CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

ĐỘC LẬP – TỰ DO – HẠNH PHÚC

TỔ CHỨC CUNG CẤP DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG CA2 (CA2)

QUY CHẾ CHỨNG THỰC CHỮ KÝ SỐ CA2

Phiên bản v1.2

CÔNG TY CỔ PHẦN CÔNG NGHỆ THẺ NACENCOMM

Hà nội, ngày tháng năm 2015

Sử dụng tài liệu:

Bản quy chế và chính sách chứng thực chữ ký số này được cung cấp cho các bên sử dụng dịch vụ của CA2, trên trang thông tin điện tử của CA2 hoặc bản in trên giấy. Xem và phân phối tài liệu không bị giới hạn. Sử dụng lại nội dung trong tài liệu phải được sự đồng ý bằng văn bản của CA2.

Bản quyền

Tóm tắt

Tài liệu cung cấp nội dung chính sách và quy chế chứng thực chữ ký số của CA2 tuân theo quy định của Thông tư ban hành "Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số" của Bộ Thông tin - Truyền thông và Khung RFC 3647.

Hướng dẫn chi tiết quy chế thực hiện chính sách cấp phát chứng thư số đối với CA2, và quy trình đăng ký, sử dụng chứng thư số của thuê bao và bên nhận.

CA2 khuyến nghị thuê bao, người nhận sử dụng dịch vụ có hiểu biết về khóa công khai, chứng thư số và chữ ký số, các quyền, nghĩa vụ và trách nhiệm của CA2, thuê bao CA2 và các bên tham gia trước khi đăng ký và sử dụng dịch vụ.

Trước khi thuê bao có thể gửi chứng thư số cho người khác, thuê bao phải chấp nhận chứng thư số và chịu các trách nhiệm liên quan.

Bên chấp nhận chứng thư số của thuê bao chịu trách nhiệm cho quyết định về việc chấp nhận hay không chấp nhận chứng thư số do CA2 cấp. CA2 khuyến cáo bên nhận kiểm tra tính hợp lệ của chứng thư số và thông tin cung cấp trong chứng thư số, bằng cách kiểm tra với hệ thống xác thực trạng thái trực tuyến chứng thư số của thuê bao do CA2 cấp, trước khi chấp nhận chữ ký số.

Các quy định của tài liệu này có thể được sửa đổi theo thời gian vào ngày hoặc sau ngày có hiệu lực của văn bản.

1. GIỚI THIỆU

1.1. Tổng quan

- Tài liệu cung cấp nội dung chính sách và quy chế chứng thực chữ ký số của CA2 tuân theo quy định của Thông tư ban hành "Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số" của Bộ Thông tin - Truyền thông và Khung RFC 3647.
- Không phải tất cả các phần của RFC 3647 được sử dụng .
- CA2 cung cấp dịch vụ chứng thực chữ ký số cho các tổ chức, doanh nghiệp và cá nhân để thực hiện giao dịch trong môi trường mạng mở an toàn và có giá trị pháp lý theo quy định của pháp luật Việt Nam trong việc sử dụng chữ ký số phục vụ chống chối bỏ, xác thực và toàn vẹn các tài liệu và giao dịch điện tử.
- Tài liệu này mô tả tập hợp các quy định và thủ tục cấp phát và quản lý chứng thư số đối với hệ thống CA2 và thủ tục quy định đăng ký, sử dụng chứng thư số đối với thuê bao của CA2 và bên nhận. Tài liệu quy định các thủ tục cấp, quản lý, tạm dừng, thu hồi và gia hạn chứng thư số trong dịch vụ chứng thực chữ ký số công cộng CA2. Là tài liệu pháp lý ràng buộc tất cả các bên tham gia sử dụng và xác nhận chứng thư số CA2; điều chỉnh quyền, nghĩa vụ và trách nhiệm các bên trong tài liệu này.

KIẾN TRÚC CA2

Hạ tầng hệ thống CA2

CA2 cung cấp dịch vụ chứng thực chữ ký số cho các tổ chức, doanh nghiệp và cá nhân để tiến hành giao dịch trong môi trường điện tử an toàn và có giá trị pháp lý theo quy định của pháp luật Việt Nam. Để đạt được mục tiêu này, các khía cạnh quan trọng sau được thực hiện đầy đủ:

- Triển khai một mô hình PKI tin cậy cao để tạo thuận lợi cho việc quản lý, kiểm soát, phát hành, tạm dừng, thu hồi, gia hạn đối với chứng thực chữ ký số;
- Đảm bảo hiệu quả cao trong việc sử dụng chữ ký số phục vụ chống chối bỏ, xác thực và toàn vẹn các tài liệu và giao dịch điện tử;
- Sự thống nhất về dịch vụ và tiêu chuẩn trên toàn hệ thống CA2 và các RA, đại lý CA2.

Mô hình tổng quan kiến trúc PKI tin cậy cao của CA2 được thể hiện một cách đơn giản hóa như sau:

Mức 5: Hệ thống chứng thực chữ ký số Quốc gia MIC National Root CA

Mức 4: Hệ thống cấp và quản lý chứng thư số CA2 Offline CA

Mức 3: Hệ thống dịch vụ trực tuyến cơ sở dữ liệu về chứng thư số CA2

Mức 2: Hệ thống đại lý phân phối và hỗ trợ dịch vụ CA2

Mức 1: Thuê bao dịch vụ CA2

Mức 0: Bên nhận

Trong mô hình này, mức 4 là điểm yếu nhất về tính tin tưởng của hạ tầng CA2. Vì vậy CA2 lựa chọn triển khai mô hình Offline CA, cách ly hoàn toàn hệ thống cấp chứng thư số. Và để đảm bảo an ninh và tính tin tưởng, Offline CA công nghệ Microsoft được trang bị khối bảo mật phần cứng HSM chuyên dụng có chứng nhận đạt tiêu chuẩn FIPS 140-2 Level 3, cùng với quy trình an ninh cấp và xác thực chứng thư số đồng bộ, giám sát nhiều lớp.

Mức 3 trong mô hình cũng được trang bị khối bảo mật phần cứng HSM chuyên dụng với tiêu chuẩn và quy trình tương tự như Offline CA.

Mức 2 tham gia thẩm định và xác thực thuê bao theo nhiều lớp, khâu thẩm định cuối cùng phải được kiểm tra chéo hồ sơ thuê bao với thông tin thuê bao được công bố trên cổng thông tin của Tổng Cục thuế và Bộ Kế hoạch và Đầu tư đối với tổ chức, doanh nghiệp, và chứng minh thư nhân dân đối với cá nhân.

Mức 1 thuê bao dịch vụ CA2 được trang bị PKI Smartcard, PKI Token, PKI Virtual Token theo tiêu chuẩn FIPS 140-2 Level 2 để đảm bảo tính chống chối bỏ, xác thực và toàn vẹn các tài liệu và giao dịch ký chữ ký số bởi thuê bao.

Mức 0 bên nhận chữ ký số, bên nhận được cung cấp hệ thống các kênh xác thực để đảm bảo việc kiểm tra chữ ký số được đáp ứng 24/7.

Cơ quan quản lý Nhà nước

Bộ Thông tin và Truyền thông

Hệ thống dịch vụ của CA2

Hệ thống cấp và quản lý chứng thư số Offline CA

- Hệ thống Offline CA cách ly với hệ thống mạng nội bộ và mạng Internet, cho cấp phát và quản lý chứng thư số.
- Hạ tầng kỹ thuật công nghệ bảo mật và xác thực tin cậy, với hệ thống quy trình nghiệp vụ chặt chẽ và rõ ràng giúp dễ dàng cho việc quản lý, kiểm soát, cấp, gia hạn, tạm dừng, phục hồi và thu hồi chứng thư số của thuê bao đảm bảo tin cậy.

Chứng thư số

- Chứng thư số dành cho tổ chức doanh nghiệp VID Stamp
- Chứng thư số dành cho cá nhân VID Sign
- Chứng thư số dành cho dịch vụ web VID Web

Dịch vụ trực tuyến

- Hệ thống thông tin và danh bạ điện tử trực tuyến CA2
- Hệ thống đăng ký dịch vụ CA2
- Hệ thống xác thực trực tuyến trạng thái chứng thư số CA2

1.2. Tên tài liệu và nhận dạng

- Tên tài liệu: Quy chế chứng thực chữ ký số CA2
- Phiên bản: v1.2
- Ngày tạo: 18/11/2014
- OID: Không áp dụng

1.3. Các bên tham gia

Các bên tham gia vào hạ tầng khóa công khai CA2 (Publick Key Infrastructure - PKI) bao gồm:

- Trung tâm Chứng thực điện tử quốc gia MIC National RootCA
- Tổ chức chứng thực chữ ký số công cộng CA2
- RA, đại lý CA2
- Thuê bao chứng thư số CA2
- Bên nhận

1.3.1. Trung tâm Chứng thực điện tử quốc gia MIC National RootCA

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

Cấp chứng thư số cho các hệ thống chứng thực chữ ký số công cộng theo giấy phép của Bộ Thông tin và Truyền thông.

Thiết lập các thông số kỹ thuật để vận hành cơ sở hạ tầng khóa công khai cho xác thực chữ ký số công cộng.

Kiểm tra kỹ thuật, điều phối các hoạt động xử lý sự cố liên quan đến dịch vụ chứng thực chữ ký số công cộng.

Thu thập, tổ chức, phân tích, thống kê và tổng hợp số liệu về dịch vụ chứng thực chữ ký số công cộng.

1.3.2. Tổ chức chứng thực chữ ký số công cộng CA2

CA2 là tổ chức chứng thực chữ ký số công cộng được MIC National RootCA cấp chứng thư số theo giấy phép của Bộ Thông tin và Truyền thông.

CA2 cung cấp dịch vụ chứng thực chữ ký số công cộng cho các tổ chức, doanh nghiệp và cá nhân để thực hiện giao dịch trong môi trường mạng mở an toàn và có giá trị pháp lý theo quy định của pháp luật Việt Nam.

CA2 xây dựng một mô hình PKI có mức độ tin cậy cao trong việc sử dụng chữ ký số phục vụ chống chối bỏ, xác thực và toàn vẹn các dữ liệu và giao dịch điện tử.

Dịch vụ chứng thực chữ ký số công cộng CA2 vận hành tuân thủ theo Qui chế Chứng thư số CA2, bao gồm:

- Tạo cặp khóa mật mã bao gồm khóa công khai và khóa bí mật CA2;
- Cấp, gia hạn, tạm dừng, phục hồi và thu hồi chứng thư số của thuê bao CA2 theo quy định của pháp luật;
- Duy trì trực tuyến cơ sở dữ liệu về trạng thái của toàn bộ chứng thư số CA2 đảm bảo đảm bảo các bên tham gia truy xuất 24 giờ / ngày, 7 ngày / tuần;
- Những dịch vụ khác có liên quan theo quy định.

1.3.3. RA, đại lý CA2

RA, đại lý CA2 là đơn vị ký với CA2 một hợp đồng ủy quyền tham gia thẩm định đăng ký và cung cấp dịch vụ chứng thực chữ ký số theo quy định của pháp luật. Quyền và nghĩa vụ của hai bên được quy định trong hợp đồng hợp tác giữa hai bên.

1.3.4. Thuê bao chứng thư số CA2

Là các tổ chức, cá nhân, doanh nghiệp sử dụng dịch vụ chứng thực chữ ký số công cộng CA2. Quyền và nghĩa vụ của hai bên được quy định trong hợp đồng cung cấp dịch vụ giữa hai bên.

1.3.5. Bên nhận

Là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký là thuê bao CA2, sử dụng chứng thư số CA2 của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.

1.4. Sử dụng Chứng thư số CA2

1.4.1. Phạm vi sử dụng

Chứng thư số CA2 chỉ được sử dụng theo đúng phạm vi quy định trong hợp đồng giữa CA2 và thuê bao.

1.4.2. Cấm sử dụng

Nghiêm cấm việc sử dụng chứng thư số CA2 trái với quy định trong hợp đồng giữa CA2 và thuê bao và trái với quy định của pháp luật.

1.5. Quản trị Quy chế chứng thực chữ ký số CA2

1.5.1. Tổ chức

- **Công ty Cổ phần công nghệ thẻ Nacencomm**
- Trung tâm chứng thư số công cộng CA2
- Địa chỉ: Số 2 Chùa Bộc, Đống Đa, HN
- Website: www.cavn.vn

1.5.2. Người liên hệ

- Điện thoại: (84-4) 3576 5146
- Đường dây nóng: 1900 54 54 07
- Email: support@cavn.vn
- Địa chỉ: Số 2 Chùa Bộc, Đống Đa, HN
- Website: www.cavn.vn

1.5.3. Người quyết định sự phù hợp của Quy chế chứng thực chữ ký số CA2

- Ông **Hoàng Quốc Khánh**
- Mobile: 0913.234.134
- Email: khanh@cavn.vn

1.5.4. Các thủ tục phê chuẩn Quy chế chứng thực chữ ký số CA2

- CA2 quy định cụ thể về việc cập nhật, sửa đổi và ban hành Quy chế chứng thực chữ ký số CA2.

1.6. Định nghĩa và viết tắt

1.6.1. Thuật ngữ, khái niệm

Các khái niệm, thuật ngữ được sử dụng trong Quy chế chứng thực chữ ký số CA2 được giải thích như dưới đây:

Chứng thư số: Hay còn gọi là chứng thư khóa công khai, là một dạng chứng thư điện tử do Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng CA2 cấp cho một khóa công khai bằng cách, ràng buộc khóa công khai của thuê bao với các thông tin định danh của thuê bao có khóa riêng là một cặp với khóa công khai này.

Chữ ký số: Là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng theo đó người có được thông điệp dữ liệu ban đầu và khoá công khai của người ký có thể xác định được chính xác:

a) Việc biến đổi nêu trên được tạo ra bằng đúng khoá bí mật tương ứng với khoá công khai trong cùng một cặp khóa;

b) Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.

Bên ký: Là thuê bao CA2 dùng khoá bí mật của mình để ký số vào một thông điệp dữ liệu dưới tên của mình.

Bên nhận: Là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng chứng thư số của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.

Thuê bao: Là tổ chức, cá nhân được CA2 cấp chứng thư số, chấp nhận chứng thư số và giữ khoá bí mật tương ứng với khoá công khai ghi trên chứng thư số được cấp đó.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số: Là tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử thực hiện hoạt động cung cấp dịch vụ chứng thực chữ ký số.

Khóa riêng CA tạo chữ ký: Khóa riêng cùng cặp với khoá công khai nằm trong chứng thực CA2 và được sử dụng để ký số.

Danh sách thu hồi chứng thư số (Certificate Revocation List - CRL): Một cơ sở dữ liệu hoặc một danh sách các chứng thư số do CA2 thu hồi hay hủy bỏ trước thời hạn so với thời hạn hiệu lực của chứng thư số.

Tạo khóa (Key Generation): là quá trình tạo một cặp khóa phi đối xứng bao gồm khóa riêng và khóa công khai

Cặp khóa (Key Pair): Hai khóa liên kết với nhau một cách chính xác (một khóa riêng và tương ứng với nó là một khóa công khai), có đặc điểm là: (i) một khóa có thể được sử dụng để mã hóa các thông tin và chỉ có thể được giải mã bằng chiếc khóa cùng cặp còn lại; (ii) Nếu biết một khóa cũng không thể có khả năng biết được một khóa còn lại.

Kiểm tra trạng thái trực tuyến (Online Certificate Status Protocol): trạng thái thời gian thực được kiểm tra trực tuyến về thời hạn hiệu lực của chứng thư số. Kiểm tra trạng thái trực tuyến liên quan tới một CRL bao gồm việc kiểm tra CRL công bố mới nhất.

Khóa riêng (Private Key): Một khóa bí mật của người giữ chứng thư số, được sử dụng để ký chữ ký số và giải mã thông tin hoặc tài liệu được mã hóa bởi khóa công khai tương ứng.

Khóa công khai (Public Key): Một khoá công khai thuộc sở hữu của người giữ khoá riêng cùng cặp với khoá công khai này. Khoá công khai được phát tán để người nhận xác thực người "ký" điện tử (người giữ khoá bí mật cùng cặp với khoá công khai này) và người gửi sử dụng khoá công khai này để mã hoá dữ liệu trước khi gửi đi, chỉ có người nhận giữ khoá bí mật cùng cặp với khoá công khai này mới giải mã được.

Cơ sở hạ tầng khóa công khai (Public Key Infrastructure - PKI): Tập hợp các kiến trúc, tổ chức, kỹ thuật, nguyên tắc thực hiện, thủ tục để hỗ trợ trong việc thực hiện và điều hành chứng thư số dựa trên hệ thống mã hóa khóa công khai.

Tổ chức đăng ký (Registration Authority – RA): là một tổ chức được CA2 ký hợp đồng đại điện có quyền tiếp nhận và giải quyết các đơn xin cấp chứng thư số và xác minh nhận dạng các chủ thể cuối cùng cũng như chứng thực các thông tin có trong đơn xin chứng thư số tuân theo những điều khoản theo Quy chế này và các thỏa thuận có liên quan.

Danh bạ chứng thư số (Repository): Hệ thống trực tuyến do CA2 phát hành duy trì để lưu trữ và phục hồi các chứng thư số hoặc các thông tin liên quan tới thuê bao chứng thư số, bao gồm các thông tin về thời hạn hiệu lực và sự thu hồi chứng thư số.

Tạm dừng chứng thư số: Là làm mất hiệu lực của chứng thư số một cách tạm thời từ một thời điểm xác định.

Thu hồi chứng thư số: Là làm mất hiệu lực của chứng thư số một cách vĩnh viễn từ một thời điểm xác định.

1.6.2. Từ viết tắt

CA	Certification Authority Tổ chức cấp chứng thư số

CRL	Certificate Revocation List Danh sách chứng thư số bị thu hồi
HTTPS	Hypertext Transfer Protocol with SSL Giao thức web với bảo mật đường truyền SSL
PIN	Personal Identification Number Mã số cá nhân
PKCS	Public Key Cryptography Standard Chuẩn khoá công khai
PKI	Public Key Infrastructure Hạ tầng kỹ thuật mã hóa công khai
LDAP	Lightweight Directory Access Protocol Giao thức truy cập danh bạ chứng thư số
RA	Registration Authority Đại lý đăng ký thẩm định thuê bao
SSL	Secure Socket Layer Giao thức bảo mật giao dịch trên Internet
X.509	ITU-T standard for Certificates format Chuẩn về định dạng chứng thư số
CA2 Offline	Máy chủ cấp và quản lý chứng thư số, hoạt động tách biệt hoàn toàn với hệ thống mạng internet, mạng LAN nghiệp vụ.
CA2 Offline Station	Máy trạm gửi yêu cầu và xác nhận chứng thư số được cấp, được kết nối duy nhất và trực tiếp với máy chủ CA2 Offline
HSM	Hardware Security Module Khối bảo mật phần cứng (HSM), là thiết bị có mức bao mật cao nhất trong hạ tầng chứng thư số.
PKI Token PKI SmartCard PKI Virtual Token	Khối bảo mật đầu cuối quản lý khóa thuê bao tuân theo chuẩn FIPS 140-2 level 2 trở lên hoặc tương đương.
Smart card chuyên dụng	Bộ thẻ nghiệp vụ chuyên dụng dùng trong hệ thống thiết bị HSM chuẩn FIPS 140-2 Level3.

FIPS 140-2	Chuẩn đánh giá an ninh an toàn cho hệ thống mật mã theo 4 mức từ Level 1 đến Level 4
FIPS 140-2 Level 2	Yêu cầu an ninh an toàn mức 2 trong hệ thống 4 mức tiêu chuẩn FIPS 140-2.
FIPS 140-2 Level 3	Yêu cầu an ninh an toàn mức 3 trong hệ thống 4 mức tiêu chuẩn FIPS 140-2.
Cơ chế 2 x 3	Cơ chế xác thực, sao lưu, dự phòng và phục hồi sử dụng Smart Card chuyên dụng. Mỗi bộ gồm 3 thẻ do 3 người giữ, mỗi nhiệm vụ phải có 2 trong 3 người tham gia, người còn lại dự phòng cho 2 người kia.

2. TRÁCH NHIỆM CÔNG BỐ VÀ QUẢN LÝ DANH BẠ CHỨNG THƯ SỐ

2.1. Hệ thống danh bạ

Công bố sẽ thực hiện tại website CA2 http://www.cavn.vn và có phương án tốt nhất để thông báo thành công đến các bên liên quan đảm bảo yêu cầu về an toàn và bảo mật.

2.2. Công bố thông tin của CA2

CA2 sẽ thực hiện công bố công khai và quản lý hệ thống danh bạ về chứng thư số của thuê bao ngay sau khi hoàn thành thủ tục cấp chứng thư số cho thuê bao. Hệ thống danh bạ chứng thư số CA2 bao gồm:

1) Chứng thư số của MIC National Root CA;
2) Chứng thư số của CA2;
3) Chứng thư số của thuê bao;
4) Danh sách chứng thư số thu hồi (CRL);
5) Quy chế chứng thực chữ ký số CA2;
6) Các thông tin liên quan khác.

2.3. Tần suất công bố

1) CA2 thực hiện công bố bản Quy chế chứng thực chữ ký số CA2 mới hoặc sửa đổi ngay sau khi được phê duyệt.
2) CA2 có trách nhiệm duy trì 24 giờ trong ngày và 7 ngày trong tuần trên trang tin điện tử của mình những thông tin sau:
   a. Quy chế chứng thực chữ ký số CA2;
   b. Danh sách chứng thư số có hiệu lực, bị tạm dừng, bị thu hồi của thuê bao;
   c. Những thông tin cần thiết khác.
3) Thời gian cập nhật cơ sở dữ liệu danh bạ chứng thư số:
   - Trong vòng 08 giờ làm việc kể từ thời điểm hoàn thành thủ tục cấp đối với chứng thư số mới cấp;
   - Ngay sau khi hoàn thành công việc tạm dừng, thu hồi chứng thư số hoặc thay đổi cặp khoá.

2.4. Kiểm soát truy cập

CA2 sẽ không áp đặt bất kỳ sự kiểm soát truy cập nào đối với: (1) Quy chế chứng thực chữ ký số CA2; (2) Chứng thư số CA2; (3) Danh sách chứng thư số thu hồi CRL.

CA2 có thể áp đặt kiểm soát truy cập vào chứng thư số của thuê bao CA2 và thông tin về tình trạng chứng thư số, tuân theo các điều khoản của chính sách này.

3. ĐỊNH DANH VÀ THẨM ĐỊNH XÁC THỰC THÔNG TIN THUÊ BAO

3.1 Đặt tên thuê bao trong chứng thư số CA2

3.1.1. Phân loại

Chứng thư số CA2 được phân loại như sau:

- VID Stamp: Chứng thư số tổ chức
- VID Sign: Chứng thư số cá nhân
- VID Web: Chứng thư số tên miền website

3.1.2. Quy định đặt tên

- VID Stamp: Đặt tên theo quyết định thành lập hoặc giấy đăng ký kinh doanh hoặc tài liệu tương đương khác của tổ chức.
- VID Sign: Đặt tên theo Chứng minh nhân dân, hộ chiếu hoặc chứng thực cá nhân hợp pháp.
- VID Web: Đặt tên theo tên miền website đăng ký hợp lệ của đơn vị đăng ký sử dụng dịch vụ CA2.

3.1.3. Nặc danh, tên giả

CA2 không đặt tên khác với quy định tại điều 3.1.2.

3.1.4. Tính duy nhất của tên

- VID Stamp: Bao gồm tên tổ chức và trường mã số thuế hoặc mã số tổ chức hợp lệ
- VID Sign: Bao gồm tên cá nhân và trường số chứng minh nhân dân, hoặc số hộ chiếu, hoặc số chứng thực cá nhân hợp pháp.
- VID Web: Tên miền hợp lệ.

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

3.2.1. Phương pháp chứng minh sở hữu khóa riêng

Thuê bao phải chứng minh được thuê bao thực sự sở hữu khóa riêng tương ứng với khóa công khai được đề nghị cấp chứng thư số.

Các phương pháp chứng minh thuê bao thực sự sở hữu khóa riêng:

- Tệp tin đề nghị cấp chứng thư số mã hóa theo chuẩn PKCS #10 sinh từ PKI Smartcard, PKI Token, PKI Virtual Token đạt chuẩn FIPS 140-2 Level 2 trở lên, hoặc tương đương do thuê bao thực hiện;

- Hoặc thuê bao ủy quyền cho CA2, CA2 sinh khóa theo ủy quyền của thuê bao sử dụng PKI Smartcard, PKI Token, PKI Virtual Token đạt chuẩn FIPS 140-2 Level 2 trở lên. Theo quy trình, CA2 đảm bảo quyền sở hữu khóa riêng của thuê bao và bàn giao an toàn tránh các rủi ro trong quá trình giao nhận.

3.2.2. Thẩm định xác thực thông tin tổ chức

Hồ sơ đề nghị cấp chứng thư số của tổ chức có thể được thực hiện qua phương thức điện tử.

CA2 sẽ thực hiện tối thiểu các bước thẩm định bao gồm: Thẩm định hồ sơ đáp ứng theo yêu cầu của pháp luật; Xác thực chéo với cổng thông tin điện tử của cơ quan quản lý Nhà nước; Xác nhận qua điện thoại hoặc email

Với đề nghị là tên miền website, ngoài những bước thẩm định trên CA2 sẽ thực hiện xác thực quyền sở hữu sử dụng tên miền của tổ chức đề nghị.

Các thông tin cần có đối với tổ chức đề nghị cấp chứng thư số như sau:

- Tên tổ chức
- Mã số thuế/Mã số tổ chức hợp lệ
- Địa chỉ theo Giấy phép đăng ký kinh doanh
- Email hợp lệ
- Số điện thoại hợp lệ
- Ngành nghề: bản sao có công chứng của giấy phép thành lập/giấy phép ĐKKD và giấy chứng nhận MST (với tổ chức có số ĐKKD khác MST)
- Thông tin về website, tên miền của tổ chức (sử dụng cho chứng thư SSL)
- Thông tin về người đại diện pháp luật của tổ chức

3.2.3. Thẩm định xác thực đối với cá nhân đại diện cho tổ chức

Hồ sơ đề nghị cấp chứng thư số của cá nhân đại diện cho tổ chức có thể được thực hiện qua phương thức điện tử.

CA2 sẽ thực hiện tối thiểu các bước thẩm định bao gồm: Thẩm định hồ sơ đáp ứng theo yêu cầu của pháp luật; Xác thực chéo với cổng thông tin điện tử của cơ quan quản lý Nhà Nước; Xác nhận qua điện thoại hoặc email.

Các thông tin cần có đối với cá nhân đại diện cho tổ chức đề nghị cấp chứng thư số như sau:

- Tên cá nhân
- Thuộc tổ chức
- Số CMND/Hộ chiếu/Số chứng thực cá nhân hợp lệ
- Địa chỉ theo CMND
- Số điện thoại hợp lệ
- Thư điện tử hợp lệ
- Văn bản của tổ chức đề nghị cấp chữ ký số cho người có thẩm quyền và chức danh;
- Bản sao có công chứng CMND/ Hộ chiếu
- Thông tin sở hữu tên miền (sử dụng cho chứng thư SSL)

3.2.4. Thẩm định và xác thực đối với cá nhân

Hồ sơ đề nghị cấp chứng thư số của cá nhân có thể được thực hiện qua phương thức điện tử.

CA2 sẽ thực hiện tối thiểu các bước thẩm định bao gồm: Thẩm định hồ sơ đáp ứng theo yêu cầu của pháp luật; Xác nhận qua điện thoại hoặc email.

Các thông tin cần có đối với cá nhân đề nghị cấp chứng thư số như sau:

- Tên cá nhân
- Số CMND/Hộ chiếu/Số chứng thực cá nhân hợp lệ
- Địa chỉ theo CMND
- Địa chỉ thường trú
- Số điện thoại hợp lệ
- Thư điện tử hợp lệ
- Bản sao hợp lệ giấy chứng minh nhân dân, hộ chiếu hoặc chứng thực cá nhân hợp pháp khác
- Thông tin sở hữu tên miền (sử dụng cho chứng thư SSL)

3.2.5. Xác thực với cơ quan quản lý Nhà Nước

CA2 sẽ thực hiện thẩm định chéo với cổng thông tin điện tử của Tổng Cục Thuế, Bộ Kế hoạch đầu tư, CMND của cơ quan Công an.

3.2.6. Tiêu chuẩn tích hợp

CA2 áp dụng theo danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số liên quan đến chuẩn kỹ thuật tích hợp.

3.3. Xác minh đề nghị thay đổi cặp khóa

Thuê bao phải có đơn xin thay đổi cặp khóa.

CA2 sẽ thực hiện thẩm định trực tiếp với thuê bao, hồ sơ thuê bao và phía yêu cầu thay đổi để đảm bảo đúng đối tượng và gắn trách nhiệm trước khi CA2 thực hiện thu hồi chứng thư số của thuê bao xin thay đổi cặp khóa.

3.3.1. Thực hiện thay đổi khóa

Quy trình thủ tục thay đổi cặp khóa được thực hiện tuân theo như các thủ tục cấp chứng thư số lần đầu Mục 3.2.

3.3.2. Thực hiện thay đổi khóa khi thuê bao đã bị thu hồi

Thuê bao đã bị thu hồi không thuộc diện xem xét thay đổi cặp khóa.

3.4. Xác minh đề nghị thu hồi

Trước khi thực hiện thu hồi một chứng thư số, CA2 tiến hành xác minh trực tiếp với thuê bao, hồ sơ thuê bao và phía yêu cầu thu hồi để đảm bảo đúng đối tượng và gắn trách nhiệm trước khi CA2 thực hiện chính thức thu hồi.

Việc thu hồi chỉ được thực hiện khi có xác nhận của thuê bao bằng văn bản.

4. CÁC YÊU CẦU TRONG HOẠT ĐỘNG CUNG CẤP DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG CA2

4.1. Đăng ký thuê bao CA2

4.1.1. Đối tượng đăng ký

Bất cứ cá nhân hay tổ chức nào đều có quyền đăng ký yêu cầu CA2 cung cấp dịch vụ.

4.1.2. Quy trình đăng ký

Thuê bao phải hoàn thành Đơn yêu cầu cấp Chứng thư số CA2 và cung cấp đầy đủ, chính xác thông tin theo mẫu của CA2.

Cung cấp hồ sơ theo yêu cầu của CA2 và tham gia quá trình thẩm định thông tin thuê bao.

Ký hợp đồng sử dụng dịch vụ giữa hai bên, thực hiện các quyền lợi và nghĩa vụ theo như hợp đồng ký kết.

4.2. Xử lý đăng ký thuê bao CA2

4.2.1. Thực hiện chức năng thẩm định

CA2 và RA, đại lý sẽ tổ chức thẩm định theo quy định tại Mục 3.2

4.2.2. Chấp thuận hoặc từ chối

CA2 hoặc RA, đại lý sẽ chấp thuận đăng ký đề nghị cấp chứng thư số thuê bao CA2, nếu việc thẩm định các thông tin như yêu cầu tại Mục 3.2 thành công, và thuê bao thanh toán theo quy định.

CA2 hoặc RA, đại lý sẽ từ chối nếu:

- Việc thẩm định không thể hoàn thành
- Thuê bao không hoàn thành hồ sơ theo như yêu cầu
- Thuê bao không thực hiện theo khung thời gian quy định
- Thuê bao không thanh toán theo quy định

4.2.3. Thời gian xử lý

Trong vòng 5 ngày làm việc CA2 sẽ trả lời về việc chấp nhận đơn yêu cầu cấp chứng thư số CA2 và việc cấp phát chứng thư số CA2. CA2 sẽ cố gắng phản hồi nhanh nhất đến tất cả các đơn yêu cầu cấp chứng thư số CA2.

4.3. Cấp chứng thư số cho thuê bao CA2

Sau khi hoàn thành quy trình đăng ký và thủ tục thẩm định thông tin trong hồ sơ là chính xác; khóa công khai trên chứng thư số sẽ được cấp là duy nhất và cùng cặp với khóa bí mật của tổ chức, cá nhân đăng ký đề nghị cấp chứng thư số, CA2 sẽ:

i. Cấp phát chứng thư số CA2 theo yêu cầu và nội dung theo Nghị định 26/2007 NĐ-CP;

ii. Thông báo cho thuê bao và nhận xác nhận của thuê bao về tính chính xác của thông tin thuê bao trên chứng thư số; và

iii. Thực hiện công bố, cung cấp cho thuê bao thông tin truy cập cơ sơ dữ liệu chứng thư số trực tuyến, cho phép thuê bao có thể tải về hoặc gửi cho thuê bao qua thư điện tử.

4.3.1. Quy trình cấp chứng thư số

- Tiếp nhận yêu cầu: Bộ phận thẩm định tiếp nhận đăng ký và yêu cầu cấp chứng thư số từ thuê bao, RA, đại lý. Xác nhận với khách hàng gói đăng ký, tình trạng bảo hiểm và thời gian đăng ký chứng thư số...

- Thẩm định: Bộ phận thẩm định tiến hành kiểm tra xác nhận thông tin hồ sơ theo quy định và chuyển yêu cầu cấp đến bộ phận cấp.

- Cấp chứng thư số: Bộ phận cấp chứng thư số tiến hành cấp, quản lý chứng thư số và cập nhật cơ sở dữ liệu ngay khi có phát sinh từ hệ thống.

- Thông báo: Bộ phận thẩm định thông báo với khách hàng. Khách hàng xác nhận thông tin chứng thư số đã được cấp theo biểu mẫu xác nhận CA2 ban hành.

- Bàn giao và công bố: Bộ phận thẩm định, bộ phận cấp tiến hành làm thủ tục bàn giao chứng thư số và công bố trên cavn.vn. Sau đó, lưu trữ chứng thư số và hồ sơ.

- Đối soát & thanh toán: Bộ phận đối soát đảm bảo việc phát sinh từ hệ thống được xác nhận bởi các cá nhân, các bộ phận nghiệp vụ có liên quan và chuyển qua bộ phận kế toán làm thủ tục thanh toán.

Chi tiết quy trình cấp chứng thư số:

+ Bước 1: Cán bộ cấp cắm thiết bị PKI Token CA2 của thuê bao vào trạm cấp Offline CA Station

+ Bước 2: Cán bộ cấp nhập thông tin thuê bao theo Hồ sơ đăng ký đã thẩm định

+ Bước 3: Cán bộ cấp kích hoạt PKI Token CA2 khởi tạo cặp khóa và gửi khóa công khai cùng thông tin yêu cầu cấp chứng thư số với thiết bị PKI Token CA2 của thuê bao đến máy chủ Offline CA

+ Bước 4: Cán bộ Security 1 cắm thẻ Smartcard chuyên dụng xác thực bước 1 kích hoạt Offline CA;

+ Bước 5: Cán bộ Security 2 cắm thẻ Smartcard chuyên dụng xác thực bước 2 chính thức kích hoạt Offline CA;

+ Bước 6: Cán bộ cấp thực hiện cấp chứng thư số khóa công khai cho cặp khóa của thuê bao do PKI Token CA2 khởi tạo;

+ Bước 7: Cán bộ Secirity rút thẻ Smartcard chuyên dụng khỏi hệ thống Offline CA;

+ Bước 8: Cán bộ cấp bàn giao PKI Token CA2 đã được cấp chứng thư số cho khóa công khai của thuê bao tới bộ phận hồ sơ làm thủ tục bàn giao và công bố chứng thư số;

+ Bước 9: Sau khi thực hiện xác nhận thành công với thuê bao, bộ phận công bố kết xuất chứng thư số khóa công khai từ thiết bị PKI Token CA2 của thuê bao và công bố chứng thư số theo quy định của CA2.

- Cuối ngày đối soát số Serial phát sinh và yêu cầu cấp CTS từ khách hàng.

4.3.2. Thông báo cho thuê bao

Thông báo cho thuê bao và ký nhận bàn giao của thuê bao về tính chính xác của thông tin thuê bao trên chứng thư số, và

Thực hiện công bố, cung cấp cho thuê bao thông tin truy cập cơ sở dữ liệu chứng thư số trực tuyến, cho phép thuê bao có thể tải về hoặc gửi cho thuê bao qua thư điện tử.

4.4. Xác nhận và công bố chứng thư số

4.4.1. Tổ chức bàn giao và xác nhận

CA2 thực hiện bàn giao chứng thư số và yêu cầu thuê bao kiểm tra, xác nhận tính chính xác của thông tin thuê bao trên chứng thư số do CA2 cấp theo đề nghị của thuê bao.

Thuê bao xác nhận tính chính xác của thông tin bằng email cấp trong chứng thư số và ký nhận biên bản bàn giao token.

CA2 sẽ tiến hành bàn giao mã PIN qua email của thuê bao sau khi thuê bao đã nhận token và có xác nhận email hợp lệ.

Thuê bao phải xác nhận trước khi CA2 công bố chứng thư số của thuê bao trên cơ sở dữ liệu trực tuyến về chứng thư số của CA2.

4.4.2. Công bố chứng thư số

Trong vòng 8 giờ làm việc sau khi có xác nhận của thuê bao, CA2 tiến hành công bố chứng thư số của thuê bao trên hệ thống cơ sở dữ liệu danh bạ chứng thư số trực tuyến của CA2.

4.4.3. Thông báo việc cấp Chứng thư số thuê bao đến các tổ chức, cá nhân khác

Thông báo việc cấp phát Chứng thư số thuê bao đến các tổ chức, cá nhân khác được thực hiện bằng cách công bố chứng thư số thuê bao trên hệ thống danh bạ trực tuyến về chứng thư số của CA2 và trên giấy chứng nhận do CA2 cấp cho thuê bao.

4.5. Sử dụng khóa và chứng thư số

4.5.1. Việc sử dụng chứng thư số và khóa riêng của thuê bao

Việc sử dụng khóa riêng tương ứng với khóa công khai trên chứng thư số của thuê bao do CA2 cấp phải tuân thủ theo đúng phạm vi trong thỏa thuận ký kết giữa hai bên.

Thuê bao phải chịu trách nhiệm bảo vệ khóa riêng, và về việc sử dụng trái phép khóa riêng, và phải ngừng sử dụng khóa riêng sau khi hết hạn hoặc bị thu hồi chứng thư số.

4.5.2. Việc sử dụng chứng thư số và khóa công khai của thuê bao CA2 đối với bên nhận

Khi đồng ý sử dụng chứng thư số của thuê bao CA2 tức là bên nhận đã đồng ý với các điều khoản áp dụng cho bên nhận.

Bên nhận phải xác thực về thông tin của chứng thư số, sự phù hợp cho mục đích sử dụng, trạng thái của chứng thư số, và chữ ký số.

4.6. Gia hạn chứng thư số

Gia hạn chứng thư số được thực hiện cho thuê bao không thay đổi khóa và thông tin trên chứng thư số.

4.6.1. Các trường hợp gia hạn chứng thư số

Trước khi hết hạn chứng thư số hoặc sau khi hết hạn chứng thư số.

4.6.2. Người yêu cầu gia hạn chứng thư số

Thuê bao phải trực tiếp yêu cầu gia hạn chứng thư số.

4.6.3. Quy trình xử lý yêu cầu gia hạn chứng thư số

Ít nhất là 30 ngày trước ngày hết hạn của chứng thư số, thuê bao phải có đơn xin gia hạn chứng thư số.

CA2 và RA, đại lý thực hiện các trình tự thủ tục thẩm định đảm bảo xác minh chính xác người yêu cầu gia hạn chứng thư số là thuê bao của chứng thư số được yêu cầu gia hạn.

4.6.4. Thông báo cho thuê bao

Thực hiện thông báo cho thuê bao và xác nhận với thuê bao về việc chứng thư số của thuê bao đã được gia hạn.

4.6.5. Bàn giao và xác nhận với thuê bao

CA2 thực hiện bàn giao chứng thư số và yêu cầu thuê bao kiểm tra, xác nhận tính chính xác của thông tin thuê bao trên chứng thư số do CA2 gia hạn theo đề nghị của thuê bao.

Thuê bao phải xác nhận trước khi CA2 công bố chứng thư số của thuê bao trên cơ sở dữ liệu trực tuyến danh bạ về chứng thư số của CA2.

4.6.6. Công bố chứng thư số

Trong vòng 8 giờ làm việc sau khi có xác nhận của thuê bao, CA2 tiến hành công bố chứng thư số của thuê bao trên hệ thống cơ sở dữ liệu danh bạ chứng thư số trực tuyến của CA2.

4.6.7. Thông báo việc hết hạn Chứng thư số thuê bao đến các tổ chức, cá nhân khác

Thông báo việc hết hạn chứng thư số thuê bao đến các tổ chức, cá nhân khác được thực hiện bằng cách công bố chứng thư số thuê bao trên hệ thống danh bạ trực tuyến về chứng thư số của CA2, và trên giấy chứng nhận do CA2 cấp cho thuê bao.

4.7. Thay đổi khóa chứng thư số

Thuê bao phải có đơn xin thay đổi khóa chứng thư số.

CA2 sẽ phải thẩm định và cấp một chứng thư số mới chứng thực cho khóa công khai thay đổi.

4.7.1. Các trường hợp thay đổi khóa chứng thư số

Trước khi hết hạn chứng thư số hoặc sau khi hết hạn chứng thư số thuê bao có thể yêu cầu thay đổi khóa chứng thư số.

4.7.2. Người yêu cầu thay đổi khóa chứng thư số

Thuê bao phải trực tiếp yêu cầu việc thay đổi khóa chứng thư số.

4.7.3. Quy trình xử lý yêu cầu thay đổi khóa chứng thư số

Khi cần thay đổi khóa chứng thư số, thuê bao phải có đơn xin thay đổi khóa chứng thư số.

CA2 và RA, đại lý thực hiện các trình tự thủ tục thẩm định đảm bảo xác minh chính xác người yêu cầu thay đổi khóa chứng thư số là thuê bao của chứng thư số được yêu cầu thay đổi khóa.

4.7.4. Thông báo cho thuê bao

Thực hiện thông báo cho thuê bao và xác nhận với thuê bao về việc cấp chứng thư số cho khóa thay đổi của thuê bao.

4.7.5. Bàn giao và xác nhận với thuê bao

CA2 thực hiện bàn giao chứng thư số và yêu cầu thuê bao kiểm tra, xác nhận tính chính xác của thông tin thuê bao trên chứng thư số với khóa thay đổi do CA2 cấp theo đề nghị của thuê bao.

Thuê bao phải xác nhận trước khi CA2 công bố chứng thư số của thuê bao trên cơ sở dữ liệu danh bạ trực tuyến về chứng thư số của CA2.

4.7.6. Công bố chứng thư số

Trong vòng 8 giờ làm việc sau khi có xác nhận của thuê bao, CA2 tiến hành công bố chứng thư số của thuê bao trên hệ thống cơ sở dữ liệu danh bạ chứng thư số trực tuyến của CA2.

4.7.7. Thông báo việc thay đổi khóa chứng thư số của thuê bao đến các tổ chức, cá nhân khác

Thông báo việc thay đổi khóa chứng thư số của thuê bao đến các tổ chức, cá nhân khác được thực hiện bằng cách công bố chứng thư số thuê bao trên hệ thống danh bạ trực tuyến về chứng thư số của CA2, và trên giấy chứng nhận do CA2 cấp thay đổi cho thuê bao.

4.8. Thay đổi chứng thư số thuê bao

4.8.1. Các trường hợp thay đổi chứng thư số

Khi thuê bao có nhu cầu thay đổi thông tin trên chứng thư số đang sử dụng của thuê bao mà không thay đổi khóa chứng thư số.

4.8.2. Người yêu cầu thay đổi chứng thư số

Thuê bao phải trực tiếp yêu cầu việc thay đổi chứng thư số.

4.8.3. Quy trình xử lý yêu cầu thay đổi chứng thư số

Thuê bao phải có đơn xin thay đổi chứng thư số.

CA2 sẽ phải thẩm định và cấp đổi một chứng thư số mới chứng thực cho khóa công của thuê bao.

CA2 và RA, đại lý thực hiện các trình tự thủ tục thẩm định đảm bảo xác minh chính xác người yêu cầu thay đổi chứng thư số là thuê bao của chứng thư số được yêu cầu thay đổi.

4.8.4. Thông báo cho thuê bao

Thực hiện thông báo cho thuê bao và xác nhận với thuê bao về việc cấp chứng thư số cho yêu cầu thay đổi chứng thư số của thuê bao.

4.8.5. Bàn giao và xác nhận với thuê bao

CA2 thực hiện bàn giao chứng thư số và yêu cầu thuê bao kiểm tra, xác nhận tính chính xác của thông tin thuê bao trên chứng thư số thay đổi với do CA2 cấp theo đề nghị của thuê bao.

Thuê bao phải xác nhận trước khi CA2 công bố chứng thư số thay đổi của thuê bao trên cơ sở dữ liệu danh bạ trực tuyến về chứng thư số của CA2.

4.8.6. Công bố chứng thư số

Trong vòng 8 giờ làm việc sau khi có xác nhận của thuê bao, CA2 tiến hành công bố chứng thư số của thuê bao trên hệ thống cơ sở dữ liệu chứng thư số trực tuyến của CA2.

4.8.7. Thông báo việc thay đổi chứng thư số của thuê bao đến các tổ chức, cá nhân khác

Thông báo việc thay đổi chứng thư số của thuê bao đến các tổ chức, cá nhân khác được thực hiện bằng cách công bố chứng thư số thuê bao trên hệ thống danh bạ trực tuyến về chứng thư số của CA2, và trên giấy chứng nhận do CA2 cấp thay đổi cho thuê bao.

4.9. Tạm dừng và thu hồi chứng thư số của thuê bao

4.9.1. Trường hợp thu hồi chứng thư số thuê bao

Các trường hợp liệt kê dưới đây CA2 sẽ thu hồi chứng thư số của thuê bao và công bố trên danh bạ chứng thư số bị thu hồi CRL của CA2. Với các trường hợp ngoài danh mục liệt kê mà do thuê bao không có nhu cầu tiếp tục sử dụng chứng thư số, CA2 sẽ thực hiện dừng hiệu lực chứng thư số của thuê bao trong cơ sở dữ liệu của CA2 mà không công bố trên danh sách chứng thư số bị thu hồi CRL của CA2.

Danh mục các trường hợp CA2 thực hiện quy trình thủ tục thu hồi chứng thư số của thuê bao:

- Khi CA2, người nhận, thuê bao có nghi ngờ về khóa bí mật của thuê bao;
- Khi thông tin của thuê bao thay đổi;
- Khi có yêu cầu của cơ quan quản lý Nhà nước;
- Khi thuê bao là cá nhân đã chết hoặc mất tích theo tuyên bố của tòa án hoặc thuê bao là tổ chức giải thể hoặc phá sản theo quy định của pháp luật;
- Khi có yêu cầu của cơ quan tiến hành tố tụng, cơ quan an ninh hoặc Bộ Thông tin và Truyền thông;
- Theo điều kiện thu hồi chứng thư số đã được quy định trong hợp đồng giữa thuê bao và CA2;
- Khi thuê bao vi phạm quy định về thỏa thuận sử dụng;
- Hợp đồng giữa CA2 và thuê bao bị hủy.

4.9.2. Người có thể yêu cầu thu hồi chứng thư số thuê bao

Thuê bao phải trực tiếp yêu cầu;

CA2, người nhận, các cơ quan Nhà nước như liệt kê ở mục 4.9.1.

Trong bất cứ trường hợp nào, việc thu hồi chứng thư số thuê bao phải được CA2 thẩm định và thông báo rõ ràng tới các bên liên quan.

4.9.3. Thủ tục yêu cầu thu hồi chứng thư số thuê bao

Ngay khi có những yêu cầu cần thu hồi chứng thư số, CA2 tiến hành xác minh trực tiếp với thuê bao, hồ sơ thuê bao và phía yêu cầu thu hồi để đảm bảo đúng đối tượng và gắn trách nhiệm trước khi CA2 thực hiện chính thức thu hồi.

4.9.4. Thời gian ân hạn

Yêu cầu thu hồi cần được thực hiện càng sớm càng tốt.

4.9.5. Thời gian xử lý thu hồi chứng thư số thuê bao

CA2 sẽ thu hồi chứng thư số của thuê bao nhanh nhất có thể được, ngay sau khi nhận được yêu cầu và thẩm định thành công. CA2 có thể tạm dừng chứng thư số của thuê bao trước khi quyết định có thực hiện việc thu hồi hay không. Ngay sau khi thu hồi chứng thư số, CA2 sẽ cập nhật trực tuyến cơ sở dữ liệu của chứng thư số và CRL. Tất cả những yêu cầu thu hồi và kết quả sẽ được CA2 lưu trữ.

4.9.6. Yêu cầu kiểm tra chứng thư số thu hồi đối với bên nhận

Sử dụng các chứng thư số của thuê bao bị thu hồi có thể làm tổn hại hoặc gây hậu quả đến nghiêm trọng tùy theo từng ứng dụng và mục đích sử dụng. Vì vậy, trước khi tin vào chứng thư số của một thuê bao, người nhận phải thực hiện kiểm tra tình trạng chứng thư số bằng kênh CRL, danh bạ chứng thư số trực tuyến và OCSP do CA2 thiết lập trực tuyến 24/7. CA2 sẽ cung cấp cho người nhận thông tin kiểm tra danh bạ, CRL và OCSP trực tuyến hỗ trợ kiểm tra trạng thái một chứng thư số.

Nếu thông tin thu hồi cho thấy một chứng thư số tạm thời không được sử dụng thì bên nhận phải từ chối sử dụng chứng thư số đó hoặc có quyết định đúng đắn và chấp nhận rủi ro xảy ra.

4.9.7. Tần suất phát hành CRL

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

4.9.8. Độ trễ tối đa của CRL

CA2 không áp dụng.

4.9.9. Tính sẵn sàng kiểm ra trạng thái chứng thư số thu hồi

Kiểm tra trạng thái chứng thư số bị thu hồi và các trạng thái khái khác của chứng thư số được cung cấp trực tuyến 24/7 bằng các kênh danh bạ chứng thư số trực tuyến

www.cavn.vn, danh sách thu hồi chứng thư số CRL và giao thức kiểm tra trực tuyến về trạng thái chứng thư số OCSP.

4.9.10. Yêu cầu kiểm tra trực tuyến chứng thư số thu hồi đối với bên nhận

Bên nhận phải thực hiện kiểm tra tình trạng chứng thư số bằng kênh CRL và OCSP do CA2 thiết lập trực tuyến 24/7. CA2 sẽ cung cấp cho người nhận thông tin kiểm tra danh bạ, CRL và OCSP trực tuyến hỗ trợ kiểm tra trạng thái một chứng thư số.

4.9.11. Hình thức khác

CA2 không áp dụng.

4.9.12. Yêu cầu đặc biệt khi có vấn đề lộ khóa thuê bao

CA2 sẽ nỗ lực cao nhất để thông báo tới bên nhận.

4.9.13. Trường hợp tạm dừng chứng thư số thuê bao

Khi CA2 đang xử lý việc thu hồi chứng thư số thuê bao.

4.9.14. Người yêu cầu tạm dừng chứng thư số thuê bao

CA2 sẽ quyết định việc tạm dừng khi có yêu cầu từ thuê bao, cơ quan quản lý Nhà nước, cơ quan tiến hành tố tụng, cơ quan an ninh hoặc Bộ Thông tin và Truyền thông.

4.9.15. Thủ tục tạm dừng chứng thư số thuê bao

Khi việc thẩm định thấy có dấu hiệu cần thu hồi nhưng chưa kết thúc.

4.9.16. Giới hạn thời gian tạm dừng chứng thư số thuê bao

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

4.10. Hệ thống dịch vụ hỗ trợ kiểm tra tình trạng chứng thư số

4.10.1. Các đặc điểm của dịch vụ

Việc kiểm tra trạng thái của một chứng thư số có các cách sau:

- Kiểm tra qua danh sách thu hồi chứng thư số CRL công bố trên website của CA2;
- Kiểm tra bằng việc tìm kiếm theo các thông tin trên chứng thư số qua hệ thống danh bạ chứng thư số LDAP của CA2;
- Kiểm tra quan giao thức trạng thái chứng thư số trực tuyến OCSP được tích hợp vào ứng dụng của bên nhận.

4.10.2. Tính sẵn sàng của dịch vụ

Dịch vụ luôn sẵn sàng 24/7.

4.10.3. Tính tùy chọn

OCSP có tính tùy chọn vì không phải ứng dụng nào cũng có sẵn tính năng OCSP để hỗ trợ việc tự động xác thực trạng thái chứng thư số trực tuyến.

4.11. Thuê bao chấm dứt dịch vụ

Thuê bao có thể đơn phương chấm dứt dịch vụ bằng các cách:

- Hủy hợp đồng thuê bao;
- Chứng thư số hết hạn nhưng không gia hạn;
- Yêu cầu thu hồi trước thời hạn.

4.12. Gửi giữ khóa riêng và phục hồi khóa riêng của thuê bao

CA2 không áp dụng.

4.12.1. Chính sách và thủ tục gửi giữ khóa riêng

CA2 không áp dụng.

4.12.2. Chính sách và thủ tục khôi phục gửi giữ khóa riêng

CA2 không áp dụng.

5. ĐẢM BẢO AN NINH AN TOÀN CƠ SỞ VẬT CHẤT, QUẢN LÝ VÀ VẬN HÀNH HỆ THỐNG

5.1. Đảm bảo an ninh cơ sở vật chất

5.1.1. Nơi đặt hệ thống và kết cấu

Hệ thống CA2 được đặt trong phòng riêng, cửa ra vào được khóa bởi 2 lớp khóa là khóa cơ và khóa điện, chỉ có những người được tin cậy được phép ra vào.

5.1.2. Kiểm soát ra vào

Vào phòng hệ thống CA2 bắt buộc phải có tối thiểu 2 người cùng một lúc, một người giữ chìa khóa cơ, một người giữ thẻ mở khóa điện tử.

Tất cả các hoạt động ra vào được camera và cán bộ giám sát ghi lại.

5.1.3. Điều hòa nhiệt độ và nguồn điện

Hệ thống và thiết bị CA2 được trang bị với hệ thống chính và hệ thống dự phòng:

- Nguồn điện gồm có: Nguồn điện lưới, hệ thống điện dự phòng UPS và máy phát điện dự phòng.
- Hệ thống điều hòa nhiệt độ và chống ẩm.

5.1.4. Hư hại do nước

Hệ thống và thiết bị CA2 được cài đặt trong phòng đảm bảo không bị trong tình trạng có nước. Toàn bộ thiết bị hệ thống được lắp đặt trong hệ thống tủ Rack công nghiệp.

5.1.5. Phòng cháy chữa cháy

CA2 thực hiện công tác phòng cháy và chữa cháy theo quy định của Cục Cảnh sát phòng cháy chữa cháy Hà Nội.

CA2 có kế hoạch xử lý rủi ro có tính tới những thiệt hại do cháy nổ.

CA2 cử cán bộ tham gia đào tạo định kỳ về phòng chống cháy nổ để đảm bảo xử lý kịp thời trong trường hợp có xự cố xảy ra.

5.1.6. Chống nhiễu điện từ

Nơi đặt hệ thống, thiết bị không gần nguồn phát nhiễu điện từ mạnh. Vỏ sắt máy thiết bị, tủ Rack được nối đất chống nhiễu điện từ. Các thành phần thiết bị có khả năng ảnh hưởng nhiễu điện từ được bảo vệ bằng bọc màng chống nhiễu điện từ.

5.1.7. Chống chịu lũ lụt, động đất

- Hệ thống chính được đặt tại Tầng 5, Số 2 Chùa Bộc, Đống Đa, Hà Nội
- Hệ thống dự phòng được đặt tại Data Center của Công ty TNHH Hanel – CSF đặt tại khu công nghiệp Sài Đồng B – Long Biên – Hà Nội
- Toàn bộ máy móc thiết bị được lắp đặt trong hệ thống tủ Rack công nghiệp không tiếp xúc trực tiếp với mặt sàn tầng nhà.
- Cơ sở dữ liệu luôn được lưu dự phòng trên hệ thống băng từ tại chỗ và offsite tại Hanel Data Center.
- Cơ sở dữ liệu dự phòng và khoá phục hồi hệ thống được quản lý bởi bộ thẻ đặc biệt, thẻ thông minh với khả năng chịu nước, va đập. Duy trì offsite cùng quy trình phục hồi toàn diện đảm bảo việc khôi phục hoàn toàn hệ thống trong trường hợp thảm hoạ xảy ra.

5.1.8. Phương tiện lưu trữ

Hệ thống lưu trữ dữ liệu, kiêm toán, sao lưu, dự phòng được đặt tại 2 nơi là trụ sở chính tầng 5, số 2 Chùa Bộc, Quận Đống Đa và tại địa điểm cách ly Hanel CSF Datacenter Sài Đồng, Gia Lâm.

Hệ thống lưu trữ được thiết kế đảm bảo kiểm soát truy xuất ở cả hai mức phần cứng và phần mềm để bảo vệ phương tiện lưu trữ với các rủi ro từ các sự cố hỏng hóc do nước, lửa, điện và điện từ trường.

5.1.9. Xử lý rác

Các tài liệu và vật tư nhạy cảm phải được xử lý trước khi vứt rác. Các phương tiện lưu trữ và bảo mật phải được phá hủy theo quy trình của nhà sản xuất trước khi vứt rác.

5. 1.10. Lưu trữ và dự phòng cách ly

CA2 thực hiện sao lưu và dự phòng các hệ thống, thiết bị chủ chốt, hệ thống dữ liệu, dữ liệu ghi log phục vụ phục hồi nguyên trạng hệ thống tại địa điểm cách ly địa lý với hệ thống chính tại Hanel Datacenter, Sài Đồng, Gia Lâm.

5.2. Quy trình kiểm soát

5.2.1. Đảm bảo tính tin tưởng

CA2 là dịch vụ tin cậy, thiết kế kỹ thuật và vận hành hệ thống tuân thủ tuyệt đối yêu cầu này.

Vai trò, trách nhiệm của cán bộ vận hành được phân định rõ ràng, và được kiểm soát chặt chẽ theo chức năng, nhiệm vụ và phải là những người được tin tưởng cao.

Nguyên tắc là tất cả những vị trí công việc nhậy cảm với cơ hội thỏa hiệp về khóa mật mã hệ thống, về cấp và quản lý chu kỳ hoạt động của chứng thư số phải được đảm bảo tin tưởng.

5.2.2. Số cán bộ yêu cầu cho mỗi nhiệm vụ

CA2 không cho phép một cán bộ thực hiện độc lập các hoạt động của hệ thống cấp và quản lý chứng thư số (CA). Từ kiểm soát vào phòng CA đến kiểm soát vận hành CA mỗi chức năng phải có tối thiểu 2 người được tin tưởng cùng tham gia.

Những chức năng nhiệm vụ sau tối thiểu phải có 2 cán bộ an ninh được tin tưởng tham gia:

- Vào phòng hệ thống.
- Thêm và xóa cán bộ an ninh hệ thống.
- Kích hoạt HSM cho các hoạt động ký số của hệ thống.
- Khởi tạo, cập nhật, lưu trữ và dự phòng cơ sở dữ liệu.

5.2.3. Xác thực và định danh với từng vai trò được tin tưởng

Mỗi cán bộ tham gia với vai trò được tin tưởng trong hệ thống CA2 được cấp sở hữu riêng một thẻ thông minh dùng cho xác thực định danh và phân quyền vận hành. Thẻ này được bảo vệ bằng mã PIN cá nhân và được cất giữ trong mỗi két an ninh riêng.

5.2.4. Yêu cầu tách nhiệm vụ

Các nhiệm vụ sau phải tách ra thực hiện:

- Thẩm định yêu cầu cấp chứng thư số.
- Thẩm định yêu cầu thu hồi, gia hạn chứng thư số.
- Cấp, thu hồi chứng thư số.
- Quản lý thông tin thuê bao.
- Đối soát.
- Vận hành hệ thống.

5.3. Quản lý cán bộ

CA2 yêu cầu toàn bộ các nhân viên thực hiện nhiệm vụ đối với hoạt động của CA sẽ:

i. Được bổ nhiệm bằng văn bản;

ii. Phải tuân theo các điều khoản và điều kiện trong hợp đồng hoặc quy chế tương ứng với vị trí họ đảm nhiệm;

iii. Đã được đào tạo một cách toàn diện về nhiệm vụ phải thực hiện;

iv. Tuân theo hợp đồng hoặc quy chế về việc không được tiết lộ các thông tin an ninh nhạy cảm hoặc thông tin của người giữ chứng thư số; và

v. Không được phân công các nhiệm vụ mà có thể gây ra xung đột trách nhiệm.

5.3.1. Yêu cầu về trình độ chuyên môn, kinh nghiệm

CA2 yêu cầu cán bộ thể hiện được sự tin tưởng, trình độ chuyên môn và kinh nghiệm phù hợp với vai trò và nhiệm vụ đảm trách.

5.3.2. Thủ tục kiểm tra năng lực

Tất cả cán bộ công tác trong vai trò được tin tưởng được yêu cầu phải qua kiểm tra nghiêm ngặt về sự tin tưởng, trình độ chuyên môn và kinh nghiệm phù hợp.

5.3.3. Yêu cầu đào tạo

Chương trình đào tạo của CA2 được thiết kế theo vai trò, nhiệm vụ và trách nhiệm của mỗi cán bộ và từng nhóm liên quan đến:

- Cơ sở pháp lý về dịch vụ chứng thực chữ ký số công cộng.
- Trách nhiệm công việc.
- Hiểu biết về PKI.
- Quy chế Chính sách an ninh CA2.

- Sử dụng và vận hành hệ thống.
- Xử lý và báo cáo sự cố.
- Báo cáo về nguy cơ thỏa hiệp.
- Quy trình khôi phục sau thảm họa.

5.3.4. Nhu cầu và tần suất đào tạo

Tổ chức hướng dẫn và đào tạo cho cán bộ mới, các cập nhật, nâng cấp hệ thống.

CA2 tổ chức đào tạo, bồi dưỡng và cập nhật cho cán bộ của mình trong phạm vi và tần suất hợp lý để đảm bảo rằng cán bộ duy trì mức độ yêu cầu về trình độ để thực hiện trách nhiệm công việc một cách thành thạo và thỏa đáng.

Đào tạo khắc phục hậu quả được thực thi khi có khuyến cáo và kiến nghị của kiểm tra kiểm toán.

5.3.5. Thứ tự và tần suất luân phiên công việc

CA2 không áp dụng.

5.3.6 Xử phạt đối với những hành động trái phép

Trong trường hợp nghi ngờ hoặc phát hiện hành động trái phép, CA2 sẽ có biện pháp thích hợp như đình chỉ và có thể áp dụng lên đến mức chấm dứt công việc.

5.3.7. Yêu cầu đối với nhà thầu

CA2 không áp dụng.

5.3.8. Tài liệu cấp cho cán bộ

Mỗi cán bộ thực hiện một vai trò nhất định sẽ được đào tạo và cung cấp đầy đủ tài liệu hướng dẫn vận hành, quy định, trách nhiệm và các thủ tục cho từng vai trò, nhiệm vụ để thực thi một cách thành thạo và thỏa đáng.

5.4. Thủ tục kiểm toán ghi log

CA2 sẽ duy trì các bản ghi log và lưu trữ thông tin chi tiết về các hoạt động của cán bộ vận hành và hệ thống.

5.4.1. Các loại sự kiện được ghi lại

CA2 thực hiện ghi lại bằng tay hoặc ghi tự động các sự kiện quan trọng sau:

- Đăng ký và thẩm định đăng ký đề nghị cấp chứng thư số.
- Các sự kiện liên quan đến khóa mật mã HSM.
- Các hoạt động liên quan đến cấp và quản lý chứng thư số.
- Các sự kiện liên quan đến hoạt động của hệ thống.
- Các hoạt động liên quan đến an ninh hệ thống.

- Các hoạt động thu hồi chứng thư số.
- Các hoạt động ra vào phòng hệ thống.
- Các sự kiện sao lưu dữ liệu, dự phòng và phục hồi.

Các sự kiện được ghi gồm các thành phần:

- Ngày, giờ sự kiện.
- Số hiệu, định danh sự kiện và danh tính của người thực hiện.
- Phân loại sự kiện.

5.4.2. Tần xuất xử lý bản ghi log

Việc kiểm tra và xử lý kiểm toán ghi log được thực hiện hàng ngày, hàng tuần, hàng tháng và hàng năm.

5.4.3. Thời gian duy trì các bản ghi log

Bản ghi kiểm toán phải được duy trì tại chỗ trước khi lưu trữ tối đa trong thời gian 3 tháng, sau đó được chuyển lưu trữ dự phòng tại Hanel Data center Sài Đồng. Các bản ghi kiểm toán được lưu trữ trong 5 năm.

5.4.4. Bảo vệ bản ghi log

Các bản ghi kiểm toán được bảo vệ và phân quyền kiểm soát xem, sửa, xóa, hoặc can thiệp.

5.4.5. Quy trình sao lưu dự phòng

CA2 thực hiện sao lưu gia tăng hàng ngày các bản ghi kiểm toán và thực hiện các bản sao lưu dự phòng đầy đủ hàng tuần.

5.4.6. Thu thập (Bên trong và bên ngoài)

Việc ghi log được thực hiện bằng tay và tự động. Dữ liệu ghi log tự động được tạo ra và được ghi lại do hệ thống ứng dụng, hệ thống mạng và hệ điều hành hệ thống. Dữ liệu ghi log bằng tay được thực hiện bởi cán bộ giám sát của CA2.

5.4.7. Thông báo sự kiện

Cán bộ vận hành chịu trách nhiệm thông báo cho ban lãnh đạo khi có sự kiện an ninh bảo mật quan trọng.

5.4.8. Đánh giá tính dễ tổn thương

Các sự kiện trong quá trình kiểm tra được ghi lại, vừa để phục vụ kiểm toán, vừa để đánh giá sự gây hại cho hệ thống. Đánh giá lỗ hổng an ninh được thực hiện hàng ngày và định kỳ hàng tuần, hàng năm.

5.5. Hồ sơ lưu trữ

5.5.1. Các loại hồ sơ được lưu trữ

CA2 tổ chức lưu trữ:

- Toàn bộ các bản ghi log kiểm toán.
- Hồ sơ thuê bao.
- Dữ liệu thẩm định.
- Dữ liệu quản lý chứng thư số và chứng thư số.

5.5.2. Thời gian lưu trữ

Thời gian lưu trữ theo quy định của pháp luật.

5.5.3. Bảo vệ hồ sơ lưu trữ

Các hồ sơ lưu trữ được bảo vệ và phân quyền kiểm soát xem, sửa, xóa, hoặc can thiệp.

5.5.4. Quy trình sao lưu dự phòng

CA2 thực hiện sao lưu gia tăng hàng ngày các bản ghi kiểm toán và thực hiện các bản sao lưu dự phòng đầy đủ hàng tuần.

5.5.5. Quy định về xác định thời gian của hồ sơ

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

5.5.6. Lưu trữ (Nội bộ hoặc bên ngoài)

CA2 tổ chức lưu trữ nội bộ.

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

Chỉ cán bộ đủ thẩm quyền được phép lấy hồ sơ lưu trữ. Tính toàn vẹn của thông tin phải được xác nhận.

5.5.8. Bảo quản dài hạn

Tối thiểu là 5 năm và tuân thủ quy định mới nhất của pháp luật.

5.6. Thay đổi khóa

CA2 hạn chế việc thay đổi khóa hệ thống, việc thay đổi khóa là hãn hữu hoặc do yêu cầu của cơ quan quản lý Nhà Nước. Trong trường hợp có yêu cầu, CA2 mong muốn việc thay đổi khóa hệ thống được thực hiện trước một đến hai năm thời hạn hết hạn của chứng thư số CA2.

Việc thay đổi khóa hệ thống sẽ gây ảnh hưởng tới việc đảm bảo dịch vụ liên tục tới thuê bao CA2 cam kết:

- Sẽ đảm bảo ảnh hưởng là nhỏ nhất tới thuê bao;
- Cung cấp đầy đủ thông tin về kế hoạch thay đổi hợp lý nhất.

5.7. Thảm họa và phục hồi

5.7.1. Xử lý sự cố thảm họa

CA2 có trách nhiệm vận hành một kế hoạch khôi phục sự cố và đảm bảo việc giữ duy trì hoạt động kinh doanh. Kế hoạch chi tiết là tài liệu nội bộ không công bố, tuy nhiên sẽ được cung cấp tới những người có trách nhiệm, và được ủy quyền tiến hành kiểm tra an ninh.

Một hệ thống sao lưu đảm bảo phục hồi nguyên trạng CA2 được đặt tại Hanel Data center, Sài Đồng, Gia Lâm.

5.7.2. Tài nguyên máy tính, phần mềm, và /hoặc dữ liệu gặp sự cố

CA2 có hệ thống chỉ dẫn chi tiết về việc quản lý phục hồi dịch vụ trong các trường hợp có sự cố hỏng hóc về tài nguyên máy tính, phần mềm, và / hoặc dữ liệu. Các tài liệu này được lưu hành nội bộ.

5.7.3. Thủ tục khi khóa mật mã bị can thiệp

Trong trường hợp có sự can thiệp vào khóa mật mã của hệ thống, cho dù là bất kỳ lý do gì, các thủ tục triển khai dừng hoạt động đối với khóa mật mã bị can thiệp phải được thực hiện ngay.

CA2 phải thu hồi toàn bộ chứng thư số đã phát hành có sử dụng khóa này và đưa ra các thông báo thích hợp. Sau khi làm rõ nguyên nhân dẫn tới việc tiết lộ này, CA2 có thể:

i. Phát hành một cặp khóa mật mã CA mới;

ii. Phát hành lại chứng thư số tới toàn bộ thuê bao.

5.7.4. Khả năng duy trì hoạt động kinh doanh sau thảm họa

CA2 có hệ thống dự phòng cách ly về địa lý đảm bảo sẵn sàng phục hồi sau thảm họa trong thời gian hợp lý và không làm ảnh hưởng đến hoạt động kinh doanh.

5.8. Ngừng dịch vụ CA2

Theo quy định của pháp luật.

5.9. Dịch vụ chăm sóc khách hàng

CA2 triển khai và duy trì một trung tâm chăm sóc khách hàng để đảm bảo chất lượng hỗ trợ và dịch vụ tốt nhất cho thuê bao.

6. ĐẢM BẢO AN TOÀN AN NINH KỸ THUẬT HỆ THỐNG

6.1. Tạo và cài đặt cặp khóa

6.1.1. Quá trình tạo cặp khóa

Quy trình thủ tục tạo cặp khóa được CA2 quy định trong hệ thống tài liệu quy định và hướng dẫn việc tuân thủ tạo cặp khóa.

Cặp khóa CA2 được tạo bởi khối bảo mật phần cứng HSM theo tiêu chuẩn FIPS 140-2 Level 3, khóa ký số trong HSM được bảo vệ bởi bộ thẻ thông minh chuyên dụng và quy trình kiểm soát nhiều lớp.

Cặp khóa thuê bao được tạo bởi PKI Smartcard, PKI Token, PKI Virtual Token theo tiêu chuẩn FIPS 140-2 Level 2, sử dụng khóa ký số phải có PKI Token và mã PIN xác thực. Mã PIN xác thực được sinh ngẫu nhiên, PKI Token và mã PIN xác thực thuê bao được bàn giao tách riêng theo quy trình thẩm định đảm bảo an toàn. Mã PIN chỉ được gửi riêng cho thuê bao sau khi CA2 xác nhận đã bàn giao Token hợp lệ cho thuê bao.

6.1.2. Chuyển giao khóa riêng đến thuê bao

Cặp khóa của thuê bao được tạo ra bởi PKI Smartcard, PKI Token, PKI Virtual Token tiêu chuẩn FIPS 140-2 Level 2.

Mã PIN kích hoạt PKI Smartcard, PKI Token, PKI Virtual Token được sinh ngẫu nhiên, và bàn giao tách riêng đến thuê bao.

PKI Token được bàn giao cho thuê bao trước khi CA2 bàn giao mã PIN kích hoạt PKI Token.

Sau khi CA2 xác nhận việc bàn giao hợp lệ PKI Token tới thuê bao, và sau khi thuê bao đã xác nhận bằng email cấp trong chứng thư số và nội dung của chứng thư số do CA2 cấp, và sau khi CA2 đã thẩm định tính hợp lệ của email xác nhận với email cấp trong chứng thư số của thuê bao, mã PIN kích hoạt Token sẽ được CA2 gửi riêng tới thuê bao qua email này.

6.1.3. Chuyển giao khóa công khai của thuê bao đến CA2

CA2, RA, đại lý hoặc thuê bao chuyển giao tệp tin đề nghị cấp chứng thư số cho thuê bao mã theo chuẩn PKCS #10 sinh từ PKI Smartcard, PKI Token, PKI Virtual Token đạt chuẩn FIPS 140-2 Level 2 trở lên, hoặc tương đương qua kênh bảo mật SSL.

6.1.4. Chuyển giao khóa công khai của CA2 tới bên nhận

CA2 cung cấp chứng thư số của CA2 kèm trong chứng thư số của thuê bao khi cấp chứng thư số cho thuê bao, và đồng thời công bố trên hệ thống danh bạ chứng thư số trực tuyến 24/7 của CA2.

6.1.5. Độ lớn của khóa

Khóa CA2: 2048 bit

Khóa thuê bao: 1024 bit

6.1.6. Hệ thống thông số tạo khóa và kiểm tra chất lượng

CA 2 không quy định riêng.

6.1.7. Mục đích sử dụng khóa (theo X.509 V3)

Trường mở rộng về mục đích sử dụng khóa trong chứng thư số của thuê bao do CA2 cấp quy định về hạn chế các mục đích sử dụng mà thuê bao được áp dụng.

Cặp khóa ký số được sử dụng để cung cấp xác thực, tính toàn vẹn và chống từ chối.

Cặp khóa mã hóa được sử dụng cho mục đích mã hóa dữ liệu, phục vụ bảo mật.

6.2. Kiểm soát và bảo vệ khóa riêng

CA2 áp dụng quy trình an ninh đồng bộ nhiều lớp bao gồm kiểm soát cơ sở vật chất hạ tầng hệ thống, hệ thống công nghệ thông tin, tiêu chuẩn bảo mật FIPS 140-2 Level 3 và các thủ tục để đảm bảo an ninh khóa riêng CA2.

Thuê bao được phổ biến và được cung cấp các điều khoản trong hợp đồng để có biện pháp phòng ngừa cần thiết để ngăn chặn sự mất mát, tiết lộ, thay đổi, hoặc sử dụng trái phép khóa riêng. Khóa riêng của thuê bao được kiểm soát và bảo vệ theo tiêu chuẩn FIPS 140-2 Level 2.

6.2.1. Tiêu chuẩn đối với mô đun mã hóa

Bảo mật cho hệ thống CA2: Sử dụng HSM chuẩn FIPS PUB 140-2 Level 3.

Bảo mật cho thuê bao: Sử dụng chuẩn FIPS 140-2 Level 2.

6.2.2. Cơ chế kiểm soát khóa riêng nhiều người M of N

CA2 áp dụng xác thực nhiều lớp sử dụng các bộ thẻ thông minh chuyên dụng, mỗi bộ áp dụng cơ chế kiểm soát 2 x 3, chia riêng cho 3 người. Để xác thực thành công luôn phải có đủ 2 trong 3 người xuất trình thẻ hợp lệ, 1 người còn lại trong 3 người dự phòng cho 2 người kia.

6.2.3. Gửi giữ khóa riêng của thuê bao

CA2 không áp dụng.

6.2.4. Sao lưu dự phòng khóa riêng

CA2 sao lưu dự phòng khóa riêng bằng bộ thẻ thông minh chuyên dụng áp dụng có chế kiểm soát 2 x 3.

CA2 không sao lưu dự phòng khóa riêng của thuê bao.

Cơ sở dữ liệu sao lưu phục hồi CA2 được thực hiện định kỳ hàng ngày, việc phục hồi chỉ có thể thực hiện được khi thực hiện hợp lệ quy trình kiểm soát 2 x 3.

6.2.5. Lưu trữ khóa riêng

CA2 không lưu trữ khóa riêng của thuê bao.

Khóa riêng của CA2 được lưu trữ ở dạng mã hóa bởi bộ thẻ chuyên dụng 2 x 3 và được bảo vệ trong két sắt chống cháy của từng người giữ thẻ.

6.2.6. Chuyển giao khóa riêng với khối bảo mật phần cứng

Khóa riêng CA2 được mã hóa và quản lý trong bộ thẻ thông minh dự phòng chuyên dụng 2 x 3 và phục vụ cho việc chuyển giao đảm bảo an toàn tuyệt đối cho khóa riêng CA2.

6.2.7. Phương pháp giữ khóa riêng CA2

Khối bảo mật phần cứng HSM 140-2 Level 3 chịu tách nhiệm giữ khóa riêng phục vụ cho hoạt động của hệ thống CA2.

6.2.8. Phương pháp kích hoạt khóa riêng

Kích hoạt khóa riêng hệ thống CA2 được quản lý bảo mật bên trong HSM chuẩn bảo mật 140-2 Level 3 và được kiểm soát bằng bộ thẻ thông minh chuyên dụng theo cơ chế 2 x 3.

Việc kích hoạt khóa riêng thuê bao được thực hiện bởi mã số PIN, khóa riêng của thuê bao được quản lý bảo mật theo tiêu chuẩn FIPS 140-2 Level 2.

6.2.9. Phương pháp khử hoạt khóa riêng

Khóa riêng hệ thống CA2 sẽ được khử hoạt khi rút thẻ thông minh chuyên dụng ra khỏi hệ thống và khi tắt hệ thống.

6.2.10. Phương pháp phá hủy khóa riêng

Tất cả khóa mật mã của CA2 được ghi đè bằng dãy số 0 khi hệ thống không hoạt động. phá hủy vĩnh viễn khóa riêng được thực hiện bằng một quy trình an ninh an toàn riêng trong nội bộ.

6.2.11. Đánh giá khối bảo mật

CA2 không áp dụng.

6.3. Các yếu tố quản lý khác đối với cặp khóa

6.3.1. Lưu trữ khóa công khai

Khóa công khai được công bố trên hệ thống danh bạ của CA2, và được lưu trữ theo quy định của pháp luật.

6.3.2. Thời hạn hiệu lực

Thời hạn hiệu lực theo quy định của pháp luật.

6.4. Kích hoạt dữ liệu

6.4.1. Khởi tạo kích hoạt dữ liệu và cài đặt

CA2 không có cơ chế kích hoạt khác với cơ chế kiểm soát cho kích hoạt vận hành khối bảo mật phần cứng.

6.4.2. Bảo vệ dữ liệu kích hoạt

CA2 không có cơ chế kích hoạt khác với cơ chế kiểm soát cho kích hoạt vận hành khối bảo mật phần cứng.

6.4.3. Các yếu tố khác

CA2 không có quy định riêng khác.

6.5. Đảm bảo an toàn an ninh hệ thống máy tính

6.5.1. Yêu cầu chi tiết kỹ thuật đối với an toàn an ninh hệ thống máy tính

CA2 thực hiện kiểm soát an ninh ra vào và sử dụng hệ thống máy tính sạch với nhiều lớp xác thực. Đặc biệt là kiểm soát và cách ly hệ thống cấp và quản lý chứng thư số, việc tách biệt này đảm bảo ngăn chặn các truy cập hệ thống không được kiểm soát.

CA2 sử dụng hệ thống tường lửa để bảo vệ hệ thống cấp và quản lý chứng thư số với kết nối từ trạm cấp cũng được quản lý hoạt động cách ly hoàn toàn với hệ thống mạng nghiệp vụ khác.

CA2 áp dụng sử dụng quy định sử dụng mật khẩu đủ mạnh sử dụng cơ chế mã hóa MD5, và yêu cầu thay đổi định kỳ thường xuyên.

6.5.2. Đánh giá mức độ an toàn an ninh của hệ thống máy tính

CA2 áp dụng ITSEC – Part 3.

6.6. Đảm bảo chu trình kỹ thuật

6.6.1. Đảm bảo chu trình phát triển hệ thống

CA2 sử dụng các hệ thống có chứng chỉ tiêu chuẩn công nghệ thông tin.

6.6.2. Đảm bảo quản lý an toàn bảo mật

CA2 áp dụng cơ chế kiểm soát và giám sát theo quy định của nhà sản xuất.

6.6.3. Quản lý chu trình an ninh

CA2 không có quy định riêng.

6.7. Đảm bảo an toàn an ninh hệ thống mạng

CA2 áp dụng mô hình an ninh an toàn hệ thống thông tin theo 7 lớp gồm:

- Lớp hệ thống dữ liệu CA2
- Lớp hệ thống ứng dụng CA2 OFFLINE
- Lớp hệ thống dịch vụ CA2
- Lớp hệ thống mạng nội bộ
- Lớp hệ thống mạng ngoại vi
- Lớp hệ thống phòng ốc
- Lớp hệ thống quy trình thủ tục CA2

CA2 tuân thủ theo hướng dẫn và yêu cầu kiểm toán để ngăn chặn sự truy cập trái phép và gây độc hại. Các thông tin, dữ liệu nhậy cảm trao đổi qua mạng được mã hóa và ký số.

6.8. Dấu thời gian

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

7. MẪU TRÍCH NGANG CHỨNG THƯ SỐ, CRL VÀ OCSP

7.1. Chứng thư số

Chứng thư số CA2 cấp tuân thủ theo tiêu chuẩn X.509 v.3, các quy định tại nội dung về khuôn dạng chứng thư số theo RFC 3280.

Các trường thông tin trong chứng thư số tối thiểu gồm các thông tin sau:

Bảng lược tả các trường cơ bản trong chứng thư số CA2

Tên trường	Giá trị
Serial number	Số seri chứng thư số có giá trị duy nhất.
Signature Algorithm	Thuật toán được sử dụng để ký chứng thư số
Issue DN	Tên tổ chức cấp chứng thư số
Valid From	Thời điểm hiệu lực của chứng thư số
Valid To	Thời điểm hết hiệu lực của chứng thư số
Subject DN	Tên của thuê bao
Subject Public Key	Khoá công khai của thuê bao

Signature	Chữ ký số của tổ chức cấp chứng thư số

7.1.1. Số phiên bản

CA2 cung cấp chứng thư số X509 phiên bản 3

(1). Phiên bản

Phiên bản X509 V.3.

(2). Số hiệu

61 0b 38 21 00 00 00 00 00 08.

7.1.2. Trường mở rộng

Trường mở rộng sẽ được thống nhất bằng thỏa thuận giữa CA2 và thuê bao.

7.1.3. Định danh thuật toán ký số

CA2 không có quy định riêng.

7.1.4. Định dạng tên

CA2 áp dụng theo quy định tại Mục 3.1.1.

7.1.5. Ràng buộc tên

CA2 áp dụng theo quy định tại Mục 3.1.4.

7.1.6. Định danh chính sách

CA2 không áp dụng.

7.1.7. Mở rộng chính sách

CA2 không quy định riêng.

7.1.8. Cú pháp và ngữ nghĩa

CA2 không có quy định riêng.

7.1.9. Xử lý ngữ nghĩa ở các trường mở rộng

CA2 không có quy định riêng.

7.2. CRL

CRL được phát hành theo phiên bản X509 v.2

CRL được CA2 ký và công bố trên website www.cavn.vn

Đường dẫn và các giao thức hỗ trợ:

http://www.cavn.vn/ca2crl.crl

http://www.cavn.vn/CertEnroll/CA2.crl

http://www.cavn.vn/ca2crl+.crl

http://www.cavn.vn/CertEnroll/ca2crl.crl

Bảng lược tả các trường cơ bản trong CRL CA2:

Tên	Giá trị
Version	Phiên bản CRL
Signature Algorithm	Thuật toán ký số áp dụng
Issue	Tổ chức phát hành
This Update	Ngày phát hành
Next Update	Lịch sẽ phát hành bản CRL mới
Revoke Certificates	Danh sách chứng thư số bị thu hồi

7.2.1. Số phiên bản

CA2 cung cấp CRL phiên bản 2

7.2.2. Trường mở rộng

CA2 không quy định riêng.

7.3. OCSP

7.3.1. Số phiên bản

CA2 áp dụng theo giao thức RFC 6960

7.3.2. Trường mở rộng

CA2 không quy định riêng.

8. TUÂN THỦ KIỂM TOÁN VÀ CÁC KIỂM ĐỊNH KHÁC

Các hoạt động của CA2 sẽ được kiểm toán thực hiện định kỳ hàng năm hoặc theo yêu cầu từ Bộ Thông tin và Truyền thông. Các hoạt động kiểm toán có thể được thực hiện bởi một đơn vị ngoài.

8.1. Tần suất thực hiện kiểm toán

CA2 tuân thủ chế độ kiểm toán quy định. Ngoài ra CA2 thực hiện tự đánh giá hoạt động của CA2, RA, đại lý ít nhất mỗi năm một lần bởi đơn vị kiểm toán đáp ứng yêu cầu theo quy định của pháp luật và yêu cầu của CA2.

8.2. Khả năng của người kiểm định

Người thực hiện kiểm định phải là đơn vị độc lập có năng lực thành thạo về công nghệ hạ tầng khóa công khai, công cụ và kĩ thuật an toàn thông tin và được chứng nhận bởi RootCA.

8.3. Mối quan hệ với tổ chức kiểm toán

Việc thực hiện các hoạt động kiểm toán sẽ được thực hiện bởi những người không phụ thuộc vào CA2.

8.4. Mối quan hệ với tổ chức kiểm định

Quá trình thực hiện kiểm định phải do đơn vị kiểm định độc lập với CA2 tiến hành.

8.5. Các nội dung kiểm toán, kiểm định khác

Phạm vị được kiểm toán, kiểm định bao gồm: môi trường hoạt động của CA2, hạ tầng hệ thống, các hoạt động quản lý khóa, các quy trình kiểm soát điều khiển và quản trị CA2 và các nội dung khác theo yêu cầu của đơn vị kiểm toán.

8.6. Các công việc đưa ra khi kết quả của sự sai sót, thiếu hụt

Sau khi có báo cáo kiểm toán, căn cứ vào kết quả các vấn đề sai sót, thiếu hụt phải được chỉ ra và xử lý bởi bộ phận quản lý của CA2.

CA2 sẽ làm việc với RootCA về những nội dung chưa phù hợp được chỉ ra.

Nếu các vấn đề sự cố và thiếu sót có ảnh hưởng nghiêm trọng tới tính an toàn và toàn vẹn của CA2, CA2 sẽ xây dựng kế hoạch hành động và thực hiện ngay trong khoảng thời gian hợp lý.

Đối với các sai sót, thiếu hụt kém nghiêm trọng hơn CA2 sẽ xem xét và xác định các hành động cần thực hiện.

8.7. Công bố kết quả:

Kết quả kiểm toán, kiểm định sẽ được CA2 công bố trên website https://cavn.vn/

9. CÁC NHIỆM VỤ KHÁC VÀ CÁC VẤN ĐỀ VỀ PHÁP LÝ

9.1. Phí

Tất cả những thông báo về việc tính phí phải được gửi tới thuê bao.

9.1.1. Phí cấp phát, gia hạn, tạm dừng, khôi phục, thay đổi khóa và thu hồi chứng thư số

- Phí cấp phát, gia hạn chứng thư số: Theo bảng giá niêm yết trên website cavn.vn
- Phí tạm dừng, khôi phục, thay đổi khóa, thu hồi chứng thư số: Miễn phí

9.1.2. Phí truy cập chứng thư số

Miễn phí

9.1.3. Phí truy cập thông tin trạng thái thu hồi (Dịch vụ xác minh hiệu lực của chứng thư số)

Miễn phí

9.1.4. Phí cho những dịch vụ khác như là thông tin về chính sách

CA2 và RA, đại lý có thể thiết lập và tính một mức phí hợp lý cho dịch vụ khác.

9.1.5. Chính sách hoàn phí

Bất kỳ các khoản phí nào cho việc đề nghị cấp chứng thư số mà không được phê chuẩn sẽ được hoàn trả.

9.2. Trách nhiệm tài chính

9.2.1. Bảo hiểm

CA2 sẽ cung cấp đa dạng các gói bảo hiểm dịch vụ chứng thực chữ ký số, khách hàng có thể tùy chọn theo mục đích sử dụng.

9.2.2. Trách nhiệm bồi thường thiệt hại cho thuê bao

CA2 có trách nhiệm bồi thường thiệt hại cho thuê bao trong những trường hợp sau:

- Thiệt hại xảy ra khi CA2 để lộ quá trình tạo khóa, lộ khóa bí mật trong quá trình chuyển giao, lưu trữ khóa bí mật và thông tin của thuê bao.

- Thiệt hại xảy ra là hậu quả của việc để lộ thông tin của thuê bao mà CA2 có nghĩa vụ lưu trữ bí mật.

- Thiệt hại xảy ra là đưa lên chứng thư số những thông tin không chính xác so với những thông tin do thuê bao cung cấp.

- Thiệt hại xảy ra là hậu quả của việc không tuân thủ các quy định tại khoản 2, 3 điều 26 Nghị định 26/2007/NĐ- CP.

- CA2 có trách nhiệm bồi thường theo các mức bảo hiểm đã công bố.

9.2.3. Trách nhiệm bồi thường của bên khác

(1). Bồi thường bởi bên vi phạm

Trong phạm vi của luật áp dụng, bên vi phạm bồi thường cho CA2 và cho các bên liên quan trong các trường hợp:

- Xuyên tạc sự thật trong đơn đăng ký cấp chứng thư số.
- Vi phạm tiết lộ những tài liệu trên đơn xin cấp chứng thư số, nếu những thông tin sai lệch hoặc bỏ sót do sự cẩu thả hay do cố ý để đánh lừa bất kỳ tổ chức nào.
- Thiếu sót trong việc bảo vệ khóa riêng, hoặc trong những hành động cảnh báo cần thiết để chống lại việc tiết lộ, mất mát, sửa chữa hoặc sử dụng trái phép khóa riêng của chủ thể cuối cùng hoặc sử dụng tên của chủ thể cuối

cùng (bao gồm, không giới hạn bởi tên thường dùng, hoặc địa chỉ email) xâm phạm quyền sở hữu trí tuệ của bên thứ ba.

(2). Bồi thường do bên nhận

Trong phạm vi của luật áp dụng, thỏa thuận bên nhận và các thỏa thuận khác yêu cầu bên nhận bồi thường cho CA2 và cho các bên liên quan về

- Bên nhận thiếu sót trong việc thực hiện các nghĩa vụ của mình;
- Sự tin tưởng của bên nhận vào chứng thư số không phù hợp trong một số trường hợp; hoặc
- Bên nhận thiếu sót trong việc kiểm tra tình trạng của chứng thư số để xác định xem liệu chứng thư số đó đã hết hạn hay bị thu hồi hay chưa.

9.3. Bảo mật thông tin trong hoạt động CA2

CA2 sẽ tập hợp tất cả các thông tin của thuê bao: tên đầy đủ, số điện thoại, chứng minh thư…. thông tin trong số các thông tin đó được dùng vào các trường thích hợp khi CA2 cấp chứng thư số.

- Các thông tin đã được ban hành trong chứng thư số và CRL không được coi là bí mật.
- CA2 sẽ không thu thập bất kỳ một thông tin bí mật nào ngoại trừ những thông tin phục vụ cho CA2, RA, đại lý trong việc xác minh danh tính, nhận dạng cá nhân phục vụ cho việc cấp chứng thư số của thuê bao.
- CA2 đảm bảo các thông tin cá nhân CA2 đã thu thập sẽ không được dùng cho bất cứ mục đích nào khác.

9.4. Thông tin riêng tư cá nhân

Các thông tin cá nhân được thu thập để phục vụ cho việc đăng ký như:

- Tên của người đăng ký
- Địa chỉ
- Tên tổ chức
- Vị trí
- Điện thoại
- Email
- …

CA2 đảm bảo không cung cấp thông tin này cho bên thứ ba trừ trường hợp khi có yêu cầu của cơ quan quản lý Nhà Nước có thẩm quyền theo quy định của pháp luật.

9.5. Quyền sở hữu trí tuệ

9.5.1. Khóa riêng

Khóa riêng sẽ được xem là một tài sản riêng của người giữ chứng thư số hợp pháp bao gồm cả khóa công khai tương ứng.

9.5.2. Quyền sở hữu trong các thông tin trong chứng thư số và thông tin thu hồi chứng thư số

CA2 có quyền sở hữu trí tuệ đối với toàn bộ thông tin chứng thư số và thông tin thu hồi chứng thư số mà CA2 phát hành.

9.5.3. Quyền sở hữu trong văn bản này

CA2 có quyền sở hữu trí tuệ đối với văn bản này và tất cả các tài liệu liên quan do CA2 phát hành.

9.6. Đại diện và các đảm bảo

Được quy định cụ thể khi chính thức cung cấp dịch vụ.

9.7. Từ chối bảo hành

Quy định cụ thể trong hợp đồng cung cấp dịch vụ.

9.8. Giới hạn trách nhiệm

Quy định cụ thể trong hợp đồng cung cấp dịch vụ.

9.9. Sự bồi thường

Quy định cụ thể trong hợp đồng cung cấp dịch vụ.

9.10. Hiệu lực và chấm dứt

- Văn bản này có hiệu lực và được công nhận từ khi CA2 được cấp phép.
- Kết thúc trong các trường hợp:
    - Hết hạn chứng thư số CA2.
    - Dịch vụ của CA2 chấm dứt.
    - Một phiên bản mới được phát hành.

9.11. Thông báo cá nhân và các giao tiếp với bên tham gia

Được quy định cụ thể khi chính thức cung cấp dịch vụ.

9.12. Sự bổ sung

Mỗi lần thay đổi, tất cả các thay đổi này được công bố trên hệ thống trực tuyến của CA2.

9.13. Thủ tục giải quyết tranh chấp

Quy định cụ thể trong hợp đồng cung cấp và các tài liệu phục vụ cung cấp dịch vụ chứng thực chữ ký số công cộng.

9.14. Luật pháp chủ đạo

Luật pháp Việt nam.

9.15. Phù hợp với luật áp dụng

Quy định cụ thể trong hợp đồng cung cấp.

9.16. Các quy định khác

Quyền và nghĩa vụ các bên:

9.16.1. Quyền và nghĩa vụ của CA2:

CA2 là đơn vị cung cấp chứng thư số và có các đơn vị RA, đại lý được ủy quyền làm nhiệm vụ thẩm định, đăng ký chứng thư cho người dùng cuối.

Quyền của CA2:

- Thay đổi các quy trình nghiệp vụ theo quy định mới ban hành của cơ quan quản lý Nhà Nước có thẩm quyền.

- Được miễn trách nhiệm trong trường hợp hệ thống xử lý, hệ thống truyền tin… bị trục trặc, hoặc vì bất cứ lý do gì ngoài khả năng kiểm soát của CA2.

- Tạm dừng, thu hồi chứng thư số khi phát hiện tài liệu, thông tin do thuê bao cung cấp còn thiếu, không chính xác, không trung thực, sai sự thật.

- Cung cấp thông tin của thuê bao cho cơ quan quản lý Nhà Nước phục vụ công tác đảm bảo an ninh thông tin, điều tra phòng chống tội phạm theo đúng trình tự, thủ tục pháp luật về tố tụng quy định.

Nghĩa vụ của CA2:

- Không cung cấp những thông tin sai lệch.

- Không mắc lỗi thông tin trong chứng thư được cấp.

- Đảm bảo cho chứng thư số của thuê bao theo tiêu chuẩn trong Quy chế này.

- Đảm bảo các dịch vụ theo tiêu chuẩn trong Quy chế này.

9.16.2. Quyền và nghĩa vụ của thuê bao

Quyền của thuê bao:

- Chứng thư số được cấp phát trực tiếp tới thuê bao theo đúng loại chứng thư số mà thuê bao đã yêu cầu.

- Chứng thư số của thuê bao được chấp nhận và hoạt động trong thời gian có hiệu lực của chứng thư số.

- Thuê bao có quyền yêu cầu gia hạn, hay cấp mới chứng thư số

- Thuê bao có quyền yêu cầu CA2 tạm dừng, thu hồi chứng thư số đã cấp và tự chịu trách nhiệm về yêu cầu đó.

Nghĩa vụ của thuê bao:

- Mọi cam kết của thuê bao liên quan đến chứng thư số là đầy đủ, chính xác và hợp lệ. Tất cả các thông tin cung cấp bởi thuê bao và chứa bên trong chứng thư số là đầy đủ, chính xác và hợp lệ. Chứng thư số phải được sử dụng cho các mục đích hợp pháp và tuân theo những yêu cầu trong Quy chế này.

- Thuê bao có nghĩa vụ bảo mật cặp khóa riêng, sử dụng hệ thống tin cậy. Ngăn chặn việc mất cắp, lộ thông tin, hay sửa đổi, phá hủy khóa bí mật. Phải thông báo tới CA2, RA, đại lý ngay khi khóa bí mật bị lộ hay sửa đổi, phá hủy.

- Đồng ý để CA2 công khai thông tin về chứng thư số của thuê bao trên cơ sở dữ liệu về chứng thư số của CA2.

- Thuê bao có nghĩa vụ cung cấp khóa bí mật và những thông tin cần thiết cho các cơ quan tiến hành tố tụng, cơ quan an ninh để phục vụ việc đảm bảo an ninh quốc gia hoặc điều tra theo quy định của pháp luật.

- Không được giả mạo chứng thư số của CA2.

- Nếu có bất kỳ sự thay đổi thông tin nào, đều phải thông báo tới CA2.

- Yêu cầu thu hồi chứng thư số trong trường hợp nhu cầu.

9.16.3. Quyền và nghĩa vụ của người nhận

Quyền của người nhận:

- Người nhận là một cá nhân hay một tập thể được tin tưởng, kiểm tra chứng thư số của đối tác theo thỏa thuận và cam kết giữa hai bên.

- Người nhận có quyền xác nhận các thông tin của thuê bao trong chứng thư số là đúng sự thật.

- Người nhận dựa vào các thông tin trong chứng thư số và các thông tin trong Quy chế này để đưa ra quyết định thực hiện thỏa thuận và cam kết giữa hai bên đối tác.

- Người nhận có thể là một thuê bao hoặc không là một thuê bao của dịch vụ CA2.

Nghĩa vụ của người nhận:

- Chỉ tin tưởng chứng thư số do CA2 cung cấp khi kiểm tra thấy hợp lệ và cập nhật thường xuyên.

- Chỉ tin tưởng vào chứng thư số CA2 đang hoạt động

- Phải thông báo cho CA2, RA, đại lý ngay lập tức nếu nghi ngờ rằng khóa bí mật bị lộ, mất cắp hay sửa đổi, phá hủy.

9.16.4. Quyền và nghĩa vụ của RA, đại lý CA2

Quyền của RA, đại lý CA2:

- Thẩm định thông tin của thuê bao theo ủy quyền của CA2.

- Đăng ký chứng thư số của thuê bao với CA2.

Nghĩa vụ của RA, đại lý CA2:

- RA, đại lý CA2 tổ chức thực hiện kinh doanh đúng loại dịch vụ sản phẩm đã được ủy quyền của CA2 và tuân theo các quy định tại Hợp đồng đại lý.

- Khi RA, đại lý CA2 yêu cầu cấp chứng thư số phải cung cấp đầy đủ hồ sơ, địa chỉ liên hệ của thuê bao để CA2 xác minh trước khi cấp phát. Sau khi CA2 nhận được sự chấp nhận của thuê bao thì thẻ nhớ bảo mật mới được kích hoạt theo quy định của Bộ Thông Tin và Truyền Thông.

- RA, đại lý CA2 có nghĩa vụ tuân thủ Quy chế chứng thực chữ ký số CA2 (CP/CPS)

- RA, đại lý CA2 được CA2 ủy quyền để cung cấp dịch vụ chứng thực chữ ký số CA2 tới khách hàng và là thành phần không thể tách rời với CA2 về mặt pháp lý.

- Các hồ sơ xin cấp chứng thư số của thuê bao phải được lập bởi cán bộ của RA, đại lý CA2 có hiểu biết pháp luật về chữ ký số và dịch vụ chứng thực chữ ký số (thể hiện bằng chứng chỉ được công nhận bởi Root-CA).

- RA, đại lý CA2 có trách nhiệm tư vấn đầy đủ, trung thực cho khách hàng về sản phẩm, dịch vụ của CA2 và chịu trách nhiệm pháp lý trước khách hàng nếu nội dung của sản phẩm dịch vụ không đúng như CA2 cung cấp.

- RA, đại lý CA2 phải sử dụng các mẫu biểu, tài liệu liên quan đến việc cung cấp và sử dụng dịch vụ do CA2 cung cấp. Nếu có bổ sung thì phải có công văn đề nghị kèm cùng biểu mẫu mới.

- Chịu trách nhiệm về thuê bao bị tạm dừng, thu hồi chứng thư số, khóa Token do lỗi của RA, đại lý CA2.

- RA, đại lý CA2 có nghĩa vụ giải trình trước CA2 khi có khiếu nại từ khách hàng và các đại lý khác. Trong trường hợp kết luận xác định lỗi thuộc về RA, đại lý CA2 thì RA, đại lý CA2 chịu trách nhiệm hoàn trả đầy đủ các khoản chi phí đã nhận từ khách hàng, bồi thường đầy đủ tất cả thiệt hại cho bên khiếu nại cũng như tổn thất về uy tín gây ra cho CA2.

- RA, đại lý CA2 có trách nhiệm cung cấp các số liệu, thông tin về công việc định kỳ hoặc đột xuất theo yêu cầu của CA2.

- RA, đại lý CA2 phải thực hiện đầy đủ theo đúng quy trình bán hàng, gia hạn, đối soát và thanh toán quy định tại Hợp đồng hợp tác.