QUY CHẾ CHỨNG THỰC
HỆ THỐNG BKAV REMOTE SIGNING

Cập nhật ngày 10/12/2022

MỤC LỤC

LỜI NÓI ĐẦU

Bản Quy chế chứng thực này được viết dựa theo RFC 3647 về "Khung quy chế chứng thực và chính sách chứng thư số", đáp ứng theo tiêu chuẩn trong Thông tư số 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.

1. Giới thiệu

- Liên minh châu Âu đã đưa ra khái niệm chữ ký điện tử được tạo ra bởi "Thiết bị tạo chữ ký số từ xa", điều đó có nghĩa thiết bị tạo chữ ký không còn là thiết bị cá nhân dưới sự kiểm soát vật lý của người dùng, mà được thay thế bằng các dịch vụ được cung cấp và quản lý bởi nhà cung cấp dịch vụ được chứng nhận. Theo thông tư số 16/2019 – BTTT đã cho phép người ký chữ ký điện tử được ủy thác cho một bên thứ ba, miễn là tổ chức đó có các cơ chế và thủ tục thích hợp đảm bảo rằng người ký có quyền kiểm soát duy nhất đối với việc sử dụng dữ liệu liên quan đến việc tạo chữ ký điện tử và đáp ứng các yêu cầu liên quan đến việc tạo chữ ký điện tử. Theo nghĩa này, Bkav Remote Signing với tư cách là nhà cung cấp dịch vụ chứng thực điện tử, đủ điều kiện cung cấp, quản lý môi trường tạo chữ ký điện tử thay mặt cho người ký.
- Trong dịch vụ này, để đảm bảo chữ ký điện tử nhận được sự công nhận pháp lý giống như chữ ký điện tử được tạo ra trong môi trường do người dùng quản lý hoàn toàn, Bkav Remote Signing áp dụng các quy trình cụ thể để đảm bảo an ninh vật lý và hành chính, sử dụng các hệ thống và sản phẩm đáng tin cậy, bao gồm cả điện tử an toàn và các kênh giao tiếp, môi trường tạo chữ ký điện tử đáng tin cậy và đảm bảo rằng môi trường được sử dụng dưới sự kiểm soát duy nhất của người ký. Việc cung cấp chữ ký đủ điều kiện được tạo bởi thiết bị phải tuân thủ các yêu cầu áp dụng cho các nhà cung cấp dịch vụ nhận đủ điều kiện trong thông tư 16/2019 – BTTTT.
- Người dùng dịch vụ là cá nhân sở hữu điện thoại thông minh, máy tính bảng hoặc thiết bị di động khác.

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 Remote Signing 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 Remote Signing được áp dụng chung khi sử dụng SSASC kiểm soát thiết bị tạo chữ ký từ xa (SCDev), Bkav Remote Signing 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 có 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 Remote Signing 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 Remote Signing 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

1.2 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"

1.3 Tên và dấu hiệu nhận diện tài liệu

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

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

1.4.1 BkavCA

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

1.4.2 Bkav Remote Signing

- Bkav Remote Signing (BRS) là dịch vụ tạo chữ ký từ xa theo chuẩn Châu Âu đáp ứng thông tư 16/2019 BTTT
- Tài liệu Quy chế chứng thực Bkav Remote Signing tập trung cho giải pháp tạo chữ ký số từ xa

1.4.3 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 Remote Signing cũng là một RA.

1.4.4 Thuê bao

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

1.4.5 Người nhận

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

1.4.6 Các đối tượng khác

- Ngoài Bkav Remote Signing, RA, thuê bao và người nhận, Bkav Remote Signing 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.

1.5 Mục đích sử dụng chứng thư số

1.5.1 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

1.5.1 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

1.6 Quản lý quy chế chứng thực

1.6.1 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.

1.6.2 Liên hệ

- Phụ trách Bkav CA
  - Giám đốc Ban Khách hàng doanh nghiệp: Nguyễn Khơ Din.
  - Email: dinnk@bkav.com
- 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 - 4 - 3763 2552

1.6.3 Công nhận sự phù hợp của quy chế chứng thực

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

1.6.4 Thủ tục phê chuẩn quy chế chứng thực

- Sự phê chuẩn được thực hiện bởi Bkav Remote Signing PMA.

- Các thay đổi, cập nhật của quy chế chứng thực được ghi lại, công bố tại https://remotesigning.bkavca.vn/CPS.pdf
- Quy chế chứng thực bản mới nhất được lưu trữ tại https://remotesigning.bkavca.vn/CPS_update.txt

1.7 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 từkhi 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 Remote Signing 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 Remote Signing 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 Bkav Remote Signing còn hạn bị thu hồi được công bố tại địa chỉ: http://crl.Bkavca.vn/BkavRemoteSigning.crl

- Bkav Remote Signing 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/
- Bkav Remote Signing công bố thông tin CA tại: https://Bkavca.vn/
- Địa chỉ truy cập OCSP Responder của Bkav Remote Signing: http://ocsprs.Bkavca.vn

2.3 Thời gian, tần suất công bố thông tin

Bkav Remote Signing 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 theo phần 11.12.
- **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

- Bkav Remote Signing 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.
Quận/Huyện (L)	Tên Quận, Huyện mà đối tượng sở hữu chứng thư số thuộc.
Tên thường gọi (CN)	Tên đối tượng sở hữu chứng thư số, tên miền nếu là chứng thư số SSL
Địa chỉ email (E)	Địa chỉ email của đối tượng sở hữu chứng thư số
Mã duy nhất (UID)	Mã định danh của đối tượng sở hữu chứng thư số. Đối với cá nhân Mã số định danh sẽ là số CMND. Đối với cơ quan tổ chức có Mã số thuế, 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.

- DN trong chứng thư số có một thành phần là CN (Common Name - tên thường gọi). CN trong chứng thư số của các tổ chức có thể là tên miền, tên pháp lý của tổ chức hay tên của đại diện được ủy quyền của tổ chức đó. CN trong chứng thư số của người dùng cá nhân là họ tên trong chứng minh thư nhân dân của người dùng đó. CN được kiểm tra tính xác thực trong quá trình cấp chứng thư số.

3.1.2 Quy định yêu cầu đối với tên

- Tên trong chứng thư số do 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.
- 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. 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.
    - 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 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 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, BkavCA sẽ xác thực bổ sung bằng cách gọi điện hoặc xác thực trực tiếp tại tổ chức về cá nhân đó.

3.3 Xác minh đề nghị thay đổi cặp khóa

- Trước khi một chứng thư số hết hạn, thuê bao cần có một chứng thư số mới. Làm mới chứng thư số có thể có 2 trường hợp:
  - Sinh một cặp khóa mới thay thế cặp khóa trong chứng thư số đã hết hạn (đổi khóa - rekey).
  - Tạo chứng thư số mới cho một cặp khóa đang tồn tại (gia hạn - renewal).
- Trong phần 3.3, thuật ngữ làm mới được dùng thay thế cho cả đổi khóa và gia hạn chứng thư.

3.3.1 Nhận dạng và xác thực yêu cầu làm mới thông thường

- Thời hạn xin làm mới của thuê bao: từ 90 ngày trước khi chứng thư số hết hạn cho tới 30 ngày sau thời điểm chứng thư số hết hạn. Sau 30 ngày hết hạn chứng thư số, yêu cầu làm mới chứng thư số sẽ không được chấp nhận, thuê bao phải thực hiện lại các bước như đăng ký mới.

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

3.3.2 Nhận dạng và xác thực yêu cầu làm mới sau khi thu hồi

- Nhận dạng và xác thực được thực hiện thông qua việc sử dụng bộ câu hỏi xác thực.
- Thuê bao không được phép làm mới chứng thư số sau khi bị thu hồi nếu lý do thu hồi chứng thư số là một trong các nguyên nhân sau:
    - BkavCA phát hiện ít nhất 1 thông tin cần xác minh trong chứng thư số không đúng.
    - Chứng thư số được sử dụng trong các hoạt động phạm pháp, các hoạt động có thể ảnh hưởng tới uy tín của BkavCA.

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 Khóa và chứng thư số thuê bao

4.1 Yêu cầu cấp chứng thư số

4.1.1 Ai có thể gửi đăng ký cấp chứng thư số

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

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

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

- Thuê bao làm thủ tục và ký một thỏa thuận với BkavCA, các điều khoản và cam kết trong thỏa thuận được mô tả trong phần 11.6.3.

4.1.2.2 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.

- BkavCA sẽ tổ chức nghi lễ sinh khóa cho RA.
- Trách nhiệm của RA được làm rõ trong phần 9.6.2.

4.2 Xử lý yêu cầu cấp chứng thư số

4.2.1 Nhận dạng và xác thực

- 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.
  - 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 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.

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:
  - Tải về từ trang Web của BkavCA.

- Trên các ứng dụng Bkav Remote Signign, Bkav Token Manager

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 trên ứng dụng Bkav Remote Signing. 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 công bố chứng thư số khi thuê bao sử dụng ứng dụng Bkav Remote Signing
- Chứng thư số sau khi được ban hành sẽ được công bố trên Web của BkavCA và cơ sở dữ liệu LDAP.

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

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

4.5 Sử dụng cặp khóa và chứng thư số

4.5.1 Sử dụng của khóa bí mật và chứng thư số

- Chứng thư số và khóa bí mật tương ứng được phép sử dụng nếu thuê bao đã đồng ý thỏa thuận với 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 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 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, mọi thông tin khác trong chứng thư số đều không thay đổi.

4.6.1 Các tình huống gia hạn chứng thư số

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

4.6.2 Ai có thể yêu cầu gia hạn chứng thư số

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

4.6.3 Xử lý yêu cầu gia hạn chứng thư số

- 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.

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

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

4.6.5 Chấp nhận chứng thư số mới 9

- Tương tự phần 4.4.1.

4.6.6 Công bố chứng thư số mới được tạo bởi CA

- Tương tự phần 4.4.2.

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

- Tương tự phần 4.4.3.

4.7 Thay đổi cặp khóa của thuê bao

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

4.7.1 Các tình huống đổi khóa

- 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

- 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 sự tạo chứng thư số mới cho thuê bao

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

4.7.5 Chấp nhận chứng thư số đổi khóa

- Tương tự phần 4.4.1

4.7.6 Công bố chứng thư số đổi khóa bởi CA

- Tương tự phần 4.4.2.

4.7.7 Thông báo đổi khóa cho các đối tượng khác

- Tương tự phần 4.4.3.

4.8 Thay đổi thông tin 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

- 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 chứng thư số mới cho CA

- Xem phần 4.3.2

4.8.5 Chấp nhận chứng thư số mới được thay đổi

- Xem phần 4.4.1

4.8.6 Công bố chứng thư số mới thay đổi bởi CA

- Xem phần 4.4.2

4.8.7 Thông báo cho các đối tượng khác

- Xem phần 4.4.3

4.9 Tạm dừng và thu hồi chứng thư số

4.9.1 Các tình huống thu hồi chứng thư số

- Yêu cầu thu hồi chứng thư số sẽ được xử lý khi thuê bao hay các đối tượng có thẩm quyền (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).

4.9.2 Ai có thể yêu cầu thu hồi chứng thư số

- Đối với chứng thư số của thuê bao:
  - Thuê bao đăng ký chứng thư số có quyền yêu cầu thu hồi chứng thư số.
  - 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.

4.9.3 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 sử dụng hệ thống quản lý chứng thư số để chuyển các yêu cầu thu hồi tới BkavCA. Mỗi yêu cầu được xác thực qua một chữ ký của RA.

4.9.4 Thời hạn gửi yêu cầu thu hồi chứng thư số

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

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

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

4.9.6 Kiểm tra trạng thái thu hồi

- Người nhận sẽ kiểm tra thông tin trạng thái chứng thư số, thông qua CRL hoặc OCSP. 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 như 2.2

4.9.7 Tần suất công bố CRL mới

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

4.9.8 Giới hạn trễ cho CRL

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

4.9.9 Kiểm tra trạng thái chứng thư số trực tuyến

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

4.9.10 Yêu cầu kiểm tra trạng thái thu hồi trực tuyến

- Người nhận phải kiểm tra trạng thái của một chứng thư số nếu muốn tin tưởng. Việc kiểm tra trạng thái chứng thư số được thực hiện thông qua OCSP Responder.

4.9.11 Các dạng thông tin trạng thái thu hồi khác

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

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

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

4.9.13 Các tình huống tạm dừng chứng thư số

- BkavCA không cung cấp dịch vụ này

4.9.14 Ai có thể yêu cầu tạm dừng chứng thư số

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

4.9.15 Thủ tục tạm dừng chứng thư số

- Không có thủ tục tạm dừng chứng thư số

4.9.16 Giới hạn xử lý tạm dừng chứng thư số

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

4.10 Kiểm tra trạng thái chứng thư số

4.10.1 Đặc điểm

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

4.10.2 Tính sẵn sàng của dịch vụ

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

4.10.3 Tùy chọn đặc biệt

- OCSP là dịch vụ tùy chọn.

4.11 Chấm dứt dịch vụ của thuê bao

- Kết thúc thuê bao chứng thư số có hiệu lực trong các trường hợp sau:
  - Thuê bao đã hết hạn mà không làm mới.
  - Thu hồi chứng thư số xảy ra mà không xin cấp một chứng thư số mới.
- 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. Các yêu cầu với Bkav Remote Signing

5.1 Yêu cầu chung

Bkav áp dụng một số yêu cầu chung:

- Bkav áp dụng bộ quy chế chứng thực phù hợp với chữ ký điện tử từ xa. Đối với mỗi dịch vụ chứng nhận được cung cấp và mỗi chứng chỉ được cấp, Bkav đã công bố trên trang web của mình một chính sách và thực hành với các số nhận dạng chứng chỉ.
- Ban quản lý của Bkav phê duyệt các quy chế và công bố, thông báo cho nhân viên và các bên liên quan
- Tài liệu này mô tả các quy chế và thủ tục được sử dụng để giải quyết các yêu cầu được xác định với chính sách Bkav hiện hành
- Bkav công bố tài liệu trên trang https://remotesigning.bkavca.vn
- Tài liệu đã được phê duyệt bởi bộ phận quản lý Bkav

- Ban quản lý Bkav quản lý thực hiện việc áp dụng chính sách
- Quy trình đánh giá và bảo trì được thực hiện ít nhất 1 năm 1 lần
- Tài liệu được cập nhật khi có thay đổi, được ban quản lý phê duyệt và xuất bản trên website của công ty
- Việc xuất bản Quy chế và chứng thực được áp dụng ngay lập tức
- Trong trường hợp các tổ chức liên kết với Bkav, nghĩa vụ các bên cũng như chính sách và thông lệ khác được áp dụng sẽ được thoả thuận sử dụng Chữ ký số tại https://remotesigning.bkavca.vn/thoa-thuan-su-dung

5.2 Yêu cầu với SSASC

Bkav áp dụng các yêu cầu sau khi cung cấp dịch vụ Thành phần ứng dụng máy chủ ký số:

- Độ dài khóa và thuật toán mã hóa theo thông tư 16/2019 – BTTT
  - Độ dài khóa của chứng thư số CA: 2048 bit đối với RSA
  - Thuật toán băm: SHA-256, SHA-384 và SHA-512
  - Độ dài khóa cho việc tạo chữ ký thông qua hệ thống Hạ tầng khóa ký: 2048 bit đối với RSA
  - Thuật toán băm: SHA-256, SHA-384 và SHA-512
- Toàn bộ chính sách và quy chế được áp dụng 24/7/365 trên website Bkav. Tài liệu bao gồm thông tin nhạy cảm như thông tin an ninh không được công khai.

5.3 Yêu cầu với SCASC

Bkav áp dụng một số yêu cầu khi cung cấp thành phần dịch vụ ứng dụng tạo chữ ký số (SCASC) theo tiêu chuẩn ETSI TS 119 431 – 2:

- Hỗ trợ module RESTful với giao diện ETSI TS 119 432. Kết nối giữa Server Signing Module (SCASC) và SAM+CM (SCDev) sử dụng cơ chế an toàn, bảo mật dựa trên chữ ký số.
- Hiện thị dữ liệu ký tới người ký đảm bảo cơ chế Những gì nhìn thấy là những gì bạn ký.

Các ứng dụng tích hợp BkavRemote Signing phải đảm bảo:

- Mô tả các thông tin được gửi cho người dùng để xác nhận dữ liệu được ký trên văn bản.
- Khi trình bày tài liệu cho người ký cần nêu rõ loại nội dung nào sẽ được trình bày chính xác.

- Khi trình bày dữ liệu ký cho người ký, giao diện sẽ cảnh báo người ký nếu nó không thể trình bày chính xác tất cả các phần dữ liệu ký theo loại nội dung dữ liệu.
- Khi trình bày dữ liệu cho người ký, sẽ có một quy trình làm việc trong đó nêu rõ cho người ký rằng người ký đồng ý với việc ký văn bản.

6. Kiến trúc Bkav Remote Signing

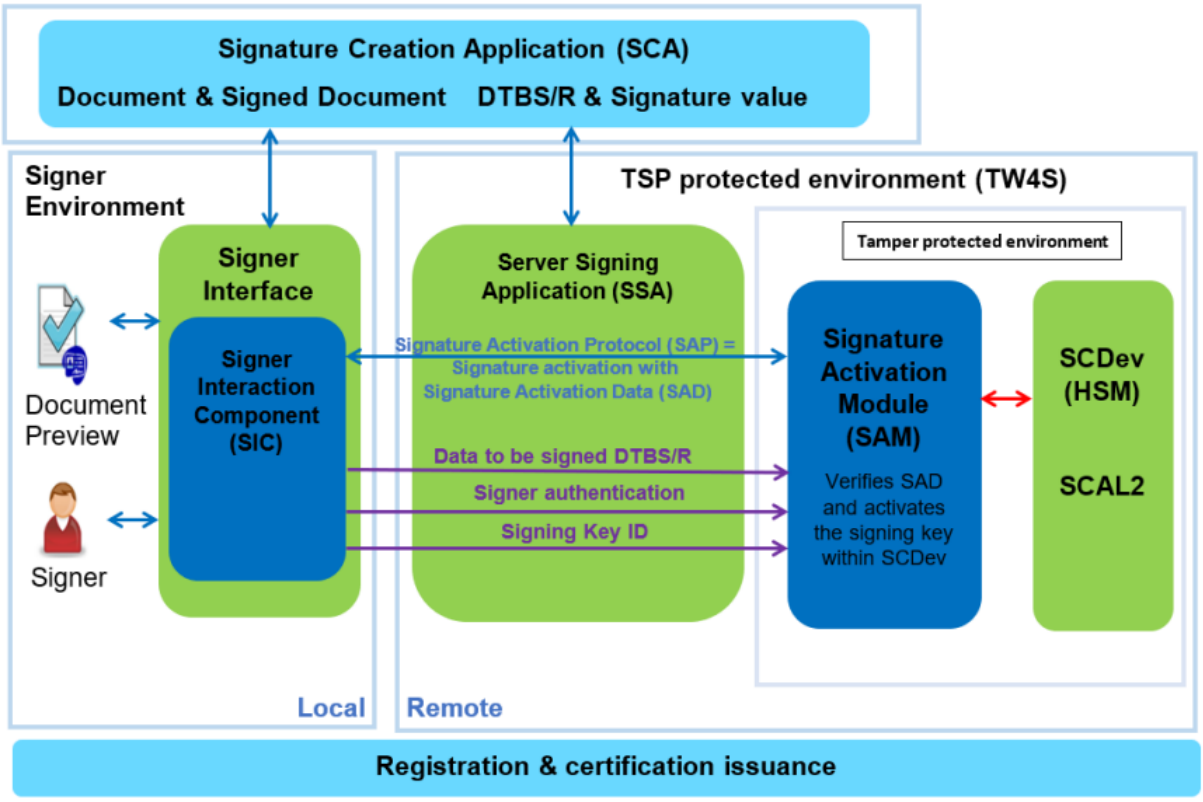
6.1 Thông tin cơ bản

Kiến trúc Bkav Remote Signing áp dụng gồm 2 thành phần môi trường chính: môi trường người bảo mật, khóa ký và mối liên kết của các khóa với người dùng được bảo vệ. Môi trường dùng và môi trường được bảo vệ. Môi trường được bảo vệ bao gồm các thiết bị mật mã đạt tiêu chuẩn CEN EN 419 221 – 5. Môi trường được bảo vệ được Bkav quản lý theo chính sách người dùng là cục bộ đối với người ký và việc bảo vệ do người dùng chịu trách nhiệm.

6.2 Mô hình áp dụng

Bkav cung cấp dịch vụ tạo chữ ký từ xa bằng hệ thống ký số máy chủ đáng tin cậy (TW4S) phù hợp với các yêu cầu bảo mật chung của tiêu chuẩn EN 41 241 – 1. Hệ thống được đặt trong môi trường an toàn bao gồm các yêu cầu, thủ tục và tài liệu bảo mật vật lý được cung cấp dịch vụ tạo chữ ký điện tử từ xa.

Bkav Remote Signing triển khai theo mô hình SCAL 2: Các khóa ký được sử dụng với mức độ tin cậy cao trong sự kiểm soát duy nhất của người ký:



Để đạt được SCAL 2, SAM quản lý việc sử dụng SAD để cung cấp "quyền kiểm soát truy cập duy nhất". Khóa ký được SAM quản lý bằng giao thức kích hoạt ký số (SAP). Thông qua giao thức này, mức độ bảo mật tương tự cho "quyền kiểm soát truy cập duy nhất" đạt được như mức độ bảo mật của QSCD.

Các chức năng chính của hệ thống TW4S:

- Tạo khóa ký trong SCDev và cung cấp việc sử dụng
- Quản ký khóa ký – xóa khóa, sao lưu, dự phòng trong SCDev
- Xác thực người dùng cho việc ký số
- Tạo chữ ký trong SCDev sau tương tác ủy quyền

Để đạt SCAL 2, cần thêm một số điều kiện sau

- Sử dụng thành phần SIC tạo liên kết giữa người ký và hệ thống ký số thông qua SAP
- Sử dụng SAM trong môi trường chống giả mạo và chịu trách nhiệm cho việc thực thi SAP. SAM bao gồm các chức năng chính sau:
    - Cung cấp dữ liệu cho việc tạo SAD trong môi trường chống giả mạo khi SAD không tạo bởi SIC

- Quản lý, xác thực SAD cho việc kích hoạt sử dụng key
- Quản lý các nhân tố xác thực người dùng với key ký và tạo key ký

TW4S sử dụng SAM, module mật mã để tạo key ký và tạo ra giá trị chữ ký. TW4S bao gồm ứng dụng máy chủ ký số (SSA), và thiết bị tạo chữ ký (SCDev).

SCDev là thiết bị được kiểm soát bởi SAM trong môi trường chống giả mạo. Module sử dụng SAD được truyền thông qua SAP để đảm bảo mức độ tin cậy cao việc sử dụng khóa ký dưới sự kiểm soát của người dùng. SSA sử dụng SCDev để tạo, duy trì và sử dụng khóa ký.

TW4S bao gồm môi trường cục bộ và môi trường từ xa. Người ký sử dụng môi trường cục bộ, tương tác thông qua các thiết bị (laptop, tablet và mobile) với ứng dụng ký số máy chủ (SSA) từ xa để sử dụng dịch vụ SSA. SSA chuyển tiếp thông tin giữa SIC hoặc SSA tới QSCD. Bên trong QSCD, SAM xác thực SAD, nếu thành công, SAM cho phép kích hoạt ký số và tạo giá trị chữ ký. Giá trị được trả lại SSA và được chuyển lại Ứng dụng tạo chữ ký số từ xa (SCA) hoặc SIC. TW4S cung cấp 3 dịch vụ sau: xác thực người dùng, xác thực khóa ký, ứng dụng tạo chữ ký chịu trách nhiệu tạo tài liệu đã ký bằng các giá trị chữ ký do TW4S cung cấp.

SAD được tạo trực tiếp hoặc gián tiếp khi dưới sự xác nhận người dùng. Tính bảo mật và toàn vẹn của khóa ký được SCDev đảm bảo. SAP là giao thức người ký thông qua SIC và TW4S giao tiếp tạo SAD. SAP xác thực người dùng, xác thực tính đúng đắn của yêu cầu chữ ký với SAD, tính hợp lệ của khóa ký đã chọn và đảm bảo an toàn với tất cả thành phần SAD. SCDev được kiểm soát bởi SIC thông qua SAP và đảm bảo hệ thống ký số hoạt động dưới quyền kiểm soát duy nhất của người dùng. Hệ thống cho phép ký số hàng loạt bằng cách sử dụng nhiều DTBS/R trong một SAD.

SIC là thành phần được quản lý bởi ứng dụng được cài đặt trên thiết bị di động, đảm bảo quyền kiểm soát duy nhất của người dùng. SIC là thành phần thiết yếu trong hoạt động của SAP cho việc tạo chữ ký bởi SSA. SIC tham gia toàn bộ trong quá trình xác thực người dụng và tạo SAD.

SAM là phần mềm sử dụng SAD để đảm bảo khóa ký được sử dụng với mức độ tin cậy cao nhất dưới sự kiểm soát của người ký với SCAL 2. SAM hoạt động trong môi trường chống giả mạo và đạt được tiêu chuẩn, SAM chịu trách nhiệm cho việc thực thi SAP. SAM cung cấp các thành phần: tạo SAD, tạo và kích hoạt ký số.

SCA là thành phần ứng dụng tạo tài liệu ký số sử dụng chữ ký số được tạo bởi Thành phần dịch vụ máy chủ ký số (SCASC). SCA quản lý dữ liệu ký số và truyền dữ liệu cho SSA. SCASC là thành phần hỗ trợ tạo chữ ký, và thực thi các quá trình tạo chữ ký, SCA

có thể tương tác với SSASC để tạo yêu cầu giá trị chữ ký. SCA nhận dữ liệu được ký và các tham số khác bao gồm chứng thư số của người dùng cũng như đầu vào và đầu ra.

Môi trường chống giả mạo TSP được kiểm tra theo các yêu cầu đối với hoạt động an toàn của hệ thống máy chủ ký số. Hệ thống bảo vệ các cuộc tấn công internet và các tiến trình kết nối hệ thống với môi trường bên ngoài. Môi trường người ký là cục bộ và người ký chịu trách nhiệm cho việc bảo vệ. Môi trường người ký bao gồm các thành phần: chuẩn bị dữ liệu ký, định dạng chữ ký và SIC. SIC được sử dụng bởi người ký để tạo mối liên kết giữa người ký và toàn bộ hoạt động ký được kích hoạt thông qua SAP.

6.3 Khóa mật mã

Bkav sử dụng hệ thống khóa mật mã đảm bảo tính toàn vẹn, bảo mật của dữ liệu trong hệ thống. Các khóa mật mã bao gồm:

- **Khóa ký người dùng**: yêu cầu mức độ bảo mật cao.
- **Khóa hạ tầng**: yêu cầu mức độ bảo mật cao nhưng do tính phân phối nên tính nhạy cảm thấp hơn khóa ký người dùng.
- **Khóa kiểm soát**: được sử dụng bởi hệ thống TW4S để quản lý người dùng, tính bảo mật thấp hơn và được sử dụng bởi các bên tin tưởng có vòng đời ngắn hơn
- **Khóa phiên**: sử dụng cho các giao dịch ngắn hạn

Khóa bí mật được tạo ra trong SCDev với mức độ an toàn đạt EAL 4 hoặc cao hơn. Protection Profile của module mật mã đạt yêu cầu tiêu chuẩn EN 419 221 – 5. Thuật toán và độ dài khóa sử dụng có trong thông tư 16/2019 BTTT. Bkav không sử dụng bất kỳ khóa bí mật mà không được bảo bệ với SCDev. Khi khóa cần thiết được sử dụng bên ngoài SCDev, Bkav Remote Signing đảm bảo tính an toàn và toàn vẹn của khóa bí mật, môi trường đạt mức an toàn tương đương hoặc cao hơn SCDev. SCDev được khởi tạo trước khi sinh khóa ký.

Bkav đảm bảo toàn bộ các bản sao lưu, lưu trữ, khôi phục được thực hiện bởi cá nhân được ủy quyền, Master Key dùng để bảo vệ khóa ký được lưu bên ngoài SCDev ở dạng được bảo vệ.

Bkav đảm bảo khóa được phân phối qua kênh an toàn. Khóa bí mật được thay đổi khi thuật toán và độ dài khóa có nguy cơ mất an toàn.

Khóa ký không được lưu trữ, được hủy khóa khi chứng thư số liên kết bị hết hạn, theo yêu cầu của người dùng, hoặc sự liên kết khóa giữa người dùng và khóa ký không được duy trì sau khoảng thời gian. Việc hủy khóa đảm bảo toàn bộ các bản sao lưu đều được hủy và không có thông tin nào có thể sử dụng để tạo lại khóa.

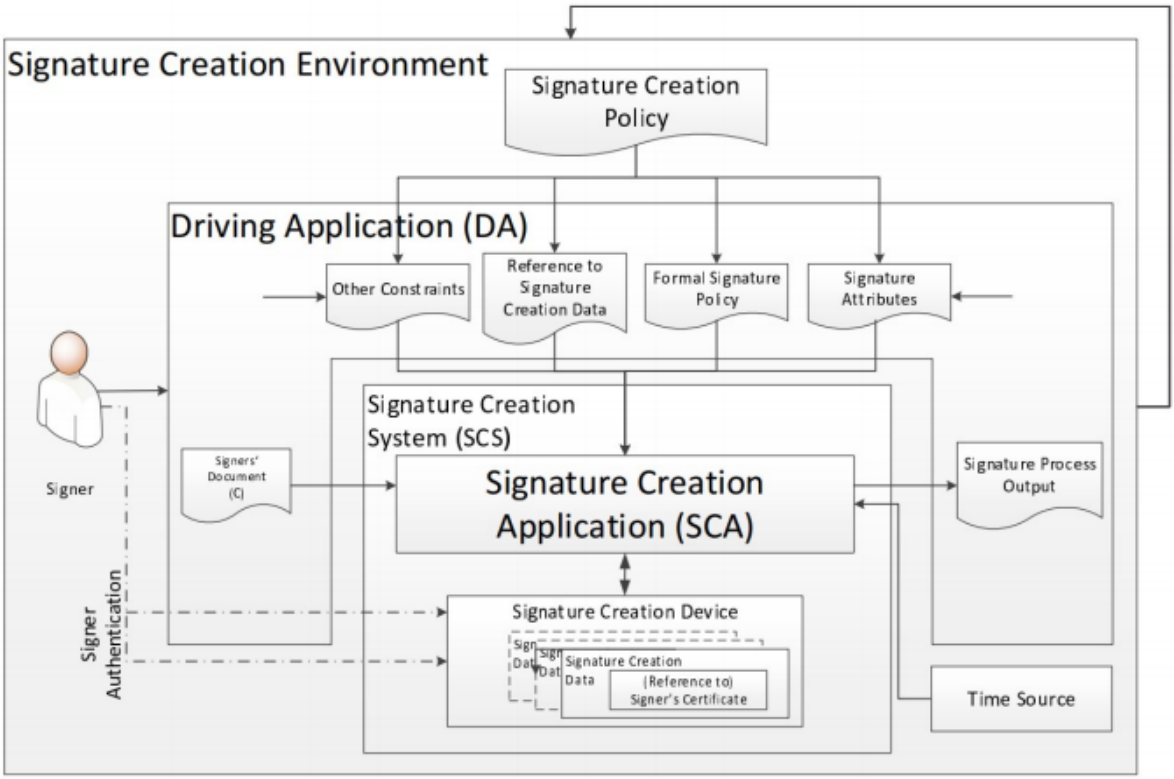
6.4 Yêu cầu về định danh và xác thực

Bkav áp dụng các yêu cầu sau:

- Định danh và xác thực được áp dụng cho người được ủy quyền, hạn chế quyền truy cập và sử dụng TW4S
- TW4S yêu cầu mỗi người dùng định danh và xác thực thành công trước khi có bất kỳ hành động nào thay mặt cho người dùng hoặc vai trò người dùng đảm nhận
- Xác thực lại khi đăng xuất khỏi hệ thống
- Bkav sử dụng kết hợp các dữ liệu xác thực không thể dự đoán
- Cơ chế phiên chấm dứt nếu thiết bị người dùng không được giám sát, sau một khoảng thời gian không hoạt động
- Nếu người dùng không được xác thực thành công đạt ngưỡng, TW4S ngăn chặn việc xác thực tiếp theo cho đến khi quản trị viện mở khóa cho người dùng hoặc trong một khoảng thời gian.

6.5 Chức năng tạo chữ ký số

Môi trường tạo chữ ký số bao gồm người ký, ứng dụng chuyển đổi (DA/DIS) và hệ thống tạo chữ ký số



Hệ thống tạo chữ ký số (SCS) bao gồm ứng dụng tạo chữ ký số (SCA) và thiết bị tạo chữ ký số (SCDev). SCA là dịch vụ của SCASC. SCS nhận dữ liệu cần ký số, cùng với các dữ liệu khác từ DA. SCS tạo dữ liệu cần được ký số (DTBS) và định dang (DTBSF).

SCDev lưu trữ chứng thư số, các dữ liệu tạo chữ ký, xác thực người ký và tạo chữ ký số. Bkav sử dụng nhiều cách khác nhau để thực hiện các thủ tục tạo chữ ký, như phần mềm ứng dụng trên máy tính có giao diện người dùng đồ họa, dịch vụ web hoặc ứng dụng web…

Quá trình tạo chữ ký được kiểm soát bằng các thủ tục ràng buộc. Bkav sử dụng các chính sách và áp dụng các biện pháp kiểm soát cụ thể cho việc tạo chữ ký, DA cung cấp các ràng buộc bổ sung cho SCA thông qua các tham số do ứng dụng hoặc người ký lựa chọn. Những ràng buộc này có ảnh hưởng đến quá trình tạo chữ ký và kết quả tạo, các ràng buộc:

- Sử dụng chính sách tạo chữ ký
- Dữ liệu được kiểm soát cụ thể trong hệ thống
- Các ràng buộc bổ sung cho SCA bằng các tham số do ứng dụng hoặc người ký

SD là tài liệu cần được ký số, là tài liệu có thể ở định dạng có thể xem như tài liệu văn bản, tin nhắn hoặc tệp tin, có thể chỉnh sửa. SD có thể ở định dạng như PDF, XML…

SDR được sử dụng để tạo ra chữ ký số. SDR được cung cấp bởi DA tới SCA. Khi SD không cung cấp bởi DA, SCA sẽ tính toán SDR từ SD. SDR thường là mã băm của SD.

DTBS là dữ liệu được tạo thành từ các đối tượng thông tin đại diện, bao phủ chữ ký. SCDev sử dụng DTBSR, và các thuật toán theo quy định tạo chữ ký số.

SDO bao gồm chữ ký số và các tham số chữ ký cũng có thể bao gồm một số tham số khác không được ký số

6.5.1 Thuộc tính chữ ký

Thuộc tính	Ý nghĩa
Signing Certificate Identifier	Thuộc tính liên kết chứng thư số. Phòng ngừa sử dụng chứng thư số khác có cùng Public Key
Signature Policy Identifier	Thuộc tính bao gồm định danh duy nhất của chính sách tạo chữ ký số áp dụng cho việc tạo chữ ký
Data Content Type	Thuộc tính loại dữ liệu
Commitment type	Thuộc tính cho biết loại cam kết được thực hiện bởi người ký khi ký một số tài liệu nhất định. Loại cam kết đã được chỉ

indication	đinh thông qua OID hoặc URI
Counter Signatures	Thuộc tính bộ đệm chữ ký
Claimed Signing Time	Thuộc tính đại diện cho thời gian ký
Claimed Signer Location	Thuộc tính đại diện cho địa điểm ký
Signer's Attributes	Thuộc tính bao gồm chứng thư số của người dùng

6.5.2 Các loại chữ ký

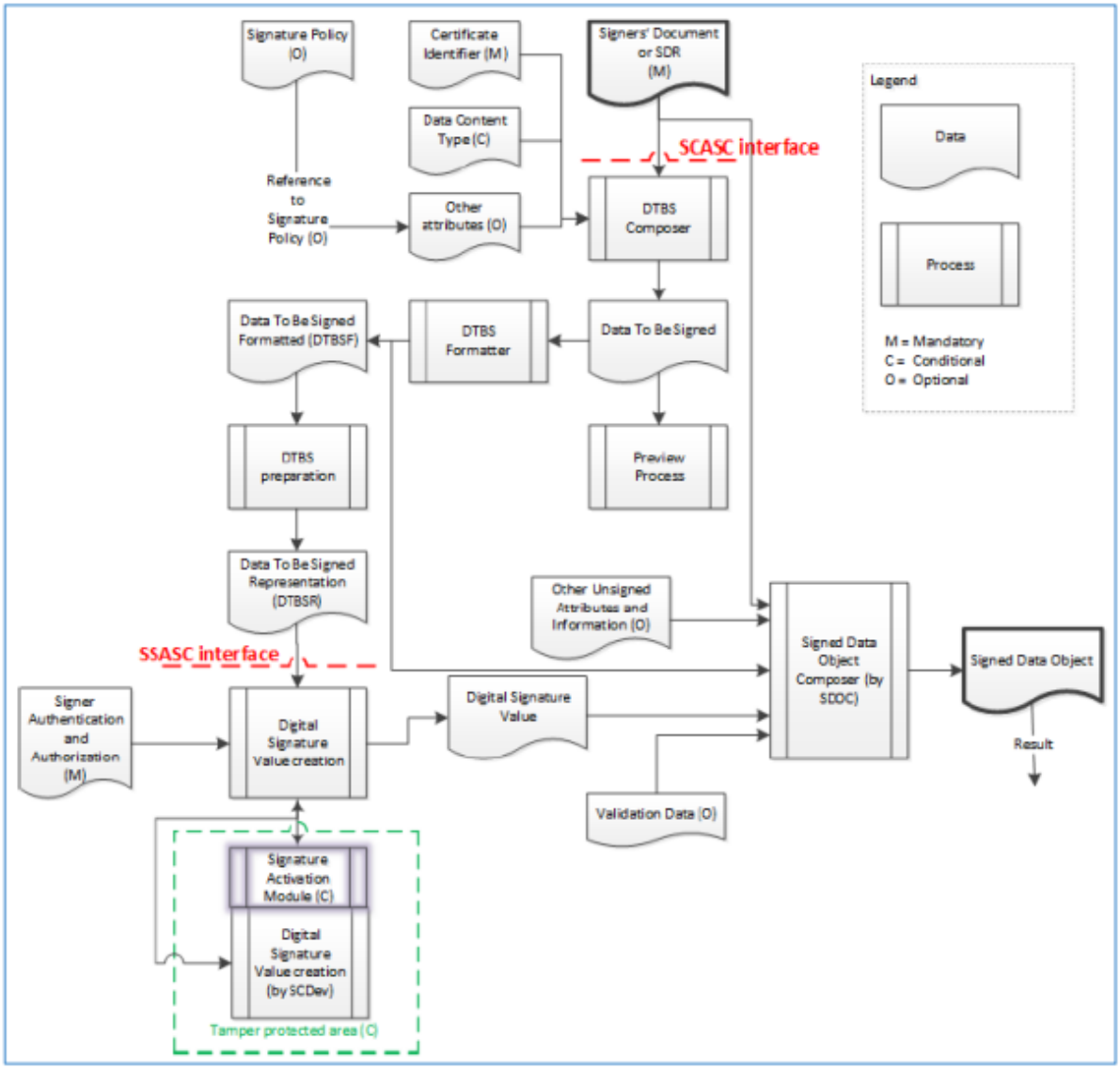
Enveloped: Chữ ký điện tử được tích hợp trong tệp bổ sung cho tệp gốc

Enveloping: Chữ ký được tích hợp trong dữ liệu gốc

Detached: Chữ ký được đính vào tài liệu được đặt trong các tệp riêng biệt

6.6 Thành phần, giao thức và giao diện dịch vụ tạo chữ ký từ xa

6.6.1 Thành phần chính và giao diện dịch vụ



Giao diện SSASC bao gồm DTBSR và các tham số khác là đầu vào và kết quả là chữ ký số. **SCASC** là thành phần hỗ trợ tạo chữ ký số và các phần chỉ định trong quy trình. SCASC tương tác với SSASC dựa trên yêu cầu tạo chữ ký số

Giao diện SCASC bao gồm dữ liệu ký số và mã băm, các tham số là đầu vào và kết quả là chữ ký số.

SCS là dịch vụ ứng dụng tạo chữ ký số SCA là SSA. Chữ ký số được tạo bởi SCA. SCA quản lý dữ liệu được ký và truyền dữ liệu tới SSA. SCA có thể tương tác với SSASC bằng yêu cầu tạo chữ ký số. Giao diện SCA nhận dữ liệu và các tham số khác bao gồm chứng thư số người ký. Tóm lại, các giao diện có thể phụ thuộc vào chức năng phân chia giữa SCS và hệ thông ký số cục bộ

6.6.2 Ứng dụng tạo chữ ký số SCA

Dữ liệu SD được băm thành SDR trong DTBS. Việc tạo SDR có thể thực hiện tại SCASC. Trong trường hợp này, SDR được truyền tới SCACS. Trường hợp khác SD được truyền tới SCASC. Dữ liệu SD là thành phần của SDO. Chức năng thành phần SDOC sẽ liên kết chữ ký số với SD.

Việc tạo và định dạng DTBS, băm SDR và băm toàn bộ thuộc tính được lưu trữ trong DTBSF.

6.6.3 Ứng dụng máy chủ ký số SSA

Mục đích của quy trình là truyền DTBSR và tạo chữ ký số dưới quyền kiểm soát của người dùng. Việc tạo chữ ký số được kiểm soát bởi SSASC. Người ký kích hoạt ký số bằng phương tiện xác thực an toàn và quy trình kích hoạt, SSASC có thể sử dụng SCDev từ xa để tạo, duy trì và sử dụng khóa ký dưới quyền kiểm soát của người dùng. Người dùng kiểm soát khóa ký từ xa với mức độ an toàn cao bằng module SAM. SAM là phần mềm sử dụng SAD để xác thực người dùng và trao quyền truy cập khóa dưới quyền kiểm soát của người dùng.

6.6.4 Tương tác SCASC và SSASC

Kiến trúc hỗ trợ máy chủ ký số từ xa bao gồm tương tác SCASC và SSASC với các thành phần các nhau trong quy trình tạo chữ ký số và mức độ tin cậy trong việc kiểm soát khóa ký.

Hệ thống bao gồm SCASC liên kết SSASC điều khiển SCDev. Dịch vụ CA, RA, OCSP và CRL, TSA và máy chủ xác thực, ủy quyền nằm ngoài mô hình.

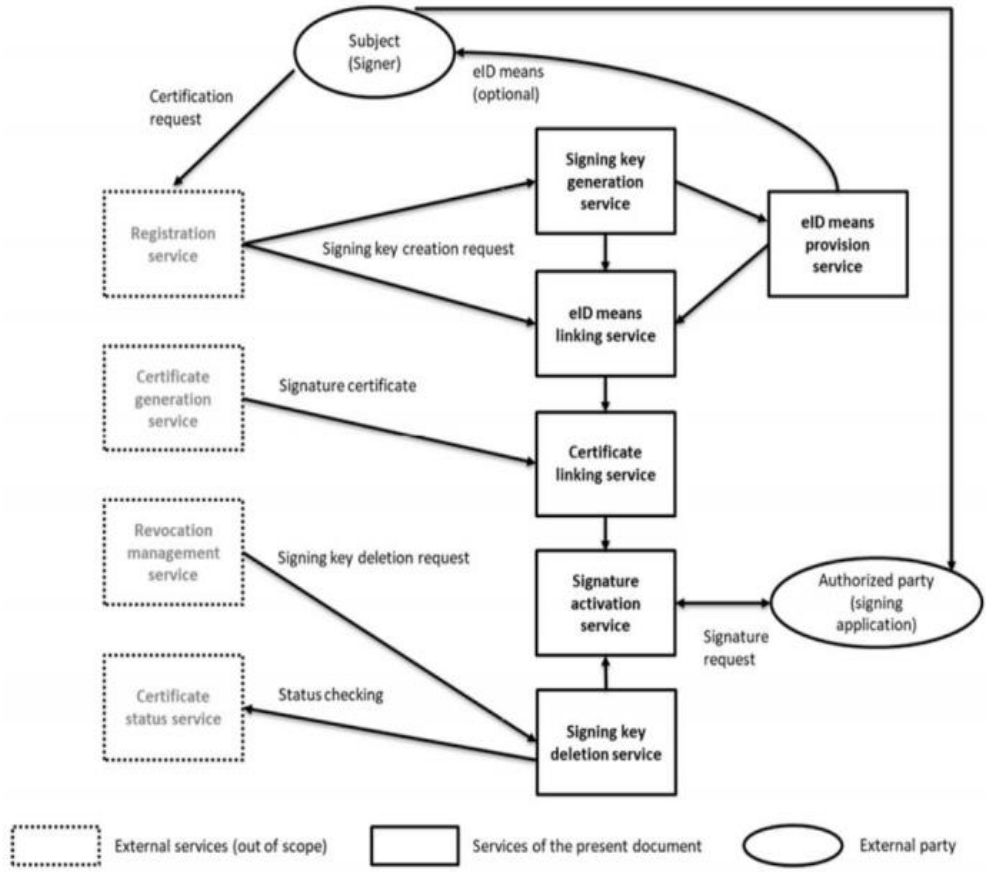
Bkav áp dụng giao thức hỗ trợ SCASC và SSASC với các dữ liệu, mã băm và DTBSR. Trong quy trình tạo chữ ký số, người ký không bắt buộc phải phê duyệt từng tài liệu

6.7 Thành phần, giao thức và giao diện địch vụ tạo chữ ký từ xa

6.7.1 Thành phần SSASC

Bao gồm các thành phần dịch vụ sau

- Tạo khóa ký
- Cung cấp phương tiện định danh
- Liên kết phương tiện định danh điện tử
- Liên kết chứng thư số
- Kích hoạt ký số
- Xóa khóa ký



Mô hình liên kết giữa dịch vụ Bkav với các dịch vụ bên ngoài

6.7.2 Khởi tạo khóa ký

6.7.2.1 Tạo khóa ký

Các yêu cầu đối với khóa ký được Bkav áp dụng

- Khóa cá nhân, khóa bí mật, khóa ký được tạo trong SCDev đạt tiêu chuẩn trong thông tư 16/2019 – BTTTT
- Thuật toán sử dụng được quy định trong thông tư 16/2019 – BTTTT
- SCDev được khởi tạo trước khi tạo bất kỳ khóa người dùng
- Hệ thống tạo chữ ký sử dụng thuật toán đảm bảo trong suốt vòng đời của chứng thư số
- Việc tạo khóa được SAM quản lý đảm bảo quyền kiểm soát duy nhất của người ký. SCDev được điều khiển từ xa băng SAM và thực hiện trong môi trường chống giả mạo

6.7.2.2 Liên kết phương tiện định danh

- SSASP liên kết khóa ký với phương tiện định danh người ký

- SSASP tạo phương tiện định danh và cung cấp tới người ký
- SSASP đảm bảo dữ liệu định danh của người ký với phương tiện eID giống với dữ liệu được liên kết

6.7.2.3 Liên kết chứng thư số

Các yêu cầu được áp dụng với SSASC:

- TW4S liên kết các khóa ký của người ký với chứng thư số tương ứng
- Khóa ký không được sử dụng trước khi TW4S liên kết khóa với chứng thư số
- TW4S bảo vệ tính toàn vẹn của liên kết này

6.7.2.4 Cung cấp phương tiện định danh

- Bkav Remote Signing cung cấp phương tiện định danh an toàn và tin tưởng tới người ký, bao gồm SSA
- SSASP cá nhân hóa phương tiện định danh của người ký với dữ liệu ký của người dùng. Dữ liệu kích hoạt được SIC chuẩn bị an toàn và được đăng ký, tách biệt với eId của người ký

6.8 Thành phần, giao thức và giao diện dịch vụ tạo chữ ký từ xa

6.8.1 Kích hoạt ký số

Bkav Remote Signing thực hiện kích hoạt ký số theo các yêu cầu sau:

- Khóa ký được sử dụng trong QSCD
- Hệ thống QSCD và cấu hình được mô tả trong chứng nhận hoặc các cấu hình tương đương mức độ bảo mật
- Bkav sử dụng giao thức SAP
- Bkav giảm thiểu các mối đe dọa với SAP và thực hiện các biện pháp báo vệ SAP khỏi tái tạo thứ cấp, các biện pháp chống lại tấn công bypass cũng như giám sát việc giả mạo người ký và SCDev
- Sử dụng SAM đảm với mức độ bảo mật cao đảm báo khóa ký được sử dụng dưới sự kiểm soát người dùng. SAM được sử dụng trong môi trương chống giả mạo.
- Bkav sử dụng SAP bảo vệ SAD bảo vệ các cuộc tấn công giả mạo
- SAP được thiết kế đảm bảo người dùng có thể luôn luôn được bảo vệ việc kích hoạt khóa ký

Bkav Remote Signing thiết kế việc kích hoạt đạt được các yêu cầu sau:

- SSA yêu cầu định danh và xác thực người dùng thành công trước khi cho phép bất kỳ hành động nào liên quan đến việc ảnh hưởng quyền kiểm soát duy nhất mỗi khóa ký
- Bkav sử dụng giao thức an toàn ngăn chặn tấn công với bất kỳ hình thức nào, trong đó người dùng có thể sử dụng dữ liệu nhận dạng không thuộc sở hữu
- Bkav áp dụng kiểm soát truy cấp đảm bảo người ký không thể truy cập vào hệ thống nhạy cảm hoặc bất kỳ chức năng nào có thể sử dụng khóa ký của người khác
- Bkav áp dụng kiểm soát chặt chẽ khóa ký, TW4S đảm bảo DTBS/R được cung cấp dưới quyền kiêm soát của người ký chỉ được ký bởi khóa người ký sở hữu
- TW4S yêu cầu người ký xác thực tạo SAD cho SAM để kích hoạt ký số
- Bkav sử dụng giao thức với độ an toàn cao bằng cách sử dụng các biện pháp kiểm soát tương ứng với mức độ rủi ro chống lại các mối đe dọa với việc sử dụng SAD: online or off-line speculations, duplication of identification data, fishing, wiretapping, replacement, session highjacking, attacks from a human in the environment, theft of identification data, frauds và mask attacks;
- Khóa kích hoạt chỉ được sử dụng duy nhất cho DTBS/R được cho phép bởi SAP
- SSASP đảm bảo chứng thư số còn giá trị sử dụng trước khi sử dụng khóa ký tương ứng
- Khóa ký chỉ được sử dụng khi được sự đồng ý của người ký
- Tham số thuật toán sử dụng cho hệ thống được quy định trong thông tư 16/2019 – BTTTT

6.8.2 Quản lý SAD

- SAD là tập hợp dữ liệu hoặc là kết quả của quy trình mã hóa
- SAD được tạo trực tiếp hoặc gián tiếp bởi SIC
- SAD bao gồm các tham số sau:
    - Một hoặc nhiều DTB/R
    - Thành phần định danh người ký
    - Khóa ký được lựa chọn
- SAD chỉ được sử dụng cho việc kích hoạt khi xác thực người dùng thành công, được kiểm tra bởi SAM
- SAD được truyền tới SAM thông qua SAP

- SAD được bảo vệ và kiểm tra sau khi kích hoạt để đảm bảo an toàn

6.8.3 Xóa khóa

- Khóa được xóa trong các trường hợp sau:
    - Chứng thư số hết hạn, thu hồi
    - Khi người dùng yêu cầu hủy khóa
    - Khóa được hủy sau khi kết thúc phiên làm việc, khi liên kết người ký và khóa ký không được duy trì
- Bkav không lưu bất kỳ bản sao lưu khóa ký và đảm báo không có bất kỳ thông tin nào có thể sử dụng để khôi phục khóa

6.8.4 Quản lý khóa

- Khóa được lưu trong HSM với cơ chế quản lý kép
- Các bản sao lưu được tạo khi khóa được khởi tạo được lưu trong thiết bị FIPS 140-2 level 3 hoặc cao hơn và CC EAL4+
- Khóa bí mật tạo chữ ký số được sao lưu ít nhất mười năm khi hết thời gian hiệu lực hoặc sau khi chấm dứt.
- Truyền khóa trong HSM được thực hiện trong các trường hợp sau:
    - Bảo vệ bảo sao lưu dự phòng của khóa được lưu trữ trong module bảo mật phần cứng
    - Khi khóa cá nhân được truyền từ hệ thống module này sang module phần bảo mật phần cứng khác

Bkav tuần thủ các yêu cầu sau trong việc quản lý khóa

- Toàn bộ khóa bí mật không được giữ trong môi trường không an toàn. Khóa được lưu an toàn trong thiết bị HSM đạt tiêu chuẩn FIPS 140-2 level 3 hoặc cao hơn
- Khóa không được truy suất khỏi HSM
- TW4S đảm bảo các bản sao lưu dự phòng được thực hiện bởi nhân viên ủy quyền. Khóa master dùng bảo bệ người dùng và khóa dược lưu trữ, khôi phục dựa trên kiểm soát hai nhân tố. Khóa không được lưu ngoài SCDev dạng không được bảo vệ
- Bkav kiểm soát số lượng bộ dữ liệu được sao chép để nó không vượt qua mức tối thiểu cần thiết đảm bảo tính liên tục của dịch vụ
- 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

7. Kiểm soát, quản lý và vận hành

7.1 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.

7.1.1 Vị trí đặt và xây dựng hệ thống

- Hệ thống thiết bị Bkav Remote Signing được đặt tại hai trung tâm dữ liệu của VDC và trên IDC.
- 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.

7.1.2 An ninh vật lý và môi trường

- Hệ thống Bkav Remote Signing 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. 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.

7.1.3 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 Remote Signing 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

7.1.4 Điều kiện về nguồn điện và không khí

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

7.1.5 Chống nước

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

7.1.6 Chống và bảo vệ trước các nguy cơ về lửa

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

7.1.7 Phương tiện lưu trữ dữ liệu

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

7.1.8 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

7.1.9 Hệ thống dự phòng ở địa điểm khác

- Bkav Remote Signing 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.

7.2 Quy trình kiểm soát

7.2.1 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.

7.2.2 Số lượng người được yêu cầu trên một nhiệm vụ

- Bkav Remote Signing 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 Remote Signing luôn đòi hỏi có ít nhất 2 người để thực hiện các công việc nhạy cảm.

7.2.3 Nhận dạng và xác thực trong mỗi vai trò

- Mọi cá nhân trước khi trở thành người được tin tưởng trong hệ thống Bkav Remote Signing 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 Remote Signing đảm bảo rằng các cá nhân hoàn toàn được tin tưởng trước khi thực hiện các công việc nhạy cảm.

7.2.4 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.

7.3 Kiểm soát nhân sự

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

- Những người tin cậy của Bkav Remote Signing 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.

7.3.2 Các thủ tục kiểm tra lý lịch, trình độ

- Trước khi bổ nhiệm nhân viên vào một nhiệm vụ cần được tin tưởng, Bkav Remote Signing 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).

7.3.3 Yêu cầu đào tạo

- Bkav Remote Signing 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 Remote Signing hướng tới trách nhiệm cụ thể của mỗi nhân viên, nội dụng huấn luyện bao gồm:
  - Các khái niệm PKI cơ bản, giải pháp Bkav Remote Signing.
  - 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 bảo sao luu 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 Remote Signing.
- 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.

7.3.4 Tần suất đào tạo và đào tạo lại

- Bkav Remote Signing 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.

7.3.5 Tần suất luân chuyển công việc

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

7.3.6 Hình phạt đối với các hành động không được phép

- Bkav Remote Signing 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 Remote Signing. 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.

7.3.7 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 Remote Signing. Những người này cũng phải tuân theo các tiêu chuẩn an ninh như nhân viên của Bkav Remote Signing. 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 Remote Signing.

7.3.8 Cung cấp tài liệu cho nhân viên

- Bkav Remote Signing 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.

7.3.9 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.

7.4 Các quy trình ghi nhật ký hệ thống

7.4.1 Các loại sự kiện được ghi lại

- Bkav Remote Signing 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

7.4.2 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.

7.4.3 Thời hạn giữ lại các nhật ký

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

7.4.4 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 Remote Signing đảm bảo tính toàn vẹn và cung cấp chứng năng xác thực thính toàn vẹn của dữ liệu

7.4.5 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 Remote Signing.
- 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.

7.4.6 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.

7.4.7 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.

7.4.8 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.

7.5 Lưu trữ các bản ghi

7.5.1 Các loại bản ghi được lưu trữ

- Mọi dữ liệu nhật ký trong phần 5.4.
- Thông tin đơn xin cấp chứng thư số.
- Các thông tin bổ sung của đơn xin cấp chứng thư số.
- Thông tin vòng đời chứng thư số như: thu hồi, đổi khóa, làm mới…

7.5.2 Thời hạn giữ lại các lưu trữ

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

7.5.3 Bảo vệ lưu trữ

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

7.5.4 Các thủ tục sao lưu lưu trữ

- Dữ liệu lưu trữ được backup theo chế độ backup chung của Bkav Remote Signing.
- Khi dữ liệu nhật ký được lưu hệ thống ngoài. Hệ thống này có thể cung cấp dữ liệu nhật ký khi cần thiết.

7.5.5 Nhãn thời gian của các bản ghi

- Hệ thống được đồng bộ với nguồn thời gian tiêu chuẩn đảm bảo chính xác
- Mỗi bản ghi trong nhật ký bao gồm thời gian khi quá trình lưu trữ diễn ra

7.5.6 Hệ thống lưu trữ

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

7.5.7 Thủ tục lấy và kiểm tra thông tin lưu trữ

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

7.6 Xử lý sự cố, thảm họa và phục hồi

7.6.1 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.

7.6.2 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

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

- Khi khóa bí mật của Bkav Remote Signing nghi ngờ bị mất/lộ, Bkav Remote Signing sẽ thực hiện thủ tục xử lý khi khóa bị lộ. Đội xử lý sự cố ninh của Bkav

Remote Signing - Bkav Remote Signing 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 Remote Signing, người phụ trách kỹ thuật và người phụ trách cấp phát chứng thư số.

- Nếu chứng thư số của Bkav Remote Signing bị thu hồi, các thủ tục sau sẽ được thực hiện:
  - Trạng thái thu hồi chứng thư số của Bkav Remote Signing sẽ được công bố bởi RootCA.
  - Bkav Remote Signing cố gắng thông báo cho toàn bộ người nhận trong hệ thống Bkav Remote Signing dừng sử dụng các chứng thư số do Bkav Remote Signing ban hành.
  - Bkav Remote Signing xin cấp chứng thư số mới từ RootCA và ban hành chứng thư số cho các thuê bao của mình để họ tiếp tục sử dụng.

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

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

7.7 Dừng hoạt động

- Khi không còn hoạt động, Bkav Remote Signing 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 Remote Signing, RA sẽ có kế hoạch kết thúc nhằm giảm thiểu thiệt hại nhất cho khách hàng. Bkav Remote Signing 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 Remote Signing 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 Remote Signing 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 Remote Signing 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 Remote Signing đảm nhiệm.
- Thực hiện các thủ tục chuẩn bị trước khi chuyển các dịch vụ chứng thực sang cho CA khác.

8. Đảm bảo an toàn an ninh về kỹ thuật

8.1 Kiểm soát và bảo vệ khóa bí mật

8.1.1 Tiêu chuẩn module mã hóa

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

8.1.2 Cơ chế kiểm soát khóa bí mật

- Cơ chế kiểm soát khóa bí mật được Bkav Remote Signing 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 Remote Signing, N = 4;

8.1.3 Lưu giữ ngoài khóa bí mật của thuê bao

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

8.1.4 Dự phòng khóa bí mật

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

8.1.5 Lưu trữ khóa bí mật

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

8.1.6 Chuyển khóa bí mật vào/ra HSM

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

8.1.7 Lưu trữ khóa bí mật trong HSM

- Bkav Remote Signing giữ khóa bí mật trong các HSM, khóa bí mật được lưu trong dạng được mã hóa.

8.1.8 Phương thức kích hoạt khóa bí mật

- Các thành viên Bkav Remote Signing sẽ có các biện pháp bảo vệ kích hoạt khóa bí mật phù hợp, cụ thể:
  - Đối với quản trị hệ thống Bkav Remote Signing/RA: khóa bí mật được lưu trong dạng bảo vệ, việc kích hoạt khóa bí mật yêu cầu mật khẩu bảo vệ. Khi không sử dụng, khóa bí mật tồn tại ở dạng mã hóa.
  - Đối với Bkav Remote Signing: sử dụng HSM để lưu trữ khóa bí mật, việc kích hoạt khóa bí mật yêu cầu các mã chia sẻ theo cơ chế chia sẻ mã trong 6.2.2.

8.1.9 Phương pháp ngừng kích hoạt khóa bí mật

- Khóa bí mật của Bkav Remote Signing/RA bị ngừng kích hoạt khi không chứa trong Token Reader (HSM). RA của Bkav Remote Signing được yêu cầu phải đăng xuất khỏi hệ thống khi rời chỗ làm việc.

- Khóa bí mật của quản trị hệ thống, của RA và của thuê bao có thể bị ngừng kích hoạt sau mỗi nhiệm vụ, sau khi đăng xuất hệ thống hoặc sau một khoảng thời gian nhất đinh.

8.1.10 Phương pháp hủy bỏ khóa bí mật

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

8.1.11 Đánh giá module mã hóa

- Xem phần 6.2.1

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

8.2.1 Lưu trữ khóa công khai

- Bkav Remote Signing sẽ lưu trữ khóa công khai của mình, của RA và toàn bộ thuê bao.

8.2.2 Thời hạn sử dụng chứng thư số và thời hạn sử dụng cặp khóa

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

8.3 Quản lý tài sản

- Bkav Remote Signing cung cấp mức độ bảo vệ thích hợp với tài sản, bao gồm tài sản thông tin
- Bkav Remote Signing duy trì danh sách kiểm kê tất cả tài sản thông tin, phân loại chúng dựa trên đánh giá rủi ro

8.4 Quản lý an ninh

- Bkav Remote Signing quản lý an ninh hệ thống TW4S cung cấp dịch vụ tạo chữ ký số
- Các vai trò trong hệ thống
  - Vai trò đặc quyền: **Security Officers, System Administrator, System Operators và System Auditor**
  - Vai trò không đặc quyền:
    - **Signer**: Đươc ủy quyền sử dụng hệ thống TW4S sử dụng SAD cũng như SAP để tạo chữ ký số
    - **SCA**: Được xác thực để gửi dữ liệu cần ký với TW4S
    - **RA**: Chịu trách nhiệm cho cấp phát chứng thư số
- TW4S đảm bảo người dùng được ủy quyền đảm nhận vai trò quản trị viên hệ thống hoạc người điều hành hệ thống không có vai trò đánh giá hệ thống hoặc vai trò của nhân viên bảo mật
- Những người thuộc nhóm người dùng hệ thống đặc quyền được tô ra trong tài liệu vai trò và nội dung họ được đào tạo
- Chỉ có vai trò đặc quyền hệ thống mới có quyền truy cập vật lý vào phần cứng và có thể quản trị hệ thống TW4S
- Chỉ có người dùng đặc quyền hệ thống mới có quyền để quản lý TW4S thông qua tất cả các ứng dụng và giao diện tương ứng

8.5 Quản lý vận hành

- Bkav Remote Signing đảm bảo hệ thống TW4S có sẵn tài liệu bao gồm các điều khoản sau: Hướng dẫn cho phép hoạt động thích hợp an toàn, các biện pháp giảm thiểu nguy cơ hỏng hóc hệ thống, và các biện pháp bảo vệ thông tin chúng xử lý khỏi virus và phần mềm độc hại
- Bkav Remote Signing đảm bảo hệ thống gồm các trách nhiệm của bốn vai trò đặc quyền và bao gồm: Hướng dẫn cài đặt, quản trị và sử dụng

8.6 Kiểm soát mật mã

Bkav Remote Signing tạo cặp khóa RSA sử dụng HSM đặt chuẩn FIP 140 -2 level 3 hoặc CC EAL4+ hoặc cao hơn. Bkav Remote Signing sử dụng khóa bí mật cho các mục đích sau:

- Ký chứng chỉ hoạt động được cấp cho các tổ chức chứng nhận trong cơ sở hạ tầng
- Ký vào danh sách chứng chỉ thu hồi (CRL) đã được cấp và xuất bản

- Tạo chữ ký của người dùng

Đối với dịch vụ tạo chữ ký từ xa, yêu cầu cấp chứng chỉ từ ứng dụng Bkav Remote Signing Mobile, toàn bộ khóa khách hàng được tạo trong HSM đạt chuẩn theo quy định. Các thiết bị tạo chữ ký đảm bảo sử dụng các phương tiện và quy trình phụ hợp với mức yêu cầu tối thiểu:

- Tính bảo mật của dữ liệu để tạo chữ ký được đảm bảo
- Ngày tạo chữ ký luôn được đồng bộ với nguồn thời gian tiêu chuẩn
- Dữ liệu tạo chữ ký được an toàn được bảo mật đầy đủ và không thể bị trích xuất và bảo vệ bằng các công nghệ hiện có
- Dữ liệu để tạo chữ ký được bảo vệ an toàn chống lại việc sử dụng bất hợp pháp

8.7 Kích hoạt dữ liệu

8.7.1 Tạo và cài đặt dữ liệu kích hoạt

- 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 9 ký tự.
  - Chứa từ 3 trong 4 loại ký tự sau: chữ hoa (A, B, C…), chữ thường (a, b, c), chữ số (0, 1, 2…) và các ký hiệu (!, @, $...)
  - Không chứa tất cả hoặc một phần tên tài khoản người dùng tương ứng.

8.7.2 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.
- RA và quản trị hệ thống được yêu cầu phải giữ khóa bí mật ở dạng mã hóa sử dụng mật khẩu bảo vệ và chọn “high security” cho trình duyệt khi sử dụng.
- Thuê bao của BkavCA được yêu cầu lưu trữ khóa bí mật dưới dạng mã hóa sử dụng USB Token và mật khẩu bảo vệ.

8.7.3 Các vấn đề khác của dữ liệu kích hoạt

8.7.3.1 Truyền, gửi dữ liệu kích hoạt

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

8.7.3.2 Hủy bỏ dữ liệu kích hoạt

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

8.8 Kiểm soát an ninh máy tính

- Hệ thống Bkav Remote Signing được vận hành trên hệ thống đảm bảo an ninh theo các chính sách của Bkav Remote Signing 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 Remote Signing 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 Remote Signing 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 Remote Signing 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 Remote Signing. Các quản trị viên của Bkav Remote Signing chỉ truy nhập và quản trị hệ thống thông qua một số giới hạn các máy tính quản trị được xác định sẵn.
- Bkav Remote Signing 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 nhiệp 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

8.9 Giám sát an ninh hệ thống mạng

- Bkav Remote Signing 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 cân thiệp hoặc mối đe dọa nào từ bên ngoài
- Bkav Remote Signing chia hệ thống thành các Zones chức năng, logic và vung 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 Remote Signing áp dụng các biện pháp kiểm soát bảo mật giống nhau khi hệ thống nằm trong cùng zone
- Bkav Remote Signing giới hạn quyền truy cập và giao tiếp giữa các zone cần thiết để thực hiện các hoạt động liên quan. Mọi nỗ lự truy cập trái phép vào hệ thống đều được ghi lại
- Bkav Remote Signing cấm hoặc hủy kích hoạt các liên kết, dịch vụ không cần thiết
- Bkav Remote Signing thường xuyên xem xét thiết lập luật bảo vệ
- Bkav Remote Signing 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.

8.10 Kiểm soát an ninh quy trình sử dụng

8.10.1 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.

8.10.2 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 ISO 27001.

8.10.3 Giám sát an ninh vòng đời

- BkavCA 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 BkavCA.

8.11 Đồng bộ thời gian.

- Để đảm bảo độ chính xác của các sự kiện, Bkav Remote Signing sử dụng nguồn thơi gian được đồng bộ hóa với nguồn thời gian chuẩn
- Để kiểm tra thời hạn hiệu lực của chứng thư số, Bkav Remote Signing sử dụng nguồn thời gain đồng bộ hóa với UTC
- Việc đồng bộ với UTC với nguồn thời gian được tự động hóa, dựa vào giao thức NTP có độ chính xác lên đến …

9. 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)

9.1 Định dạng 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. 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

9.1.1 Phiên bản

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

9.1.2 Trường mở rộng

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

9.1.2.1 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

9.1.2.2 Certificate policies

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

9.1.2.3 Subject Alternative Name

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

9.1.2.4 Basic Constraints

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

9.1.2.5 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

9.1.2.6 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.

9.1.2.7 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 BkiCA do Root CA ban hành.

9.1.2.8 Subject Key Identifier

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

9.1.3 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.

9.1.4 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 Organiztional Unit.

9.1.5 Ràng buộc tên

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

9.1.6 Định danh chính sách và quy chế chứng thư số

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

9.1.7 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.

9.1.8 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.

9.1.9 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.

9.2 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
Signture 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.

9.2.1 Phiên bản

- BkavCA ban hành X.509 Version 2 CRL.

9.2.2 CRL và các trường mở rộng của CRL

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

9.3 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.

9.3.1 Phiên bản

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

9.3.2 Phần mở rộng OCSP

- Không quy định.

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

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

10.1 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.

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

10.3 Các nội dung kiểm tra kỹ thuật

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

10.4 Xử lý khi phát hiện sai sót

- Sau khi có báo cáo kiểm toán kỹ thuật, Bkav Remote Signing sẽ làm việc với RootCA về những nội dung chưa phù hợp.
- Bkav Remote Signing 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 Remote Signing sẽ bị ngừng trong các tình huống sau:
  - Báo cáo kiểm toán kỹ thuật cho thấy có lỗi nghiêm trọng có thể ảnh hưởng ngay lập tức tới an an ninh của hệ thống Bkav Remote Signing.
  - Bkav Remote Signing thực hiện kế hoạch xử lý nhưng không có kết quả.

10.5 Công bố kết quả kiểm tra kỹ thuật

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

11. Các nội dung nghiệp vụ và pháp lý khác

11.1 Phí/Giá

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

11.2 Trách nhiệm tài chính

- Bkav duy trì một mức mức bảo hiểm hợp lý cho các lỗi Bkav Remote Signing.
- 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 Remote Signing trong trường hợp bị thu hồi giấy phép.

11.3 Bảo mật thông tin nghiệp vụ

11.3.1 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 Bkav Remote Signing.
  - Báo cáo kiểm tra Bkav Remote Signing.
  - 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 Remote Signing Remote Signing: phần cứng, phần mềm và quản trị của dịch vụ của Bkav Remote Signing.

11.3.2 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.

11.3.3 Trách nhiệm bảo vệ các thông tin bí mật

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

11.4 Bảo mật thông tin cá nhân

11.4.1 Kế hoạch bảo mật thông tin cá nhân

- Chính sách bảo mật được Bkav công bố tại https://remotesigning.bkavca.vn/thoa-thuan-su-dung.

11.4.2 Phạm vi các thông tin bí mật

- Ngoài những thông tin được nêu tại mục 8.3..2 được coi là bí mật.

11.4.3 Những thông tin ngoài phạm vi thông tin bí mật

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

11.4.4 Trách nhiệm bảo vệ các thông tin bí mật

- Bkav Remote Signing 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.

11.4.5 Thông báo và sự đồng thuận sử dụng thông tin mật

- Thông tin bí mật sẽ không được sử dụng mà không có sự cho phép của người sở hữu thông tin hoặc đại điện sở hữu thông tin đó, trừ những trường hợp được quy định trong quy chế này hoặc trong thỏa thuận sử dụng tại https://bkavca.vn/thoa-thuan-su-dung.

11.4.6 Cung cấp thông tin theo yêu cầu của cơ quan pháp luật

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

11.4.7 Các tình huống cung cấp thông tin khác

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

11.5 Quyền sở hữu trí tuệ

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

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

11.5.2 Quyền sở hữu quy chế chứng thực

- Bkav Remote Signing giữ mọi quyền sở hữu trí tuệ quy chế chứng thực này.

11.5.3 Quyền sở hữu tên

- Đối tượng đăng ký chứng thư số phải có quyền sở hữu về nhãn hiệu đăng ký, nhãn hiệu dịch vụ, hoặc tên tổ chức (danh nghiệp) trong đơn xin cấp chứng thư số và tên đặc trưng trong chứng thư số.

11.5.4 Quyền sở hữu khóa

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

11.6 Tuyên bố và cam kết

11.6.1 Tuyên bố và cam kết của Bkav Remote Signing

- Bkav Remote Signing đảm bảo rằng:
  - Không thay đổi thông tin đăng ký chứng thư số được cung cấp bởi đối tượng đăng ký.
  - Chứng thư số do Bkav Remote Signing 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.
  - Đảm bảo an toàn khóa bí mật của thuê bao
  - Đảm bảo mối liên kết giữa thuê bao với khóa ký, liên kết thuê bao với Chứng thư số, liên kết Chứng thư số với với khóa ký
  - Thời điểm ký chứng thư số còn hiệu lực (không hết hạn, không thu hồi…)
- Chịu trách nhiệm về việc quản lý và xác minh các điều kiện hoạt động của RA theo quy định của pháp luật.

11.6.2 Tuyên bố và cam kết của RA

- RA đảm bảo rằng:
  - Không thay đổi thông tin đăng ký chứng thư số được cung cấp bởi đối tượng đăng ký.
  - Tuân thủ theo quy trình quản lý vòng đời chứng thư số của Bkav Remote Signing.
- 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 Remote Signing đã nhận đầy đủ hồ sơ của thuê bao, và thông tin thuê bao được thẩm định.
- Cam kết của RA với Bkav Remote Signing 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.

11.6.3 Tuyên bố và cam kết của thuê bao

- Khi ký: sử dụng đúng thông tin tài khoản tương ứng với khóa công khai trong chứng thư số.
- Tại thời điểm ký :
  - Không cung cấp thông tin thuê bao, tài khoản 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.

11.6.4 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 Remote Signing 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.

11.6.5 Tuyên bố và cam kết của các đối tượng khác

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

11.7 Từ chối trách nhiệm

- Bkav Remote Signing không quy định cụ thể về việc từ chối trách nhiệm.

11.8 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 Remote Signing. Trong mọi trường hợp, khoản tiền mà Bkav Remote Signing 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 Tổ chức	20.000 USD

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

11.9 Bồi thường thiệt hại

11.9.1 Bồi thường của thuê bao

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

11.9.2 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 Remote Signing 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 Remote Signing
- Thỏa thuận người nhận tương ứng có thêm các điều khoản bồi thường khác.

11.10 Hiệu lực của Quy chế chứng thực

11.10.1 Thời hạn bắt đầu có hiệu lực

- Quy chế chứng thư số này có hiệu lực khi được công bố trên trang https://remotesigning.bkavca.vn. Các sự bổ sung cho quy chế chứng thư số này có hiệu lực khi được công bố.

11.10.2 Thời hạn hết hiệu lực

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

11.10.3 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.

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

- Trừ khi được quy định rõ ràng, các thành viên Bkav Remote Signing 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.

11.12 Bổ sung và sửa đổi

11.12.1 Thủ tục bổ sung

- Quy chế này được bổ sung, sửa đổi bởi Bkav Remote Signing PMA. Nội dung sửa đổi được lưu tại https://remotesigning.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.

11.12.2 Cơ chế và thời hạn thông báo

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

11.12.2.1 Kỳ hạn góp ý

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

11.12.2.2 Cơ chế quản lý góp ý

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

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

- Định danh quy chế chứng thực được thay đổi theo yêu cầu của Bkav Remote Signing PMA.

11.13 Thủ tục giải quyết tranh chấp

11.13.1 Tranh chấp giữa Bkav Remote Signing với RA

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

11.14 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.

11.15 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.

11.16 Các điều khoản chung

11.16.1 Thỏa thuận bao trùm mọi thành viên

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

11.16.2 Sự chuyển nhượng

- Bkav Remote Signing không quy định các trường hợp chuyển nhượng khác.

11.16.3 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

11.16.4 Sự ép buộc

- Không có sự ép buộc nào đưa đến việc ban hành chứng thư của Bkav Remote Signing.

11.16.5 Trường hợp bất khả kháng

- Thỏa Thực hiện theo thoả thuận sử dụng Chữ ký số tại https://bkavca.vn/thoa-thuan-su-dung.

12. Phụ lục

12.1 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 Remote Signing	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 Remote Signing 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 Remote Signing.
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 Remote Signing, chính sách hoàn phí đi kèm trong thỏa thuận thuê bao.
8.	Chủ thể chứng thư số	Chủ sở hữu của chứng thư số, chủ thể chứng thư số có thể là thuê bao chứng thư số hoặc các thiết bị như máy chủ Web.
9.	CN	Common Name – một thuột tính trong trường DN của chứng thư số, CN biểu diễn tên thường

		gọi của đối tượng là chủ thể của chứng thư số.
10.	CRL	Danh sách chứng thư số thu hồi.
11.	DN	Distinguished Names – một trường trong chứng thư số, DN chưa thông tin nhận dạng đối tượng là chủ thể chứng thư số.
12.	ISO/IEC 15408-3:1999	Tiêu chuẩn đánh giá an ninh hệ thống phần mềm.
13.	ITU-T X.509	Tiêu chuẩn về chứng thư số và danh sách thu hồi chứng thư số do tổ chức viễn thông quốc tế quy định.
14.	Khóa bí mật	Thành phần bí mật của cặp khóa được sử dụng trong hạ tầng khóa công khai (PKI – Public Key Infrastructure).
15.	Khóa công khai	Thành phần công khai của cặp khóa được sử dụng trong hạn tầng khóa công khai.
16.	Người nhận	Là đối tượng tin tưởng chứng thư số hay một chữ ký số được cung cấp bởi CA.
17.	RA	Registration Authority – Nhà thẩm quyền có chức năng giúp đỡ CA duyệt đơn đăng ký chứng thư số, đơn gia hạn chứng thư số, đơn thu hồi chứng thư số và quản lý thông tin thuê bao.
18.	Root CA	CA có chứng thư số được ký bởi chính khóa bí mật của CA. Root CA công cộng của Việt Nam được quản lý bởi Trung Tâm Chứng Thực Chữ Ký Số Quốc Gia – Bộ Thông Tin và Truyền Thông.
19.	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 udngj 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 chữu 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 chử 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	Nhà cung cấp dịch vụ vụ máy chủ/ ứng dụng ký

	Application Service Provider (SSASP)	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 dụng
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