải tuân thủ.

9.16.2 Sự chuyển nhượng

- Bkav RS 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 Bkav RS.

9.16.5 Trường hợp bất khả kháng

- Thực hiện theo thỏa thuận sử dụng Chữ ký số tại <https://remotesigning.bkavca.vn/thoa-thuan-su-dung>

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	Bkav RS	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	Bkav RS 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 Bkav RS.

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 Bkav RS, 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 thuộc 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 chứa 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 hạ 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	Thuê bao/người dùng	Đối tượng đăng ký sử dụng chứng thư số.
20	USB token	Thiết bị phần cứng được sử dụng để bảo quản và sử dụng cặp khóa trong hạ tầng khóa công khai.
21	Electronic Signature Creation Data	Dữ liệu duy nhất được sử dụng cho việc tạo chữ ký điện tử
22	Electronic Signature	Dữ liệu điện tử được sử dụng ký số
23	Signer Interaction Component (SIC)	Thành phần tương tác người dùng
24	Signature Activation Module (SAM)	Module kích hoạt ký số được thực thi trong môi trường được bảo vệ chống lại việc sử dụng trái phép
25	SAD	Dữ liệu kích hoạt ký số
26	SAP	Giao thực kích hoạt ký số
27	Trustworthy System Supporting Server Signing (TW4S)	Hệ thống đáng tin cậy bao gồm máy chủ/ client để tạo chữ ký điện tử, sử dụng khóa ký dưới sự kiểm soát duy nhất của người ký
28	Data to be Signed Representation (DTBS/R)	Định dạng dữ liệu để tạo ra chữ ký điện tử (ví dụ: mã hash)
29	Remote Signature Creation Device (SCDev)	Thiết bị tạo chữ ký điện tử hoạt động dưới sự kiểm soát truy cập duy nhất của người ký, có thể là phần mềm hoặc phần cứng được cấu hình tạo ra chữ ký điện tử
30	Server Signing Application (SSA)	Ứng dụng máy chủ ký số tạo chữ ký từ xa
31	Signature Creation Application (SCA)	Ứng dụng tạo chữ ký từ xa
32	Signature Creation System (SCS)	Hệ thống tạo chữ ký điện tử
33	Signature Creation Application Service Component (SCASC)	Thành phần dịch vụ ứng dụng tạo chữ ký số

34	Server Signing Application Service Component (SSASC)	Thành phần dịch vụ ứng dụng tạo chữ ký từ xa sử dụng ứng dụng máy chủ ký số cho việc tạo giá trị chữ ký thay mặt người dùng
35	Server Signing Application Service Provider (SSASP)	Nhà cung cấp dịch vụ máy chủ/ ứng dụng ký số từ xa
36	Signature Creation Application Service Provider (SCASP)	Nhà cung cấp ứng dụng tạo chữ ký số từ xa
37	Electronic Identification (eID)	Quy trình định danh người dùng
38	Means of Electronic Identification	Phương tiện định danh
39	Personal Identification Data	Tập hợp dữ liệu cho phép thiết lập danh tính của một cá nhân, pháp nhân hoặc một các nhân đại diện cho một pháp nhân