CÔNG TY CỔ PHẦN CÔNG NGHỆ SAVIS

QUY CHẾ CHỨNG THỰC

DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG THEO MÔ HÌNH KÝ SỐ TỪ XA

Phiên bản: v1.1

Hà Nội, năm 2023

MỤC LỤC

1 GIỚI THIỆU

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.

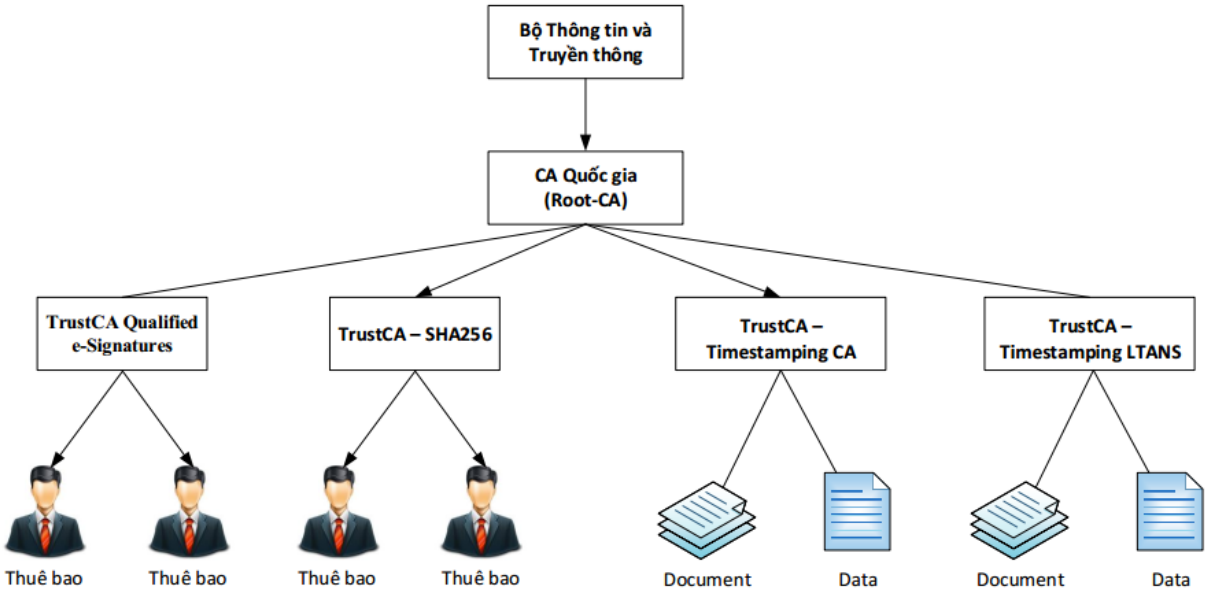
TrustCA bao gồm một CA, các tổ chức đăng ký chứng thư số RA và các đại lý được ủy quyền. RA và các đại lý có trách nhiệm tiếp nhận và xác thực thông tin từ phía khách hàng sử dụng dịch vụ.

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. Đây là tài liệu Quy chế chứng thực (CPS) của hệ thống cung cấp dịch vụ chứng thực chữ ký số theo mô hình ký số từ xa **TrustCA Qualified e-Signatures**

1.1. Tổng quan

CPS này mô tả các thông lệ và quy trình được sử dụng để giải quyết tất cả các yêu cầu được xác định theo Quy định (EU) N ° 910/2014, để cấp phát, duy trì và quản lý vòng đời cho Chứng thư số.

TrustCA hiện đang sử dụng chuỗi chứng thư như sau:



TrustCA thiết lập cơ sở hạ tầng bảo mật khép kín, hệ thống CA, bao gồm các module mã hoá bảo mật, lưu khoá bí mật cho quy trình cấp phát chứng thư số. TrustCA thực hiện nhiệm vụ bao gồm tất cả các dịch vụ quản lý vòng đời chứng thư từ khi phát hành, quản lý, thu hồi, Cấp mới chứng thư số.

Các CA khác được quản lý bởi TrustCA nhưng không được nêu tên trong tài liệu này sẽ nằm ngoài phạm vi áp dụng của CPS. Các CA được quản lý bởi các tổ chức khác cũng nằm ngoài phạm vi của bản CPS này.

TrustCA công bố bản quy chế chứng thực nhằm tuân thủ theo các yêu cầu về pháp lý và tiêu chuẩn/yêu cầu của Bộ Thông tin và Truyền thông

1.2. Tên tài liệu và nhận dạng

Văn bản này là một bộ quy chế chứng thực (CPS) tuyên bố về mặt nguyên tắc các chính sách (CP) quản trị của SAVIStrong 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)
- Tên tài liệu: Quy chế chứng thực (CPS) của hệ thống cung cấp dịch vụ chứng thực chữ ký số theo mô hình ký số từ xa **TrustCA Qualified e-Signatures**.

1.3. Các bên tham gia

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)

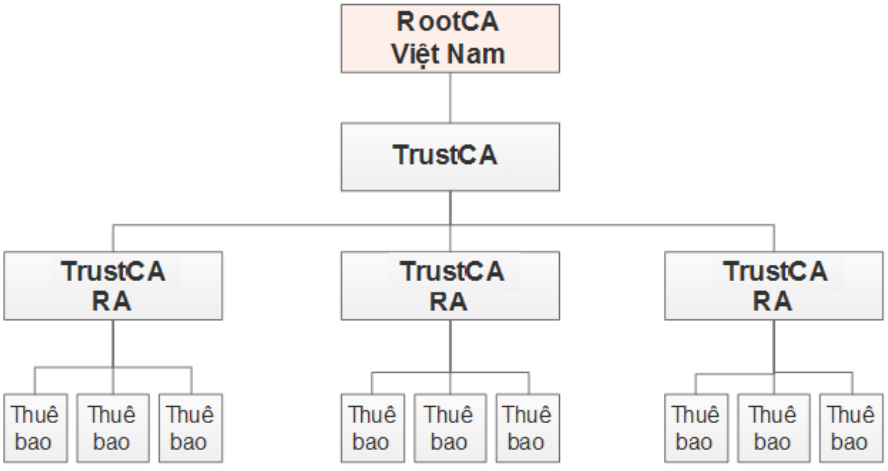
Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng – CA là thành phần quan trọng nhất trong hệ thống PKI. CA xác thực thông tin thuê bao cũng như đảm bảo tính bí mật và toàn vẹn nội dung thông tin mà các thành phần tham gia dịch vụ chứng thực chữ ký số công cộng trao đổi thông qua hệ thống của CA.

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 Công ty Cổ phần Công nghệ 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.



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 Công ty Cổ phần Công nghệSAVIS.

1.3.5 Thành phần khác

TrustCA không quy định dịch vụ này.

1.4 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 thông qua thiết bị tạo chữ ký đảm bảo (QSCD) đáp ứng 16/2019/TT-BTTTT Quy định Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa.
- 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 Cấm sử dụng chứng thư số vào các mục đích sau

Mọi chứng thư số do hệ thống TrustCA của Công ty Cổ phần Công nghệ 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 Công ty Cổ phần Công nghệ 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 đòi 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 chính sách

1.5.1 Tổ chức quản lý tài liệu

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 Liên hệ

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 Người quyết định sự phù hợp của qui chế chứng thực

Tổng Giám Đốc Công ty Cổ phần Công nghệ SAVIS là người có quyền xem xét và phê chuẩn Qui chế chứng thực chữ ký số này.

1.5.4 Thủ tục phê chuẩn 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 Tổng Giám Đốc Công ty Công ty Cổ phần Công nghệ SAVIS
- Các thay đổi, cập nhật của quy chế chứng thực được ghi lại, công bố tại https://trustca.vn/tai-ve/

1.6 Định nghĩa và 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

Thuật ngữ - Từ viết tắt	Giải thích
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
GDPR (General Data Protection Regulation)	Quy định chung về bảo mật dữ liệu bao gồm các yêu cầu về quyền riêng tư của dữ liệu thuộc khối EU và có hiệu lực hoạt động từ ngày 25/5/2018.

2 TRÁCH NHIỆM CÔNG BỐ THÔNG TIN VÀ LƯU TRỮ

2.1 Lưu trữ

Các thông tin về thuê bao và chứng thư số được lưu trữ tập trung, bảo mật, an toàn, hạn chế tiếp xúc với môi trường mạng Internet.

Các thông tin được lưu trữ trực tuyến là các thông tin về chính sách, Quy chế chứng thực chữ ký số, CRL và các thông tin tối thiểu về chứng thư số được ánh xạ từ cơ sở dữ liệu gốc nêu trên.

2.2 Công bố thông tin chứng thư số

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 / 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

2.3 Tần suất công bố

- Đối với các thông tin về chứng thư số được cập nhật thường xuyên, liên tục và cho phép truy cập 24/7.
- Đối với các thông tin về Quy chế chứng thực chữ ký số, chính sách được cập nhật khi có sự thay đổi.
- Danh sách chứng thư số bị thu hồi: được cập nhật khi có sự thay đổi.

2.4 Kiểm soát truy cập kho lưu trữ 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 Công ty Cổ phần Công nghệ SAVIS mới có quyền thay đổi, bổ sung, cập nhật.

3 NHẬN DẠNG VÀ XÁC THỰC

3.1 Đặt tên

3.1.1 Các loại 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 Đặt tên có ý nghĩa

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.

3.1.3 Tên ẩn danh hay bút danh

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

3.1.4 Quy định về diễn giải các mẫu tên khác nhau

Không có qui định.

3.1.5 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.

3.1.6 Công nhận, xác thực và vai trò của thương hiệu

Người gửi đơn xin cấp chứng thư số không được sử dụng những tên vi phạm quyền sở hữu trí tuệ. Nếu có sự tranh chấp xảy ra về sở hữu thì 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

3.2 Xác minh nhận dạng đối tượng đăng ký chứng thư số lần đầu

3.2.1. Phương thức chứng minh sở hữu khóa bí mật

Người gửi yêu cầu xin cấp chứng thư số phải chứng minh quyền sở hữu khóa bí mật tương ứng với khóa công khai trong chứng thư số. Phương pháp chứng minh sở hữu khóa bí mật sẽ tuân theo chuẩn PKCS#10 hoặc một phương pháp mật mã tương ứng hoặc một phương pháp khác được TrustCA công nhận. Điều kiện này không áp dụng khi cặp khóa được CA sinh ra theo yêu cầu của thuê bao (ví dụ trường hợp khóa được sinh ra và lưu trữ trên USB token).

3.2.2. Xác thực định danh của tổ chức

Khi có một yêu cầu đăng ký chứng thư số nhận dạng cho tổ chức, thông tin nhận

dạng của tổ chức đó được xác minh. 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 - bao gồm toàn bộ các thông tin quan trọng để nhận dạng chủ thể đăng ký.
- TrustCA, hoặc các RA của TrustCA thực hiện xác thực nhận dạng của tổ chức theo các thông tin nêu trên thông qua hình thức gặp mặt trực tiếp hoặc gián tiếp với phương tiện nhận dạng và xác thực tương đương.
- 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.
- Đối với trường hợp xác minh thông tin thuê bao sử dụng công cụ xác minh danh tính điện tử, nội dung xác thực gồm:
  + Đơn đăng ký sử dụng dịch vụ có xác nhận của Người đại diện của Tổ chức;
  + Xác minh Giấy chứng nhận đăng ký doanh nghiệp hoặc Giấy tờ tương đương (Giấy phép kinh doanh, Quyết định thành lập…);
  + Xác minh giấy tờ tùy thân của Người đại diện pháp luật của Tổ chức (CMND/CCCD/Hộ chiếu)
  + So khớp khuôn mặt và giấy tờ tùy thân của Người đại diện pháp luật của Tổ chức và so khớp thông tin Giấy chứng nhận đăng ký doanh nghiệp.
  + Dịch vụ không hỗ trợ cơ chế ủy quyền giữa chủ thể chứng thư với người khác trong quá trình đăng ký cấp chứng thư số.
  + Quá trình xác minh danh tính của Thuê bao được thực hiện tự động thông qua công cụ điện tử được mô tả tại *"Quy trình cấp chứng thư số bằng phương thức điện tử"*.

3.2.3. Xác thực định danh cá nhân

Khi có một yêu cầu đăng ký chứng thư số nhận dạng cho cá nhân, thông tin nhận dạng của cá nhân đó được xác minh. TrustCA sẽ xác minh các thông tin bắt buộc sau: Tên cá nhân; Địa chỉ; Chứng minh nhân dân/Căn cước công dân/Hộ chiếu; Địa chỉ thư điện tử; Thông tin về website, quyền sở hữu tên miền của cá nhân (dùng cho việc cấp chứng thư số SSL). TrustCA/RA thực hiện định danh bằng hình thức trực tiếp và hình thức điện tử.

a) Xác thực định danh bằng hình thức trực tiếp

- -Các thông tin cần thu thập để xác minh thông tin đăng ký của thuê bao theo quy định tại Nghị định số 130/2018/NĐ-CP. Các thành phần hồ sơ thuê bao yêu cầu xuất trình bản gốc.TrustCA, hoặc các RA của TrustCA thực hiện xác thực nhận dạng của cá nhân thông qua một trong các giấy tờ sau: Căn cước công dân/chứng minh nhân dân/hộ chiếu, có xác minh của chính quyền – bao gồm toàn bộ các thông tin quan trọng để định danh xác thực chủ thể đăng ký thuê bao.
- Hồ sơ xin cấp gồm có: Đơn xin cấp chứng thư (theo mẫu của TrustCA), 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.

b) Xác minh thông tin bằng phương thức điện tử:

- Trong trường hợp người đăng ký sử dụng hồ sơ điện tử, hệ thống SAVIS sử dụng các công nghệ đáp ứng tiêu chuẩn để xác thực cho khách hàng (công cụ xác minh danh tính điện tử), nội dung xác minh bao gồm:
  - Đơn đề nghị cấp chứng thư số bằng phương thức điện tử.
  - Xác minh thông tin của người đề nghị, thời hạn hiệu lực của các thông tin dựa trên thời hạn hiệu lực của hồ sơ thuê bao (xác minh giấy tờ tùy thân CMND/CCCD/Hộ chiếu bản gốc).
  - Đối chiếu với người đề nghị (So khớp khuôn mặt với giấy tờ tùy thân).
- Dịch vụ không hỗ trợ cơ chế ủy quyền giữa chủ thể chứng thư với người khác trong quá trình đăng ký cấp chứng thư số.
- Quá trình xác minh danh tính của Thuê bao được thực hiện bán tự động thông qua công cụ điện tử, tuân thủ quy định của Bộ thông tin truyền thông và được mô tả chi tiết tại *"Phương án kỹ thuật TrustCA Remote Signing"* và "*Quy trình cấp chứng thư số bằng phương thức điện tử"*.

3.2.4. Thông tin thuê bao không được xác minh

TrustCA không quy định dịch vụ này

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 1ủy 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 hoạt động liên thông

TrustCA không quy định dịch vụ này

3.3 Xác thực và định danh đối với yêu cầu thay 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 qui 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.

3.3.3. Xác thực và định danh đối với yêu cầu 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. QUÁ TRÌNH SINH KHÓA VÀ TẠO CHỨNG THƯ SỐ CHO TRUSTCA

TrustCA sẽ tổ chức buổi lễ tạo khóa để tiến hành sinh cặp khóa vào HSM thông qua phần mềm CoreCA và tạo yêu cầu cấp chứng thư số gửi NEAC.

Sau khi nhận được yêu cầu xin cấp phát chứng thư số, NEAC sẽ kiểm tra lại thông tin yêu cầu. Sau khi được phê duyệt, NEAC sẽ tiến hành cấp chứng thư số từ yêu cầu trên và gửi lại cho nhà cung cấp dich vụ CA.

Sau khi nhận được chứng thư số do NEAC cấp, TrustCA sẽ import chứng thư số đó vào trong hệ thống CoreCA để hoàn thành quá trình khởi tạo chứng thư số.

5 CÁC YÊU CẦU QUẢN LÝ VÒNG ĐỜI CỦA CHỨNG THƯ SỐ THUÊ BAO

5.1 Đăng ký chứng thư số

5.1.1 Các đối tượng có thể xin 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 trên 18 tuổi đứng ra bảo lãnh và 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.

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

5.1.2.1 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.

5.1.2.2 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 muc 9.6.2.

5.2 Thủ tục xử lý yêu cầu cấp chứng thư số

5.2.1 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.

5.2.2 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.

5.2.3 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.

5.3 Phát hành chứng thư số

5.3.1 Hoạt động của CA khi phát hành chứng thư số

Chứng thư số được ban hành sau khi TrustCA/RA chấp nhận đơn xin cấp chứng thư số trực tiếp từ thuê bao hoặc thông qua RA. TrustCA ban hành cho thuê bao một chứng thư số dựa vào những thông tin trong đơn xin cấp chứng thư số.

5.3.2 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: Tải về từ trang Web của TrustCA.

5.4 Chấp nhận chứng thư số

5.4.1 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 phù hợp với thông tin thuê bao. Biên bản giao nhận này được TrustCA lưu trữ.

Thuê bao sẽ nhận chứng thư số thông qua địa chỉ email CKSH hoặc cổng dịch vụ RA. Trong trường hợp sử dụng cổng dịch vụ RA, TrustCA sẽ duy trì dịch vụ 24x7.

5.4.2 CA công bố chứng thư số

Sau khi thuê bao chấp nhận chứng thư số (theo mục 5.4.1), 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.

5.4.3 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

5.5 Sử dụng cặp khóa và chứng thư số

5.5.1 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.

5.5.2 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.

5.6 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

5.6.1 Các tình huống gia hạn chứng thư số

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

5.6.2 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.

5.6.3 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.

5.6.4 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 5.3.2.

5.6.5 Cách thức thể hiện sự chấp nhận gia hạn chứng thư số

Tương tự mục 5.4.1

5.6.6 Công bố chứng thư số được gia hạn

Tương tự mục 5.4.2

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

Tương tự mục 5.4.3

5.7 Thay đổi khóa chứng thư số

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.

5.7.1 Các tình huống thay đổi khóa

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

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

5.7.2 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.

5.7.3 Xử lý yêu cầu thay đổi 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

5.7.4 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 5.3.2

5.7.5 Cách thức thể hiện sự chấp nhận thay khóa chứng thư số

Tương tự phần 5.4.1

5.7.6 Công bố chứng thư số đã thay khóa

Tương tự phần 5.4.2.

5.7.7 Thông báo đổi khóa cho các đối tượng khác

Tương tự phần 5.4.3.

5.8 Sửa đổi chứng thư số

5.8.1 Các tình huống sửa đổi chứng thư số

Sửa đổi chứng thư số xem như yêu cầu cấp chứng chỉ số theo phần 5.1

5.8.2 Đối tượng được phép yêu cầu sửa đổi chứng thư số

Xem phần 5.1.1

5.8.3 Xử lý yêu cầu sửa đổi chứng thư số

Xem phần 3.2

5.8.4 Thông báo cho thuê bao về việc sửa đổi chứng thư số

Xem phần 5.3.2

5.8.5 Cách thức thể hiện sự chấp nhận sửa đổi chứng thư số

Xem phần 5.4.1

5.8.6 Công bố chứng thư số đã sửa đổi

Xem phần 5.4.2

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

Xem phần 5.4.3

5.9 Tạm dừng và thu hồi chứng thư số

5.9.1 Các tình huống thu hồi chứng thư số

Yêu cầu thu hồi chứng thư số sẽ được xử lý khi thuê bao hay các đối tượng có thẩm quyền (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; đồng thời thuê bao và các bên liên quan sẽ được thông báo qua Email hoặc cổng dịch vụ CSKH. 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 sẽ không được khôi phục sau khi bị thu hồi.

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.
- Thuê bao mất khả năng sử dụng QSCD hoặc thiết bị di động cần thiết để truy cập Remote QSCD

5.9.2 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.

5.9.3 Thủ tục yêu cầu thu hồi chứng thư số

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 3.2

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.

5.9.4 Thời gian tiến hành yêu cầu thu hồi

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

Quản trị hệ thống 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.

5.9.5 Thời gian bắt đầu xử lý yêu cầu thu hồi chứng thư số

TrustCA sẽ xử lý ngay khi nhận được yêu cầu thu hồi chứng thư số. Thời gian trễ từ khi tiếp nhận yêu cầu đến khi phản hồi dịch vụ tối đa là 24h. Thời gian thực hiện lệnh thu hồi đến khi có hiệu lực tối đa là 60 phút. Để đảm bảo tính toàn vẹn và chính xác

của thời gian, hệ thống TrustCA được đồng bộ với nguồn thời gian quốc gia qua giao thức NTP (Network Time Protocol).

5.9.6 Yêu cầu kiểm tra việc thu hồi cho người nhận

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.

5.9.7 Tần suất phát hành chứng thư số bị thu hồi

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

5.9.8 Thời gian trễ lớn nhất của CRL

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

5.9.9 Kiểm tra trực tuyến trạng thái chứng thư số trực tuyến

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

5.9.10 Điều kiện kiểm tra thu hồi chứng thư số trực tuyến

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

5.9.11 Các định dạng quảng bá chứng thư số bị thu hồi khác

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

5.9.12 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.

5.9.13 Các trường hợp tạm dừng

TrustCA không quy định dịch vụ này

5.9.14 Đối tượng được phép yêu cầu tạm dừng

TrustCA không quy định dịch vụ này

5.9.15 Thủ tục yêu cầu tạm dừng

TrustCA không quy định dịch vụ này

5.9.16 Giới hạn thời gian tạm dừng

TrustCA không quy định dịch vụ này

5.10 Dịch vụ kiểm tra trạng thái chứng thư số

5.10.1 Các đặc tính hoạt động

Trạng thái của chứng thư số được công bố qua CRL (Web hoặc LDAP) và OCSP responder. Thông tin trạng thái chứng thư số bao gồm thông tin về trạng thái hoạt động của chứng thư số đến khi chứng thư số hết hạn. Ngoài ra, thông tin thu hồi chứng thư số sẽ được duy trì ngoài vòng đời của chứng thư số. Tính toàn vẹn và tin cậy của thông điệp dịch vụ kiểm tra trạng thái chứng thư số được bảo vệ bằng chữ ký số của CA. Trong trường hợp khóa bí mật của CA bị lộ, TrustCA thực hiện theo quy trình tại Mục 6.7.3 của tài liệu này.

5.10.2 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.

5.10.3 Các đặc tính tùy chọn

OCSP là dịch vụ tùy chọn, có phí. Trạng thái thu hồi chứng thư số được cập nhật trên cả phương thức OCSP và CRL.

5.11 Kết thúc thuê bao

Kết thúc thuê bao chứng thư số có hiệu lực trong các trường hợp sau:

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

5.12 Ủy thác và phục hồi khóa

TrustCA không quy định dịch vụ này.

6 KIỂM SOÁT VẬN HÀNH, QUẢN LÝ VÀ THIẾT BỊ

6.1 Kiểm soát an toàn vật lý

6.1.1. 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.

6.1.2. 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.

6.1.3. 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.

6.1.4. Chống nước

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

6.1.5. 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.

6.1.6. Phương tiện lưu trữ

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.

6.1.7. Xử lý rác thải

Tất cả các bản copy của dữ liệu nhạy cảm (bản in) được tiêu hủy tại chỗ trước đưa vào quy trình xử lý chất thải. Toàn bộ các bản lưu điện tử chứa thông tin nhạy cảm được tiêu hủy vật lý hoặc ghi đè nhiều lần để tránh phục hồi dữ liệu.

6.1.8. 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.

6.2 Các thủ tục kiểm soát

6.2.1 Những vai được tin cậy

Những nhân sự thực hiện vai tin cậy bao gồm cán bộ quản lý hệ thống của CA, RA hoặc TSA cùng nhân viên thực hiện xác thực định danh thuê bao và cấp phát/thu hồi chứng thư số. Chức năng và nhiệm vụ của những nhân sự tin cậy được phân quyền để đảm bảo một cá nhân không thể qua mặt các biện pháp an ninh an toàn hệ thống hoặc chỉnh sửa bất hợp pháp các chức năng quan trọng của hệ thống PKI. Danh sách nhân sự tin cậy được chỉ định và phê duyệt thường xuyên bởi Ban Giám đốc (theo quý, theo năm…)

Nhân sự tin cậy là những người có thể truy cập hay điều khiển các thao tác xác thực, mã hóa, liên quan đến:

- Việc xác minh các thông tin trong đơn xin cấp chứng thư số.
- Việc chấp nhận, loại bỏ, hay các xử lý khác đối với đơn xin cấp chứng thư số, yêu cầu thu hồi, làm mới, hay thông tin đăng ký.
- Việc ban hành, thu hồi chứng thư số.
- Việc quản lý thông tin thuê bao, thông tin yêu cầu từ thuê bao.

Những Nhân sự tin cậy đều được xác minh về nhân thân, khả năng đảm bảo đáp ứng yêu cầu công việc trước khi được giao nhiệm vụ.

6.2.1.1. Giám sát an ninh hệ thống

Nhân viên giám sát an ninh hệ thống chịu trách nhiệm quản lý và triển khai các chính sách, thông lệ về an ninh bảo mật. Vị trí này chỉ có quyền truy cập vào các thông tin liên quan đến an ninh an toàn hệ thống.

6.2.1.2. Quản trị hệ thống

Quản trị viên hệ thống được cấp phép để cài đặt, cấu hình và duy trì hệ thống ký số nhưng chỉ được truy cập các thông tin được phép đối với chức năng an ninh.

6.2.1.3. Vận hành hệ thống

Nhân viên vận hành hệ thống chịu trách nhiệm duy trì hoạt động của hệ thống ký số

theo tác vụ và được phép truy cập chức năng bảo trì – phục hồi hệ thống.

6.2.1.4. Kiểm toán hệ thống

Kiểm toán viên hệ thống được phép xem dữ liệu lưu trữ và bản ghi log của toàn hệ thống với mục đích thực hiện kiểm toán nội bộ, tuân thủ quy trình quy định tại chính sách an toàn thông tin.

6.2.2 Số lượng người được yêu cầu trên một nhiệm vụ

TrustCA thiết lập các chính sách và thủ tục kiểm soát đảm bảo nguyên tắc Principle of Least Priviledge khi thực hiện một công việc nhạy cảm như truy cập, điều khiển module phần cứng mã hóa. Mỗi nhân sự chỉ có quyền theo đúng nghĩa vụ và trách nhiệm với vị trí được giao.

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

6.2.3 Nhận dạng và xác thực trong mỗi vai

Mọi cá nhân trước khi trở thành Nhân sự tin cậy trong hệ thống CA đề 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.

6.2.4 Những vai cần phân tách nhiệm vụ

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

- Xác minh thông tin trong đơn xin cấp chứng thư số,
- Chấp nhận, từ chối hay các xử lý khác với đơn xin cấp chứng thư số, yêu cầu thu hồi, làm mới chứng thư số
- Ban hành, thu hồi chứng thư số.
- Quản lý thông tin, yêu cầu của thuê bao.
- Đối với các nhân sự tin cậy như giám sát an ninh, vận hành hệ thống, kiểm toán viên hệ thống phải được phân lập bởi cơ chế dual-control.

6.3 Quản lý nhân sự

6.3.1 Yêu cầu phẩm chất, kinh nghiệm và tin tưởng

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.

6.3.2 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).

6.3.3 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.
- TrustCA lưu trữ các bản ghi vết về nhân sự được đào tạo kèm cấp độ đào tạo. Các nhân viên thực hiện xác thực danh tính của thuê bao được đào tạo riêng biệt để có kỹ năng cần thiết trong quá trình xác thực giấy tờ trước khi được truy cập hệ thống. Tất cả các nhân viên thực hiện xác thực danh tính thuê bao đều được yêu cầu tuân thủ đầy đủ nội quy, chính sách bảo mật thông tin, an toàn thông tin được quy định bởi chính sách nội bộ và các quy định tại nghị định 130/2018/ND-CP (Điều 23).

6.3.4 Yêu cầu đào tạo lại thường xuyên

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.

6.3.5 Tần suất luân chuyển công tác

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

6.3.6 Kỉ luật 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, đình chỉ công việc tạm thời hoặc cho thôi việc, tùy thuộc vào mức độ nghiêm trọng của vi phạm.

6.3.7 Các yêu cầu kí kết độc lập

Trong một số trường hợp, các cố vấn độc lập có thể được thuê để thực hiện một số công việc cần sự tin tưởng của 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 Nhân sự tin cậy của CA.

6.3.8 Cung cấp tài liêu cho nhân viên

CA cung cấp các tài liệu cần thiết cho nhân viên, đảm bảo các nhân viên có thể thực hiện tốt công việc với các tài liệu được cung cấp.

6.4 Các thủ tục kiểm tra nhật ký

6.4.1 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 kiên được ghi lại bao gồm:

- Chứng thư số của CA và các sự kiện quản lý vòng đời khoá:
  - Tạo khóa, sao lưu, lưu trữ, phục hồi, lưu trữ và hủy khoá
  - Thay đổi về thông tin của CA hoặc của các khoá
  - Các sự kiện trong quản lý vòng đời của thiết bị mã hóa
- Chứng thư số của thuê bao và các sự kiện quản lý vòng đời khoá:
  - Đơn yêu cầu cấp Chứng thư số, cấp lại, cấp mới và thu hồi

- Tạo khóa, sao lưu, lưu trữ, phục hồi, lưu trữ và hủy
- Xử lý yêu cầu thành công hoặc không thành công
- Thay đổi trong chính sách tạo Chứng thư số
- Tạo và phát hành Chứng thư số cùng CRL.

- Sự kiện hoạt động của các nhân viên tin cậy (trusted employee):
  - Đăng nhập và đăng xuất
  - Nỗ lực tạo, xóa, đặt mật khẩu hoặc thay đổi quyền hệ thống của bất kỳ người dùng được cấp quyền (Privileged User) nào
  - Thay đổi về nhân sự
- Tất cả các sự kiện quan trọng liên quan đến bảo mật:
  - Nỗ lực truy cập hệ thống PKI thành công và không thành công
  - Khởi động và tắt hệ thống/ứng dụng
  - Sở hữu dữ liệu kích hoạt của các hoạt động liên quan đến khoá bí mật của CA
  - Thay đổi. bảo trì, cấu hình hệ thống
  - Các hành động liên quan đến hệ thống an ninh và PKI được thực hiện bởi nhân viên của TrustCA
  - Các tệp hoặc hồ sơ nhạy cảm được đọc, viết hoặc xóa
  - Thay đổi cài đặt của chính sách bảo mật
  - Sự cố hệ thống, lỗi phần cứng và các lỗi bất thường khác
  - Hoạt động của tường lửa và bộ định tuyến
  - Khách thăm ra vào cơ sở của CA
  - Hành động ra/vào cơ sở đặt Remote QSCD
  - Quy trình khởi động, vận hành và quản trị thiết bị QSCD
- Biên mục Log bao gồm các phần tử sau:
  - Ngày và giờ nhập log
  - Số serial hoặc dãy số của biên mục, đối với biên mục log tự động
  - Danh tính của thực thể thực hiện ghi biên mục
  - Loại biên mục
- TrustCA ghi log đơn yêu cầu cấp chứng thư số:
  - Loại tài liệu nhận dạng do người nộp đơn xin cấp chứng thư số xuất trình
  - Ghi chép dữ liệu nhận dạng danh tính duy nhất, dạng số hoặc dạng kết hợp của những dữ liệu đó (ví dụ: số chứng minh thư của Thuê bao chứng thư số) từ các giấy tờ nhận dạng, nếu có thể. Vị trí lưu trữ các bản sao của các đơn yêu cầu cấu chứng thư số và giấy tờ nhận dạng đi kèm
  - Bất kỳ lựa chọn cụ thể nào trong đơn yêu cầu cấp Chứng thư số
  - Danh tính của thực thể chấp nhận đơn đăng ký và trong trường hợp Con dấu điện tử, danh tính của thể nhân đại diện cho pháp nhân được cấp chứng thư số dành cho con dấu điện tử
  - Phương pháp được sử dụng để xác thực các giấy tờ nhận dạng, nếu có
  - Tên của CA tiếp nhận hoặc RA gửi hồ sơ, nếu có thể

6.4.2 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.

6.4.3 *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
- Hồ sơ lưu trữ vật lý hoặc kỹ thuật số về các đơn yêu cầu cấp chứng thư, thông tin đăng ký và yêu cầu hoặc đơn xin thu hồi được lưu giữ ít nhất bảy (7) năm sau khi bất kỳ Chứng thư số nào dựa trên các hồ sơ này không còn hiệu lực.

Trong trường hợp CA chấm dứt hoạt động, log kiểm toán của TrustCA và hồ sơ lưu trữ được giữ lại, có thể truy cập được trong thời hạn lưu trữ.

6.4.4 *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 thông qua chữ ký số chứng thực của CA.

6.4.5 *Thủ tục sao lưu nhật ký*

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

6.4.6 *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

6.4.7 *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.

6.4.8 *Đánh giá lỗ hổng hệ thống*

TrustCA thực hiện quy trình đánh giá và phân tích rủi ro thường xuyên (ít nhất 1 tháng/lần) nằm tìm kiếm các lỗ hổng về an ninh an toàn hệ thống. Trong trường hợp phát hiện rủi ro an toàn thông tin nghiêm trọng, CA sẽ thực hiện tất cả các biện pháp cần thiết trong phạm vi năng lực để xử lý trong 48h kể từ khi phát hiện. Trường hợp CA cần nhiều hơn 48h để xử lý, thuê bao và các bên liên quan bị ảnh hưởng sẽ được thông báo qua Email hoặc dịch vụ CSKH.

6.5 *Lưu trữ các bản ghi*

6.5.1. *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…

6.5.2. *Thời hạn giữ lại các lưu trữ*

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

6.5.3. *Bảo vệ bản lưu trữ*

Hệ thống lưu dữ liệu lưu trữ được bảo vệ để chỉ những người được phép mới có thể truy nhập. Dữ liệu lưu trữ được bảo vệ theo các phương pháp cần thiết, chống lại việc xem,

thay đổi, xóa hay các thao tác khác không được cho phép. Hệ thống chứa dữ liệu lưu trữ và ứng dụng xử lý dữ liệu lưu trữ được duy trì để đảm bảo dữ liệu lưu trữ có thể được truy nhập trong khoảng thời gian được quy định trong quy chế chứng thực này. Ngoài ra, các bản lưu đều được ký chứng thực & đóng dấu thời gian bởi CA để đảm bảo tính toàn vẹn.

6.5.4. Các thủ tục sao lưu lưu trữ

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

6.5.5. Dấu thời gian của các bản lưu trữ

Dấu thời gian có thể áp dụng hoặc không áp dụng cho thuê bao. Nếu áp dụng, TrustCA sử dụng nguồn thời gian chuẩn quốc gia theo giấy phép dịch vụ Qualified Timestamping để cung cấp dịch vụ.

6.5.6. 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.

6.5.7. Thủ tục lấy và kiểm tra thông tin lưu trữ

Chỉ những người được cấp quyền mới được phép truy nhập tới thông tin lưu trữ. Thông tin lưu trữ sẽ được kiểm tra tính toàn vẹn khi được lấy ra. Ngoài ra, các bản lưu trữ có thể được cung cấp làm bằng chứng chứng cứ trước tòa.

6.6 Chuyển tiếp 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

6.7 Xử lý khi có sự cố và thảm họa

6.7.1 Các thủ tục kiểm soát sự cố và thảm họa

Trong trường hợp xảy ra sự cố, các nhân sự giám sát liên quan lập tức thông báo trong vòng 24h đến Ban Giám đốc. 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 lưu trữ chứng thư số được tạo ra. Khi có sự cố, các dữ liệu được phục hồi theo các thủ tục đã có.

6.7.2 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 bởi nhân sự tin cậy.

6.7.3 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 trang điện tử 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 thông qua Email hoặc dịch vụ CSKH
- 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.

Trong trường hợp khóa bí mật của CA bị lộ hoặc bất hoạt do thuật toán mã hóa lỗi thời hay các tham số khác trong quá trình sinh khóa – quản lý khóa, CA sẽ thông báo cho thuê bao và các bên liên quan thông qua Email, thông cáo báo chí hoặc dịch vụ CSKH để thông báo về việc tạm dừng các chứng thư số của các thuê bao liên quan. Quy trình tái tạo khóa bí mật của CA sẽ được kích hoạt dưới sự hướng dẫn và giám sát của NEAC.

6.7.4 Khả năng phục hồi hoạt động sau thảm họa

TrustCA luôn có hệ thống phục hồi để fallover trong trường hợp xảy ra sự cố. Thời gian phục hồi lâu nhất là 8 tiếng. Thời gian tái cấp danh sách thu hồi CRL tối đa là 24h kể từ khi sự cố gây ảnh hưởng đến tính liên tục của dịch vụ. Trong trường hợp thời gian phục hồi kéo dài lâu hơn thời gian nêu trên, thuê bao và các bên liên quan sẽ được thông báo qua Email hoặc dịch vụ CSKH. Một đội phản ứng nhanh sẽ được thành lập để đánh giá tình hình và báo cáo trực tiếp với Ban Giám Đốc.

Hệ thống dịch vụ của TrustCA được bảo vệ với cơ chế sẵn sàng cao thông qua các thành phần sẵn sàng cung ứng khi hệ thống chính gặp sự cố. Trong trường hợp xảy ra tổn thất về tài nguyên điện toán, phần mềm hoặc dữ liệu, quy trình phục hồi sau sự cố và kế hoạch duy trì liên tục dịch vụ sẽ được kích hoạt tại một cơ sở riêng biệt để tiếp tục cung cấp dịch vụ (cách 50km).

Ngay khi hệ thống của TrustCA được phục hồi tại cơ sở dự phòng, đội phản ứng nhanh sẽ thực hiện các tác vụ cần thiết trên cơ sở chính để đánh giá tình hình. Trong trường hợp thực hiện tác vụ cấp/thu hồi chứng thư số, đội phản ứng nhanh sẽ cập nhật các thông tin tra cứu cần thiết trên máy chủ Web của TrustCA. Đội phản ứng nhanh thực hiện quy trình chuyển giao dữ liệu từ cơ sở dự phòng đến cơ sở chính thông qua quy trình được phê duyệt bởi Ban Giám Đốc. Sau khi chuyển giao hoàn tất, hệ thống sẽ được kiểm tra lần cuối trước khi thông báo kết thúc xử lý sự cố. Toán bộ quy trình được ghi vết để xem xét, rút kinh nghiệm cho các kỳ xử lý sự cố sau này.

6.8 Kết thúc nhiệm vụ của CA/RA

Trong trường hợp kết thúc CA và RA, Công ty Cổ phần Công nghệ 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. Kế hoạch kết thúc nhiệm vụ của CA được thiết kế để giảm thiểu tối đa sự gián đoạn dịch vụ cho thuê bao và các bên liên quan, bao gồm:

- Công báo cho thuê bao và các bên liên quan bị ảnh hưởng, bao gồm cả RootCA

- Cung cấp thông tin về kế hoạch kết thúc kinh doanh cho thuê bao, các bên liên quan, đối tác thông qua Email, trang điện tử hoặc dịch vụ CSKH

- Duy trì và lưu trữ các bản lưu điện tử của CA trong thời gian cần thiết được quy định tại văn bản này

- Chuyển giao toàn bộ trách nhiệm cho cơ quan tiếp nhận có đủ năng lực hoặc tương đương theo quy định của pháp luật.

Trong trường hợp không thể chuyển giao cho cơ quan tiếp nhận nào đủ năng lực hoặc tương đương, hoặc không thể có thỏa thuận giữa TrustCA và đối tác tiếp nhận dữ liệu, TrustCA sẽ:

- Duy trì dịch vụ chăm sóc khách hàng và Help Desk

- Duy trì dịch vụ tra cứu trạng thái chứng thư số (VD: CRL)

- Tiêu hủy khóa bí mật của CA

- Chuyển giao các chức năng có thể chuyển giao cho các bên thứ ba tin cậy để lưu trữ, duy trì dữ liệu hoặc tổ chức, cơ sở chính quyền với đủ thẩm quyền tiếp nhận dữ liệu

- Thu hồi tất cả các chứng thư số chưa bị thu hồi hoặc chưa hết hạn theo quy định vận hành hệ thống hoặc theo thông báo của TrustCA, đồng thời cung cấp CRL cuối cùng

- Thu xếp các quy trình cần thiết để chuyển giao chức năng, nhiệm vụ CA

7 KIỂM SOÁT AN TOÀN KỸ THUẬT

7.1 Tạo khóa và phân phối khóa

7.1.1. 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 bí mật tới bất kỳ người nào khác
- Các khóa được tạo ra trong phần cứng HSM trong đó có khóa bí mật 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) và chủ thể cuối cùng phải được sinh và lưu trữ trong HSM.

Việc tạo các cặp khóa cho thuê bao của người dùng cuối thường được thực hiện bởi Thuê bao. Thuê bao sử dụng mô-đun mật mã được chứng nhận QSCD và tuân thủ các yêu cầu Quy định của eIDAS.

7.1.2. Gửi khóa bí mật cho thuê bao

Trong hầu hết các trường hợp, một khóa bí mật 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 bí mật. 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 đun 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.

7.1.3. 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 bí mật 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, yêu cầu này không được áp dụng.*

7.1.4. Gửi khóa công khai của CA cho các bên tin cậy

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.

Thuê bao, trong quá trình nhận chứng thư, tự động tải xuống và cài đặt vào máy tính của họ, các khóa công khai trung gian và phát hành CA. Trong mọi trường hợp nếu người dùng cần xác minh và / hoặc tải xuống khóa chung của CA, họ có thể làm như vậy bằng cách truy cập vào kho lưu trữ trên web của TrustCA (https://www.trustca.vn).

7.1.5. Độ dài khóa

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

7.1.6. Các tham số sinh khóa công khai và kiểm tra chất lượng

Không quy định.

7.1.7. Mục đích sử dụng khóa (trường Key Usage của X.509 v3)

Các khóa có thể được sử dụng cho việc xác thực, chống chối bỏ và tính toàn vẹn của thông điệp. Chúng cũng có thể được sử dụng cho việc thành lập các phiên khóa. Khóa ký riêng CA chỉ được cho phép sử dụng cho việc ký vào chứng thư số và các CRL. Trường sử dụng khóa chứng thư số phải tuân theo chứng thư số X.509 và hồ sơ CRL. Một trong những giá trị sử dụng của khóa phải được thể hiện trong tất cả các Chứng thư số:

- Chữ ký số
- Chống chối bỏ
- Một trong những giá trị tiếp theo dưới đây phải được thể hiện trong chứng thư số

CA ký chứng thư số

- Khóa ký chứng thư số
- Ký CRL
- Sử dụng một khóa đặc trưng được xác định bởi quy định chứng thư số X509 về sử dụng khóa.

7.2 Bảo vệ khóa bí mật và kiểm soát Module mã hóa bảo mật

7.2.1. Tiêu chuẩn đối với Module mã hóa

Hệ thống TrustCA Qualified e-Signatures sử dụng HSM nCipher đạt chứng nhận đạt tiêu chuẩn FIPS PUB 140-2 level 3 cho máy chủ CoreCA và HSM nCipher chứng nhận đạt tiêu chuẩn Common Criteria EAL4+ (AVA_VAN.5) certifed cho máy chủ ký số đáp ứng theo thông tư số 16/2019/TT-BTTTT. Module mã hóa được vận chuyển đến cơ sở của TrustCA từ nhà kho của Vendor dưới sự giám sát chặt chẽ, gắn tem chống chỉnh sửa và đi kèm tài liệu hướng dẫn. Khi thực hiện tiếp nhận, TrustCA thực hiện kiểm tra phiên bản Firmware như trên tài liệu của hãng thông qua Command Lines.

7.2.2. Kiểm soát khóa bí mật nhiều người dùng

TrustCA áp dụng các cơ chế kỹ thuật và quy trình thủ tục đòi hỏi sự tham gia của nhiều cá nhân tin cậy để thực hiện các hoạt động mã hóa nhạy cảm của CA. TrustCA sử dụng phương thức "Secret Sharing" để phân tách dữ liệu kích hoạt khóa bí mật của CA thành các phần riêng biệt gọi là "Secret Shares" được sở hữu bởi các cá nhân tin cậy gọi là "Shareholders". Ngưỡng số lượng Secret Share (m) trên tổng số Secret Share được tạo và phân phát (n) đối một thiết bị mã hoá phần cứng bảo mật là yêu cầu cần thiết để kích hoạt khoá bí mật được lưu trên thiết bị (module) đó.

Số lượng shares cần thiết để ký lên chứng thư số của CA là ba (3). Cần lưu ý rằng số lượng shares được phân phối cho các token với vai trò khắc phục thảm hoạ có thể ít hơn số lượng share được phân phối cho các token hoạt động thông thường, trong khi số lượng share được yêu cầu để kích hoạt vẫn giữ nguyên. Secret share được bảo vệ theo như CPS này.

Không áp dụng phương thức kiểm soát xác thực thông qua nhiều người với Khoá bí mật của thuê bao sử dụng dịch vụ.

7.2.3. Ủy quyền giữa các khóa bí mật

Không qui định.

7.2.4. Sao lưu khóa bí mật

Một bên tham gia có thể lựa chọn để sao lưu khóa bí mật 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. Các phiên bản sao lưu khóa bí mật không được tạo nhiều hơn nhu cầu cần thiết hoặc trái với quy định về chính sách an toàn thông tin.

TrustCA tạo bản sao dự phòng của Khoá bí mật của CA, và Khoá bí mật của Thuê bao được tạo và lưu trữ bởi Remote QSCD phục vụ cho mục đích khôi phục định kỳ và khôi phục sự cố. Các khóa như vậy được lưu trữ ở dạng mã hóa trong các mô-đun mã hóa phần cứng và các thiết bị lưu trữ khóa liên quan. Các mô-đun mã hóa được sử dụng để lưu trữ Khoá bí mật đáp ứng các yêu cầu của CPS này. Các Khoá bí mật được sao chép vào các mô-đun mã hóa phần cứng dự phòng theo CPS này. Quy trình sao lưu khóa bí mật được thực

hiện bởi nhân sự tin cậy theo quy tắc phân lập (dual-control) và least priviledge.

Các mô-đun chứa bản sao dự phòng Khoá bí mật của CA phải tuân theo các yêu cầu của CPS này. Các mô-đun chứa các bản sao khôi phục sự cố Khoá bí mật của CA phải tuân theo các yêu cầu của CPS này.

Trong trường hợp Local QSCD, Khoá bí mật của Thuê bao không thể được trích xuất hoặc khôi phục từ QSCD và không được sao lưu.

7.2.5. Lưu trữ khóa bí mật

Theo thoả thuận với chủ thể dùng cuối. Thiết bị QSCD được vận hành trong môi trường vật lý an toàn tuân thủ theo mục 2.1.2 của tài liệu Phương án kỹ thuật TrustCA Remote Signing.

7.2.6. Quá trình đưa Private key vào Module 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 RSA- 2048 cho việc tạo khóa và AES-256 cho việc mã hóa khóa bí mật.

Thiết bị mã hóa lưu tCrữ khóa CA đạt tiêu chuẩn bảo mật FIPS 140-2 Level 3.

TrustCA tạo các cặp khóa của thuê bao trên các mô-đun hóa phần cứng mà các khóa đó sẽ được sử dụng. Ngoài ra, TrustCA tạo các bản sao của các cặp khóa Thuê bao với mục đích khắc phục sự cố và sẵn sàng cao. Trong khi các cặp khóa của Thuê bao được sao lưu vào một mô-đun mật mã phần cứng khác, các cặp khóa sẽ được vận chuyển giữa các mô-đun ở dạng mã hóa.

Thiết bị mã hóa lưu trữ khóa thuê bao đạt tiêu chuẩn bảo mật Common Criteria EAL4+ (AVA_VAN.5).

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

7.2.7. Lưu trữ khóa bí mật trên Module mã hóa

Quy trình lưu trữ khóa bí mật vào Module 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.

7.2.8. Phương pháp kích hoạt khóa bí mật

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

Khoá bí mật của Thuê bao trên Local QSCD được bảo vệ bằng mã PIN. Các quy tắc sau được áp dụng:

- Thuê bao cần nhập mã PIN vào QSCD cho mỗi giao dịch.
- Thuê bao có nghĩa vụ thay đổi mã PIN và mã PUK trước khi bắt đầu quá trình đăng ký
- Trong trường hợp Thuê bao nhập mã PIN sai 5 lần liên tiếp, QSCD sẽ bị chặn
- Có thể bỏ chặn mã PIN bằng mã PIN của quản trị viên
- Việc sử dụng mã PIN của quản trị viên sẽ bị chặn sau 3 lần thử sai liên tiếp
- Người dùng có thể thay đổi mã PIN và mã PUK.

Khoá bí mật của Thuê bao trên Remote QSCD được bảo vệ bởi tên truy cập, mật khẩu và mã OTP. Các quy tắc sau được áp dụng:

• Thuê bao cần nhập tên truy cập, mật khẩu và mã OTP vào QSCD cho mỗi giao dịch.

• Trong trường hợp Thuê bao nhập sai tên truy cập, mật khẩu và mã OTP 5 lần liên tiếp, tài khoản Remote QSCD sẽ bị khóa

• Tài khoản Remote QSCD không thể đặt lại mật khẩu

• Người dùng có thể thay đổi mật khẩu.

Khóa bí mật trực tuyến của CA sẽ được kích hoạt bởi một số ngưỡng "Shareholders" nhất định, như được định nghĩa trong Mục 7.2.2, cung cấp dữ liệu kích hoạt (được lưu trữ trên phương tiện bảo mật). Khi khóa bí mật được kích hoạt, khóa bí mật có thể được kích hoạt trong một khoảng thời gian không giới hạn cho đến khi bị vô hiệu hóa khi CA ở trạng thái ngoại tuyến. Tương tự, cần phải có một ngưỡng Shareholders cần thiết để cung cấp dữ liệu kích hoạt cho việc khởi động Khoá bí mật của một CA đang ngoại tuyến. Khi khóa bí mật được kích hoạt, khoá sẽ chỉ hoạt động một lần.

7.2.9. Phương pháp làm khóa bí mật ngừng hoạt động

Các Module 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 Module mã hóa sẽ được gỡ bỏ và lưu trữ, trừ khi chúng hoàn toàn nằm trong sử kiểm soát của chủ thể cuối cùng.

7.2.10.Phương pháp hủy bỏ khóa bí mật

Các khóa bí mật 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 Module 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". Chỉ có Instance của khóa bí mật được lưu trữ trên module HSM nêu trên mới bị tiêu hủy.

7.2.11.Đánh giá Module mã hóa

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

7.3 Các khía cạnh khác của quản lý cặp khóa

7.3.1 Lưu trữ khóa công khai

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

7.3.2 Thời hạn hiệu lực của chứng thư số và 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 1 đến 3 năm. Mức thời gian hiệu lực của chứng thư số được ghi trên chứng thư số.

Thời hạn hiệu lực của cặp khóa của chứng thư số TrustCA tuân theo quy định của Bộ Thông tin và Truyền thông. Thời gian có hiệu lực được quy định 5 năm. Mức thời gian hiệu lực của cặp khóa tương ứng với chứng thư số và được ghi trên chứng thư số. Cặp khóa của CA được sử dụng cho mục đích cấp phát chứng thư số và kiểm tra trạng thái chứng thư số sẽ không được sử dụng cho bất cứ mục đích nào khác ngoài các hạng mục được quy định bởi cơ quan giám sát (VD: NEAC).

7.4 Kích hoạt dữ liệu

7.4.1 Khởi tạo kích hoạt dữ liệu và cài đặt

TrustCA thực hiện kích hoạt Module mã hóa chứa khóa bí mật của CA theo các quy trình và tham số khuyến nghị của nhà cung cấp theo chuẩn FIPS PUB 140-2 Level 3 và/hoặc Common Criterial EAL4+ cho CEN EN 419 221-5. Thiết bị mã hóa bảo mật được vận hành bởi tối thiểu hai nhân sự (tại mục 6.2.2 của văn bản CPS này). TrustCA chỉ chuyển giao dữ liệu kích hoạt thông qua các kênh/phương thức bảo mật, với khung thời gian và địa điểm khác so với thời gian và địa điểm tiếp nhận thiết bị.

Dữ liệu kích hoạt (Secret Share) được sử dụng để bảo vệ HSM có chứa Khoá bí mật của TrustCA được tạo theo các yêu cầu tại Mục 7.2.2 và Hướng dẫn tham khảo Lễ tạo khóa (Key Ceremoney Reference Guide). Việc tạo và phân phối Secret Shares được ghi lại.

Dữ liệu kích hoạt sử dụng để bảo vệ Local QSCD (PIN) có chứa các khóa bí mật của Đối tượng sử dụng, sẽ được tạo theo hướng dẫn sử dụng của QSCD.

• Trường hợp các cặp khóa của thuê bao đăng ký được TrustCA tạo trước, dữ liệu kích hoạt được gửi đến Thuê bao bằng dịch vụ chuyển phát.

• Trường hợp các cặp khóa của thuê bao được tạo bởi thuê bao đăng ký dịch vụ, dữ liệu kích hoạt định sẵn phải phải được thay đổi ngay lập tức trước thời điểm tạo khóa.

Dữ liệu kích hoạt sử dụng (tên truy cập, mật khẩu và mã OTP) để bảo vệ Remote QSCD có chứa khóa bí mật của Đối tượng sử dụng, được tạo ra theo các tiêu chuẩn tuân thủ của QSCD.

7.4.2 Bảo vệ dữ liệu kích hoạt

Nếu dữ liệu kích hoạt phải được chuyển cho đối tượng sử dụng, dữ liệu này được bảo về thông qua các kênh/phương thức bảo mật với khung thời gian và địa điểm khác biệt so với thời gian và địa điểm tiếp nhận thiết bị. Dữ liệu kích hoạt phải được ghi nhớ, không được ghi giấy. Mã PIN có thể được cung cấp cho đối tượng sử dụng thành hai phần với hai phương thức vận chuyển khác nhau (như dùng email và dùng thư tín) để tăng cường an ninh bảo mật trước nguy cơ mất cắp toàn bộ mã PIN. Dữ liệu kích hoạt không bao giờ được chia sẻ.

TrustCA Shareholders được yêu cầu bảo vệ Secret Shares của họ và Secret Shares của Remote QSCD, đồng thời ký thỏa thuận thừa nhận trách nhiệm của ShareHolder.

Thuê bao đăng ký sẽ phải ghi nhớ thông tin xác thực kích hoạt (PIN, PUK, tên truy cập, mật khẩu, OTP) và không chia sẻ với bất kỳ ai khác. Dữ liệu kích hoạt không chỉ bao gồm các thông tin có thể dễ dàng bị đoán được, ví như thông tin cá nhân.

7.4.3 Các khía cạnh khác của dữ liệu kích hoạt

Quy chế chứng thực này không quy định vòng đời của dữ liệu kích hoạt, tuy nhiên nên thay đổi định kỳ để giảm khả năng nó bị tiết lộ. CA có thể xác định các yêu cầu của dữ liệu kích hoạt trong CPS hoặc thỏa thuận chứng thư số.

7.5 Kiểm soát mức độ an ninh của máy tính

TrustCA ban hành chính sách an toàn thông tin với các chính sách, tiêu chuẩn và hướng dẫn thực hiện quy trình giám sát an ninh hệ thống. Chính sách an toàn thông tin được

phê duyệt bởi ban giám đốc và giám sát thực hiện bởi bộ phận TrustCA, đảm bảo toàn bộ nhân sự vận hành hệ thống nắm rõ các quy tắc an ninh bảo mật.

7.5.1 Yêu cầu chi tiết kỹ thuật về mức độ an ninh của máy tính

TrustCA thực hiện bảo mật toàn bộ hệ thống CA và xác thực kết nối giữa các thành phần của hệ thống cũng như phân hệ phụ trách bởi các vai tin cậy. Các máy chủ của TrustCA và các máy tính phục vụ mạng lưới hỗ trợ, phê duyệt hồ sơ cấp chứng thư số được vận hành trên các hệ thống tin cậy, được cấu hình và tăng cường an ninh với những thông lệ và quy tắc bảo mật tốt nhất trên thị trường. Tất cả các hệ thống của CA được quét mã độc, virus và phần mềm gián điệp. Thời gian tự động log-out được cấu hình theo chính sách an toàn thông tin để đảm bảo quy trình bảo mật khi vận hành hệ thống.

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 lưu trữ kiểm tra được bảo vệ

Ngoài ra, TrustCA áp dụng cơ chế xác thực đa yếu tố MFA cho tất cả các hệ thống và tài khoản chịu trách nhiệm phê duyệt, cấp chứng thư số.

7.5.2 Cấp độ an toàn hệ thống

Phiên bản phần mềm CoreCA của TrustCA đạt chứng chỉ Common Criteria EAL 4+

khi triển khai dịch vụ.

7.6 Kiểm soát quản lý kỹ thuật vòng đời

7.6.1. 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.

TrustCA có các cơ chế để kiểm soát và giám sát việc thu mua và phát triển các hệ thống CA. Yêu cầu thực hiện thay đổi trên hệ thống cần có sự chấp thuận của ít nhất một quản trị viên khác với người gửi yêu cầu. TrustCA chỉ cài đặt phần mềm trên hệ thống CA nếu phần mềm cần thiết cho hoạt động của CA. Phần cứng và phần mềm CA được phân lập để thực hiện các hoạt động của CA.

Các nhà cung cấp phần cứng và phần mềm được lựa chọn dựa trên tín nhiệm, khả năng cung cấp sản phẩm chất lượng và tiềm năng đối tác trong tương lai. Ban giám đốc tham gia vào quá trình lựa chọn nhà cung cấp. Tất cả phần cứng và phần mềm được vận chuyển trong các điều kiện tiêu chuẩn theo hướng dẫn của nhà cung cấp để đảm bảo việc chuyển giao hàng hóa trực tiếp cho nhân sự tin cậy của TrustCA, đảm bảo rằng hàng hóa chuyển giao không bị chỉnh sửa và giả mạo.

Quy trình kiểm định chất lượng được duy trì thông qua các quy trình kiểm thử hoặc thu mua từ các nhà cung cấp tin cậy nêu trên. Các bản cập nhật của linh kiện, phần mềm, hoặc thiết bị sẽ được TrustCA thu mua hoặc tự phát triển theo phương thức tương tự như đối với linh kiện, phần mềm hoặc thiết bị ban đầu và được cài đặt, kiểm tra bởi các nhân sự có trình độ nghiệp vụ. Tất cả phần cứng, phần mềm cần thiết cho hoạt động của hệ thống TrustCA được quét mã độc trong lần hoạt động đầu tiên và định kỳ thông qua nền tảng TrustCA SOC.

7.6.2. 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.

7.6.3. 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.

7.7 Kiểm soát an toàn, an ninh mạng

Áp dụng các quy trình được đề cập tại mục 2.9 của tài liệu Phương án kỹ thuật hệ thống TrustCA. Ngoài ra, TrustCA hình thành tài liệu và quy trình kiểm soát đối với việc cấu hình hệ thống, bao gồm các bản cập nhật và chỉnh sửa. Khóa bí mật của CA (Root Keys) được lưu ở chế độ ngoại tuyến (offline) và chỉ hoạt động khi cần thiết để ký phát hành chứng thư số thuê bao, chứng thư số của phản hồi OCSP hoặc danh sách CRL theo định kỳ. Hệ thống tường lửa và các thiết bị giám sát ngoại vi được cấu hình để đảm bảo chỉ có những địa chỉ, cổng port hoặc giao thức protocol cần thiết cho hoạt động của hạ tầng PKI được

thông qua. Chính sách an toàn thông tin của TrustCA yêu cầu việc chặn toàn bộ các cổng port và giao thức protocol không cần thiết và chỉ mở những cổng port và giao thức quan trọng đối với các chức năng của CA. Tất cả các thiết bị phục vụ hoạt động của CA được cấu hình để chạy số lượng service tối thiểu, và tất cả các cổng port hoặc service không cần thiết đều bị vô hiệu hóa.

7.8 Dấu thời gian

Các quy chế áp dụng được nêu tại văn bản "Quy chế - chính sách chứng thực dịch vụ dấu thời gian TrustCA Qualified Timestamping CA".

8 HỒ SƠ CHỨNG THƯ SỐ, CRL VÀ OCSP

8.1 Hồ sơ 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.

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 điểm 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

8.1.1. Số phiên bản

TrustCA cung cấp chứng thư số X509 phiên bản 3

8.1.2. Trường 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.

8.1.3. Số hiệu thuật toán

Chứng thư số của TrustCA sử dụng các thuật toán sau đây:

- sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) memberbody(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

8.1.4. Định dạng tên

Định dạng tên của chứng thư số tuân theo quy định trong mục 3.1.1

8.1.5. Thuộc tính ràng buộc của tên

Chủ thể và các tên cấp phát riêng biệt phải tuân theo chuẩn X.509 và được thể hiện trong tất cả các chứng thư số.

8.1.6. Định dạng quy chế chứng thực

Số hiệu (OID) của CP/CPS này sẽ được đăng ký khi hệ thống TrustCA chính thức đi vào hoạt động.

8.1.7. Sử dụng thuộc tính ràng buộc để mở rộng chính sách chứng thư số

Không quy định

8.1.8. Cú pháp và ngữ nghĩa của quy chế

Không quy định

8.1.9. Xử lý ngữ nghĩa các trường mở rộng quy chế chứng thư số quan trọng

Không quy định

8.2. Hồ sơ 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/qes-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

8.2.1. Số phiên bản của CRL

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

8.2.2. CRL và các trường mở rộng của CRL

Không quy định.

8.3. Hồ sơ 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://ocsp3.trustca.vn

8.3.1. Số phiên bản của OCSP

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

8.3.2. Trường mở rộng của OCSP

Không quy định.

9. TUÂN THỦ KIỂM TOÁN VÀ CÁC KIỂM ĐỊNH KHÁC

9.1. Tần suất thực hiện kiểm định

TrustCA sẽ tuân thủ kiểm toán. Ngoài ra TrustCA thực hiện tự đánh giá hoạt động của TrustCA /RA/ ít nhất mỗi năm một lần

9.2. Khả năng của người kiểm định

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

9.3. Mối quan hệ của người kiểm định với tổ chức được kiểm định

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

9.4. Các nội dung cần kiểm định

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

9.5. Xử lý khi phát hiện sai sót

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

9.6. Công bố kết quả kiểm định

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

9.7. Phương án cung cấp trực tuyến thông tin thuê bao cho Tổ chức cung cấp dịch vụ chứng thực chữ ký số Quốc gia

Hệ thống TrustCA có máy chủ Web cổng thông tin điện tử (RA portal Front-end) cung cấp trên mạng Internet được kết nối tích hợp với máy chủ RA Backend thông qua API nhằm sẵn sàng cung cấp trực tuyến thông tin thuê bao cho tổ chức cung cấp dịch vụ chứng thực chữ ký số Quốc gia, phục vụ công tác quản lý Nhà nước về dịch vụ chứng thực chữ ký số. Đồng thời đảm bảo và nâng cao về an toàn cơ sở dữ liệu người dùng, thông tin CSDL chứng thư số của hệ thống.

Máy chủ Web RA này được kết nối đến máy chủ CSDL lưu trữ và quản lý chứng thư số (RA Back-end) và cho phép người sử dụng truy nhập trực tuyến 24 giờ trong ngày và 7 ngày trong tuần để tra cứu kiểm tra trạng thái chứng thư số của người dùng.

Để sẵn sàng cung cấp trực tuyến thông tin thuê bao cho tổ chức hoặc ra bên ngoài khi có yêu cầu, Máy chủ Web RA portal cổng thông tin điện tử của hệ thống TrustCA có chức năng cung cấp các hàm API với yêu cầu xác thực quyền bảo mật theo từng API cho phép cung cấp thông tin dữ liệu của thuê bao cho Tổ chức cung cấp dịch vụ chứng thực chữ ký số Quốc gia.

9.8. Thực hiện cung cấp thông tin phục vụ kiểm tra, đánh giá theo quy định

TrustCA cam kết thực hiện cung cấp thông tin cho Trung tâm chứng thực điện tử quốc gia phụ vụ đánh giá, kiểm tra định kỳ 06 tháng 1 lần theo quy định.

10 CÁC NHIỆM VỤ KHÁC VÀ CÁC VẤN ĐỀ VỀ PHÁP LÝ

10.1. Phí

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

10.1.1 Phí cấp phát, 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.

10.1.2 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.

10.1.3 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.

10.1.4 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.

10.1.5 Chính sách hoàn phí

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

10.2 Trách nhiệm tài chính

10.2.1 Bảo hiểm

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

10.2.1.1 **Bồi thường bởi chủ thể cuối cùng**

Trong phạm vi của luật áp dụng, thỏa thuận chủ thể cuối cùng và các thỏa thuận khác yêu cầu chủ thể cuối cùng bồi thường cho TrustCA và cho các tổ chức CA không phải là TrustCA, và RA trong các trường hợp:

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

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

10.2.1.2 Bồi thường do RP

Trong phạm vi của luật áp dụng, thỏa thuận RP và các thỏa thuận khác yêu cầu RP bồi thường cho TrustCA và thuê bao của TrustCA, và RA về

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

10.2.2 Các tài sản khác

TrustCA có quyền tự chủ tài chính để duy trì hoạt động và thực hiện các nhiệm vụ của mình, đồng thời có trách nhiệm pháp lý đối với các rủi ro cho thuê bao và người nhận.

10.3 Bảo mật thông tin trong hoạt động TrustCA

10.3.1 Phạm vi các thông tin bí mật

Các thông tin được đảm bảo bí mật bao gồm:

- Các thông tin liên quan đến TrustCA, trừ khóa công khai;
- Dữ liệu cá nhân 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.

Thông tin của thuê bao là cá nhân hoặc tổ chức được lưu trữ bởi TrustCA trong quá trình khởi tạo hợp đồng và cấp chứng thư số được coi là thông tin cấp độ mật. Do đó, các thông tin này không được cung cấp trước khi có sự chấp thuận của thuê bao, trừ trường hợp cần thiết do yêu cầu của cơ quan pháp luật hoặc phục vụ các yêu cầu đề ra tại văn bản CPS này.

Tất cả các thông tin bí mật (bao gồm dữ liệu cá nhân và/ hoặc thông tin riêng tư của 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 không cần được bảo vệ: 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.

10.3.2. Những thông tin ngoài phạm vi thông tin bí mật:

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.

10.3.3. Trách nhiệm bảo vệ các thông tin bí mật

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

10.4 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 theo mô hình ký số từ xa TrustCA Remote Signing"**
- Ngoài ra, giữa TrustCA và bên cung cấp dịch vụ eKYC đã có ký cam kết các điều khoản về bảo mật, đảm bảo an toàn, an ninh thông tin của khách hàng.
- 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 đề nghị cung cấp Dịch vụ chứng thực chữ ký số bằng phương thức điện tử, Điều Kiện Điều Khoản được hiển thị trên ứng dụng cấp chứng thư số của TrustCA. Khách hàng bắt buộc phải đọc và đồng ý với Điều Kiện Điều Khoản trên thì mới có thể thực hiện các bước đề nghị cấp chứng thư số TrustCA. Khách hàng thể hiện nội dung đã đồng ý bằng việc tick chọn/xác nhận.
  - 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.

10.4.1 Kế hoạch bảo vệ thông tin riêng tư

TrustCA sẽ đảm bảo bí mật các thông tin bí mật cá nhân thuê bao, không được cung cấp cho bên thứ ba trừ trường hợp có yêu cầu của cơ quan nhà nước có thẩm quyền hoặc thoả thuận khác giữa thuê bao và TrustCA. Chính sách bảo vệ thông tin cá nhân tuân thủ quy định GDPR trong quy trình quản lý và bảo mật tính riêng tư của thuê bao và các bên liên quan. 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.

10.4.2 Loại hình dữ liệu thu thập

Tất cả các 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, bao gồm (nhưng không giới hạn bởi) các thông tin:

- Tên đầy đủ của thuê bao
- Số điện thoại của thuê bao
- Địa chỉ của thuê bao
- Số chứng minh nhân dân, căn cước công dân, hộ chiếu
- Địa chỉ Email (nếu có)

10.4.3 Dữ liệu sử dụng dịch vụ của thuê bao

Dữ liệu sử dụng dịch vụ của thuê bao sẽ được thu thập tự động. Dữ liệu này có thể

bao gồm các thông tin như địa chỉ IP của thuê bao, loại trình duyệt, phiên bản trình duyệt, trang tin đã truy cập, thời gian và thời lượng truy cập, thời gian hoạt động trên mỗi trang, định danh thiết bị (UID) và các thông tin phân tích dữ liệu khác.

Khi thuê bao sử dụng dịch vụ thông qua thiết bị di động, TrustCA có thể thu thập các thông tin về thiết bị như chủng loại thiết bị, mã UID của thiết bị di động, địa chỉ IP của thiết bị di động, hệ điều hành của thiết bị di động, loại trình duyệt trên di động, tính năng hỗ trợ sinh trắc học và các thông tin phân tích dữ liệu khác.

TrustCA có thể thu thập thông tin mà trình duyệt của thuê bao gửi tới khi thuê bao truy cập dịch vụ hoặc khi thuê bao sử dụng thiết bị di động để truy cập dịch vụ.

10.4.4 Mục đích sử dụng dữ liệu cá nhân của thuê bao

TrustCA có thể sử dụng dữ liệu cá nhân cho các mục đích như:

- **Cung cấp và duy trì** dịch vụ, bao gồm việc giám sát dữ liệu sử dụng dịch vụ.
- **Quản lý tài khoản của thuê bao**: dữ liệu cá nhân mà thuê bao cung cấp giúp tối ưu hóa các chức năng cần thiết trong quy trình sử dụng.
- **Thực hiện hợp đồng**: quy trình phát triển, cung cấp sản phẩm, dịch vụ theo hợp đồng giữa nhà cung cấp và thuê bao.
- **Liên hệ thuê bao**: thông qua phương thức email, số điện thoại, SMS, hoặc các phương tiện điện tử tương đương khác, như thông báo Push Notification qua app điện thoại về bản cập nhật hoặc các thông tin liên quan đến chức năng, bảo mật của sản phẩm, dịch vụ, khi cần thiết hoặc hợp lý để triển khai.
- **Cung cấp tin tức, thông tin** hoặc chương trình chăm sóc khách hàng về các sản phẩm, hàng hóa hoặc sự kiện liên quan đến sản phẩm, dịch vụ thuê bao đã sử dụng hoặc yêu cầu tư vấn, trừ trường hợp thuê bao lựa chọn không muốn nhận thông tin này.
- **Xử lý yêu cầu của thuê bao**: bao gồm việc truy vấn và quản lý các yêu cầu của thuê bao về sản phẩm, dịch vụ.
- **Chuyển giao kinh doanh**: thông tin của thuê bao có thể được sử dụng trong hoạt động đánh giá hoặc chuyển nhượng, tái cấu trúc, tái tổ chức, hay các hình thức kinh doanh khác để chuyển giao toàn bộ hoặc một phần tài sản thông tin của TrustCA, phục vụ mục đích được đề ra tại văn bản CPS này về kế hoạch kinh doanh liên tục hay các quy trình tương tự khác liên quan đến việc xử lý thông tin cá nhân của thuê bao được lưu trữ bởi TrustCA.
- **Các mục đích khác**: sử dụng thông tin cá nhân của thuê bao để thực hiện phân tích dữ liệu, nhận diện thói quen tiêu dùng, đánh giá mức độ hài lòng với sản phẩm, dịch vụ và xây dựng phương án cải tiến kinh doanh cũng như trải nghiệm người dùng.

10.4.5 Lưu trữ thông tin cá nhân của thuê bao

TrustCA chỉ lưu trữ thông tin cá nhân của thuê bao theo thời hạn cần thiết được đặt ra tại văn bản CPS này. TrustCA sẽ thực hiện lưu trữ và sử dụng thông tin cá nhân của thuê bao một cách hợp lý để tuân thủ trách nhiệm pháp lý (ví dụ: luật lưu trữ hoặc luật chuyên ngành), giải quyết tranh chấp, hoặc giám sát tuân thủ đối với các quy định tại hợp đồng với

thuê bao.

TrustCA có thể sử dụng dữ liệu cá nhân được lưu trữ cho mục đính kiểm toán, đánh giá và phân tích nội bộ. Dữ liệu tiêu dùng của thuê bao có thể được lưu trữ trong thời gian ngắn, trừ khi được sử dụng để phân tích tăng cường an ninh hoặc cải tiến chất lượng dịch vụ. TrustCA cũng tuân thủ các quy định về lưu trữ điện tử khi nghiệp vụ của thuê bao yêu cầu.

10.4.6 Chuyển giao thông tin cá nhân của thuê bao

Thông tin của thuê bao, bao gồm thông tin cá nhân, được xử lý tại văn phòng của TrustCA hoặc tại bất cứ địa điểm nào khác các của bên liên quan trong quy trình xử lý thông tin hoặc trường hợp chuyển giao thông tin. Điều này có nghĩa thông tin có thể được chuyển giao – và duy trì – tại các máy tính ngoài khu vực hoạt động của TrustCA, hoặc khu vực mà chính sách bảo vệ thông tin có điểm khác biệt với chính sách của TrustCA. Việc chấp thuận của thuê bao với chính sách này của TrustCA, cùng với hành vi gửi các thông tin theo hợp đồng, thỏa thuận với TrustCA thể hiện thuê bao đồng ý thực hiện chuyển giao thông tin trong trường hợp cần thiết.

TrustCA cam kết thực hiện tất cả các quy trình yêu cầu để đảm bảo dữ liệu cá nhân của thuê bao được xử lý an toàn và tuân thủ theo chính sách bảo vệ thông tin cá nhân này; đồng thời không thực hiện chuyển giao thông tin cá nhân cho các tổ chức, cơ quan trừ khi các tổ chức, cơ quan đó cũng chứng minh được khả năng bảo vệ an ninh an toàn thông tin cá nhân của thuê bao cũng như các thông tin có liên quan.

10.4.7 Trường hợp chia sẻ thông tin cá nhân của thuê bao

Trong trường hợp công ty của TrustCA tham gia vào quy trình xác nhập, mua lại hoặc chuyển giao tài sản, thông tin cá nhân của thuê bao có thể được chuyển giao. TrustCA sẽ thông báo cho thuê bao trước khi dữ liệu cá nhân được chuyển giao.

10.4.8 Với các cơ quan quản lý, hành pháp

Trong một số trường hợp nhất định, TrustCA có thể tiết lộ thông tin cá nhân của thuê bao theo yêu cầu của cơ quan có thẩm quyền hoặc phục vụ tranh chấp, kiện tụng theo yêu cầu của pháp luật hiện hành.

10.4.9 Các yêu cầu pháp lý khác

TrustCA có thể chia sẻ, tiết lộ thông tin cá nhân của thuê bao nếu việc đó là cần thiết để đảm bảo:

- Tuân thủ với các quy định pháp luật
- Bảo vệ và đảm bảo quyền lợi hợp pháp/tài sản của TrustCA
- Phòng chống hoặc điều tra các hoạt động bất hợp pháp liên quan tới dịch vụ, sản phẩm cung cấp
- Bảo vệ an toàn thuê bao sử dụng dịch vụ hoặc cộng đồng
- Thực thi trách nhiệm trước pháp luật

10.4.10 An ninh dữ liệu cá nhân

TrustCa cam kết đảm bảo an ninh an toàn dữ liệu cá nhân của thuê bao thông qua các phương tiện, phương thức hợp lý.

10.4.11 Thay đổi, cập nhật chính sách bảo mật thông tin cá nhân

TrustCA có thể cập nhật chính sách bảo mật thông tin cá nhân của thuê bao định kỳ. TrustCA sẽ thông báo cho thuê bao trong trường hợp thay đổi chính sách bảo mật thông tin qua trang điện tử, email hoặc cổng dịch vụ khách hàng, trước khi các thay đổi có hiệu lực và cập nhật ngày ban hành phiên bản.

10.5 Quyền sở hữu trí tuệ

10.5.1 Khóa bí mật

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

10.5.2 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.

10.5.3 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

10.6 Tuyên bố và các đảm bảo

TrustCA đảm bảo:

- Cung cấp các dịch vụ phù hợp với các yêu cầu và quy trình được quy định trong CPS và các tài liệu liên quan;
- Tuân thủ quy định của eIDAS và các yêu cầu pháp lý liên quan được quy định trong CPS và các tài liệu liên quan;
- Công bố CPS và các tài liệu liên quan, đảm bảo tài liệu truy cập được trên mạng công cộng;
- Công bố và đáp ứng các yêu cầu về điều khoản sử dụng đối với thuê bao đăng ký và đảm bảo tính khả dụng, quyền truy cập của thuê bao trên mạng công cộng;
- Duy trì bảo mật thông tin không được phép công bố trong quá trình cung cấp dịch vụ;
- Theo dõi Trusted Service Token đã cấp cũng như tính hợp lệ của Token, đảm bảo chức năng kiểm tra tính hợp lệ của Chứng thư số;
- Đảm bảo quyền truy cập các khóa bí mật trên Remote QSCD với các thuê bao được ủy quyền
- Đảm bảo tuân thủ các biện pháp quản lý Remote QSCD
- Thông báo cho Cơ quan giám sát về bất kỳ thay đổi nào đối với khóa công khai sử dụng trong việc cung cấp Dịch vụ tin cậy;
- Thông báo cho Cơ quan giám sát và, nếu có thể, các cơ quan có liên hoặc Thanh tra dữ liệu quốc gia, về bất kỳ lỗ hổng an ninh hoặc mất tính toàn vẹn nào ảnh hưởng đến Dịch vụ tin cậy cung cấp hoặc dữ liệu của cá nhân trong vòng 24 giờ sau khi phát hiện
- Trong trường hợp xuất hiện lỗ hổng an ninh hoặc mất tính toàn vẹn dự liệu có khả năng ảnh hưởng nguy hại đến một cá nhân hoặc pháp nhân mà Dịch vụ tin cậy đã cung cấp, sẽ nhanh chóng thông báo cho cá nhân hoặc pháp nhân về lỗ hổng an ninh an ninh hoặc mất tính toàn vẹn dữ liệu trong vòng 24h kể từ khi phát hiện;
- Trong trường hợp xuất hiện lỗ hổng an ninh hoặc mất tính toàn vẹn dữ liệu ảnh hưởng

nghiêm trọng đến các dịch vụ tin cậy và/hoặc liên quan đến dữ liệu cá nhân của thuê bao, tất cả các đối tác và thuê bao liên quan sẽ được TrustCA thông báo qua email và dịch vụ CSKH trong vòng 24h kể từ khi phát hiện;

- Bảo quản tất cả các tài liệu, hồ sơ và log liên quan đến Dịch vụ tin cậy theo Mục 6.4 và 6.5;
- Có tài chính ổn định và các nguồn lực cần thiết để duy trì hoạt động phù hợp với CPS;
- Công bố các điều khoản về chính sách bảo hiểm bắt buộc và kết luận của cơ quan đánh giá tuân thủ trên mạng công cộng;
- Cung cấp quyền truy cập vào các dịch vụ của mình cho người khuyết tật nếu có thể. TrustCA thực hiện trong phạm vi cho phép để đảm bảo quyền lợi công bằng cho tất cả các thuê bao sử dụng dịch vụ, đặc biệt là các thuê bao khuyết tật. TrustCA công nhận rằng thuê bao sử dụng dịch vụ cần sở hữu năng lực pháp lý nhất định, nhưng sẽ thực hiện trong khả năng để không xảy ra tình trạng phân biệt đối xử khi cung ứng dịch vụ và giải pháp kỹ thuật.
- Không có sự sai lệch về thông tin trong Chứng thư số đã được tiếp nhận hoặc có nguồn gốc từ các các cơ quan phê duyệt Đơn đăng ký Chứng thư số hoặc cấp Chứng thư số,
- Không phát sinh lỗi sai trong thông tin của Chứng thư số khi tiếp nhận yêu cầu từ cơ quan chấp thuận đơn đăng ký cấp Chứng thư số/phát hành chứng thư số do bất cẩn khi quản lý đơn đăng ký hoặc quy trình tạo Chứng thư số
- Dịch vụ thu hồi và sử dụng kho lưu trữ Repository tuân thủ với CPS,

Các điều khoản sử dụng của TrustCA về việc sử dụng Chứng thư số có thể bao hàm các đại diện và bảo đảm bổ sung.

10.7 Từ chối bảo hành

Trừ các điều khoản được nêu tại mục 10.6, chứng thư số được cung cấp "theo nguyên trạng" và "theo sẵn có", tuân thủ các yêu cầu của pháp luật áp dụng. TrustCA từ chối mọi suy luận, suy diễn về trách nhiệm bảo hành, bao gồm các bảo đảm về khả năng thay đổi linh hoạt, phù hợp với mục đích cụ thể và không vi phạm quy định. Trustca không bảo đảm rằng tất cả chứng thư số sẽ đáp ứng được kỳ vọng của thuê bao hoặc của bất kỳ bên khác, hoặc đối với khả năng tiếp cận và sử dụng chứng thư số kịp thời và không xảy ra vấn đề nào.

TrustCA không đảm bảo tính khả dụng của bất kỳ chứng thư số nào và có thể thay đổi hoặc ngừng cung cấp chứng thư số. TrustCA sử dụng mọi nguồn lực hợp lý để tiến hành sửa lỗi trong quá trình sử dụng chứng thư số của thuê bao, kể từ khi nhận được thông báo của thuê bao, trừ trường hợp TrustCA không có nghĩa vụ đối với các lỗi phát sinh từ (i) sử dụng chứng thư số sai mục đích, gây tổn thất hoặc tự ý chỉnh sửa, gây hư hại đối với chứng thư số hoặc tổ hợp của các sản phẩm/dịch vụ bên thứ ba khác sử dụng cùng chứng thư số của TrustCA, hoặc (ii) khi thuê bao vi phạm bất cứ điều khoản nào về hợp đồng đã ký với TrustCA.

10.8 Giới hạn trách nhiệm

Không tính đến các điều khoản trong văn bản CP/CPS này, trách nhiệm tối đa của TrustCA đối với bất cứ tổn thất nào về thỏa thuận sử dụng chứng thư số sẽ không quá 10.000.000 VND.

Trong mọi trường hợp, TrustCA sẽ không chịu trách nhiệm pháp lý đối với chủ sở hữu chứng thư số hoặc bất kỳ bên thứ ba nào phụ thuộc hoặc sử dụng chứng thư số của TrustCA gây ra bất kỳ thiệt hại gián tiếp, đặc biệt, ngẫu nhiên, bị trừng phạt hoặc do hậu quả gây nên, ngay cả khi TrustCA đã được thông báo về khả năng xảy ra những tổn thất đó từ trước.

10.9 Sự bồi thường

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

10.10 Hiệu lực và chấm dứt

- CP/CPS có hiệu lực và được công nhận từ khi TrustCA công nhận
- Kết thúc của CP/CPS trong các trường hợp:
  - Hết hạn/thu hồi toàn bộ chứng thư số TrustCA
  - Dịch vụ của TrustCA chấm dứt
  - Một phiên bản mới của CP/CPS được công nhận

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

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

10.12 Bổ sung, thay đổi quy chế chứng thực

- 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 đáng kể 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

10.13 Thủ tục giải quyết tranh chấp

Áp dụng mục 9 & 10 trong tài liệu Điều khoản và Điều kiện sử dụng dịch vụ.

10.14 Luật áp dụng

Hệ thống cung ứng dịch vụ TrustCA Remote Signing tuân thủ các quy định của pháp luật về chữ ký điện tử, chữ ký số và mô hình ký số từ xa như:

- Luật giao dịch điện tử 2005
- Nghị định 130/2018/ND-CP
- Thông tư 06/2015/TT-BTTTT
- Thông tư 16/2019/TT-BTTTT
- Thông tư 22/2020/TT-BTTTT

10.15 Tính tuân thủ

Áp dụng khung pháp lý tại mục 10.14.

10.16 Các quy định chung

Hệ thống cung ứng dịch vụ TrustCA Remote Signing tuân thủ nghiêm ngặt các quy tắc về an toàn thông tin cá nhân của GDPR. Ngoài ra, TrustCA cam kết trong phạm vi cho phép về việc cung ứng dịch vụ công bằng cho mọi thuê bao, kể cả người dùng khuyết tật.

10.17 Các quy định 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 bí mật 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 bí mật 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 bí mật CA tạo chữ ký (CA Private Signing	Khóa bí mật cùng cặp với khoá công khai nằm trong chứng thực CA và được sử dụng để ký chứng thực
Khóa gốc riêng CA (CA Private Root Key)	Khóa bí mật sử dụng để ký chứng thư số CA.
Chứng thư số (Certificate)	Một bản lưu trữ 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 bí mật 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 (Cross-Certificate)	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 lưu trữ điện tử do một người sử dụng khóa bí mật và khóa công khai tạo ra, và người nhận có bản lưu trữ 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 bí mật tương ứng với khóa chung hay không; và (ii) liệu bản lưu trữ 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 lưu trữ điện tử, và không bị kiểm soát hay tác động bởi chính người thực hiện.
Chủ thể cuối cùng (End-entity(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 bí mật 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 chỉ 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	Trạng thái thời gian thực được kiểm tra trực tuyến về thời hạn hiệu lực của chứng thư số. Kiểm tra trạng thái trực

Check)	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 bí mật (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 bí mật 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 qui 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 nghệSAVIS
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 Union-T) 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 Requirements 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 Requirements 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	Áp dụng tiêu chuẩn RSA: + Phiên bản 2.1 + Áp dụng lược đồ RSAES-OAEP để mã hóa và RSASSA-PSS để ký. + Độ dài khóa tối thiểu là 2048 bit
		TCVN 7816:2007 (FIPS PUB 197)	Công nghệ thông tin - Kỹ thuật mật mã - Thuật toán mã hóa dữ liệu AES		

2,2	Mật mã đối xứng	NIST 800-67	Recommendation for the Triple Data Encryption Algorithem (TDEA) Block Cipher	Áp dụng một trong hai tiêu chuẩn	AES
Số TT	**Loại tiêu chuẩn**	**Ký hiệu tiêu chuẩn**	**Tên đầy đủ của tiêu chuẩn**	**Quy định áp dụng**	**Trust CA áp dụng**
2,3	Hàm băm an toàn	FIPS PUB 180-4	Secure Hash Standard	Áp dụng một trong sáu hàm băm: SHA-224, SHA-256, SHA-384, 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 Infrastructure 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 bí mật	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
Số TT	**Loại tiêu chuẩn**	**Ký hiệu tiêu chuẩn**	**Tên đầy đủ của tiêu chuẩn**	**Quy định áp**	**Trust CA áp dụng**
	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 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 4511, RFC 4512, RFC 4513	
		RFC 4513	Lightweight Directory Access Protocol (LDAP):		
Số TT	**Loại tiêu chuẩn**	**Ký hiệu tiêu chuẩn**	**Tên đầy đủ của tiêu chuẩn**	**Quy định áp**	**Trust CA áp dụng**
			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 - On- line 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
		TCVN 7818-1:2007 (ISO/IEC 18014-1:2002)	Công nghệ thông tin - Kỹ thuật mật mã - Dịch vụ tem thời gian - Phần 1: Khung tổng quát		

7,2	Dịch vụ cấp dấu thời gian	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	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 7818-3:2010 (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		