CÔNG TY CỔ PHẦN CÔNG NGHỆ SAVIS

QUY CHẾ CHỨNG THỰC

DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG TRUSTCA

Phiên bản: v1.6

Hà Nội, năm 2023

MỤC LỤC

1 GIỚI THIỆU

1.1 Tổng quan

Công ty Cổ phần Công nghệ SAVIS (SAVIS) là một trong những công ty công nghệ hàng đầu trong khu vực với đội ngũ chuyên môn có kinh nghiệm, tâm huyết, sáng tạo và tài năng; chuyên cung cấp các sản phẩm, giải pháp và dịch vụ công nghệ thông tin cho các khách hàng thuộc khối Chính phủ, Tài chính - Ngân hàng, Truyền hình - Viễn thông, Y tế, Giáo dục...

SAVIS được thành lập từ năm 2004. Trong suốt quá trình hình thành và phát triển, SAVIS không ngừng nghiên cứu và phát triển sản phẩm, dịch vụ theo các xu hướng công nghệ mới nhất nhằm đáp ứng các yêu cầu khắt khe và mang lại sự hài lòng cao nhất cho khách hàng.

Năm 2018, SAVIS vinh dự lần thứ ba liên tiếp được Hiệp hội Phần mềm và Dịch vụ Công nghệ thông tin Việt Nam (VINASA) bình chọn là một trong 50 doanh nghiệp CNTT hàng đầu Việt Nam.

Bên cạnh đó, SAVIS là thành viên của các tổ chức quốc tế lớn như Hội đồng Lưu trữ Quốc tế ICA, Hiệp hội Xây dựng chuẩn mở về truyền hình AMWA, Hiệp hội kiến trúc tích hợp dịch vụ truyền hình FIMS…

Nhiều dự án của SAVIS đã đem lại giá trị lớn cho xã hội, nhiều thành quả được ghi nhận và nhiều sản phẩm được ứng dụng thành công, gây được tiếng vang lớn. Với tầm nhìn sâu rộng, SAVIS hướng đến trở thành một thương hiệu quốc tế có chất lượng, tên tuổi và uy tín trên thị trường khu vực và thế giới.

Công ty SAVIS là một trong số những doanh nghiệp được Bộ Thông tin và Truyền thông lựa chọn cấp phép trở thành đơn vị cung cấp dịch vụ chứng thực chữ ký số. TrustCA là tên gọi của dịch vụ chứng thực chữ ký số công cộng do SAVIS cung cấp. SAVIS có đầy đủ thẩm quyền cấp chứng thư số cho các tổ chức, doanh nghiệp, cá nhân có yêu cầu xin cấp và sử dụng chứng thư số.

TrustCA bao gồm một CA, các tổ chức đăng ký chứng thư số RA và các đại lý được ủy quyền. RA và các đại lý có trách nhiệm tiếp nhận và xác thực thông tin từ phía khách hàng sử dụng dịch vụ.

TrustCA dự kiến triển khai cung cấp dịch vụ chứng thực chữ ký số công cộng phục vụ khách hàng trên toàn quốc với các đối tượng chính khách hàng cá nhân, các cá nhân thuộc tổ chức doanh nghiệp và tổ chức, doanh nghiệp.

Bản Quy chế chứng thực này tuân thủ theo "Khung quy chế chứng thực và chính sách chứng thư" RFC 3647.

1.2 Tên và dấu hiệu nhận diện tài liệu

Tên tài liệu: Quy chế chứng thực dịch vụ Chứng thực chữ ký số công cộng TrustCA.

Dấu hiệu nhận diện tài liệu:

- Văn bản này là một bộ quy chế chứng thực (CPS) tuyên bố về mặt nguyên tắc các chính sách (CP) quản trị của SAVIS trong quá trình cung cấp dịch vụ chứng thực chữ ký số. Bản CP/CPS đưa ra các yêu cầu pháp lý, các yêu cầu về kỹ thuật, cũng như yêu cầu kinh doanh cho quá trình chấp thuận, cấp phát, quản lý, sử dụng, thu hồi và cấp lại chứng thư số trong hệ thống TrustCA. Các yêu cầu của CP/CPS đảm bảo tính bảo mật và toàn vẹn cho dịch vụ TrustCA, được áp dụng cho tất cả các thành phần tham gia dịch vụ chứng thực chữ ký số TrustCA. Bản CP/CPS này không phải thỏa thuận về mặt luật pháp giữa SAVIS và các thực thể sử dụng dịch vụ chứng thực chữ ký số công cộng.

- Mục tiêu của văn bản này là:

+ Nhà cung cấp dịch vụ TrustCA hoạt động với quy chế chứng thực chứng thư số và tuân thủ theo các yêu cầu trong bản CPS này.

+ Cung cấp cho khách hàng sử dụng dịch vụ TrustCA về quá trình xác thực và trách nhiệm của họ.

+ Cung cấp thông tin cho đối tác tin cậy (Relying party) về mức độ đảm bảo mà chứng thư số SAVIS cung cấp.

+ Bản CPS này tuân theo luật pháp Việt Nam cũng như tuân theo các chính sách, quy chế ban hành bởi cơ quan chức năng nhà nước Bộ Thông tin và Truyền thông và các cơ quan chức năng có liên quan khác.

+ Tài liệu được cấu trúc theo chuẩn RFC 3647 (Khung quy chế chứng thực và chính sách chứng thư)

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

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

1.3.1 Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng (Certificate Authority)

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng – CA là thành phần quan trọng nhất trong hệ thống PKI. CA xác thực thông tin thuê bao cũng như đảm bảo tính bí mật và toàn vẹn nội dung thông tin mà các thành phần tham gia dịch vụ chứng thực chữ ký số công cộng trao đổi thông qua hệ thống của CA.

Mỗi CA là tổng thể hệ thống thiết bị phần cứng, phần mềm và đội ngũ quản trị hệ thống nhằm thực hiện các chức năng chính sau:

- Thẩm định tất cả các yêu cầu cấp phát chứng thư từ RA gửi lên;

- Tạo cặp khóa bao gồm khóa công khai và khóa bí mật cho thuê bao;

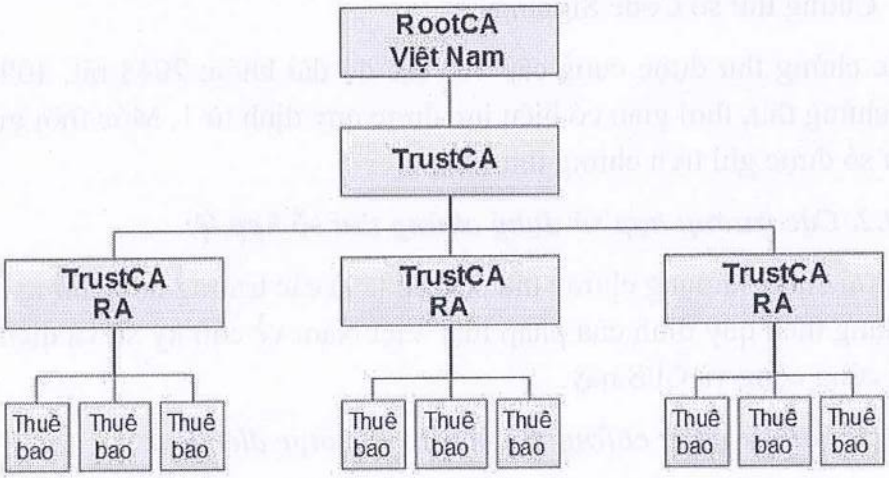
- Cấp, gia hạn, tạm dừng, phục hồi, thu hồi chứng thư số của thuê bao theo quy định của pháp luật và CP/CPS;

- Duy trì trực tuyến cơ sở dữ liệu về chứng thư số (còn hiệu lực, hết hạn, gia hạn, cấp mới, thu hồi);

- Cung cấp các dịch vụ khác có liên quan cho người sử dụng.

CA nhất thiết phải đảm bảo thực hiện các chức năng trên một cách trực tiếp.

Hệ thống TrustCA của SAVIS được tổ chức theo quy định của pháp luật Việt Nam, trực thuộc RootCA (Trung tâm chứng thực điện tử quốc gia) do Bộ Thông tin và Truyền thông quản lý, được trình bày ở Hình 1.



Hình 1: Sơ đồ tổ chức hệ thống TrustCA

1.3.2 Tổ chức tiếp nhận yêu cầu cung cấp dịch vụ và xác thực thông tin thuê bao (Registration Authority - RA)

RA là một tổ chức được CA tin cậy, ủy quyền tiếp nhận yêu cầu cung cấp dịch vụ và xác thực thông tin của thuê bao nhằm đảm bảo tính chính xác các thông tin trong chứng thư số của thuê bao trên toàn hệ thống. Nhiệm vụ của RA bao gồm:

- Tiếp nhận các yêu cầu từ thuê bao (cấp mới, gia hạn, tạm dừng, thu hồi, khôi phục) và chuyển yêu cầu này về TrustCA thông qua hệ thống thiết bị kết nối với TrustCA và phương thức nhân công (đối với các hồ sơ về thông tin thuê bao).

- Xác thực thông tin thuê bao nhằm đảm bảo tính chính xác của các yêu cầu và thông tin về nhân thân của thuê bao.

1.3.3 Thuê bao dịch vụ chứng thực chữ ký số (gọi tắt là thuê bao)

Là các tổ chức/cá nhân có đủ điều kiện theo quy định của pháp luật Việt Nam về dịch vụ chứng thực chữ ký số và quy định tại Quy chế chứng thực chữ ký số này đồng ý sử dụng và được TrustCA cấp chứng thư số.

1.3.4 Người nhận

Là các tổ chức/cá nhân sử dụng dịch vụ xác thực thông tin thuê bao dịch vụ chứng thực chữ ký số thông qua hệ thống cung cấp dịch vụ chữ ký số của SAVIS

1.3.5 Thành phần khác: Không có.

1.4 Mục đích sử dụng chứng thư số

1.4.1 Chứng thư số hợp pháp

Hệ thống TrustCA cung cấp các loại chứng thư số như sau:

- Chứng thư số cho người dùng cá nhân, tổ chức, doanh nghiệp.
- Chứng thư số SSL.
- Chứng thư số Code Signing

Các chứng thư được cung cấp với các độ dài khóa: 2048 bit, 4096 bit. Tùy theo từng loại chứng thư, thời gian có hiệu lực được quy định từ 1. Mức thời gian hiệu lực của chứng thư số được ghi trên chứng thư số.

1.4.2. Các trường hợp sử dụng chứng thư số hợp lệ:

Trường hợp sử dụng chứng thư số hợp lệ là các trường hợp chứng thư số hợp pháp được sử dụng theo quy định của pháp luật Việt Nam về chữ ký số và dịch vụ chứng thực chữ ký số công cộng và CPS này.

1.4.3 Cấm sử dụng chứng thư số vào các mục đích sau

Mọi chứng thư số do hệ thống TrustCA của SAVIS cấp được sử dụng theo các quy định của pháp luật Việt Nam về dịch vụ chứng thực chữ ký số công cộng.

Thuê bao phải sử dụng chứng thư số đã được SAVIS cấp đúng mục đích, đúng quy định của pháp luật và phải chịu mọi trách nhiệm trách nhiệm khi sử dụng chứng thư số trong các trường hợp dòi hỏi mức độ an toàn tuyệt đối có ảnh hưởng trực tiếp đến môi trường tự nhiên, sinh mạng con người.

Chứng thư số do TrustCA 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 TrustCA cấp không được sử dụng ngoài mục đích dân sự như trong lĩnh vực an ninh, quân sự, đảm bảo an ninh quốc gia.

1.5 Quản lý quy chế chứng thực

1.5.1 Tổ chức quản lý quy chế chứng thực:

- Tên tổ chức: Công ty Cổ phần Công nghệ SAVIS

- Địa chỉ: Tầng 9, tòa nhà Việt Á, Số 9 Duy Tân, Phường Dịch Vọng Hậu, Quận Cầu Giấy, TP Hà Nội, Việt Nam.

1.5.2 Thông tin liên hệ

- Tên tổ chức: Công ty Cổ phần Công nghệ SAVIS

- Địa chỉ: Tầng 9, tòa nhà Việt Á, Số 9 Duy Tân, Phường Dịch Vọng Hậu, Quận Cầu Giấy, TP Hà Nội, Việt Nam.

- Điện thoại: 024.37822345
- Email: TrustCA_info@savis.vn
- Website: https://www.trustca.vn

1.5.3 Thủ tục phê duyệt, ban hành quy chế chứng thực

Mọi thay đổi trong Quy chế chứng thực chữ ký số này đều phải đảm bảo tuân thủ đúng quy định của pháp luật Việt Nam về dịch vụ chứng thực chữ ký số công cộng, phù hợp với tiêu chuẩn RFC 3647, và đảm bảo không ảnh hưởng đến quyền lợi của thuê bao.

- Sự phê chuẩn được thực hiện bởi Chủ tịch Hội đồng quản trị Công ty Cổ phần Công nghệ SAVIS.

- Các thay đổi, cập nhật của quy chế chứng thực được ghi lại, thông báo đến Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia, công bố tại: *https://trustca.vn/tai-ve/*

1.6 Các định nghĩa và từ viết tắt

Thuật ngữ - Từ viết tắt	Giải thích
3DES (Triple DES)	Thuật toán mã hóa dữ liệu được cải tiến từ DES bằng cách thêm các vòng mã hóa.
AES (Advanced Encryption Standard)	Chuẩn mã hóa dữ liệu nâng cao được phát triển nhằm thay thế DES. Thuật toán này có ưu điểm nhanh và độ mật cao hơn so với DES.
CA (Certification Authority)	Hệ thống cấp phát chứng thư số
CP (Certificate Policy)	Chính sách chứng thực
CPS (Certificate Practice Statement)	Quy trình chứng thực
CRL (Certificate Revocation List)	Danh sách các chứng thư số bị thu hồi
DC (Digital Certificate)	Chứng thư số
DES (Data Encription Standard)	Chuẩn mã hóa dữ liệu đối xứng được sử dụng rộng rãi.
TrustCA (Trust Certification Authority)	Hệ thống cung cấp dịch vụ chứng thực chữ ký số TrustCA

HSM (Hardware Security Module)	Thiết bị phần cứng bảo mật dùng để tạo, lưu trữ và bảo vệ các khóa sử dụng trong mã hóa. Trong hệ thống PKI, HSM thường được dùng để bảo vệ các cặp khóa quan trọng như các cặp khóa của RootCA và SubCA.
LDAP (Lightweight Directory Access Protocol)	Giao thức chuẩn truy nhập thư mục
PKI (Public Key Infrastructure)	Hạ tầng khoá công khai
OCSP (Online Certificate Status Protocol)	Giao thức kiểm tra trạng thái chứng thư số trực tuyến
RA (Registration Authority)	Đơn vị có thẩm quyền thay mặt CA kiểm tra đăng ký xin chứng thư số cho thuê bao. Việc cấp chứng thư số thực sự do CA đảm nhận.
RootCA (Root Certification Authority)	Hệ thống cấp phát chứng thư số mức gốc
RSA	Thuật toán mã hóa công khai có độ an toàn rất cao sử dụng một cặp khóa. Một khóa dùng để mã, khóa còn lại dùng để giải mã hoặc ngược lại.
SubCA (Subordinate Certification Authority)	Hệ thống cấp phát chứng thư số mức con
USB Token	Thiết bị bảo vệ khóa của người dùng trong hệ thống PKI
CTS	Chứng thư số

2. TRÁCH NHIỆM LƯU TRỮ VÀ CÔNG BỐ THÔNG TIN

2.1. Lưu trữ

TrustCA lưu trữ thông tin, bao gồm:

- Lưu trữ và sử dụng thông tin của thuê bao một cách bí mật, an toàn và chỉ được sử dụng thông tin này vào mục đích liên quan đến chứng thư số.

- Lưu trữ đầy đủ, chính xác và cập nhật thông tin của thuê bao phục vụ việc cấp chứng thư số trong suốt thời gian chứng thư số có hiệu lực và trong thời gian ít nhất 05 năm, kể từ khi chứng thư số hết hiệu lực.

- Lưu trữ đầy đủ, chính xác và cập nhật danh sách các chứng thư số có hiệu lực, đang tạm dừng và đã hết hiệu lực và cho phép, hướng dẫn người sử dụng Internet truy nhập trực tuyến 24 giờ trong ngày và 7 ngày trong tuần.

- Lưu trữ toàn bộ thông tin liên quan đến việc tạm đình chỉ hoặc thu hồi giấy phép và các cơ sở dữ liệu về thuê bao, chứng thư số trong thời gian ít nhất 05 (năm) năm, kể từ khi giấy phép bị tạm đình chỉ hoặc thu hồi.

2.2. Công bố thông tin

Cơ sở dữ liệu thông tin về chứng thư số của hệ thống TrustCA được đảm bảo duy trì thường xuyên, liên tục cung cấp cho thuê bao và người nhận khả năng kiểm tra trạng thái chứng thư số cũng như thông tin về chính sách, Quy chế chứng thực của Công ty. Các thông tin bao gồm:

- Thông tin về danh sách chứng thư số đã được cấp.
- Thông tin về danh sách chứng thư số đã bị tạm dừng/ bị thu hồi.
- Thông tin về chính sách, Quy chế chứng thực chữ ký số.
- Các thông tin khác có liên quan (mẫu hợp đồng, chính sách, …). Các thông tin trên sẽ được công bố tại website của hệ thống TrustCA như sau: *https://trustca.vn/tai-ve/*

2.3. Thời gian, tần suất công bố thông tin

TrustCA 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 thay đổi.

2.4. Kiểm soát truy nhập thông tin

- Các thông tin về chứng thư số được công bố công khai trên website của hệ thống TrustCA chỉ cho phép người sử dụng được quyền xem, download và không được phép chỉnh sửa, bổ sung.
- Các thông tin về chính sách, quy chế chứng thực chữ ký số, thông tin trạng thái chứng thư số hay danh sách chứng thư số bị thu hồi sẽ được cập nhật và công bố công khai khi có thay đổi. Chỉ có SAVIS mới có quyền thay đổi, bổ sung, cập nhật.

3. NHẬN DẠNG VÀ XÁC THỰC YÊU CẦU XIN CẤP CHỨNG THƯ SỐ

3.1. Đặt tên trong chứng thư số

3.1.1 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.509 trong trường Issuer và Subject.

Các thuộc tính trong một DN mà TrustCA 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, sẽ sử dụng Mã số thuế làm Mã định danh. Đối với cơ quan tổ chức nhà nước không có Mã số thuế, 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 Yêu cầu đối với tên

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

Thuê bao không được phép sử dụng tên ẩn danh hoặc bút danh khác với tên thật của mình.

Thê bao không được sử dụng những tên vi phạm quyền sở hữu trí tuệ. Nếu có sự tranh chấp xảy ra về sở hữu thì TrustCA 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.

3.1.3 Cú pháp định dạng tên

Không quy định

3.1.4 Tính duy nhất của tên (Uniqueness Of Names)

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

3.2. Xác minh đề nghị cấp chứng thư số

Quy trình, thủ tục xác minh, kiểm tra hồ sơ đề nghị cấp chứng thư số của thuê bao thực hiện như sau:

3.2.1. Phương thức chứng minh sở hữu khóa bí mật

Để chứng minh thuê bao được cấp chứng thư số sở hữu khóa bí mật của họ, TrustCA đảm bảo các thuê bao gửi yêu cầu cấp chứng thư số theo chuẩn PKCS#10 chứa các thông tin định danh của thuê bao được ký bởi khóa bí mật của thuê bao đó. Việc chứng minh sự sở hữu khóa bí mật không phải thực hiện khi cặp khóa được TrustCA sinh ra trên USB token.

3.2.2. Xác thực định danh của tổ chức

Khi có một đề nghị cấp chứng thư số nhận dạng cho tổ chức, thông tin nhận dạng của tổ chức đó được xác minh . Cần 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 hoặc quyết định thành lập, địa chỉ.
- Tổ chức phải có Đơn xin cấp chứng thư (theo mẫu của TrustCA) kèm theo hồ sơ thuê bao và phải xác nhận trực tiếp vào Đơn xin cấp chứng thư.
- TrustCA 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 mục 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 TrustCA.

3.2.3. Xác thực định danh cá nhân

Khi có một đề nghị cấp chứng thư số nhận dạng cho cá nhân, thông tin nhận dạng của cá nhân đó được xác minh. TrustCA sẽ xác minh các thông tin bắt buộc sau:

- TrustCA 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 TrustCA) có xác nhận của cá nhân, giấy tờ xác thực nhận dạng của cá nhân, các giấy tờ liên quan (nếu có).
- Địa chỉ email khi cần xác thực được xác minh bằng cách yêu cầu trả lời lại email đã được gửi từ TrustCA.

• Quản trị viên của TrustCA cũng phải được cấp chứng thư số, tuy nhiên việc xác thực nhận dạng cá nhân khi cấp chứng thư số không phải thực hiện lại, do đã có xác thực trước khi tham gia quản trị hệ thống.

• Quy trình xác thực nhận dạng của cá nhân đăng ký chứng thư số như sau:

- Người đăng ký chứng thư số nộp hồ sơ cho TrustCA/RA của TrustCA.

- RA của TrustCA thu thập hồ sơ thuê bao và chuyển cho TrustCA (đối với trường hợp Người đăng ký nộp hồ sơ cho RA của TrustCA).

- TrustCA 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 xác minh

Không có quy định

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 mục 3.2.2

- Xác thực cá nhân như mục 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, TrustCA sẽ xác thực bổ sung bằng cách gọi điện hoặc xác thực trực tiếp tại tổ chức về cá nhân đó.

3.2.6. Các tiêu chuẩn cho sự tương tác Không có quy định

3.3. Xác minh đề nghị thay đổi cặp khóa

3.3.1. Xác thực và định danh yêu cầu thay khóa thông thường

Trước khi chứng thư số hết hạn hoặc thuê bao có nhu cầu cấp lại khóa mới để tiếp tục sử dụng dịch vụ, thuê bao cần làm các thủ tục như việc gia hạn chứng thư số. Quy trình tạo lại khóa và phân phối khóa tiến hành như trường hợp cấp mới chứng thư số thông thường.

3.3.2. Xác thực và định danh đối với yêu cầu thay khóa sau khi thu hồi

Đối với các thuê bao sau khi bị thu hồi chứng thư số nếu muốn xin cấp mới chứng thư số khác để sử dụng thì ngoài các nội dung tài liệu phải cung cấp theo quy định đối với trường hợp cấp chứng thư số mới, thuê bao phải cung cấp thêm các thông tin như sau:

- Lý do bị thu hồi chứng thư số.

- Cam kết thực hiện các yêu cầu về giải quyết các lý do bị thu hồi.

Các trường hợp sau sẽ không được cấp lại chứng thư số sau khi đã bị thu hồi:

- Thuê bao sử dụng chứng thư số đã được cấp vào các mục đích trái pháp luật;

- Thuê bao sử dụng các thông tin giả mạo để xin cấp chứng thư số.

3.4. Xác minh đề nghị thu hồi chứng thư số

Chỉ có người đứng tên thuê bao mới được phép thực hiện yêu cầu thu hồi chứng thư số.

Để yêu cầu thu hồi chứng thư số, thuê bao cần liên hệ với TrustCA hoặc RA của TrustCA thông qua phương tiện liên lạc thích hợp bao gồm điện thoại, thư điện tử, giao dịch trực tiếp để chỉ định rõ chứng thư số cụ thể nào cần thu hồi.

Sau khi nhận được yêu cầu thu hồi, TrustCA sẽ tiến hành xác minh bằng phương thức thích hợp và gửi xác nhận cho thuê bao một lần nữa. Chỉ sau khi thuê bao xác nhận lại, TrustCA mới thực hiện thu hồi chứng thư số và công bố danh sách thu hồi lên phương tiện công bố thích hợp. Thông báo thu hồi sẽ được gửi cho thuê bao và đến địa chỉ của đối tượng được chỉ định từ trước.

4. CÁC YÊU CẦU ĐỐI VỚI VÒNG ĐỜI HOẠT ĐỘNG CỦA CHỨNG THƯ SỐ THUÊ BAO

4.1. Yêu cầu cấp chứng thư số

Tổ chức/Cá nhân có nhu cầu cấp chứng thư số nộp hồ sơ yêu cầu cấp chứng thư số cho TrustCA/RA của TrustCA tại các địa điểm giao dịch của TrustCA/RA hoặc nhân viên của TrustCA/RA gặp trực tiếp Tổ chức/Cá nhân để thực hiện (tùy từng trường hợp và/hoặc thỏa thuận giữa TrustCA/RA với Khách hàng).

4.1.1. Đối tượng đề nghị cấp chứng thư số

Các tổ chức/cá nhân đáp ứng đủ các điều kiện sau đây đều có thể xin cấp chứng thư số:

- Là công dân đủ 18 tuổi trở lên. Trường hợp công dân dưới 18 tuổi phải có người đại diện theo pháp luật chịu trách nhiệm về mọi hoạt động sử dụng chứng thư số của người đó.
- Không trong thời gian chấp hành phạt tù hoặc bị quản chế theo quy định của pháp luật.
- Đáp ứng đủ các điều kiện về quản lý và sử dụng chứng thư số theo quy định của pháp luật hiện hành.
- Đối với trường hợp tổ chức xin cấp chứng thư số sử dụng cho các thiết bị thì các thiết bị này đã phải được đầu tư và triển khai trên thực tế.
- Đại diện theo pháp luật của tổ chức đủ điều kiện theo quy định của pháp luật và CPS này có nhu cầu sử dụng chứng thư số.

4.1.2 Hồ sơ đề nghị cấp chứng thư số

Hồ sơ đề nghị cấp chứng thư số thực hiện theo quy định của pháp luật, gồm:

- Đơn cấp chứng thư số theo mẫu của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng, phải có xác nhận nhận của đối tượng xin cấp chứng thư số.

- Giấy tờ kèm theo bao gồm:

• Đối với cá nhân: Chứng minh nhân dân hoặc căn cước công dân hoặc hộ chiếu;

• Đối với tổ chức: Quyết định thành lập hoặc quyết định quy định về chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức hoặc giấy chứng nhận đăng ký doanh nghiệp hoặc giấy chứng nhận đầu tư; chứng minh nhân dân, hoặc căn cước công dân hoặc hộ chiếu của người đại diện theo pháp luật của tổ chức.

Cá nhân, tổ chức có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc nộp bản sao xuất trình kèm bản chính để đối chiếu.

4.2. Xử lý yêu cầu cấp chứng thư số

Trách nhiệm và quy trình cấp chứng thư số cho thuê bao

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

Thuê bao có thể lựa chọn một trong 2 hình thức sau:

- Tạo khóa phía TrustCA: Thuê bao hoàn thành đơn đăng ký chứng thư số và cung cấp tài liệu xác minh thông tin đã kê khai.

- Tạo khóa phía thuê bao: thuê bao đăng ký thực hiện các bước sau:

• Thuê bao hoàn thành đơn đăng ký chứng thư sốvà cung cấp tài liệu xác minh thông tin đã kê khai.

• Tạo hoặc chuẩn bị cặp khóa.

• Gửi khóa công khai trực tiếp cho TrustCA hoặc thông qua RA.

• Chứng minh quyền sở hữu và tính duy nhất của khóa bí mật tương ứng với khóa công khai vừa gửi theo mục 3.2.1.

4.2.2 Chứng thư số của RA

Thuê bao làm thủ tục và ký một thỏa thuận Hợp đồng dịch vụ với TrustCA, các điều khoản và cam kết trong Hợp đồng dịch vụ được mô tả trong phần 9.6.3.

Để đăng ký cấp chứng thư số từ TrustCA, RA phải thực hiện việc ký hợp đồng với TrustCA và tiến hành các thủ tục đăng ký cấp chứng thư số tương tự như các thuê bao.

- TrustCA sẽ tổ chức nghi lễ sinh khóa cho RA.

- Trách nhiệm của RA được làm rõ trong mục 9.6.2.

4.2.3 Xác thực và định danh

Sau khi nhận được yêu cầu xin cấp chứng thư số của tổ chức/cá nhân thì bộ phận RA sẽ tiến hành việc xác thực và định danh thông tin về tổ chức/cá nhân đó theo quy trình nêu tại mục 3.2.

4.2.4 Chấp nhận hoặc từ chối cấp chứng thư số

- TrustCA chấp nhận yêu cầu cấp chứng thư số nếu thỏa mãn tất cả các điều kiện sau:

- Thực hiện xác thực định danh thành công tất cả các thông tin về đối tượng yêu cầu cấp chứng thư số theo mục 3.2.
- Đối tượng yêu cầu cấp chứng thư số nộp đầy đủ phí dịch vụ cấp chứng thư số cho TrustCA.

- TrustCA từ chối yêu cầu cấp chứng thư số nếu thỏa mãn một trong các điều kiện sau:

- Xác thực định danh không thành công ít nhất một trong các thông tin về đối tượng yêu cầu cấp chứng thư số theo mục 3.2.
- Đối tượng yêu cầu cấp chứng thư số không cung cấp đủ tài liệu theo yêu cầu của TrustCA
- Đối tượng yêu cầu cấp chứng thư số không trả lời yêu cầu liên lạc trong hạn thời gian xác định.
- Đối tượng yêu cầu cấp chứng thư số chưa thanh toán phí dịch vụ cấp chứng thư số.
- Có căn cứ cho rằng việc TrustCA cấp chứng thư số cho đối tượng yêu cầu có thể ảnh hưởng tới uy tín và độ tin cậy của TrustCA.

4.2.5 Thời gian xử lý yêu cầu cấp chứng thư số

TrustCA có trách nhiệm xử lý yêu cầu chứng thư số trong một khoảng thời gian phù hợp. Không quy định thời gian hoàn thành quá trình xử lý một yêu cầu cấp chứng thư số khi có thỏa thuận trong Hợp đồng dịch vụ hoặc CPS, tuy nhiên thời gian tối đa là 5 ngày làm việc.

4.3. Cấp chứng thư số

4.3.1 Hoạt động của CA khi phát hành chứng thư số

Chứng thư số được ban hành sau khi TrustCA chấp nhận đơn xin cấp chứng thư số trực tiếp từ thuê bao hoặc thông qua RA của TrustCA. TrustCA 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 về phát hành chứng thư số

TrustCA sau khi ban hành chứng thư số cho sẽ thông báo cho thuê bao (trực tiếp hoặc gián tiếp thông qua RA). Thuê bao có thể lấy được chứng thư số bằng cách:

- Nhận qua USB token.
- Tải về từ trang Web của TrustCA.

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

Thuê bao thể hiện sự chấp nhận một chứng thư số khi ký vào biên bản giao nhận chứng thư số của TrustCA. Biên bản giao nhận có sự xác nhận thông tin trên chứng thư số được cấp là chính xác của thuê bao. Biên bản giao nhận này được TrustCA lưu trữ.

4.4.2 CA công bố chứng thư số

Sau khi thuê bao chấp nhận chứng thư số (theo mục 4.4.1), TrustCA sẽ công bố chứng thư số khi thuê bao sử dụng USB token lần đầu tiên.

Chứng thư số sau khi được phát hành sẽ được công bố trên Web của TrustCA và cơ sở dữ liệu LDAP theo mục 2.

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

TrustCA 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 Cách sử dụng chứng thư số và khóa bí mật của thuê bao

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

Các thuê bao có trách nhiệm bảo vệ khóa bí mật của mình, không được sử dụng khóa bí mật nếu chứng thư số tương ứng hết hạn hay bị thu hồi.

4.5.2 Cách sử dụng chứng thư số và khóa công khai của người nhận

Người nhận sẽ được TrustCA đảm bảo các điều khoản về độ tin cậy của chứng thư số. Độ tin cậy của chứng thư số được xác định dựa vào từng hoàn cảnh cụ thể. Nếu hoàn cảnh chỉ ra rằng cần phải thêm sự bảo đảm thì người nhận phải đạt được sự bảo đảm mà nó cần phải có.

Trước khi được tin cậy, 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 Key Usage).

- Mục đích sử dụng của chứng thư số thể hiện trong các tài liệu: thỏa thuận thuê bao, quy chế chứng thực, chính sách chứng thư số.

- Trạng thái của chứng thư số: kiểm tra trạng thái thu hồi của chứng thư số cũng như các chứng thư số khác trong chuỗi chứng thư số

4.6. Gia hạn chứng thư số

Gia hạn chứng thư số là quá trình ban hành một chứng thư số mới cho thuê bao mà ngoài thời hạn sử dụng chứng thư số, mọi thông tin khác trong chứng thư số đều không thay đổi

4.6.1 Các trường hợp được gia hạn chứng thư số của thuê bao

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

4.6.2 Đối tượng được phép yêu cầu gia hạn

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

Sau khi thuê bao điền đầy đủ các thông tin yêu cầu gia hạn chứng thư số theo mẫu và gửi đến bộ phận RA thì bộ phận RA có trách nhiệm tiếp nhận, xác thực thông tin của thuê bao theo mục 3.3.

Trường hợp xác thực thông tin yêu cầu của thuê bao là chính xác thì bộ phận RA chuyển yêu cầu này về bộ phận CA để tiến hành gia hạn cho thuê bao. Trường hợp thông tin yêu cầu của thuê bao là không chính xác, bộ phận RA có trách nhiệm thông báo cho khách hàng biết rõ lý do từ chối gia hạn chứng thư số.

4.6.4 Thông báo về việc phát hành 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 Cách thức thể hiện sự chấp nhận gia hạn chứng thư số

Tương tự mục 4.4.1

4.6.6 Công bố chứng thư số được gia hạn

Tương tự mục 4.4.2

4.6.7 Thông báo đến đối tượng khác về việc gia hạn chứng thư số

Tương tự mục 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 Đối tượng được phép yêu cầu thay đổi khóa

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

4.7.2 Các trường hợp được thay đổi cặp khóa của thuê bao

Trước khi hết hạn một chứng thư số, thuê bao đổi khóa chứng thư số để tiếp tục duy trì giá trị sử dụng của chứng thư số. Một chứng thư số có thể được đổi khóa sau khi đã hết hạn.

Trong trường thuê bao nghi ngờ bị lộ khóa bí mật, thuê bao cần yêu cầu thu hồi khóa cũ và đổi khóa mới để duy trì giá trị sử dụng của chứng thư số.

4.7.3 Xử lý yêu cầu thay đổi cặp khóa

TrustCA /RA tiến hành xác minh yêu cầu đổi khóa chứng thư số như trong mục 3.3.

Nếu thông tin thuê bao không thay đổi, chứng thư số mới của thuê bao sẽ được ban hành ngay sau khi TrustCA nhận được yêu cầu mà không cần có sự hiện diện vật lý của thuê bao tại TrustCA hoặc RA

4.7.4 Thông báo phát hành chứng thư 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 Cách thức thể hiện sự chấp nhận thay khóa chứng thư số

Tương tự phần 4.4.1

4.7.6 Công bố chứng thư số đã thay khóa

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

Xem phần 4.1.1

4.8.2 Các trường hợp được thay đổi thông tin chứng thư số

Sửa đổi chứng thư số xem như yêu cầu cấp chứng chỉ số theo phần 4.1.1

4.8.3 Xử lý yêu cầu thay đổi thông tin chứng thư số

Xem phần 3.2

4.8.4 Thông báo cho thuê bao về việc thay đổi thông tin chứng thư số

Xem phần 4.3.2

4.8.5 Cách thức thể hiện sự chấp nhận thay đổi thông tin chứng thư số

Xem phần 4.4.1

4.8.6 Công bố chứng thư số đã thay đổi

Xem phần 4.4.2

4.8.7 Thông báo cho các đối tượng khác về việc thay đổi chứng thư số

Xem phần 4.4.3

4.9. Tạm dừng và thu hồi chứng thư số

4.9.1 Đối tượng được phép yêu cầu thu hồi chứng thư số

Đối với chứng thư số của thuê bao:

- Thuê bao đăng ký chứng thư số có quyền yêu cầu thu hồi chứng thư số.
- TrustCA/RA có quyền yêu cầu thu hồi chứng thư số mà nó đã duyệt cho thuê bao đó.

Các cơ quan nhà nước có thẩm quyền có thể yêu cầu thu hồi chứng thư số nếu như hồ sơ không đầy đủ.

4.9.2 Các trường hợp được phép 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 (TrustCA, 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, CA sẽ thu hồi chứng thư số sau khi xác minh.

Chứng thư số bị thu hồi trong những trường hợp sau:

- Khóa bí mật của thuê bao có chứng thư số bị lộ.
- Thỏa thuận với thuê bao kết thúc trước thời hạn.
- Thông tin trong chứng thư số sai khác so với thực tế. - Thuê bao vi phạm thỏa thuận đã ký với TrustCA.
- 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 TrustCA.

4.9.3 Quy trình, thủ tục yêu cầu thu hồi chứng thư số

Bước 1: Yêu cầu thu hồi:

Thuê bao sẽ gửi yêu cầu thu hồi chứng thư số ngay lập tức khi phát hiện hay nghi ngờ khóa bí mật bị mất/lộ.

Quản trị hệ thống CA/RA sẽ gửi yêu cầu thu hồi chứng thư số ngay khi nhận được yêu cầu từ thuê bao hoặc nhận sau khi xác thực thông tin phàn nàn.

Sau khi RA của TrustCA tiếp nhận yêu cầu thu hồi, việc xác thực đề nghị thu hồi sẽ được tiến hành theo nội dung mục 3.4.

Trường hợp kết quả trả về chưa hợp lý, RA sẽ hủy bỏ đề nghị và gửi kết quả tới thuê bao.

Trường hợp kết quả trả về hợp lý, RA có trách nhiệm báo cho TrustCA yêu cầu thu hồi chứng thư số của thuê bao. TrustCA sẽ gửi thông báo thu hồi kèm theo lý do thu hồi trực tiếp đến thuê bao hoặc thông qua RA đã tiếp nhận và xác thực đề nghị thu hồi.

Bước 2: Thu hồi chứng thư số

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

CRL cho chứng thư số của thuê bao được cập nhật ít nhất một ngày một lần và được công bố ngay lập tức sau khi được tạo ra.

Chứng thư số hết hạn sẽ bị loại khỏi CRL.

Bước 3: Kiểm tra việc thu hồi

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

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

4.9.4 Thông báo, công bố việc thu hồi chứng thư số của thuê bao

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

Thông tin thu hồi và trạng thái chứng thư số được công bố qua trang Web và OCSP như trong mục 2.2. TrustCA không sử dụng dạng thông tin trạng thái thu hồi nào khác ngoài CRL và OCSP.

4.9.5 Công bố việc cập nhật danh sách thu hồi chứng thư số (CRL)

CRL cho chứng thư số của thuê bao được cập nhật ít nhất một ngày một lần và được công bố ngay lập tức sau khi được tạo ra.

4.9.6 Các điều kiện đặc biệt khi khóa bị xâm phạm

Khi khóa bí mật TrustCA bị mất/lộ hoặc nghi ngờ mất/lộ, TrustCA 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.

4.9.7 Đối tượng được phép yêu cầu tạm dừng

Không có quy định

4.9.8 Các trường hợp tạm dừng

Không có quy định

4.9.9 Thủ tục yêu cầu tạm dừng

Không có quy định

4.9.10 Giới hạn thời gian tạm dừng

Không có quy định

4.10. Dịch vụ kiểm tra trạng thái chứng thư số

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

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

4.10.2 Tính sẵn sàng của dịch vụ

Dịch vụ trạng thái chứng thư số được duy trì 24x7. Nếu có gián đoạn sẽ có thông báo trước 24 giờ.

4.10.3 Các đặc tính khác

OCSP là dịch vụ tùy chọn, có phí.

4.11 Chấm dứt dịch vụ thuê bao

Các trường hợp thuê bao chấm dứt dịch vụ:

- Thuê bao đã hết hạn mà không làm mới.
- Thu hồi chứng thư số xảy ra mà không xin cấp một chứng thư số mới.

Thủ tục chấm dứt dịch vụ: Không quy định

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

Không có quy định.

5. KIỂM SOÁT, QUẢN LÝ VÀ VẬN HÀNH

5.1 Kiểm soát an toàn, an ninh vật lý

5.1.1 Vị trí lắp đặt và xây dựng

Hệ thống thiết bị CA được đặt tại trung tâm dữ liệu của Công ty FPT Telecom được xây dựng theo tiêu chuẩn Tier 3 quốc tế của Uptime Institude. Các thiết bị được trang bị nhiều lớp bảo vệ khác nhau: bảo vệ vật lý vòng ngoài của tòa nhà, bảo vệ khu đặt thiết bị, bảo vệ tủ đặt thiết bị, bảo vệ chống cháy nổ.

5.1.2 Truy cập vật lý

Hệ thống TrustCA được bảo vệ nhất bởi các lớp an ninh vật lý, phải vượt qua được lớp bảo vệ thấp trước khi có thể tiếp cận được lớp bảo vệ cao hơn. Hệ thống camera giám sát hoạt động 24/7 cho phép ghi lại toàn bộ các hoạt động.

- Lớp bảo vệ vòng ngoài - bảo vệ tòa nhà.
- Lớp bảo vệ khu đặt thiết bị.

Việc truy nhập qua các lớp được được kiểm soát chặt chẽ, chỉ những người có quyền truy cập mới được truy nhập vào các lớp tương ứng. Càng truy nhập vào các lớp quản lý yêu cầu an ninh cao, sự hạn chế càng tăng. Tất cả mọi truy nhập đều được ghi nhận.

5.1.3 Điều hòa và Nguồn điện

TrustCA sử dụng nguồn điện ổn định, được thực hiện như sau:

- Sử dụng hệ thống lưu điện 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.

TrustCA sử dụng hệ thống điều hòa chính xác để làm mát cho hệ thống thiết bị. Hệ thống cảnh báo khi nhiệt độ vượt ngưỡng cho phép.

5.1.4 Chống nước

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

5.1.5 Phòng cháy, chữa cháy

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

5.1.6 Thiết bị lưu trữ dữ liệu

Phương tiện lưu trữ dữ liệu của CA được bảo vệ tương đương với mức độ quan trong của dữ liệu mà hệ thống đó lưu trữ.

Phương tiện lưu trữ dữ liệu backup cũng được bảo vệ tương tự như hệ thống chính.

5.1.7 Hệ thống dự phòng

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

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

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

5.2 Quy trình kiểm soát

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

Người được tin tưởng là những người có thể truy nhập 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.

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.

TrustCA thiết lập các chính sách và thủ tục kiểm soát đảm bảo có nhiều người tin tưởng thực hiện một công việc nhạy cảm như truy cập, điều khiển module phần cứng mã hóa.

Các chính sách và thủ tục kiểm soát này của TrustCA luôn đòi hỏi có ít nhất 2 người để thực hiện các công việc nhạy cảm.

5.2.2 Nhận dạng và xác thực cho từng thành viên

Mọi cá nhân trước khi trở thành người được tin tưởng trong hệ thống CA đều phải được xác minh nhân thân, nhận dạng và trình độ.

CA đảm bảo rằng các cá nhân hoàn toàn được tin tưởng trước khi thực hiện các công việc nhạy cảm.

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

Các vai trò cần phải có sự phân tách nhiệm vụ, bao gồm nhưng không giới hạn:

- Xác minh thông tin trong đơn xin cấp chứng thư số
- Chấp nhận, từ chối hay các xử lý khác với đơn xin cấp chứng thư số, yêu cầu thu hồi, làm mới chứng thư số
- Ban hành, thu hồi chứng thư số.
- Quản lý thông tin, yêu cầu của thuê bao.

5.3 Kiểm soát nhân sự

5.3.1 Yêu cầu kinh nghiệm, bằng cấp, chứng chỉ của đội ngũ nhân sự liên quan đến quản lý và vận hành hệ thống

- Những người tin cậy của CA được xác minh dựa trên: khả năng và kinh nghiệm chuyên môn đáp ứng các nhu cầu công việc, các bằng chứng chứng minh sự trong sạch về lý lịch.

Thủ tục kiểm tra lý lịch:

Trước khi bổ nhiệm nhân viên vào một nhiệm vụ cần được tin tưởng, CA kiểm tra các thông tin sau:

- Kiểm tra, xác minh thông tin theo sơ yếu lý lịch.
- Xác minh trình độ học vấn cao nhất đạt được
- Xem xét các thông tin tiền án/tiền sự (nếu có).
- Yêu cầu về bằng cấp, chứng chỉ:

Nhân sự chịu trách nhiệm quản trị hệ thống, vận hành hệ thống và cấp chứng thư số, bảo đảm an toàn thông tin của hệ thống: có bằng đại học trở lên, chuyên ngành an toàn thông tin hoặc công nghệ thông tin hoặc điện tử viễn thông.

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 CA. Những người này cũng phải tuân theo các tiêu chuẩn an ninh như nhân viên của CA. Nếu các cố vấn không đáp ứng đủ các tiêu chí, họ chỉ được phép thực hiện công việc khi có sự giám sát của người được tin tưởng của CA.

5.3.2 Yêu cầu đào tạo

CA thực hiện các chương trình đào tạo nội bộ cho đội ngũ nhân viên, quá trình đào tạo được thực hiện theo quy trình, có ghi lại nhật ký đào tạo cho từng cá nhân.

Chương trình huấn luyện của CA hướng tới trách nhiệm cụ thể của mỗi nhân viên, nội dụng huấn luyện bao gồm:

- Các khái niệm PKI cơ bản.
- Trách nhiệm công việc.
- Các chính sách và thủ tục an ninh của CA.
- Sử dụng và vận hành các thiết bị phần cứng và phần mềm.
- Xử lý các sự cố.
- Các thủ tục duy trì tính liên tục của dịch vụ khi có thảm họa.

CA duy trì và thực hiện chương trình đào tạo với tần suất đào tạo và thời gian đào tạo lại đảm bảo các nhân viên đều thành thạo và thực hiện tốt công việc được giao.

5.3.3 Xử lý đối với hành vi vi phạm

CA thực hiện các hình thức kỷ luật các nhân viên có những hành động không được phép, vi phạm các chính sách, thủ tục của CA. Hình thức kỷ luật có thể gồm khiển trách, kéo dài thời hạn nâng lương không quá 06 tháng, cách chức, hoặc sa thải, tùy thuộc vào mức độ nghiêm trọng của vi phạm.

Ngoài ra, trường hợp hành vi vi phạm gây thiệt hại vật chất, thì ngoài các hình thức kỷ luật, nhân viên phải chịu trách nhiệm vật chất và bồi thường thiệt hại cho CA theo quy định của Nội quy lao động và quy định của pháp luật.

5.4. Các quy trình ghi nhật ký hệ thống

5.4.1 Các loại sự kiện được ghi lại

CA lưu trữ nhật ký tự động mọi thao tác trên hệ thống cấp phát và hệ thống máy tính. Các sự kiện được ghi lại bao gồm:

- Có tác động, thay đổi cấu hình hệ thống hoặc có sự cố xảy ra trong hệ thống
- Có thao tác tạo, thay đổi hoặc thu hồi cặp khóa.
- Có truy cập vào nơi đặt thiết bị phục vụ cho CA và trụ sở làm việc

5.4.2 Cách thức ghi vào nhật ký

Mỗi bản ghi nhật ký gồm các thông tin sau:

- Thời gian của bản ghi.
- Thứ tự của bản ghi (đối với bản ghi được tạo tự động).
- Đối tượng tạo ra bản ghi.
- Loại bản ghi.

5.4.3 Tần suất xử lý nhật ký

Các nhật ký sẽ được lưu lại tức thời khi có sự kiện liên quan đến hệ thống CA và các sự kiện sẽ được xử lý hằng ngày.

5.4.4 Thời gian lưu trữ nhật ký

CA quy định thời hạn lưu trữ nhật ký đối với từng loại sự kiện như sau:

- Thông tin: thời hạn lưu ít nhất 1 năm
- Cảnh báo: Thời hạn lưu ít nhất 1 năm
- Lỗi: Thời hạn lưu ít nhất 1 năm
- Nhật ký vào ra trụ sở và nơi đặt thiết bị: thời gian lưu là 5 năm

5.4.5 Bảo vệ nhật ký

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

5.4.6 Thủ tục sao lưu nhật ký

Nhật ký được backup theo chế độ backup chung của CA.

5.4.7 Hệ thống kiểm tra

Phương thức ghi sổ nhật ký kiểm toán có 2 loại:

- Log: Tự động được lưu lại trên các thiết bị và sẽ được tổng hợp xử lý
- Sổ nhật ký: Dưới dạng giấy

5.4.8 Thông báo cho đối tượng gây ra sự kiện

Khi một sự kiện được ghi nhật ký, không có thông báo cho đối tượng gây ra sự kiện đó.

5.4.9 Đánh giá lỗ hổng hệ thống

CA đưa ra quy trình đánh giá hệ thống hàng tháng và trên kết quả đánh giá sẽ phân tích và tìm ra các lỗ hổng và sự cố có thể xảy ra trong tương lai. Giúp phòng ngừa rủi ro.

5.5 Lưu trữ các bản ghi

5.5.1 Các loại bản ghi cần lưu trữ

CA sẽ lưu trữ các thông tin sau:

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

5.5.2 Thời hạn lưu trữ các bản ghi

Thời gian lưu trữ các bản ghi ít nhất là 10 năm.

5.5.3 Bảo vệ bản ghi nhật ký

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

5.5.4 Quy trình lưu trữ bản ghi

a) Các thủ tục sao lưu lưu trữ

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

b) Nhãn thời gian của các bản ghi

Nhãn thời gian có thể áp dụng hoặc không áp dụng. Nếu áp dụng, phải sử dụng thời gian ở nguồn đáng tin cậy.

c) Hệ thống lưu trữ

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

d) Thủ tục lấy và kiểm tra thông tin lưu trữ

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

5.6. Thay đổi khóa

Trước khi chứng thư số của CA hết hạn, theo quy định, CA sẽ xin cấp một chứng thư số mới cho CA của mình và sử dụng chứng thư số mới để ban hành chứng thư số cho các thuê bao.

Trong giai đoạn này, chứng thư số do CA ban hành có thời gian sử dụng không quá thời gian sử dụng chứng thư số của CA được dùng để ký lên nó.

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

Trước khi hết hạn chứng thư số của CA, các thủ tục được ban hành cho phép chuyển tiếp (changeover) từ cặp khóa cũ sang cặp khóa mới cho các thực thể thuộc phạm vi quản lý của CA. Quá trình chuyển tiếp khóa của CA đảm bảo rằng:

- CA chỉ ban hành chứng thư số mới cho thuê bao trước thời điểm nhất định so với ngày hết hạn cặp khóa. Thời điểm này là thời điểm tạm dừng ban hành chứng thư số, do pháp luật quy định.
- Khi nhận được yêu cầu ban hành chứng thư số sau thời điểm tạm dừng ban hành chứng thư số trên, CA sử dụng cặp khóa mới để ban hành chứng thư số cho thuê bao

5.7 Xử lý khi có sự cố, thảm họa và phục hồi

5.7.1 Các thủ tục kiểm soát sự cố và thảm họa

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

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

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

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

Khi khóa bí mật của CA nghi ngờ bị mất/lộ, CA sẽ thực hiện thủ tục xử lý khi khóa bị lộ. Nếu chứng thư số của CA bị thu hồi, các thủ tục sau sẽ được thực hiện: □ Trạng thái thu hồi chứng thư số của CA sẽ được công bố bởi RootCA.

- CA cố gắng thông báo cho toàn bộ người nhận trong hệ thống CA dừng sử dụng các chứng thư số do CA ban hành.
- CA xin cấp chứng thư số mới từ RootCA và ban hành chứng thư số cho các thuê bao của mình để họ tiếp tục sử dụng.

5.7.4 Khả năng phục hồi hoạt động sau thảm họa

Luôn có hệ thống dự phòng và sẽ hoạt động khi có thảm họa xảy ra. Thời gian nhậm nhất để phục hồi là 8 giờ.

5.8 Dừng hoạt động của CA/RA

Trong trường hợp CA và RA dừng hoạt động, SAVIS sẽ thực hiện chuyển tất cả các thuê bao qua nhà cung cấp dịch vụ khác hoặc thực hiện đền bù và thu hồi các chứng thư cần thiết và thông báo công khai về việc dừng hoạt động của CA và RA.

6. KIỂM SOÁT AN TOÀN KỸ THUẬT

6.1 Tạo và phân phối khóa

6.1.1 Sinh cặp khóa

Các cặp khóa sử dụng cho toàn bộ dịch vụ cung cấp PKI và các chủ thể cuối cùng phải được tạo ra theo cách mà chỉ có người giữ khóa mới có thể biết được. Một số cách thực hiện:

- Yêu cầu tới tất cả những người tham gia trong quá trình tạo khóa phải sử dụng một hệ thống an toàn
- Những người tham gia trực tiếp không tiết lộ các khóa riêng tới bất kỳ người nào khác
- Các khóa được tạo ra trong phần cứng Token, HSM hoặc SmartCard trong đó có khóa riêng không thể bị lấy ra hoặc tiết lộ.

Như đã đề cập ở trên, toàn bộ khóa của nhà cung cấp dịch vụ PKI (không chỉ là bộ phận lưu trữ) phải được sinh và lưu trữ trong Token, HSM hoặc SmartCard. Cặp khóa cho bộ phận lưu trữ và chủ thể cuối cùng có thể được sinh và lưu trữ trong phần cứng hoặc phần mềm môđun mã hóa.

6.1.2 Kích thước cặp khóa

Độ lớn nhỏ nhất của khóa là 2048 bit và sử dụng thuật toán RSA là thuật toán sinh khóa.

6.1.3 Quy trình phân phối cặp khóa

a) Gửi khóa bí mật cho thuê bao

Trong hầu hết các trường hợp, một khóa riêng sẽ được tạo ra và được duy trì trong phạm vi mã hóa của mô đun mã hóa. Nếu như chính người giữ mô đun mã hóa tạo khóa thì sẽ không cần chuyển khóa riêng. Nếu một khóa không được tạo ra bởi người dự định giữ khóa, thì những người tạo ra khóa trong mô đun mã hóa (như smart card) phải đảm bảo phân phối mô đun mã hóa một cách bảo mật tới người giữ khóa.

Trách nhiệm lưu trữ và giữ mô đun mã hóa phải được duy trì đến khi khóa được phân phối tới người giữ khóa. Người nhận sẽ xác nhận về việc nhận được mô dun mã hóa đến CA hoặc RA. Nếu chủ thể cuối cùng tạo ra khóa và khóa này sẽ được lưu trữ và sử

dụng bởi các ứng dụng tạo khóa hoặc trên một phần cứng Token, HSM hoặc SmartCard của chủ thể cuối cùng, thì không cần thực hiện các bước tiếp theo. Nếu khóa được lấy ra để sử dụng bằng các ứng dụng hoặc ở các địa điểm khác, thì cấu trúc bảo mật dữ liệu phải được thực hiện. Các file kết quả phải được lưu trữ trong một phương tiện lưu trữ bằng băng từ hoặc được chuyển tiếp bằng điện tử.

b) Gửi khóa công khai cho CA

Các khóa công khai phải được chuyển đến TrustCA một cách an toàn và bảo mật như là một thông điệp yêu cầu của chứng thư số. Quá trình phân phối này cũng có thể được thực hiện không phải là phương tiện điện tử. Các phương tiện này có thể bao gồm, nhưng không giới hạn, đĩa mềm (hoặc các phương tiện lưu trữ khác), gửi qua mail đã đăng ký hoặc người đưa thư, hoặc bởi sự phân phối của một Token hoặc HSM đến CA cho sự tạo khóa vùng tại điểm cấp phát hoặc yêu cầu chứng thư số. Các phương tiện offline sẽ bao gồm quá trình kiểm tra nhận dạng và không bị hạn chế chứng minh quyền sở hữu khóa riêng tương ứng. Bất kỳ các phương tiện nào khác được sử dụng cho việc phân phối khóa công khai sẽ được quy định trong CPS hoặc thỏa thuận chứng thư số. Trong các trường hợp khi các cặp khóa được tạo *ra bởi TrustCA đại diện cho chủ thể cuối cùng, CA sẽ thực hiện cơ chế an toàn để đảm* bảo rằng Token chứa cặp khóa phải được gửi an toàn đến chủ thể cuối cùng phù hợp, và Token đó không được kích hoạt trước khi chủ thể cuối cùng phù hợp nhận được.

c) Gửi khóa công khai của CA cho người nhận

Khóa công khai tương ứng với khóa ký riêng CA của TrustCA có thể được phân phối đến các chủ thể cuối cùng trong một giao dịch trực tuyến theo cơ chế thích hợp.

6.2 Kiểm soát và bảo vệ khóa bí mật

6.2.1 Tiêu chuẩn kỹ thuật đối với thiết bị mật mã

TrustCA sử dụng HSM của hãng nCipher -Thales đạt chuẩn FIPS PUB 140-2 Level 3 cho Quản lý mật mã trên thiết bị phần cứng phục vụ khởi tạo khoá mật mã CA, sinh chữ ký CA, xác nhận, lưu trữ và sao lưu/ phục hồi khoá CA.

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

a) Kiểm soát khóa riêng nhiều người dùng

TrustCA áp dụng xác thực nhiều lớp sử dụng thẻ thông minh (xác thực n thẻ / 1 quyền) mỗi khi quản trị và khởi động hệ thống mật mã.

b) Ủy thác giữa khóa riêng

Không quy định.

c) Sao lưu khóa riêng

Một bên tham gia có thể lựa chọn để sao lưu khóa riêng của mình. Nếu như vậy thì khóa phải được sao lưu và lưu trữ tại một mức độ an ninh và được bảo vệ không thấp hơn mức đã được quy định.

d) Lưu trữ khóa riêng

Theo thoả thuận với chủ thể dùng cuối.

e) Quá trình đưa Private key vào môđun mã hóa

Quá trình tạo khóa sẽ được thực hiện qua các bước: khởi tạo kích hoạt thiết bị mã hóa phần cứng (token), thông qua phần mềm quản trị cho việc tạo khóa để thực hiện tạo cặp khóa trực tiếp vào thiết bị mã hóa. Hệ thống TrustCA sử dụng các thuật toán RSA2048 cho việc tạo khóa và AES-256 cho việc mã hóa khóa bí mật. Thiết bị mã hóa đạt tiêu chuẩn bảo mật FIPS 140-2 Level 3.

Khóa riêng chỉ có thể chuyển ra khỏi thiết bị mã hóa khi thực hiện quá trình sao lưu khóa riêng và không thể tồn tại bên ngoài thiết bị mã hóa ở bất cứ thời gian nào.

f) Lưu trữ khóa riêng trên môđun mã hóa

Quy trình lưu trữ khóa riêng vào môđun mã hóa được tiến hành theo hướng dẫn của nhà cung cấp thiết bị và tuân theo chuẩn do Bộ Thông tin và Truyền thông ban hành.

g) Phương pháp kích hoạt khóa riêng

Việc kích hoạt được thực hiện bởi mã số PIN. Khi không hoạt động, các khóa riêng phải được đặt trong môi trường mã hóa hoàn toàn

h) Phương pháp làm khóa riêng ngừng hoạt động

Các môđun mã hóa không được kích hoạt khi không có sự giám sát hoặc khi tự do truy cập. Sau khi sử dụng, chúng phải ngừng hoạt động, ví dụ sử dung một thủ tục hướng dẫn thoát ra bằng tay hoặc một chương trình tự ngừng hoạt động sau một khoảng thời gian. Khi không sử dụng, phần cứng môđun mã hóa sẽ được gỡ bỏ và lưu trữ, trừ khi chúng hoàn toàn nằm trong sử kiểm soát của chủ thể cuối cùng.

i) Phương pháp hủy bỏ khóa riêng

Các khóa riêng sẽ được hủy bỏ khi chúng không cần thiết, hoặc khi các chứng thư số tương ứng hết hạn hoặc bị thu hồi. Đối với phần mềm môđun mã hóa, việc phá hủy có thể thực hiện bằng cách ghi đè lên dữ liệu. Với Token, điều này được thực hiện bằng cách thực hiện một lệnh "zeroize". Sự phá hủy có tính chất vật lý sẽ không được áp dụng.

j) Đánh giá môđun mã hóa

Áp dụng chuẩn đánh giá thiết bị mật mã quy dịnh tại nội dung 6.2.1.

6.2.3 Dự phòng khóa bí mật

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

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

6.3.1 Lưu trữ cặp khóa

CA phải giữ lại toàn bộ chứng thực của khóa công khai

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

Chứng thư số có hiệu lực từ khi thuê bao được cấp chứng thư. Tùy theo từng loại chứng thư, thời gian có hiệu lực từ 06 tháng đến 03 năm. Mức thời gian có hiệu lực của chứng thư số được ghi trên chứng thư số.

Thời gian hiệu lực của cặp khóa sau khi chứng thư hết hạn theo hướng dẫn của Bộ Thông tin và Truyền thông. Mức thời gian sử dụng cặp khóa tương ứng với thời hạn có hiệu lực của chứng thư số và được ghi trên chứng thư số.

6.4 Kích hoạt dữ liệu

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

Một mật khẩu, PIN hoặc các dữ liệu kích hoạt khác sẽ được sử dụng để bảo vệ sự truy cập đến khóa riêng. Thành viên của TrustCA tạo ra và cài đặt dữ liệu kích hoạt cho khóa bí mật sử dụng những phương pháp để bảo vệ dữ liệu kích hoạt đối với các phạm vi cần thiết nhằm tránh sự mất mát, sự ăn cắp, sự cải biến, sự tiết lộ trái phép, hoặc sử dụng trái phép các khóa bí mật. Dữ liệu kích hoạt có thể được người dùng lựa chọn.

Đối với phạm vi mật khẩu được sử dụng cho dữ liệu kích hoạt, những người đăng ký sẽ thiết lập mật khẩu, những mật khẩu này không dễ dàng bị đoán nhận hoặc bị tấn công bởi kiểu tấn công từ điển.

6.4.2. Quy trình kích hoạt dữ liệu

Nếu dữ liệu kích hoạt phải được chuyển tới người dùng cuối cùng, nó sẽ thực hiện qua một kênh bảo vệ thích hợp, và phân biệt trong thời gian và địa điểm từ môđun mã hóa liên kết. Nếu điều này không thực hiện bằng tay, người dùng cuối cùng sẽ được thông báo ngày gửi, phương pháp gửi và dự kiến ngày nhận dữ liệu kích hoạt. Như là một phần của phương pháp phân phối, các người dùng cuối cùng nên có hiểu biết về việc nhận mô đun mã hóa và dữ liệu kích hoạt. Thêm nữa các người dùng cuối cùng cũng nên nhận (và có sự hiểu biết) các thông tin đối với việc sử dụng và điều khiển môđun mã hóa. Xem trong mục 1.2 phần VI.

6.5 Kiểm soát an ninh của máy tính

6.5.1 Yêu cầu an ninh đối với hệ thống máy tính

Tất cả các máy chủ CA phải bao gồm cả các chức năng sau đây hoặc được cung cấp bởi hệ điều hành hoặc thông qua sự kết hợp giữa hệ điều hành, ứng dụng PKI, và cơ chế bảo vệ:

- Kiểm soát truy cập tới các dịch vụ của CA và vai trò PKI
- Thi hành phân công nhiệm vụ trong vai trò PKI
- Nhận dạng và xác thực vai trò của PKI và nhận dạng liên quan
- Sử dụng lại đối tượng hoặc phân chia bộ nhớ truy xuất ngẫu nhiên CA
- Sử dụng mật mã cho các phiên giao dịch và an toàn cơ sở dữ liệu

- Lưu trữ quá trình hoạt động của CA và chủ thể cuối cùng cũng như dữ liệu kiểm tra
- Kiểm tra các sự kiện liên quan đến an ninh bảo mật
- Tự kiểm tra tính bảo mật liên quan tới các chức năng CA
- Phương thức nhận dạng đáng tin cậy trong vai trò của PKI và các nhận dạng liên quan.
- Cơ chế khôi phục cho các Key và hệ thống CA
- Đảm bảo tính toàn vẹn trong giới hạn an ninh thực hiện.
- Mức độ an ninh của máy tính

Thiết bị CA sẽ đáp ứng hoạt động cho ít nhất mức độ C2 [TCSEC] hoặc E2/F-C2[ITSEC] hoặc tương đương. Thiết bị CA hoạt động tương đương mức độ C2 ít nhất có khả năng:

- Tự động bảo vệ;
- Xử lý độc lập;
- Kiểm soát truy cập tùy ý;
- Kiểm soát đối tượng tái sử dụng;
- I&A cá nhân; và
- Bản ghi kiểm tra được bảo vệ

6.5.2 Định kỳ đánh giá an ninh hệ thống máy tính

TrustCA thực hiện đánh giá an ninh hệ thống máy tính định kỳ ít nhất mỗi năm một lần.

6.6 Kiểm soát an ninh quy trình sử dụng

6.6.1 Kiểm soát phát triển hệ thống

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

Phần mềm được TrustCA phát triển sẽ được ký số đảm bảo trong quá trình phân phối không bị thay đổi nội dung hoặc phiên bản. Chữ ký trên phần mềm sẽ được kiểm tra khi phần mềm được cài đặt.

6.6.2 Kiểm soát quản lý an ninh, an toàn

TrustCA có các cơ chế, chính sách để kiểm soát và giám sát cấu hình hệ thống TrustCA. Với các phần mềm được TrustCA phát triển sẽ được ký số đảm bảo tính toàn vẹn khi chuyển đến người dùng.

6.6.3 Kiểm soát an ninh, an toàn vòng đời

TrustCA không quy định cụ thể quy trình kiểm soát an ninh vòng đời phát triển, triển khai và vận hành hệ thống cung cấp dịch vụ của TrustCA.

6.7 Giám sát an ninh hệ thống mạng

TrustCA thực hiện bảo vệ tất cả các chức năng của CA và RA có sử dụng mạng tuân theo các tiêu chuẩn quy định trong chính sách về bảo mật nhằm ngăn chặn các truy cập trái phép và các hoạt động tấn công khác.

6.8. Dấu thời gian (Time-Stamping)

Dấu thời gian sử dụng để làm bằng chứng và xác thực sự tồn tại của dữ liệu tại một mốc thời gian nhất định. Tài liệu, hồ sơ, thông điệp điện tử khi được đóng dấu thời gian sẽ đảm bảo tính chống chối bỏ về thời gian và tính toàn vẹn dữ liệu.

TrustCA sử dụng độ dài khóa RSA từ 2048 bit trở lên và chuẩn băm SHA-256 hoặc cao hơn cho tính an toàn, bảo mật tối đa.

Dịch vụ cấp dấu thời gian của TrustCA đáp ứng tiêu chuẩn ký nâng cao cho lưu trữ lâu dài: Bao gồm các tiêu chuẩn ký số nâng cao như: CAdES, XAdES, PAdES, ETSI ES-A… cho lưu trữ điện tử lâu dài và vĩnh viễn.

7. ĐỊNH DẠNG CHỨNG THƯ SỐ, DANH SÁCH THU HỒI CHỨNG THƯ SỐ (CRL), GIAO THỨC KIỂM TRA TRẠNG THÁI CHỨNG THƯ SỐ TRỰC TUYẾN (OCSP)

7.1 Định dạng của chứng thư số

Chứng thư số sẽ chứa các khóa công khai được sử dụng cho việc xác thực người gửi thông điệp điện tử và xác nhận sự toàn vẹn của các thông điệp- ví dụ, các khóa công khai được sử dụng cho việc xác thực chữ ký số. Chứng thư số sẽ được cấp phát theo chuẩn X509 phiên bản 3 trừ khi sử dụng định dạng khác là cần thiết để tạo điều kiện an toàn trong giao tiếp không dây hoặc thao tác với các thiết bị sử dụng WAP (Giao thức ứng dụng không dây) hoặc các công nghệ khác. Mọi yêu cầu đối với ARP trong CP/CPS đều sử dụng hoặc thực hiện theo chuẩn chứng thư số. Khi áp dụng, chứng thư số sẽ bao gồm một tham chiếu đến OID cho các loại chứng thư số được xác định bởi CP/CPS này theo trường hợp thích hợp. CP/CPS hoặc các tài liệu công khai khác sẽ nhận dạng các phần hỗ trợ mở rộng chứng thư số các chứng thư số được mở rộng, và mức hỗ trợ cho sự mở rộng đó.

TrustCA cung cấp chứng thư số X509 phiên bản 3

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

Tên trường	Giá trị
Serial Number	Giá trị duy nhất được gán chỗ mỗi tên phân biệt. Giá trị này được sinh theo quy tắc do TrustCA quy định.

Signature Algorithm	Định danh (OID) của thuật toán được sử dụng để ký chứng thư số.
Issuer DN	Tên của chứng thư số
Valid From	Thời diểm có hiệu lực của chứng thư số tuân thủ theo tiêu chuẩn RFC 5280
Valid To	Thời điểm hết hiệu lực của chứng thư số tuân thủ theo tiêu chuẩn RFC 5280
Subject DN	Tên của thuê bao tuân thủ theo tiêu chuẩn RFC 5280
Subject Public Key	Khoá công cộng tương ứng với khóa bí mật của chứng thư số
Signature	Chữ ký số được tạo và lưu theo định dạng tuân thủ theo tiêu chuẩn RFC 5280

Các trường thông tin mở rộng chứng thư số:

- Các trường mở rộng có thể có trong chứng thư số của TrustCA và thường phải có sự thoả thuận nhất trí giữa thuê bao và TrustCA.
- Không có sự mở rộng nào sẽ chỉnh sửa hoặc làm tổn hại đến việc sử dụng các trường cơ sở X509.

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

Các CRL sẽ được phát hành theo phiên bản X509 định dạng 3. CP/CPS hoặc các tài liệu công khai khác sẽ nhận dạng các phần hỗ trợ mở rộng chứng thư số các chứng thư số được mở rộng, và mức hỗ trợ cho sự mở rộng đó.

- Đường dẫn công bố thông tin chứng thư số bị thu hồi http://crl.trustca.vn/trustca-sha256.crl

Các trường thông tin trong CRL tối thiểu gồm các thông tin sau:

Tên trường	Giá trị
Version	Mô tả phiên bản của CRL
Signture Algorithm	Mô tả phương pháp nhận diện chữ ký số mà TrustCA sử dụng để ký vào CRL
Issuer	Thực thể ký và phát hành CRL
Effective Date	Ngày có hiệu lực của CRL
Next Update	Ngày cập nhật phiên bản tiếp theo của CRL

Revoked Certificates	Danh sách các chứng thư số bị thu hồi, bao gồm số hiệu (Serial Number) của chứng thư số bị thu hồi và ngày thu hồi

7.2.1 Số phiên bản của CRL

Các CRL sẽ được phát hành theo phiên bản X509 định dạng 3.

7.2.2 CRL và các trường mở rộng của CRL

Không quy định.

7.3 Định dạng giao thức kiểm tra trạng thái chứng thư số trực tuyến (OCSP)

OCSP là giao thức cho phép lấy thông tin cập nhật về trạng thái thu hồi của một chứng thư số cụ thể. Dịch vụ OCSP tuân theo RFC 6960. Đường dẫn truy cập: http://ocsp.trustca.vn

7.3.1 Số phiên bản của OCSP

TrustCA cung cấp dịch vụ OCSP Version 1 theo RFC 6960.

7.3.2 Trường mở rộng của OCSP

Không quy định.

8. KIỂM TRA TÍNH TUÂN THỦ VÀ CÁC ĐÁNH GIÁ KHÁC

8.1 Tần suất và các tình huống kiểm tra kỹ thuật

- TrustCA thực hiện kiểm tra kỹ thuật định kỳ của TrustCA/RA ít nhất mỗi năm một lần.
- TrustCA kiểm tra kỹ thuật đột xuất khi có yêu cầu của Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia.
- Ngoài các kiểm tra kỹ thuật trên, TrustCA có thể thực hiện những kiểm tra kỹ thuật khác để đảm bảo tính tin cậy của TrustCA. Các kiểm tra kỹ thuật đó có thể được thực hiện bởi một đơn vị bên ngoài

8.2 Đơn vị, người thực hiện kiểm tra kỹ thuật

- Người thực hiện kiểm tra kỹ thuật được chỉ định bởi RootCA để thực hiện các cuộc kiểm tra kỹ thuật TrustCA.
- Kiểm tra kỹ thuật được thực hiện bởi những người không phụ thuộc vào TrustCA.

8.3. Các nội dung kiểm tra kỹ thuật

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

- Hạ tầng hệ thống.
- Các quy trình quản lý khóa.

- Quy trình vận hành hệ thống.
- Các nội dung khác theo yêu cầu của đơn vị kiểm tra kỹ thuật.

8.4. Xử lý khi phát hiện sai sót

8.4.1. Mô tả kịch bản xử lý khi phát hiện sai sót, sự cố xảy ra:

- Sau khi có báo cáo kiểm tra kỹ thuật, TrustCA sẽ làm việc với RootCA về những nội dung chưa phù hợp.
- TrustCA 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.

8.4.2. Dịch vụ của TrustCA sẽ bị ngừng trong các tình huống sau:

- Báo cáo kiểm tra kỹ thuật cho thấy có lỗi nghiêm trọng có thể ảnh hưởng ngay lập tức tới an an ninh của hệ thống TrustCA.
- TrustCA thực hiện kế hoạch xử lý nhưng không có kết quả.

8.5. Công bố kết quả kiểm tra kỹ thuật

Báo cáo kết quả kiểm tra kỹ thuật được TrustCA công bố tại https://trustca.vn/

8.6. Tần suất và các trường hợp đánh giá.

- Các hoạt động của TrustCA sẽ được kiểm toán thực hiện định kỳ hàng năm hoặc theo yêu cầu từ RootCA. Các hoạt động kiểm toán có thể được thực hiện bởi một đơn vị ngoài.
- Ngoài ra TrustCA thực hiện tự đánh giá hoạt động của TrustCA/RA định kỳ ít nhất mỗi năm một lần hoặc theo thời hạn chứng chỉ của các thành phần hệ thống bởi đơn vị kiểm định đáp ứng yêu cầu theo quy định của pháp luật và yêu cầu của TrustCA. Ngoài các trường hợp đánh giá trên, TrustCA có thể thực hiện những đánh giá khác để đảm bảo tính tin cậy của TrustCA.
- TrustCA kiểm tra đánh giá đột xuất khi có yêu cầu của Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia.

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

Đơn vị kiểm định thực hiện kiểm tra TrustCA phải là đơn vị độc lập có khả năng sau:

- Có năng lực thành thạo về công nghệ hạ tầng khóa công khai, công cụ và kĩ thuật an toàn thông tin.
- Được chứng nhận bởi RootCA.

9. CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC

9.1 Phí

Tất cả những thông báo về việc tính phí phải được gửi tới người sử dụng và RP.

9.1.1 Phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số

Phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số theo quy định tại Thông tư số 17/2018/TT-BTC ngày 09/02/2018 của Bộ Tài chính sửa đổi, bổ sung một số

điều của Thông tư số 305/2016/TT-BTC và Thông tư số 305/2016/TT-BTC ngày 15/11/2016 của Bộ Tài chính quy định mức thu, chế độ thu, nộp, quản lý và sử dụng phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số.

9.1.2 Giá cấp, gia hạn và thu hồi chứng thư số

TrustCA có thể thiết lập và tính một mức phí hợp lý cho việc phát hành chứng thư số khi cung cấp dịch vụ I&A, đăng ký và phát hành chứng thư số tới các chủ thể cuối cùng tiềm năng.

9.1.3 Các loại chi phí khác

a) Phí truy cập chứng thư số

TrustCA có thể thiết lập và tính một mức phí hợp lý cho dịch vụ cung cấp thông tin về tình trạng chứng thư số.

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

TrustCA và RA có thể thiết lập và tính một mức phí hợp lý cho dịch vụ cung cấp thông tin về sự thu hồi của chứng thư số.

c) Phí cho những dịch vụ khác như là thông tin về chính sách

TrustCA và RA có thể thiết lập và tính một mức phí hợp lý cho dịch vụ khác. Tuy nhiên không tính mức phí cho việc truy cập để xem xét các điều khoản trong chính sách CP.

9.2 Trách nhiệm tài chính

9.2.1 Nghĩa vụ nộp phí trong quá trình cung cấp dịch vụ

CA thực hiện nghĩa vụ nộp phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số theo quy định của pháp luật.

9.2.2 Nghĩa vụ tài chính trong trường hợp bị thu hồi giấy phép

Trong trường hợp bị thu hồi giấy phép, CA có nghĩa vụ:

- Giải quyết các rủi ro và các khoản đền bù xảy ra trong quá trình cung cấp dịch vụ do lỗi của CA.
- Thanh toán chi phí tiếp nhận và duy trì cơ sở dữ liệu của doanh nghiệp.

9.3 Bảo mật các thông tin nghiệp vụ

9.3.1 Phạm vi các thông tin nghiệp vụ cần được bảo vệ

Các thông tin nghiệp vụ được đảm bảo bí mật bao gồm:

- Các thông tin liên quan đến TrustCA, trừ khóa công khai;
- Các thông tin nhân thân của thuê bao;
- Khóa bí mật của thuê bao;

- Các dữ liệu chi tiết liên quan đến kiểm tra kỹ thuật;
- Các thông tin về đảm bảo an toàn, khắc phục sự cố thảm họa, …
- Một số thông tin khác theo thoả thuận giữa thuê bao và TrustCA.

Những thông tin nằm ngoài phạm vi bí mật bao gồm: Các thông tin về danh sách chứng thư số, chứng thư số bị thu hồi, trạng thái chứng thư số không thuộc phạm vi thông tin bí mật và được công bố công khai bởi TrustCA và các thông tin không được chỉ rõ trong mục 9.3.1 được coi là không bí mật.

9.3.2 Trách nhiệm bảo mật thông tin nghiệp vụ

TrustCA có trách nhiệm thực hiện các biện pháp đảm bảo an ninh cho các thông tin bí mật.

9.4 Bảo mật thông tin cá nhân

9.4.1 Phạm vi thông tin bí mật cần được bảo vệ

Tất cả các dữ liệu cá nhân, thông tin cá nhân riêng tư hoặc tổ chức được thuê bao cung cấp trong quá trình làm thủ tục cấp chứng thư số hay các yêu cầu khác trong quá trình quản lý, sử dụng chứng thư số được bảo vệ bí mật.

Những thông tin ngoài phạm vi thông tin bí mật cần được bảo vệ: Các thông tin ngoài phạm vi thông tin cá nhân không thuộc phạm vi phải bảo vệ bí mật bao gồm các thông tin công khai trên chứng thư số đã cấp cho thuê bao, hoặc các thông tin khác theo thoả thuận giữa thuê bao và TrustCA.

9.4.2 Trách nhiệm bảo mật thông tin cá nhân

Những người tham gia vào dịch vụ TrustCA nhận các thông tin mật phải đảm bảo tính mật cho các thông tin này không được tiết lộ cho bên thứ 3 và tuân thủ theo quy định của pháp luật trong phạm vi quyền hạn của mình.

TrustCA sẽ đảm bảo bí mật các thông tin bí mật cá nhân thuê bao, không được cung cấp cho bên thứ 3 trừ trường hợp có yêu cầu của cơ quan nhà nước có thẩm quyền hoặc thoả thuận khác giữa thuê bao và TrustCA, cụ thể:

- Việc sử dụng thông tin riêng tư của thuê bao chỉ được phép khi có sự đồng ý của thuê bao hoặc thoả thuận giữa thuê bao và TrustCA trong hợp đồng cung cấp dịch vụ chứng thực chữ ký số.
- Trong trường hợp có yêu cầu của cơ quan chức năng, TrustCA sẽ cung cấp thông tin bí mật cho cơ quan quan pháp luật có thẩm quyền và tuân thủ theo quy định của pháp luật.

9.4.3. Chính sách bảo vệ thông tin cá nhân.

TrustCA cam kết có chính sách bảo vệ dữ liệu cá nhân tuân thủ Nghị định 13/2023/NĐ-CP, đồng thời xây dựng hệ thống kỹ thuật và phương án kỹ thuật đảm bảo tuân thủ theo quy định của Nghị định 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân.

- Về dữ liệu cá nhân của khách hàng, TrustCA lưu trữ ở môi trường được đảm bảo an ninh và an toàn. Chi tiết quy định tại "Phương án kỹ thuật hệ thống cung cấp dịch vụ chứng thực chữ ký số công cộng TrustCA"

- Đối với Khách hàng sử dụng dịch vụ Chứng thực chữ ký số của TrustCA, Khách hàng sẽ được thông báo về "Điều Kiện và Điều Khoản về bảo vệ Dữ liệu cá nhân" của TrustCA ("Điều Kiện Điều Khoản") qua các phương thức:

  - "Điều Kiện và Điều Khoản về bảo vệ dữ liệu cá nhân" của TrustCA được công bố công khai tại trụ sở, đại lý, chi nhánh và website https://trustca.vn/download/dkdk_bvdlcn_savis_trustca.pdf.
  - Điều Kiện Điều Khoản được Nhân viên của TrustCA phổ biến cho các Khách hàng sử dụng dịch vụ của TrustCA trong quá trình tư vấn dịch vụ.
  - Trong trường hợp khách hàng giao dịch trực tiếp với nhân viên của TrustCA, Khách hàng ký ghi rõ họ tên và số giấy tờ tùy thân vào Điều Kiện Điều Khoản trước khi thực hiện cung cấp thông tin để sử dụng dịch vụ của TrustCA.

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

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

9.5.3 Quyền sở hữu trong CP/CPS này

TrustCA có quyền sở hữu trí tuệ đối với CP và CPS và tất cả các tài liệu liên quan do nó phát hành

9.6 Tuyên bố và cam kết

9.6.1 Đại diện TrustCA tuyên bố và cam kết

TrustCA đảm bảo rằng:

- Không làm sai lệch thông tin đăng ký chứng thư số được cung cấp bởi đối tượng đăng ký;
- Không có lỗi trong quá trình duyệt và ban hành chứng thư số;
- Chứng thư số do TrustCA ban hành đáp ứng các yêu cầu trong bản CPS này;
- Dịch vụ thu hồi chứng thư số và sử dụng kho lưu trữ phù hợp với tiêu chuẩn trong CPS này;

- Thỏa thuận với thuê bao có thể có thêm các tuyên bố và cam kết khác.

9.6.2 Đại diện RA tuyên bố và cam kết

Các RA đảm bảo rằng:

- Không làm sai lệch thông tin đăng ký chứng thư số được cung cấp bởi đối tượng đăng ký;
- Không có lỗi trong quá trình duyệt và ban hành chứng thư số;
- Chứng thư số do TrustCA ban hành đáp ứng các yêu cầu trong bản CPS này;
- Dịch vụ thu hồi chứng thư số và sử dụng kho lưu trữ phù hợp với tiêu chuẩn trong CPS này;
- Thỏa thuận với thuê bao có thể có thêm các tuyên bố và cam kết khác.

9.6.3 Đại diện thuê bao tuyên bố và cam kết

Thuê bao cam kết rằng:

- Mỗi chữ ký số được tạo sử dụng khóa bí mật tương ứng với khóa công khai liệt kê trong chứng thư số là chữ ký số của thuê bao. Chứng thư số được chấp nhận và hoạt động (khi chưa hết hạn hay bị thu hồi) trong thời gian chữ ký số này được tạo.
- Khóa bí mật được bảo vệ và người không có thẩm quyền không thể truy cập vào khóa này.
- Tất cả các cam kết được đưa ra bởi thuê bao trong ứng dụng chứng thư số là đúng sự thật.
- Tất cả những thông tin cung cấp bởi thuê bao và chứa bên trong chứng thư số là đúng sự thật.
- Chứng thư số được sử dụng cho các mục đích hợp pháp và tuân theo những yêu cầu trong CPS này.
- Thuê bao là người dùng cuối và không phải là một CA, không được phép sử dụng khóa bí mật kết hợp với bất kì khóa công khai nào được liệt kê trong chứng thư số cho các mục đích ký số, hay đưa ra CRL, như là một CA.
- Hợp đồng dịch vụ giữa TrustCA với thuê bao có thể có thêm các thỏa thuận và cam kết khác

9.6.4 Đại diện người nhận tuyên bố và cam kết

Người nhận tuyên bố và cam kết rằng:

- Thỏa thuận với người nhận yêu cầu người nhận phải có đủ thông tin để đưa ra một quyết định dựa vào các thông tin trong chứng thư số. Họ có trách nhiệm quyết định tin tưởng hay không vào các thông tin trong chứng thư số. Người

nhận phải chịu trách nhiệm pháp lý nếu vi phạm các điều khoản về nghĩa vụ của người nhận quy định trong CPS này.

- Thỏa thuận giữa TrustCA và người nhận có thể bao gồm thêm các tuyên bố và cam kết khác

9.7 Từ chối trách nhiệm

Trong các trường hợp quy định của pháp luật cho phép, hợp đồng thuê bao và người nhận có thể bị TrustCA từ chối trách nhiệm.

9.8 Giới hạn trách nhiệm

Trong giới hạn của pháp luật cho phép, hợp đồng thuê bao và người nhận có thể có giới hạn khả năng chịu trách nhiệm pháp lý của TrustCA.

Trách nhiệm pháp lý của thuê bao và TrustCA sẽ được thiết lập trong hợp đồng cung cấp dịch vụ.

9.9 Sự bồi thường

9.9.1 Vấn đề bồi thường của thuê bao

Trong phạm vi pháp luật cho phép, thuê bao phải bồi thường cho TrustCA khi xảy ra một trong các trường hợp sau:

- Thuê bao cung cấp thông tin sai lệch, không đúng với thực tế hoặc giả mạo khi yêu cầu cung cấp dịch vụ chứng thư số;
- Lỗi của thuê bao để lộ những nhân tố, yếu tố liên quan đến dịch vụ chứng thư số, sự bỏ sót hay làm sai lệch do sự cẩu thả hay với mục đích lừa đảo;

  Lỗi của thuê bao trong việc bảo vệ khóa bí mật, sử dụng hệ thống tin cậy, hoặc không thực hiện các biện pháp phòng ngừa cần thiết để tránh gây hậu quả;
- Việc sử dụng tên của thuê bao (kể cả việc không giới hạn tên chung, tên miền, hoặc địa chỉ thư điện tử) vi phạm quyền sở hữu trí tuệ của một bên thứ ba.
- Hợp đồng dịch vụ có thể có thêm các thỏa thuận khác.

9.9.2 Vấn đề bồi thường của người nhận

Trong trường hợp pháp luật cho phép, TrustCA có quyền yêu cầu người nhận bồi thường trong các trường hợp sau:

- Lỗi của người nhận trong việc thực thi nghĩa vụ với một bên đối tác;
- Sự tin cậy của người nhận về một chứng thư số không được đáp ứng trong một số trường hợp;
- Lỗi của người nhận trong việc kiểm tra trạng thái của chứng thư số để xác định chứng thư số đã hết hạn hay bị thu hồi.
- Hợp đồng với người nhận sẽ bao gồm thêm một số nghĩa vụ khác.

9.10 Hiệu lực của Quy chế chứng thực

- CP/CPS có hiệu lực và được công nhận từ khi TrustCA chính thức đi vào hoạt động. Các điều sửa đổi, bổ sung cho CPS này có hiệu lực khi có sự công bố từ kho lưu trữ của dịch vụ TrustCA.
- Kết thúc của CP/CPS trong các trường hợp:
  - Hết hạn chứng thư số TrustCA
  - Dịch vụ của TrustCA chấm dứt
  - Một phiên bản mới của CP/CPS được công nhận

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

TrustCA sẽ sử dụng các biện pháp thích hợp để thông báo cho các bên liên quan về nội dung sửa đổi, bổ sung CPS này.

9.12 Bổ sung, thay đổi quy chế chứng thực

9.12.1 Các trường hợp được sửa đổi, bổ sung quy chế

TrustCA có quyền quyết định việc sửa đổi, bổ sung quy chế là cần thiết hay không cần thiết. TrustCA sẽ quyết định sửa đổi, bổ sung quy chế khi xảy ra một trong các trường hợp sau đây:

- Thay đổi quy định của pháp luật làm ảnh hưởng đến tính hợp pháp, hợp lệ của quy chế;
- Nội dung của quy chế không còn phù hợp với hoạt động của TrustCA.

9.12.2 Quy trình sửa đổi, bổ sung quy chế

Quy chế này được sửa đổi, bổ sung bởi TrustCA. Nội dung sửa đổi, bổ sung có thể ở dạng tài liệu chứa tất cả những điều sửa đổi, bổ sung cho CPS hoặc ở dạng phiên bản cập nhật.

Nội dung sửa đổi, bổ sung CPS sẽ được thông báo đến Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia và được công bố sau khi nhận được sự đồng ý bằng văn bản của Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia đối với các nội dung thay đổi.

Khi tiến hành sửa đổi, bổ sung quy chế:

- Người dùng sẽ không được thông báo trước về sự thay đổi của các chính sách TrustCA như CP/CPS
- Bất cứ sửa đổi nào sẽ được chỉ rõ bởi TrustCA và được chấp thuận bởi TrustCA – PMA
- Các thay đổi nhỏ trong tài liệu này có thể được sửa đổi mà không cần sự chấp thuận của TrustCA –PMA

- Các thay đổi lớn như thay đổi về chính sách, thay đổi về các điều khiển kỹ thuật an toàn phải được sự chấp thuận của TrustCA –PMA - OID mới sẽ được gán cho những thay đổi trong tài liệu này
- Mỗi lần thay đổi, sẽ được thông báo bằng email tới tất cả các bên liên quan. Tất cả các thay đổi này cũng được công bố trên kho lưu trữ của TrustCA

9.13 Thủ tục giải quyết tranh chấp

9.13.1 Tranh chấp giữa TrustCA, đối tác và thuê bao

Việc giải quyết tranh chấp giữa TrustCA, đối tác và thuê bao phải tuân thủ theo các điều khoản được ghi trong hợp đồng và trên cơ sở quy định của pháp luật Việt Nam.

9.13.2 Tranh chấp với thuê bao hay người nhận

Trường hợp này được thực hiện theo quy định của pháp luật.

9.14 Hệ thống pháp lý điều chỉnh

Tài liệu Quy chế chứng thực của TrustCA được điều chỉnh bởi các văn bản quy phạm pháp luật, bao gồm:

- Luật giao dịch điện tử năm 2005;
- Nghị định số 130/2018/NĐ-CP ngày 27/9/2020 của Chính phủ quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số;
- Thông tư 31/2020/TT-BTTTT về Quy chế chứng thực của Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia do Bộ trưởng Bộ Thông tin và Truyền thông ban hành;
- Các văn bản pháp luật khác có liên quan.

CPS này được xây dựng theo quy định của pháp luật nước Cộng hòa xã hội chủ nghĩa Việt Nam. Trong quá trình cung cấp, sử dụng dịch vụ TrustCA cũng như giải quyết các tranh chấp phát sinh, các thành phần tham gia dịch vụ TrustCA cũng như các bên liên quan sẽ áp dụng pháp luật của nước Cộng hòa xã hội chủ nghĩa Việt Nam.

9.15 Phù hợp với pháp luật hiện hành

Trong trường hợp có sự xung đột giữa quy định của văn bản pháp luật và bản CPS này, quy định tại văn bản pháp luật sẽ có hiệu lực.

9.16 Các điều khoản chung

9.16.1.Điều khoản thỏa thuận chung

Không có quy định.

9.16.2. Trách nhiệm

Trách nhiệm của các bên được quy định và giới hạn theo hợp đồng đã ký kết.

9.16.3. Tính độc lập của các điều khoản

Trong trường hợp một điều khoản hay sự sửa đổi bổ sung của CPS được giữ lại không thể thi hành được bởi quy định của pháp luật hoặc quyết định của cơ quan nhà nước có thẩm quyền thì phần còn lại của Quy chế vẫn có hiệu lực.

9.16.4. Sự thực thi (quyền ủy nhiệm và quyền khước từ)

Bất kỳ một bên nào chiếm ưu thế trong những tranh chấp nảy sinh ngoài hợp đồng đều được quyền ủy nhiệm hoặc quyền khước từ do sự vi phạm một trong các điều khoản trong hợp đồng.

9.16.5. Chính sách bắt buộc thực thi

Trong phạm vi pháp luật cho phép, thỏa thuận của thuê bao và thỏa thuận bên liên quan bắt buộc phải tuân theo các điều khoản bảo vệ dịch vụ TrustCA.

9.17 Các điều khoản khác

Không quy định.

PHỤ LỤC 1

Danh mục định nghĩa và thuật ngữ viết tắt

Bảng 1: Danh mục định nghĩa và thuật ngữ

Thuật ngữ	Giải thích
Chấp nhận (Accept or Acceptance)	Chủ thể cuối cùng hành động theo quyền và nghĩa vụ tương ứng với chứng thư số tuân theo thỏa thuận chứng thư số (Certificate Agreement) hoặc thỏa thuận với bên tin cậy được ủy quyền (Authorized Relying Party Agreement). Dấu hiệu của sự chấp nhận có thể bao gồm, không giới hạn ở các hành động Sử dụng chứng thư số (sau khi phát hành) Không thông báo tới tổ chức phát hành chứng thư số bất cứ vấn đề gì về chứng thư số trong một khoảng thời gian hợp lý sau khi phát hiện. Hoặc các dấu hiệu chấp nhận khác khác
Kích hoạt dữ liệu (Activation Data)	Dữ liệu được sử dụng hoặc được yêu cầu khi truy cập hoặc kích hoạt module mã hóa (ví dụ mã số nhận dạng cá nhân (PIN), chuỗi mật mã hoặt một tổ hợp phím bằng tay, được sử dụng để mở khóa riêng trước khi khởi tạo chữ ký số.)
Cá nhân được ủy quyền (Affiliated Individual)	Một cá nhân có mối quan hệ với một tổ chức và được tổ chức đó trao quyền nắm giữ chứng thư số để xác định tổ chức đó cũng như mối quan hệ giữa cá nhân và tổ chức đó.
Đối tượng nộp đơn (Applicant)	Một cá nhân hoặc một tổ chức gửi các thông tin tới một RA hoặc một CA phát hành với mục đích nhận được hoặc hồi phục lại chứng thư số.
Danh sách hủy bỏ/thu hồi chứng thư số (Authority Revocation List - ARL)	Danh sách các chứng thực CA bị hủy bỏ/thu hồi. Một ARL là một CRL đối với chứng thư số CA
Bên tin cậy được ủy quyền (Authorized Relying Party)	Một cá nhân hay một tổ chức ký kết thỏa thuận bên tin cậy được ủy quyền (Authorized Relying Party Agreement).
Thỏa thuận bên tin cậy được ủy quyền (Authorized Relying Party Agreement)	Một hợp đồng giữa một cá nhân hoặc một tổ chức với một CA phát hành cho phép bên đó (cá nhân hoặc tổ chức) tin tưởng vào chứng thư số tuân theo quy định trong CP này.

Chứng thư số CA (CA Certificate)	Một chứng thực là mắt xích đầu tiên trong chuỗi chứng thực của hệ thống hạ tầng khóa công khai TrustCA.
	Một chứng thực CA như một phần của việc thiết lập và kích hoạt CA phát hành. Chứng thực CA bao gồm khóa công khai (Puclic Key) tương ứng với khóa riêng ký CA (CA Private Signing Key) là hai khóa mà CA phát hành sử dụng để tạo ra hoặc quản lý chứng thư số. Chứng thư số CA và khóa công khai tương ứng có thể được nhúng trong phần mềm, hoặc có được hay được tải xuống bởi hành động xác nhận của ARP nhằm mục đích thiết lập chuỗi chứng thực.
Khóa riêng CA tạo chữ ký (CA Private Signing Key)	Khóa riêng cùng cặp với khoá công khai nằm trong chứng thực CA và được sử dụng dể ký chứng thực TrustCA.
Khóa gốc riêng CA (CA Private Root Key)	Khóa riêng sử dụng để ký chứng thư số CA.
Chứng thư số (Certificate)	Một bản ghi ở trong máy tính hoặc một thông tin điện tử để (i) nhận dạng tổ chức CA phát hành; (ii) đặt tên hoặc nhận dạng người giữ chứng thư số hoặc ARP; (iii) bao gồm khóa công khai của người giữ chứng thư số hoặc ARP; (iv) nhận dạng thời gian hiệu lực của chứng thư số; (v) được ký điện tử bởi một tổ chức chứng thực số và (vi) các ý nghĩa gắn liền tuân theo tiêu chuẩn áp dụng. Một chứng thư số bao gồm không chỉ nội dung thực mà còn bao gồm toàn bộ tài liệu chỉ tới hoặc gắn liền với nó.
Thỏa thuận chứng thư số (Certificate Agreement)	Hợp đồng giữa bên giữ chứng thư số với CA hoặc RA trong đó chi tiết hóa toàn bộ quá trình, quyền và nghĩa vụ của mỗi bên tương ứng với chứng thư số phát hành cho người giữ chứng thư số.
Người giữ/sở hữu chứng thư số (Certificate Holder)	Một cá nhân hoặc một tổ chức (i) được đặt tên hoặc nhận dạng trong chứng thư số , hoặc có trách nhiệm với các thiết bị điện tử (Electronic Device) được đặt tên, như là một phần của chứng thư số ; và (ii) giữ một khóa riêng tương ứng với khóa công khai nêu trong chứng thư số ; tuy nhiên, để hiểu theo CP này, những người giữ chứng thư số cho mục đích quản lý hành chính (ví dụ đối tượng của chứng thư số ARP được sử dụng để truy cập vào bộ phận lưu trữ (Repository) để xác thực trạng thái của chứng thư số) không được xem như là "Người giữ chứng thư số" tương ứng với chứng thư số được phát hành theo CP này.

Quy định chứng thư số (Certificate Policy - CP)	Là tập hợp các quy định đưa ra có thể áp dụng chứng thư số vào từng ứng dụng và chỉ rõ quá trình nhận dạng và chứng thực được thực hiện trước khi cấp chứng thư số,
	CP và các quy định khác công nhận quyền sử dụng của chứng thư số.
CP (Certificate Policy)	Quy định chứng thư số của tổ chức chứng thực số TrustCA.
Danh sách thu hồi chứng thư số (Certificate Revocation List - CRL)	Một cơ sở dữ liệu hoặc một danh sách các chứng thư số bị thu hồi hay hủy bỏ trước thời hạn so với thời hạn hiệu lực của chứng thư số.
Tổ chức chứng thực số (Certification Authority - CA)	Một chủ thể có thể tạo, phát hành, quản lý và hủy bỏ chứng thư số (xem trong CA phát hành).
Bản quy định thực hiện cấp chứng thư số (Certification Practice Statement - CPS)	Một tài liệu quy định CA áp dụng trong việc tạo, cấp phát, quản lý và hủy bỏ chứng thư số.
Chứng thực chéo (CrossCertificate)	Một chứng thư số sử dùng để thiết lập mối quan hệ tin tưởng giữa hai CA phát hành.
Mô đun mã hóa (Cryptomodule)	Phần mềm bảo mật, thiết bị hoặc một thực thể có thể (i) tạo ra cặp khóa, (ii) lưu trữ thông tin mã hóa, và/hoặc (iii) thực hiện chức năng mã hóa.
Chữ ký số/Ký điện tử (Digital Signature/Digitally Sign)	là sự chuyển đổi mã hóa một bản ghi điện tử do một người sử dụng khóa riêng và khóa công khai tạo ra, và người nhận có bản ghi bị mã hóa đó cùng với khóa công khai tương ứng có thể xác định chính xác: (i) liệu sự chuyển đổi này được tạo ra có sử dụng khóa riêng tương ứng với khóa chung hay không; và (ii) liệu bản ghi này có bị thay đổi kể từ khi mã hóa hay không.
Tên riêng (Distinguished Name - DN)	Sự xác nhận duy nhất đối với chủ sử hữu chứng thư số rằng người đó có được nằm trong một danh mục hay không (ví dụ, DN cho chủ sở hữu chứng thư số có thể bao gồm các đặc điểm sau đây: tên thông thường, địa chỉ email, tên tổ chức, đơn vị tổ chức, vị trí, thành phố và quốc gia).
Thiết bị điện tử (Electronic Device)	Phần mềm máy tính, phần cứng hoặc các thiết bị tự động hay thiết bị điện tử khác được một người cài đặt và sử dụng để thiết bị đó hoạt động, khởi động và phản ứng với bản ghi điện tử, và không bị kiểm soát hay tác động bởi chính người thực hiện.

Chủ thể cuối cùng (Endentity(ies))	Là chủ sở hữu chứng thư số hoặc các RP.
Khu vực an ninh cao (High-Security Zone)	Là một khu vực trong đó việc ra vào bị kiểm soát tại từng điểm và bị giới hạn quyền truy cập chỉ trong khu vực an ninh, khách ra vào khu vực có thể bị quan sát trên màn hình hoặc được hộ tống khi vào khu vực này; khu vực này được tách biệt với khu vực an ninh và khu vực điều hành bởi một vành đai ngăn cách. Khu vực an ninh cao được nhân viên an ninh, nhân viên khác hoặc thiết bị điện tử kiểm soát liên tục 24 giờ trong một ngày và 7 ngày trong một tuần.
Nhận dạng và xác thực (Identification and Authentication - I&A)	Để chắc chắn và đảm bảo thông tin thông qua tìm hiểu và kiểm tra khi xác minh nhân dạng về một chủ thể hoặc tổ chức.
Cá nhân (Individual)	Một người không có hành vi phạm pháp hoặc liên quan tới pháp luật.
Phát hành chứng thư số (Issue Certificates/Issuance)	Hành động được CA thực hiện khi tạo ra một chứng thư số, gọi là tổ chức phát hành, thông báo tới những người nộp đơn cấp chứng thư số về nội dung của nó và thông báo rằng chứng thực đã sẵn sàng để người nộp đơn chấp nhận.
Tổ chức phát hành chứng thực (Issuing CA)	Một tổ chức được PMA ủy quyền phát hành và ký các chứng thư số.
Khóa (Key)	Một thuật ngữ chung được sử dụng theo CP này để chỉ toàn bộ khóa được đề cập trong phần khái niệm chung.
Tạo khóa (Key Generation)	Là quá trình tạo một cặp khóa
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 chung), 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) thậm chí nếu biết khoá công khai thì cũng không có khả năng biết được khoá bí mật.
Giao thức truy cập danh sách Lightweight (Lightweight Directory Access Protocol - LDAP)	Giao thức giữa máy chủ và máy trạm được sử dụng để truy cập dịch vụ cây thư mục X.500 thông qua Internet.
Nhận dạng đối tượng (Object Identifier - OID)	Nhận dạng một dãy số/chữ duy nhất được đăng ký theo tiêu chuẩn đăng ký ISO để tham chiếu tới một đối tượng cụ thể hoặc lớp đối tượng.

Kiểm tra trạng thái trực tuyến (Online Status Check)	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 (ví dụ, không liên quan tới những CRL đã bị cất giữ).
Thời gian hoạt động (Operational Period)	Một chứng thư số trong thời hạn hiệu lực bắt đầu tại thời điểm bắt đầu của thời hạn hiệu lực và kết thúc sớm hơn (i) thời điểm kết thúc của thời hạn hiệu lực được nêu ra trong chứng thư số, hoặc (ii) chứng thư số bị hủy bỏ/thu hồi.
Khu vực điều hành (Operations Zone)	Khu vực trong đó số lượng người làm bị giới hạn và khách ra vào được hộ tống. Trong Khu vực điều hành nên được kiểm soát ít nhất theo chu kỳ và nên ra vào thông qua thu vực lễ tân (Reception Zone).
Các bên tham gia (Participants)	Toàn bộ các nhà cung cấp dịch vụ PKI và chủ thể cuối cùng được quyền tham gia vào PKI được định nghĩa theo CP/CPS.
Nguyên tắc chủ yếu PMA (PMA Charter)	Là tài liệu PMA chấp nhận để xác định các quy định và thủ tục để quản lý.
CP	Toàn bộ các quy định chứng thư số.
Khóa riêng (Private Key)	Một khóa được người giữ chứng thư số giữ bí mật, 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 là sở hữu cá nhân 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.
Sự tin cậy phù hợp (Reasonable Reliance)	Theo mục đích của CP này, quyết định của ARP tin tưởng vào chứng thư số sẽ được xem là sự tin cậy phù hợp nếu người đó Tham gia vào thỏa thuận ARP (Authorized Relying Party Agreement) và chấp nhận bị ràng buộc theo những điều khoản và điều kiện của CP này;

	Xác nhận rằng chữ ký số được tạo ra bởi khóa riêng cùng cặp với khóa công khai trong chứng thư số trong suốt thời gian hiệu lực của chứng thư số, và mọi thông tin trao đổi được ký với chữ ký số không được thay đổi; Xác nhận rằng chứng thư số có hiệu lực trong thời gian có hiệu lực với sự tin cậy của ARP, bằng cách sau đó hướng dẫn kiểm tra trạng thái của chứng thư số - giá trị pháp lý hiện thời - khi CA phát hành yêu cầu; và Sử dụng chứng thư số cho mục đích phù hợp với CP này và theo tình huống sự tin cậy là hợp lý và rõ ràng trong trường hợp mà ARP được biết hoặc đáng lẽ nên biết trước khi tin cậy. (ARP chịu mọi rủi ro khi tin cậy vào chứng thư số khi bên đó biết hoặc có lý do để biết một vấn đề nào đó gây ra cho một người với sự cẩn thận thông thường)
Khu vực lễ tân (Reception Zone)	Là khu vực diễn ra những tiếp xúc đầu tiên giữa công chúng với TrustCA hoặc TrustCA -RA, là nơii dịch vụ được cung cấp, thông tin được trao đổi và sự ra vào khu vực giới hạn bị kiểm soát.
Tổ chức đăng ký (Registration Authority - RA)	Là một tổ chức được TrustCA 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 CP này và các thỏa thuận có liên quan.
Tài liệu hoạt động và an ninh của RA (RA Security and Operations Manual)	Tài liệu hướng dẫn sử dụng hoặc ấn phẩm khác có thể ở dạng bản cứng hoặc bản mềm trong đó nêu rõ tiêu chuẩn và các quy định về vấn đề an ninh và hoạt động chung cho một PKI riêng biệt.
Bộ phận lưu trữ (Repository)	Một hệ thống trực tuyến do CA phát hành duy trì để lưu trữ và phục hồi các chứng thư số hoặc các thông tin liên quan tới chứng thư số, bao gồm các thông tin về thời hạn hiệu lực và sự thu hồi/hủy bỏ chứng thư số.
Khu vực bị giới hạn (Restricted Zones)	Là bất kỳ khu vực nào gồm có (i) Khu vực điều hành (Operations Zone); (ii) Khu vực an ninh (Security Zone); và (iii) khu vực an ninh cao (High Security Zone).
Thu hồi/hủy bỏ (Revocation)	Hành động làm một chứng thức số vĩnh viễn mất hiệu lực bắt đầu từ một thời điểm cụ thể. Sự hủy bỏ có hiệu lực kể từ khi có thông báo hoặc nằm trong một chứng thực bị hủy bỏ hoặc trong một cơ sở dữ liệu khác về các chứng thư số bị hủy bỏ (ví dụ như trong một CRL).
Khu vực an ninh (Security	Là khu vực trong đó số lượng người làm việc bị giới hạn

Zone)	và khách ra vào khu vực này được hộ tống. Khu vực điều hành nên được kiểm soát ít nhất theo chu kỳ và nên được vào từ khu vực điều khiển với một điểm kiểm soát ra vào. Khu vực an ninh không cần cách ly với khu vực điều khiển bằng một vành đai. Khu vực an ninh được nhân viên an ninh, nhân viên khác hoặc thiết bị điện tử kiểm soát liên tục 24 giờ trong một ngày và 7 ngày trong một tuần.
Bí mật được chia sẻ (Shared Secret)	Việc kích hoạt dữ liệu được sử dụng để hỗ trợ các bên trong việc chứng thực, nhận dạng và thiết lập các kênh trao đổi thông tin đáng tin cậy. Với mục đích xác minh giữa RA và một người sở hữu chứng thư số, bí mật được chia sẻ có thể bao gồm PIN hoặc mật mã ngân hàng trực tuyến được chia sẻ riêng giữa RA và người giữ chứng thư số, nhưng không phải là bên phát hành CA. Với mục đích thiết lập sự nhận dạng giữa người giữ chứng thư số và CA phát hành cần thiết cho việc phát hành, bí mật được chia sẻ có thể bao gồm các sự kích hoạt dữ liệu khác nhau, điều này được chia sẻ giữa RA, người giữ chứng thư số và CA phát hành.
Tên đối tượng (Subject Name)	Một trường riêng biệt trong chứng thư số bao gồm tên nhận dạng riêng biệt đối với người sở hữu chứng thư số.
Mã thông báo (Token)	Một mô đun mã hóa nằm trong một đối tượng phần cứng (ví dụ thẻ thông minh), thường bao gồm bộ nhớ hoặc chip vi xử lý.
Chứng thư số	Là một chứng thư số được phát hành theo CP này.
Thời hạn hiệu lực (Validity Period)	chỉ thời hạn hiệu lực của chứng thư số, bắt đầu là ngày cấp phát (Issuance) ("Có hiệu lực từ ngày" hoặc ngày "Kích hoạt"), và kết thúc từ ngày kết thúc nêu trong chứng thư số ("Có hiệu lực tới" hoặc ngày "Hết hiệu lực").

Bảng 2: Danh mục từ viết tắt

ARP	Authorized Relying Party Bên tin cậy được ủy quyền
ANSI	The American National Standards Institute Viện tiêu chuẩn quốc gia Hoa Kỳ

ARL	Authority Revocation List Danh sách hủy bỏ quyền
CA	Certification Authority Tổ chức cấp chứng thư số
CMA	Certificate Manufacturing Authority Tổ chức cấp phát chứng thư số
CPS	Certification Practice Statement Bản quy chế cấp phát và sử dụng chứng thư số
CRL	Certificate Revocation List Danh sách chứng thư số bị thu hồi
DN	Distinguished Name Tên riêng
DSA	Digital signature algorithm Thuật toán chữ ký số
EDI	Electronic Data Interchange Trao đổi dữ liệu điện tử
HTTPS	Hypertext Transfer Protocol with SSL Giao thức web với bảo mật đường truyền SSL
I&A	Identification and Authentication Nhận dạng và xác thực
LDAP	Lightweight Directory Access Protocol Giao thức truy cập danh mục Lightweight
CP	TrustCA Certificate Policy Quy định chứng thư số của tổ chức chứng thực số Công ty Cổ phần Công nghệ SAVIS
S/MIME	Secure Multipurpose Internet Mail Extentions. Chuẩn bảo mật thư điện tử
OID	Object Identifier Đối tượng nhận dạng

PIN	Personal IdentifiCAtion Number Mã số nhận dạng cá nhân
PKCS	Public Key Cryptography Standard Chuẩn mã hoá bằng khoá công khai
PKI	Public Key Infrastructure Hạ tầng kỹ thuật mã hóa công khai
PMA	Policy Management Authority Tổ chức quản lý các chính sách
RA	Registration Authority Tổ chức đăng ký
SSL	Secure Socket Layer Giao thức bảo mật giao dịch trên Internet
X.500	X.500 The ITU-T (International Telecommunication Union-T) standard that establishes a distributed, hierarchical directory protocol organized by country, region, Organization, etc. Chuẩn T-Liên đoàn truyền thông quốc tế ITU-T thiết lập giao thức danh mục được phân theo cấp bậc được các quốc gia, khu vực, tổ chức tổ chức thực hiện
X.501	The ITU-T (International TelecommuniCAtion UnionT) standard for use of Distinguished Names in an X.500 directory. Chuẩn ITU-U cho sử dụng tên riêng trong danh mục X.500
X.509	ITU-T standard for Certificates format Chuẩn ITU-T định dạng chứng thư số

PHỤ LỤC 2:

THAM KHẢO

Chi tiết Bảng tham chiếu đáp ứng quy định danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số của thông tư 06/2015/TT-BTTTT

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng	Trust CA áp dụng
1	**Tiêu chuẩn bảo mật cho HSM và thẻ mật mã**				
1,1	Yêu cầu an ninh đối với khối an ninh phần cứng HSM	FIPS PUB 140-2	Security Requyrements for Cryptographic Modules	- Yêu cầu tối thiểu mức 3 (level 3)	FIPS 140-2 Level 3
1.2	Yêu cầu an ninh đối với thẻ Token và Smart card	FIPS PUB 140-2	Security Requyrements for Cryptographic Modules	- Yêu cầu tối thiểu mức 2 (level 2)	FIPS 140-2 level 3
2	**Tiêu chuẩn mật mã và chữ ký số**				
2,1	Mật mã phi đối xứng và chữ ký số	PKCS #1	RSA Cryptography Standard	- Phiên bản 2.1 - Áp dụng lược đồ RSAES-OAEP để mã hoá và RSASSA-PSS để ký	- PKCS #1 RSA Cryptograph y Standard phiên bản 2.1 trở lên - Áp dụng lược đồ RSAESOAEP để mã hoá và RSASSA-PSS để ký
2,2	Mật mã đối xứng	TCVN 7816:2007 (FIPS PUB 197) NIST 80067	Công nghệ thông tin - Kỹ thuật mật mã - Thuật toán mã hóa dữ liệu AES Recommendation for the Triple Data Encryption Algorithem (TDEA) Block Cipher	Áp dụng một trong hai tiêu chuẩn	AES

2,3	Hàm băm an toàn	FIPS PUB 180-4	Secure Hash Standard	Áp dụng một trong sáu hàm băm: SHA224, SHA256, SHA384, SHA-512, SHA-512/224, SHA-512/256	SHA-2 (SHA-256)
3	**Tiêu chuẩn thông tin, dữ liệu**				
3,1	Định dạng chứng thư số và danh sách thu hồi chứng thư số	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile		RFC5280 (Internet X.509 Public Key Infrastructur e Certificate and CRL Profile).
3,2	Cú pháp thông điệp mật mã	PKCS #7	Cryptographic Message Syntax Standard	Phiên bản 1.5	PKCS #7
3,3	Cú pháp thông tin khóa riêng	PKCS #8	Private-Key Information Syntax Standard	Phiên bản 1.2	PKCS #8
3,4	Cú pháp yêu cầu chứng thực	PCKS #10	Certification Request Syntax Standard	Phiên bản 1.7	PCKS #10
3,5	Giao diện giao tiếp với các thẻ mật mã	PKCS #11	Cryptographic token interface standard	Phiên bản 2.20	PKCS #11
3,6	Cú pháp trao đổi thông tin cá nhân	PKCS #12	Personal Information Exchange Syntax Standard	Phiên bản 1.0	PKCS #12
4	**Tiêu chuẩn chính sách và quy chế chứng thực chữ ký số**				
	Khung quy chế chứng thực và	RFC 3647	Internet X.509 Public Key		RFC 3647

	chính sách chứng thư		Infrastructure - Certificate Policy and Certification		
			Practices Framework		
5	**Tiêu chuẩn giao thức lưu trữ và truy xuất chứng thư số**				
5,1	Lược đồ Giao thức truy nhập thư mục	RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema	Áp dụng một trong hai tiêu chuẩn	X.509 v3
		RFC 4523	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates		
5,2	Giao thức truy nhập thư mục	RFC 2251	Lightweight Directory Access Protocol (v3)	Áp dụng tiêu chuẩn RFC 2251 hoặc bộ bốn tiêu chuẩn: RFC 4510, RFC 4511, RFC 4512, RFC 4513	RFC 2251
		RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map		
		RFC 4511	Lightweight Directory Access Protocol (LDAP): The Protocol		
		RFC 4512	Lightweight Directory Access Protocol (LDAP): Directory Information Models		
		RFC 4513	Lightweight Directory Access Protocol (LDAP):		

			Authentication Methods and Security Mechanisms		
6	**Tiêu chuẩn kiểm tra trạng thái chứng thư số**				
6,1	Giao thức truyền, nhận chứng thư số và danh sách chứng thư số bị thu hồi	RFC 2585	Internet X.509 Public Key Infrastructure - Operational Protocols:FTP and HTTP	Áp dụng một hoặc cả hai giao thức FTP và HTTP	Áp dụng giao thức HTTP
6,2	Giao thức cho kiểm tra trạng thái chứng thư số trực tuyến	RFC 2560	X.509 Internet Public Key Infrastructure - Online Certificate status protocol		RFC 2560 (OCSP)
7	**Tiêu chuẩn dịch vụ cấp dấu thời gian**				
7,1	Giao thức cấp dấu thời gian	RFC 3161	Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)		RFC 3161
7,2	Dịch vụ cấp dấu thời gian	TCVN 7818-1:2007 (ISO/IEC 180141:2002)	Công nghệ thông tin - Kỹ thuật mật mã - Dịch vụ tem thời gian - Phần 1: Khung tổng quát	Áp dụng bộ ba tiêu chuẩn: TCVN 7818-1:2007 TCVN 7818-2:2007 TCVN 7818-3:2010	RFC#3161, RFC#5816 and MS Authenticode; EN 319 422
		TCVN 7818-2:2007 (ISO/IEC 18014 - 2: 2002)	Công nghệ thông tin - Kỹ thuật mật mã - Dịch vụ tem thời gian - Phần 2: Cơ chế tạo thẻ độc lập		
		TCVN 7818-3:2010 (ISO/IEC 18014- 3: 2009)	Công nghệ thông tin - Kỹ thuật mật mã - Dịch vụ tem thời gian - Phần 3: Cơ chế tạo thẻ liên kết		