CÔNG TY TNHH PHÁT TRIỂN CÔNG NGHỆ THÁI SƠN

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

Số: 01/2023/CPS-TSD

Hà Nội, ngày 13 tháng 07 năm 2023

QUY CHẾ CHỨNG THỰC E-CA

(Thông tư số 31/2020/TT-BTTTT ngày 30 /10/ 2020 của Bộ trưởng Bộ Thông tin và Truyền thông)

Phiên bản: 01

OID: 2.16.704.100.23.3

MỤC LỤC

1. GIỚI THIỆU.

1.1. Tổng quan.

Tài liệu này là quy chế chứng thực chữ ký số của E-CA. Tài liệu nêu rõ các quy trình, thủ tục cấp, quản lý chứng thư số, sử dụng chứng thư số của thuê bao và mối quan hệ giữa E-CA với đại lý và thuê bao của mình.

Tài liệu Quy chế chứng thực tuân thủ theo "Khung quy chế chứng thực và chính sách chứng thư" RFC 3647 (IETF Certificate Policy and Certification Practice Statement)

1.2. Tên và dấu hiệu nhận diện tài liệu.

Tài liệu này được xác định bởi bộ định dạng đối tượng (OID).

OID của quy chế chứng thực này là 2.16.704.100.23.3, được cấp bởi Trung tâm Chứng thực chữ ký số quốc gia.

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

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

Tổ chức cung cấp dịch vụ CA là thành phần quan trọng nhất trong hệ thống PKI. CA xác thực thông tin thuê bao cũng như đảm bảo tính bảo 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 những người quản trị hệ thống đó nhằm thực hiện các chức năng chính sau:

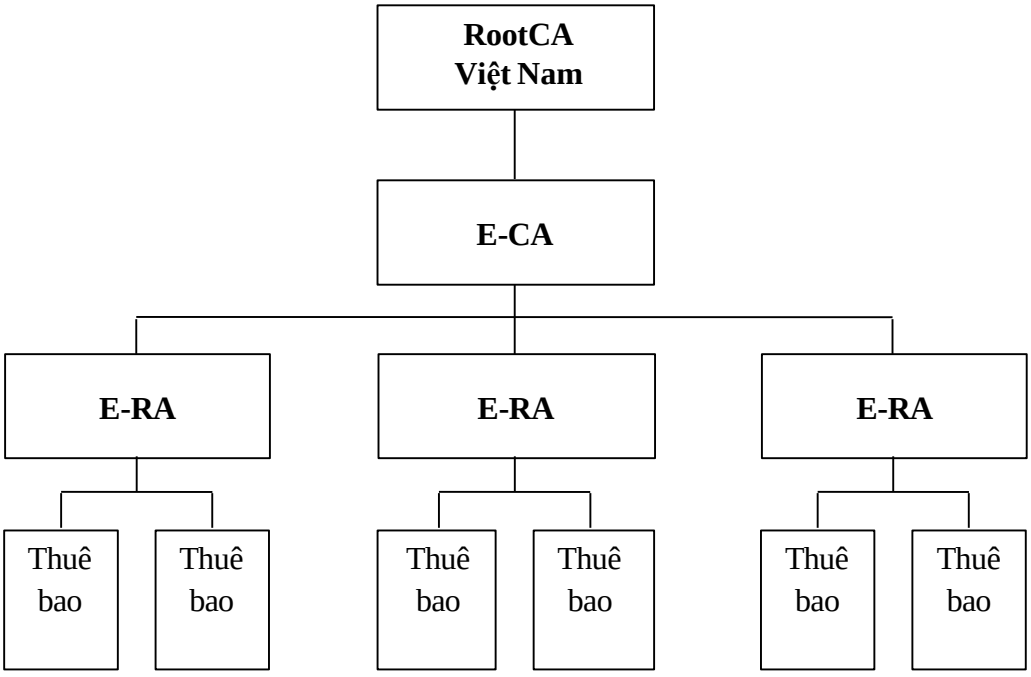
- Tạo cặp khóa bao gồm khóa công khai và khóa bí mật cho thuê bao;
- Cấp, gia hạn, tạm dừng, phục hồi và thu hồi chứng thư số của thuê bao theo quy định của pháp luật và CPS;
- Duy trì trực tuyến cơ sở dữ liệu về chứng thư số (còn hiệu lực, hết hạn, gia hạn, cấp mới, thu hồi);
- Cung cấp các dịch vụ khác có liên quan cho người sử dụng.

CA có thể thực hiện các chức năng trên một cách trực tiếp hoặc ủy quyền cho đối tượng khác tiến hành theo quy định của pháp luật, các đối tượng này được gọi là RA (Registration Authority).

Hệ thống E-CA được tổ chức theo quy định của pháp luật Việt Nam, trực thuộc RootCA (Trung tâm Chứng thực chữ ký số quốc gia) do Bộ Thông tin và

Truyền thông quản lý.

E-CA được Bộ Thông tin và Truyền thông cấp phép cung cấp dịch vụ chứng thực chữ ký số công cộng, do đó có quyền cấp chứng thư số cho các cơ quan, tổ chức, doanh nghiệp, cá nhân (đủ điều kiện theo quy định của pháp luật và CPS này), có yêu cầu cấp chứng thư số.



Hình 1 – Sơ đồ tổ chức hệ thống E-CA

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, uỷ 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:

- Xác thực cá nhân chủ thể đăng ký chứng thư số.
- Kiểm tra tính hợp lệ của thông tin do chủ thể cung cấp.
- Xác nhận quyền của chủ thể đối với những thuộc tính chứng thư số yêu cầu.
- Kiểm tra xem chủ thể có thực sự sở hữu khóa bí mật đang được đăng ký hay không.
- Thay mặt chủ thể thực thể cuối khởi tạo quá trình đăng ký với CA.
- Khởi sinh quá trình khôi phục khoá.

Trong hệ thống E-CA, RA được gọi là E-RA là các chi nhánh của TSD trên toàn quốc có khả năng kiểm tra, xác thực định danh các thuê bao.

1.3.3. Thuê bao.

Thuê bao là tổ chức, cá nhân (đủ điều kiện theo quy định của pháp luật và CPS này) được E-CA cấp, chấp nhận chứng thư số và giữ khóa bí mật tương ứng với khóa công khai ghi trên chứng thư số đó.

1.3.4. Đối tác tin cậy (hay bên Nhận).

Là cá nhân hay thực thể, hoạt động của họ dựa trên sự tin cậy chứng thư số cũng như chữ ký số được cấp bởi E-CA. Một đối tác tin cậy có thể là một thuê bao hoặc không phải một thuê bao của dịch vụ E-CA.

Đối tác tin cậy có hệ thống dịch vụ sử dụng chữ ký số, chấp nhận tính chất pháp lý hoặc xác thực sự tin cậy của chứng thư số được cấp bởi E-CA cho các giao dịch mà mình cung cấp.

1.3.5. Thành phần khác

Không có quy định.

1.4. Mục đích sử dụng chứng thư số.

1.4.1. Các trường hợp sử dụng chứng thư số hợp lệ.

Chứng thư số cấp cho cá nhân (Personal Certificate).

Chứng thư cá nhân thường được các cá nhân sử dụng để ký và mã hóa thư điện tử, sử dụng trong các giao dịch điện tử có yêu cầu xác thực nhận diện cá nhân.

E-CA cung cấp những loại chứng thư số cá nhân cho người dùng tự do, cho nhân viên cán bộ trong một tổ chức… Phù hợp với quy định pháp luật của Việt Nam.

Các ứng dụng chủ yếu: Ký, mã hoá email, ký văn bản bản phát hành cho đơn vị/cơ quan/tổ chức, ký các hồ sơ điện tử của hệ thống dịch vụ công (theo chính sách các dịch vụ công 1 cửa của nhà nước yêu cầu chữ ký số cá nhân đại diện, *vd: cổng đăng ký kinh doanh của Bộ KH&ĐT*) chứng thực quyền truy cập hệ thống CNTT, mạng của cá nhân, hoặc sử dụng cho mục đích nội bộ theo chính sách áp dụng của từng đơn vị.

Độ dài khóa bí mật: 2048 bit.

Chứng thư cấp cho doanh nghiệp/tổ chức (Bussiness Certificate).

Chứng thư số sẽ được cấp cho các tổ chức sau khi E-CA xác minh được tính hợp lệ trong hồ sơ xin cấp chứng thư số của tổ chức. Chứng thư số cho tổ chức thường được sử dụng để ký, mã hóa email, thực hiện giao dịch điện tử, hành chính công...

Các ứng dụng chủ yếu: Ký văn bản (dưới định dạng MS.Word, Excel, PDF, XML. ....), Các hồ sơ giao dịch với các hệ thống dịch vụ công (TVAN, IVAN, Hải Quan điện tử …). Ký Hóa đơn điện tử, biên lai điện tử, hợp đồng điện tử…. Xác thực giao dịch, mã hóa tài liệu.

Độ dài khóa bí mật: 2048 bit.

Gói chứng thư dành cho thiết bị (DeviceID- Máy chủ và HSM).

Gói chứng thư dành cho các dịch vụ ứng dụng chữ ký số như SSL, SigningServer … nhằm xác thực website, xác thực dịch vụ, xác thực thiết bị, ký số giao dịch …

Bảng tóm tắt các gói dịch vụ chứng thư số của E-CA

STT	Tên gọi	Độ dài khóa - bit	Chức năng			Thời hạn chứng thư
			Ký, mã hoá email	Ký văn bản	Chứng thực đăng nhập	
1	Personal	2048	✓	✓	✓	Các gói 1 năm, 2 năm, 3 năm
2	Business		✓	✓	✓	Các gói 1 năm, 2 năm, 3 năm
3	DeviceID (dùng cho Server hoặc HSM)		✓	✓	✓	Các gói 1 năm, 2 năm, 3 năm

1.4.2. Các trường hợp không được sử dụng chứng thư số.

Các chứng thư số của E-CA được sử dụng trong phạm vi phù hợp với quy định của pháp luật. Các mục đích không phù hợp với quy định của pháp luật đều không được E-CA cấp chứng thư số.

1.5. Quản lý quy chế chứng thực.

1.5.1. Cơ quan, Tổ chức quản lý quy chế chứng thực.

Tên cơ quan: Công ty TNHH Phát triển công nghệ Thái Sơn.

Địa chỉ: Số 362 Phố Huế, Phường Phố Huế, Quận Hai Bà Trưng, Thành Phố Hà Nội, Việt Nam.

Địa chỉ giao dịch: Số 15, Đặng Thùy Trâm, phường Cổ Nhuế 1, quận Bắc Từ Liêm, TP. Hà Nội.

Điện thoại: 0243.7545222

E-mail: info@thaison.vn

Website: www.thaison.vn

1.5.2. Thông tin liên hệ.

Chịu trách nhiệm quản trị hệ thống

Họ và tên: Ngô Trinh Huấn

Điện thoại: 0363.931.857

E-mail: huannt@thaison.vn

Chịu trách nhiệm đảm bảo an toàn thông tin hệ thống

Họ và tên: Vũ Thọ Tuyền

Điện thoại: 0906.010.487

E-mail: tuyenvt@thaison.vn

Chịu trách nhiệm vận hành hệ thống và cấp chứng thư số

Họ và tên: Lê Văn Nam

Điện thoại: 0937.979.186

E-mail: nam@thaison.vn

1.5.3. Công nhận sự phù hợp của CPS.

Bộ Thông tin và Truyền Thông và Công ty TNHH Phát triển Công nghệ Thái Sơn xác nhận sự phù hợp của quy chế chứng thực này.

1.5.4. Thủ tục phê chuẩn CPS.

Công ty TNHH Phát triển Công nghệ Thái Sơn sẽ phê chuẩn CPS. Mỗi phiên bản của CPS có một bộ định danh đối tượng duy nhất (OID). Các thay đổi, cập nhật của CPS được ghi trong một tài liệu chứa các sửa đổi của CPS hay các thông tin về quá trình cập nhật và được công bố tại https://ECA.com.vn/cps

1.6. Các định nghĩa và từ viết tắt.

1.6.1. Các định nghĩa.

Thuật ngữ	Giải thích
Chứng thư số E-CA	Là một dạng chứng thư điện tử do E-CA số cấp.
Chứng thư số có hiệu lực	Là chứng thư số chưa hết hạn, không bị tạm dừng hoặc bị thu hồi.
Chữ ký số	Là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng theo đó người có được

	thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định được chính xác: - Việc biến đổi nêu trên được tạo ra bằng đúng khóa bí mật tương ứng với khóa công khai trong cùng một cặp khóa; - Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.
Dịch vụ chứng thực chữ ký số	Là một loại hình dịch vụ chứng thực chữ ký điện tử, do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp. Dịch vụ chứng thực chữ ký số bao gồm: - Tạo cặp khóa bao gồm khóa công khai và khóa bí mật cho thuê bao; - Cấp, gia hạn, tạm dừng, phục hồi và thu hồi chứng thư số của thuê bao; - Duy trì trực tuyến cơ sở dữ liệu về chứng thư số; - Cung cấp thông tin cần thiết để giúp chứng thực chữ ký số của thuê bao đã ký số trên thông điệp dữ liệu.
Hệ thống mật mã bất đối xứng	Là hệ thống mật mã có khả năng tạo được cặp khóa bao gồm khóa bí mật và khóa công khai.
Khoá	Là một chuỗi các số nhị phân (0 và 1) dùng trong các hệ thống mật mã.
Khóa bí mật	Là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được dùng để tạo chữ ký số.
Khóa công khai	Là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được sử dụng để kiểm tra chữ ký số được tạo bởi khóa bí mật tương ứng trong cặp khoá.
Ký số	Là việc đưa khóa bí mật vào một chương trình phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu.
Người ký	Là thuê bao dùng đúng khóa bí mật của mình để ký số vào một thông điệp dữ liệu dưới tên của mình.
Người nhận	Là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng chứng thư số của

	người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.
Thuê bao	Là tổ chức, cá nhân được cấp chứng thư số, chấp nhận chứng thư số và giữ khóa bí mật tương ứng với khóa công khai ghi trên chứng thư số được cấp đó.
Tạm dừng chứng thư số	Là làm mất hiệu lực của chứng thư số một cách tạm thời từ một thời điểm xác định.
Thu hồi chứng thư số	Là làm mất hiệu lực của chứng thư số một cách vĩnh viễn từ một thời điểm xác định.

1.6.2. Từ viết tắt.

Từ viết tắt	**Tên đầy đủ**	**Ý nghĩa**
CA	Certificate Authority	Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng
CP	Certificate Policy	Chính sách chứng nhận
CPS	Certification Practice Statement	Tuyên bố cung cấp dịch vụ chứng thực
CRLs	Certificate Revocation Lists	Danh sách chứng chỉ thu hồi
CSP	Certification Service Provider	Nhà cung cấp dịch vụ chứng thực
DNS	Domain Name System	Hệ thống quản lý tên miền
HTTPS	Secure Hypertext Transaction Standard	Giao thức truyền tải siêu văn bản bảo mật
LDAP	Lightweight Directory Access Protocol	Giao thức truy nhập nhanh dịch vụ thư mục
OCSP	Online Certificate Status Protocol	Giao thức cho kiểm tra trạng thái chứng thư số trực tuyến.

PKCS	Public Key Cryptography Standards	Tiêu chuẩn mật mã khóa công khai
PKI	Public Key Infrastructure	Hạ tầng khóa công khai
RA	Registration Authorities	Thành phần quản lý thông tin đăng ký
RFC	Request For Comments	Bộ tài liệu kiến nghị, đề xuất về công nghệ, các giao thức kết nối
RSA	Rivest Shamir Adleman	Thuật toán mật mã không đối xứng
SHA-1 , SHA-256	Secure Hash Standard	Các hàm băm mật mã tiêu chuẩn
SSL	Secure Socket Layer	Giao thức kết nối bảo mật qua mạng
TLS	Transport Layer Security	Giao thức kết nối bảo mật qua mạng
X.500 X.501	X.500 The ITU-T (International Telecommunication Union-T) standard that establishes a distributed, hierarchical directory protocol organized by country, region, Organization, etc.	Tiêu chuẩn về cấu trúc định danh
X.509	ITU-T standard for Certificates format	Tiêu chuẩn định dạng chứng thư số và danh sách thu hồi chứng thư số
TSD	Công ty TNHH Phát triển công nghệ Thái Sơn	

2. TRÁCH NHIỆM LƯU TRỮ VÀ CÔNG BỐ THÔNG TIN.

2.1. Lưu trữ.

Trung tâm chứng thực E-CA có trách nhiệm duy trì việc phát hành trực tuyến chứng thư số. Việc lưu trữ được tiến hành trên cả hai nền tảng LDAP và nền tảng Web với cơ sở dữ liệu MariaDB để cung cấp dữ liệu cần thiết cho người dùng như chứng thư số cấp bởi E-CA hay danh sách thu hồi chứng thư số (CRLs). Các tài liệu liên quan đến dịch vụ của E-CA (CPS) cũng được cung cấp thông qua giao diện Web. E-CA cam kết:

- Lưu trữ và sử dụng thông tin của thuê bao một cách bí mật, an toàn và chỉ được sử dụng thông tin này vào mục đích liên quan đến chứng thư số.
- Lưu trữ đầy đủ, chính xác và cập nhật thông tin của thuê bao phục vụ việc cấp chứng thư số trong suốt thời gian chứng thư số có hiệu lực và trong thời gian ít nhất 05 năm, kể từ khi chứng thư số hết hiệu lực.
- Lưu trữ đầy đủ, chính xác và cập nhật danh sách các chứng thư số có hiệu lực, đang tạm dừng và đã hết hiệu lực và cho phép, hướng dẫn người sử dụng Internet truy nhập trực tuyến 24 giờ trong ngày và 7 ngày trong tuần.
- Lưu trữ toàn bộ thông tin liên quan đến việc tạm đình chỉ hoặc thu hồi giấy phép và các cơ sở dữ liệu về thuê bao, chứng thư số trong thời gian ít nhất 05 (năm) năm, kể từ khi giấy phép bị tạm đình chỉ hoặc thu hồi.

2.2. Công bố thông tin.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số E-CA thực hiện lưu trữ trực tuyến an toàn gồm:

- Chứng thư số của E-CA.
- Danh sách chứng thư số có hiệu lực, bị tạm dừng, bị thu hồi của thuê bao.
- Bản sao CP/CPS của E-CA và các phiên bản trước của các tài liệu này
- Các thông tin liên quan khác.

Tra cứu thông tin chứng thư số tại địa chỉ:

https://ECA.com.vn/tracuuCTS

Danh sách chứng thư số thu hồi công bố tại địa chỉ URL sau:

http://crl.ECA.com.vn/ECA.crl.

Địa chỉ công bố truy cập trả lời OCSP

http://ocsp.ECA.com.vn

2.3. Thời gian, tần suất công bố thông tin.

Chứng thư số E-CA sẽ được công bố ngay sau khi có sự chấp nhận của thuê bao phù hợp với các thủ tục mà E-CA yêu cầu.

Tần suất công bố các dữ liệu thu hồi là: 01 ngày (24 giờ).

Tần suất công bố CP/CPS: Một phiên bản mới của CP/CPS sẽ được công bố ngay sau khi được phê chuẩn và phiên bản cũ sẽ được lưu trữ trong kho lưu trữ một cách an toàn.

2.4. Kiểm soát truy nhập thông tin.

E-CA không yêu cầu xác thực truy cập đối với bên thứ 3 khi truy cập vào các thông tin thu hồi (CRL), chứng thư số của E-CA, và các tài liệu (CP/CPS) của E-CA thông qua địa chỉ công bố truy cập trực tuyến.

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

3.1. Đặt tên trong chứng thư số.

3.1.1. Quy định về các kiểu tên.

- Trường “subject” của chứng thư số tuân theo chuẩn X.509 v3. Nội dung của trường "subject" của chứng thư số chứa tên các thành phần sau đây:

- CommonName (CN): Tên của thuê bao được cấp chứng thư số. Phân biệt cho mỗi cá nhân, mỗi host, mỗi dịch vụ.

- OrganizationName (O): Tên của tổ chức/đơn vị quản lý thuê bao (nếu có).

- Title (T): Chức vụ của thuê bao trong tổ chức (nếu có).

- State/Province (S): Tên tỉnh/TP nơi sống/làm việc của thuê bao.

- CountryName (C): Tên nước. Giá trị của thành phần CountryName được định nghĩa trước (VN) và nó cũng là thành phần gốc của LDAP.

  + Trong trường hợp chứng thư số cấp cho cá nhân nội dung trường “subject” phải bao gồm Họ và tên của thuê bao.

  + Trong trường hợp chứng thư số cấp cho Host/Server nội dung trường “subject” phải bao gồm FQDN (Fully Qualified Domain Name) của Host/Server.

Minh hoạ đầy đủ nội dung của trường “subject” của một chứng thư số cấp cho đối tượng

+ Tổ chức/Doanh nghiệp:

CN= CÔNG TY TNHH PHÁT TRIỂN CÔNG NGHỆ THÁI SƠN 0.9.2342.19200300.100.1.1= MST: 0101300842, S= Hà Nội, C=VN

+ Cá nhân:

CN= Nguyễn Hương Nga 0.9.2342.19200300.100.1.1=CCCD: 001188046781, S= Hà Nội, C=VN

+ Cá nhân thuộc tổ chức:

CN= Nguyễn Minh Anh 0.9.2342.19200300.100.1.1=CCCD: 001188046782, T= Kế toán, O= CÔNG TY TNHH PHÁT TRIỂN CÔNG NGHỆ THÁI SƠN, S= Hà Nội, C=VN

3.1.2. Quy định yêu cầu đối với tên

Nội dung của chứng thư số và các trường tên phải có một sự kết hợp với tên được xác thực của thuê bao. Trong trường hợp là các cá nhân, tên thường dùng được xác thực sẽ kết hợp với họ, tên đệm và các chữ cái đầu tùy chọn khác. Đối với các cá nhân đại diện cho một tổ chức, doanh nghiệp có thể bao gồm vị trí và vai trò của tổ chức đó. Trong trường hợp thuê bao là một tổ chức, doanh nghiệp sẽ phản ánh tên đăng ký theo luật pháp của thuê bao đó. Khi mà chứng thư số chỉ tới một vai trò hay một vị trí, nó cũng phải bao gồm nhận dạng của người có vai trò hay vị trí đó. Một chứng thư số được cấp phát cho một thiết bị điện tử phải bao gồm cả việc tên được xác thực của thiết bị điện tử và/hoặc tên của cá nhân hay tổ chức chịu trách nhiệm.

Tên trong chứng thư số của dịch vụ E-CA phải là chính danh của chủ thể đăng ký sử dụng dịch vụ, không sử dụng các bí danh, biệt hiệu… Các yêu cầu sử dụng tên là bí danh, biệt hiệu… trong chứng thư sẽ được E-CA xem xét và đánh giá dựa theo điều kiện hợp lý.

STT	**Trường**		**Ý nghĩa**	**Quy định** **Chứng thư số công cộng**
1	Issuer	common Name	Tên của CA cấp chứng thư số	E-CA
		organization Name	Tên của tổ chức/doanh nghiệp vận hành CA	THAISONSOFT
		countryName	Tên nước	VN
2	Subject	userID	Định danh của thuê bao	MST:[mã số thuế] hoặc MNS:[mã quan hệ ngân sách] hoặc BHXH:[mã số bảo hiểm xã hội] hoặc CMND:[số chứng

				minh nhân dân] hoặc HC:[số hộ chiếu] hoặc CCCD:[số thẻ căn cước công dân] *Các trường hợp khác theo thỏa thuận giữa thuê bao và E-CA.*
		commonName	Tên của thuê bao	Tên của thuê bao được cấp chứng thư số
		organization Name	Tên của tổ chức/đơn vị quản lý thuê bao	Tên của tổ chức/đơn vị quản lý thuê bao (nếu có)
		stateOrProvin ceN ame	Tên tỉnh/TP nơi sống/làm việc của thuê bao	Tên của tỉnh/TP nơi sống/làm việc của thuê bao bằng tiếng Việt, có dấu, các chữ cái đầu viết hoa.
		countryName	Tên nước	VN

3.1.3. Quy định cú pháp định dạng tên

- Tên của nhà cung cấp dịch vụ E-CA

  CN= E-CA

  O= THAISONSOFT

  C= VN

- Chứng thư E-CA cấp cho người dùng cá nhân

  CN= Tên người dùng

  0.9.2342.19200300.100.1.1 = CMND: 012389725 (hoặc passport, ID, …)

  S= Hà Nội

  C= VN

- Chứng thư E-CA cấp cho tổ chức, doanh nghiệp

  CN = Tên tổ chức/doanh nghiệp

  0.9.2342.19200300.100.1.1 = MST:21312312

  S= Hà Nội

  C= VN

3.1.4. Quy định tính duy nhất của tên

Tên thuê bao được nêu ra trong chứng thư số phải rõ ràng và duy nhất với toàn bộ các chứng thư số do CA phát hành cấp phát, và tuân theo tiêu chuẩn X.509 về tính duy nhất của tên. Khi cần thiết, có thể thêm số hoặc các ký tự vào tên gốc để đảm bảo tính duy nhất của tên trong toàn bộ danh mục chứng thư số do CA phát hành. Ở đây không cho phép bất kỳ sự tạo thành tên một cách lộn xộn nào. Mỗi tên sẽ phải là duy nhất đối với thuê bao duy nhất.

3.2. Xác minh đề nghị cấp chứng thư số.

3.2.1. Cách thức chứng minh sở hữu khóa bí mật.

Trường hợp Token đã được giao tới cho thuê bao, thuê bao đăng ký cấp chứng thư số phải chứng minh tính sở hữu khóa bí mật của họ thích hợp với khóa công khai trong một yêu cầu cấp chứng thư số thông qua việc ký yêu cầu với khóa bí mật. E-CA sẽ xác minh rằng người nộp đơn có phải là người sở hữu khóa bí mật tương ứng với khóa công khai đã được đưa ra cùng với các ứng dụng phù hợp với một giao thức an toàn hay không.

Trong trường hợp khóa bí mật được tạo ra trực tiếp trên một Token, hoặc khóa được tạo ra bằng cách chuyển tiếp từ khóa vào Token, sau đó chuyển tới thuê bao, thuê bao được coi là sở hữu khóa bí mật tại thời điểm tạo ra hoặc chuyển tiếp. Token sẽ được chuyển ngay lập tức đến thuê bao qua một phương pháp tin cậy và có trách nhiệm.

3.2.2. Nhận dạng và xác thực đối với chủ thể cá nhân.

Việc cấp phát chứng thư số được dựa trên cơ sở xác thực và nhận dạng thẩm quyền. Tài liệu của quá trình này phải được những người xác minh, nhận dạng ký (bằng văn bản hoặc ký số) để xác minh cá nhân được nhận dạng phù hợp.

- Thực hiện nhận dạng cá nhân:

  Toàn bộ thông tin được người nộp đơn gửi tới để nhận dạng cá nhân phải được kiểm tra và xác thực chéo để xác định rằng:

  - Tính hợp lệ của thông tin do chủ thể cung cấp.
  - Thông tin thống nhất trong đơn nộp cấp chứng thư số.

- Tài liệu nhận dạng danh tính cá nhân:

  Tất cả cá nhân nộp đơn muốn được cấp chứng thư số phải chứng minh thỏa mãn yêu cầu nhận dạng. Các loại tài liệu, thẻ được sử dụng để chứng minh danh tính vào lúc bắt đầu đăng ký bao gồm:

  - Căn cước công dân
  - Chứng minh thư nhân dân.
  - Chứng minh thư quân đội.
  - Hộ khẩu hoặc giấy khai sinh.
  - Hộ chiếu.
  - Bằng lái xe hoặc các giấy tờ nhận dạng khác do cơ quan chính phủ cấp.
  - Giấy xác nhận hộ khẩu do Cơ quan Công an xác nhận có đăng ký hộ khẩu thường trú.

3.3. Xác minh đề nghị thay đổi cặp khóa.

3.3.1. Nhận dạng và xác thực trong thủ tục cấp lại khoá.

Trong thời hạn hiệu lực của chứng thư số thuê bao của E-CA có thể yêu cầu thay đổi cặp khóa. Cấp lại khóa trước khi chứng thư số hết hạn được thực hiện bằng cách gửi yêu cầu cấp lại khóa dựa trên khóa công khai mới trong một email được ký với khóa bí mật cũ tới RA của E-CA. RA đảm bảo rằng cá nhân hay một tổ chức muốn cấp lại khóa cho chứng thư số phải là chủ thuê bao của chứng thư số đó.

Để chấp thuận yêu cầu cấp lại khóa của thuê bao RA phải nhận dạng và xác nhận các thông tin thuê bao đưa ra là chính xác và không thay đổi. Sau khi cấp lại khóa CA hoặc RA của E-CA sẽ xác nhận lại việc nhận dạng và xác thực thuê bao sao cho phù hợp với các yêu cầu của đơn xin cấp chứng thư ban đầu.

3.3.2. Nhận dạng và xác thực việc cấp lại khóa sau khi đã bị thu hồi.

Chứng thư số đã bị thu hồi và hết hạn sử dụng có thể không được cấp lại khóa, làm mới hoặc cập nhật. Việc xin cấp lại khóa sau khi thu hồi và hết hạn sẽ

được tuân theo các thủ tục giống như lần đăng ký đầu tiên.

3.4. Xác minh đề nghị thu hồi chứng thư số.

Quy trình, thủ tục xác minh yêu cầu yêu cầu thu hồi chứng thư số của thuê bao như sau:

Thuê bao có thể yêu cầu thu hồi chứng thư số của mình tại bất kỳ thời điểm nào với bất kỳ lý do nào. E-CA đảm bảo cơ chế xác thực để ngăn chặn các yêu cầu trái phép, đồng thời đảm bảo đề nghị thu hồi chứng thư số được tiếp nhận một cách nhanh chóng. Yêu cầu có thể được gửi tới E-CA thông qua thư điện tử được ký số. Nếu yêu cầu được ký bởi khóa bí mật tương ứng với khóa công khai của người gửi yêu cầu, yêu cầu này sẽ được xem là có hiệu lực.

Tất cả những yêu cầu thu hồi chứng thư số phải được gửi đến E-CA hoặc RA thay mặt cho E-CA, thông qua một quá trình xử lý trực tuyến được chấp nhận hoặc thông qua văn bản. Yêu cầu thu hồi được xác thực hoặc bất kỳ các hành động tương ứng nào của CA sẽ được ghi và giữ lại theo quy định. Trong trường hợp khi một chứng thư số bị thu hồi, sự đánh giá về việc thu hồi này cũng sẽ được lưu giữ bằng văn bản. Khi chứng thư số của thuê bao bị thu hồi, việc thu hồi sẽ được công bố tại CRL thích hợp của E-CA.

Trong trường hợp thuê bao bị mất thiết bị lưu trữ khóa bí mật (Token/Smartcard) thuê bao phải báo ngay cho RA mà thuê bao đã đăng ký trước kia theo một trong các cách sau: điện thoại, fax, thư điện tử, thư tín hay các dịch vụ đưa tin khác. Để yêu cầu thu hồi chứng thư số của mình, thuê bao phải đến trực tiếp RA trước kia xác thực lại các thông tin sở hữu chứng thư số. Khi đó yêu cầu thu hồi chứng thư mới được xem là hợp lệ.

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

4.1. Yêu cầu cấp chứng thư số.

4.1.1. Đối tượng đề nghị cấp chứng thư số.

- Cá nhân là công dân Việt Nam.
- Tổ chức/Đơn vị hoạt động hợp pháp tại Việt nam, tuân thủ luật pháp Việt Nam.

4.1.2. Hồ sơ đề nghị cấp chứng thư số.

- Bản đăng ký sử dụng dịch vụ theo mẫu quy định của nhà cung cấp E-CA.

  + Bản cứng ký đóng dấu, hoặc:

  + Bản ký số bằng chữ ký số còn hiệu lực.

a) Đối với tổ chức:

+ Quyết định thành lập hoặc quyết định quy định về chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức hoặc giấy chứng nhận đăng ký doanh nghiệp hoặc giấy chứng nhận đầu tư;

+ Chứng minh nhân dân, hoặc căn cước công dân hoặc hộ chiếu của người đại diện theo pháp luật của tổ chức.

b) Đối với cá nhân:

+ Chứng minh nhân dân hoặc căn cước công dân hoặc hộ chiếu

c) Nếu CTS cấp cho cá nhân là người có chức danh, thẩm quyền của cơ quan, tổ chức thì phải cung cấp thêm các tài liệu sau:

+ Văn bản của cơ quan, tổ chức đề nghị cấp chứng thư số cho người có chức danh, thẩm quyền.

+ Bản sao hợp lệ quyết định thành lập, quyết định quy định chức năng, nhiệm vụ, quyền hạn hoặc văn bản xác nhận chức danh của người có thẩm quyền của cơ quan, tổ chức.

- Hợp đồng cung cấp dịch vụ theo mẫu quy định của thông tư 31/2020/TT-BTTTT.
- Giấy tờ khác có liên quan: Bản sao hợp lệ của: Quyết định, giấy ủy quyền, CMND/CCCD/Hộ chiếu của người được ủy quyền…

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

4.2. Xử lý yêu cầu cấp chứng thư số.

Người đăng ký phải hoàn thành Đơn xin cấp chứng thư số và cung cấp các thông tin trong một mẫu do E-CA đưa ra. Tất cả các đơn xin cấp này phải được E-CA xem xét, phê duyệt và chấp nhận.

Quá trình xử lý một đơn xin cấp phát chứng thư số như sau:

- Người xin cấp chứng thư số phải có mặt tại RA gần nhất để nộp đơn đăng ký cấp phép chứng thư số tới RA (mẫu đăng ký được công bố trên web E-CA)
- RA sẽ chịu trách nhiệm xem xét đơn đăng ký xin cấp CTS của thuê bao
- Khi người đăng ký được xác nhận thông tin chính xác, RA sẽ chuyển các đơn xin cấp phép đến CA
- Nếu đơn xin được phê duyệt, E-CA sẽ thông báo tới người đăng ký là đơn đã được chấp nhận và gửi cho người sử dụng các thông tin cần thiết để hoàn tất thủ tục và có thể dùng chứng thư số của mình

4.3. Cấp chứng thư số.

Quy trình cấp chứng thư số thực hiện theo các bước như sau:

Bước 1: Gửi yêu cầu cấp phát:

Khi khách hàng có nhu cầu sử dụng dịch vụ chữ ký số, cần liên hệ với nhà cung cấp E-CA hoặc đại lý. Lúc này Giao dịch viên sẽ hỗ trợ, hướng dẫn khách hàng hoàn thiện các thủ tục và gửi yêu cầu trên hệ thống.

Bước 2: Quản trị viên đại lý duyệt lệnh cấp CTS:

Hầu hết thuê bao làm việc qua đại lý của E-CA, do đó yêu cầu cấp CTS này sẽ được gửi tới quản trị viên đại lý. Nếu quản trị viên từ chối, yêu cầu sẽ không được thực hiện, thuê bao hay giao dịch viên cần phối hợp để giải quyết.

Trường hợp yêu cầu được duyệt thì sẽ đẩy lên để thẩm định viên E-CA xử lý.

Bước 3: Thẩm định viên CA duyệt lệnh cấp CTS:

Thẩm định viên E-CA kiểm tra các thông tin và điều kiện được cung cấp để thực hiện phê duyệt hay không. Trong trường hợp không phê duyệt, thẩm định viên sẽ phản hồi lý do để thuê bao và đại lý phối hợp giải quyết.

Trường hợp yêu cầu được duyệt thì sẽ đẩy lên để lên quản trị viên E-CA xử lý.

Bước 4: Quản trị viên CA duyệt lệnh cấp CTS:

Quản trị viên E-CA kiểm tra các thông tin và điều kiện được cung cấp để thực hiện phê duyệt hay không. Trong trường hợp không phê duyệt, quản trị viên sẽ phản hồi lý do để thuê bao và đại lý phối hợp giải quyết.

Nếu yêu cầu cấp CTS là hợp lệ, quản trị viên thực hiện phê duyệt.

Bước 5: Hệ thống gửi email cung cấp mã kích hoạt:

Để đảm bảo chính xác và an toàn, hệ thống sẽ gửi 1 email chứa mã kích hoạt và thông tin yêu cầu đăng ký CTS về địa chỉ mail dùng để đăng ký thuê bao.

Bước 6: Kết nối token với hệ thống qua Token Manager:

Để kích hoạt và cài đặt CTS vào token, người dùng cần cắm token vào máy tính online, kết nối với hệ thống ECA-RA qua công cụ Token Manager.

Bước 7: Hệ thống cấp CTS & cài đặt CTS vào token cho thuê bao:

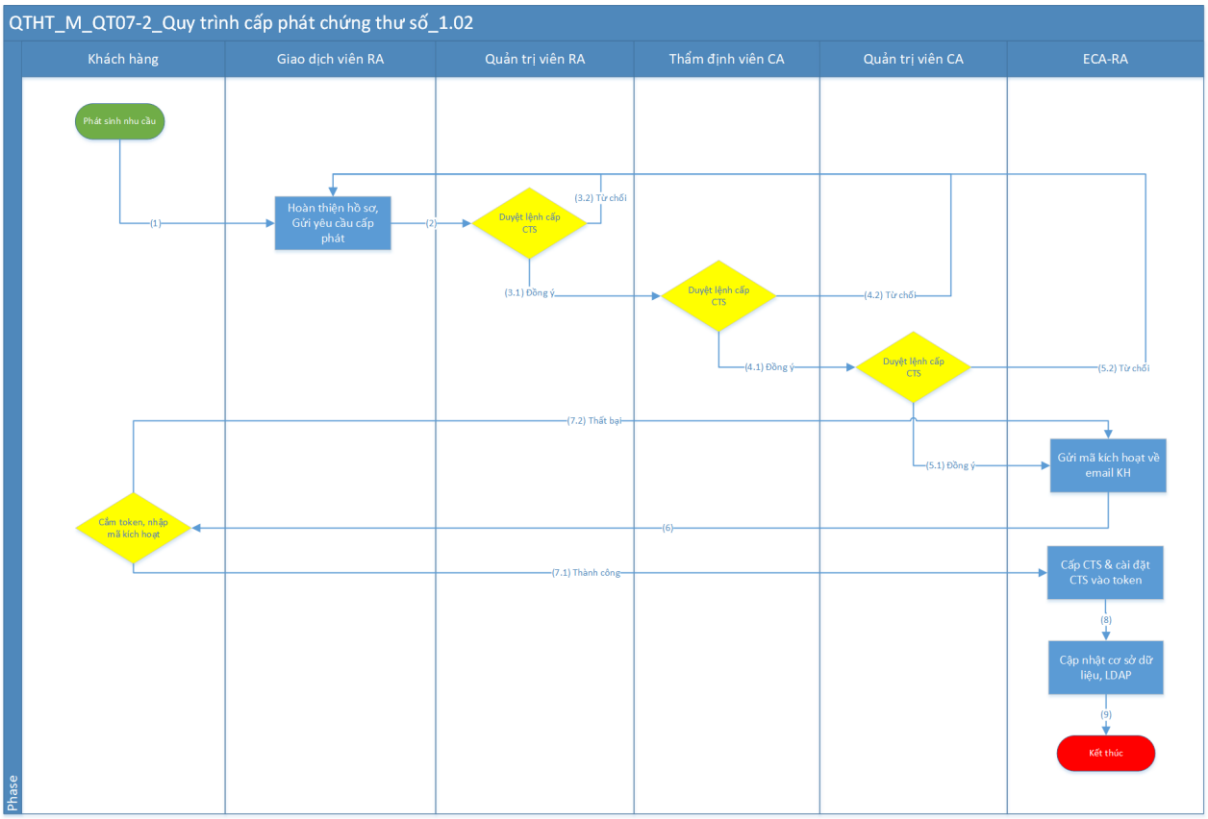
Khi đã kết nối thành công với ECA-RA, hệ thống ECA-RA cấp CTS & import CTS vào token đang cắm trên máy

Bước 8: Cập nhật thông tin:

Khi hoàn tất việc cấp phát, kích hoạt, thông tin sẽ được cập nhật tự động vào CSDL OCSP để phục vụ tra cứu online.

Bước 9: Kết thúc:

Lúc này CTS đã được import thành công vào token, thuê bao có thể thực hiện đầy đủ các chứng năng của chữ ký số. Đồng thời thông tin CTS của thuê bao cũng được lưu trữ đầy đủ, chính xác và an toàn trên hệ thống E-CA.



Hình 1: Sơ đồ quy trình cấp chứng thư số.

4.4. Xác nhận và công bố công khai chứng thư số.

4.4.1. Thuê bao xác nhận các thông tin trên chứng thư số được cấp.

Trong vòng một tuần kể từ khi thuê bao nhận được chứng thư số mà không trả lời thông báo của E-CA, chứng thư số đó coi như được thuê bao chấp nhận.

Trong trường hợp từ chối, thuê bao phải thông báo cho E-CA và giải thích lý do từ chối.

4.4.2. Công bố công khai chứng thư số của thuê bao theo quy định.

Sau khi có xác nhận của thuê bao về tính chính xác của thông tin trên chứng thư số, E-CA tiến hành công bố chứng thư số lên website chậm nhất sau 24 giờ.

4.5. Sử dụng cặp khóa và chứng thư số.

Sau khi thuê bao được tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp chứng thư số thì có thể sử dụng cặp khóa cũng như chứng thư số của mình một cách hợp pháp theo các quy định của pháp luật và theo hợp đồng đã ký với CA.

4.5.1. Sử dụng chứng thư và khóa bí mật của thuê bao.

- Chứng thư số phát hành bởi E-CA và khóa bí mật tương ứng với khóa công khai trong chứng thư được sử dụng hợp pháp theo bản thoả thuận của thuê bao với các điều khoản có trong CP/CPS của nhà cung cấp chứng thư.
- Chứng thư sử dụng phải phù hợp với nội dung quy định trong trường Key Usage có trong chứng thư
- Thuê bao có trách nhiệm bảo vệ khóa bí mật khỏi việc truy cập bất hợp

pháp và sẽ không được sử dụng khóa bí mật khi chứng thư hết hạn hay bị thu hồi.

4.5.2. Sử dụng chứng thư và khóa công khai của đối tác tin cậy.

Các đối tác tin cậy phải đánh giá một cách độc lập các chứng thư số phát hành bởi E-CA, phải kiểm tra chứng thư số hợp lệ bằng cách:

- Kiểm tra có đúng chứng thư số do E-CA phát hành;
- Kiểm tra chứng thư số chưa bị thu hồi
- Chứng thư sử dụng phải phù hợp với nội dung quy định trong trường Key Usage có trong chứng thư
- Việc sử dụng chứng thư cho các mục đích phù hợp và xác định rằng chứng thư sẽ được sử dụng đúng mục đích quy định trong chính sách này.

4.6. Gia hạn chứng thư số.

4.6.1. Các trường hợp gia hạn CTS.

- Trường hợp gia hạn CTS cần phải có đơn đăng ký gia hạn ít nhất 30 ngày trước ngày hết hạn CTS.
- Trường hợp khi hết hạn mà thuê bao không gia hạn CTS.

4.6.2. Xử lý yêu cầu gia hạn CTS.

- Trường hợp gia hạn CTS cần phải có đơn đăng ký gia hạn ít nhất 30 ngày trước ngày hết hạn CTS:
  - + Bộ phận tiếp nhận hồ sơ xác thực đơn đăng ký và gửi yêu cầu tới bộ phận thẩm định
  - + Bộ phận thẩm định tiến hành xác thực hồ sơ DN, nếu đạt yêu cầu sẽ chuyển tới bộ phận kỹ thuật
  - + Bộ phận kỹ thuật hệ thống tiến hành gia hạn CTS và thông báo tới BP tiếp nhận hồ sơ
  - + Bộ phận tiếp nhận hồ sơ có trách nhiệm thông báo tới thuê bao và cập nhật thông tin lên hệ thống và các bên liên quan.
- Trường hợp khi hết hạn mà thuê bao không gia hạn CTS:
  - + Bộ phận tiếp nhận thông báo tới thuê bao về CTS đã hết hiệu lực
  - + Nếu thuê bao gửi đơn đăng ký gia hạn, quá trình thực hiện trường hợp ở trên.

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

Thông báo, cập nhật công bố CTS như mô tả trong Mục 2.2 của tài liệu này.

4.7. Thay đổi cặp khóa của thuê bao.

4.7.1. Đối tượng được gửi yêu cầu thay đổi khóa.

- Chỉ có thuê bao của chứng thư mới có thể yêu cầu thay đổi khóa

- Nếu chứng thư hết hạn thì thủ tục yêu cầu chứng thư tuân theo như yêu cầu khi cấp chứng thư đầu tiên .

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

- Thuê bao có nhu cầu có thể yêu cầu thay đổi cặp khóa
- E-CA khi phát hiện dấu hiệu nghi ngờ bị lộ cặp khóa sẽ đề nghị thuê bao thay đổi cặp khóa

4.7.3. Xử lý yêu cầu thay đổi cặp khóa.

- Khi nhận được yêu cầu xác nhận từ RA, CA sẽ xử lý yêu cầu thay đổi khóa như yêu cầu tạo mới chứng thư ban đầu.

4.7.4. Thông báo, cập nhật chứng thư số sau khi thay đổi cặp khóa đến thuê bao.

Việc thông báo, cập nhật chứng thư sau khi thay đổi cặp khóa được tiến hành như yêu cầu tạo mới chứng thư số thuê bao.

4.8. Thay đổi thông tin chứng thư số.

4.8.1. Đối tượng được gửi yêu cầu thay đổi thông tin chứng thư số

- Chủ thể chứng thư số.
- Đại diện của tổ chức trên chứng thư số.

4.8.2. Các trường hợp được thay đổi thông tin chứng thư số của thuê bao.

Việc sửa đổi được áp dụng cho các thông tin đang tồn tại khi đăng ký chứng thư số của thuê bao như:

- Thay đổi tên chủ thể trên thuê bao chứng thư số được xác nhận bởi cơ quan chức năng.
- Thay đổi tỉnh/thành phố nơi ở, trụ sở đăng ký.
- Thay đổi loại mã, mã thuê bao
- Sáp nhập tổ chức, mã căn cước với chủ thể là cá nhân.

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

Khi nhận được yêu cầu xác nhận từ RA, chủ thể thuê bao, CA sẽ tiến hành xác minh thông tin và xử lý thay đổi thông tin chứng thư số theo đúng đề nghị dựa trên hồ sơ pháp lý của chủ thể thuê bao.

4.8.4. Thông báo, cập nhật chứng thư số sau khi thay đổi thông tin đến thuê bao

Thông báo, cập nhật công bố CTS như mô tả trong Mục 2.2 của tài liệu này.

4.9. Tạm dừng và thu hồi chứng thư số.

4.9.1. Đối tượng được phép yêu cầu tạm dừng, thu hồi chứng thư số.

- Những thuê bao cá nhân có thể yêu cầu thu hồi chứng thư cá nhân của chính họ.
- Trong trường hợp chứng thư của tổ chức, một đại diện được uỷ quyền hợp

pháp của tổ chức được quyền yêu cầu thu hồi chứng thư đã ban hành cho tổ chức.

- Đại diện được uỷ quyền hợp pháp của E-CA hoặc RA sẽ được quyền yêu cầu thu hồi chứng thư quản trị của RA.
- Đơn vị phê chuẩn đơn xin cấp chứng thư của người đăng ký cũng sẽ được quyền thu hồi hoặc yêu cầu thu hồi chứng nhận của thuê bao

4.9.2. Các trường hợp được phép tạm dừng, thu hồi chứng thư số của thuê bao.

- Khi thuê bao yêu cầu bằng văn bản và yêu cầu này được E-CA xác minh là chính xác
- Khi E-CA có căn cứ khẳng định chứng thư số được cấp không tuân theo các quy định trong quy chế chứng thực E-CA đưa ra hoặc khi phát hiện sai sót có ảnh hưởng tới quyền lợi của Thuê Bao và người nhận.
- Theo điều kiện tạm dừng, thu hồi chứng thư số được quy định trong hợp đồng giữa thuê bao và E-CA
- Khi thuê bao là cá nhân đã chết hoặc mất tích theo tuyên bố của tòa án hoặc thuê bao là tổ chức giải thể hoặc phá sản theo quy định của pháp luật.
- Khi có yêu cầu của cơ quan tiến hành tố tụng, cơ quan công an hoặc Bộ thông tin và truyền thông.

4.9.3. Quy trình, thủ tục thu hồi, tạm dừng chứng thư số.

Theo trình tự thu hồi, tạm dừng chứng thư, E-CA xác nhận thuê bao yêu cầu thu hồi, tạm dừng chứng thư là cá nhân hay tổ chức được chấp nhận đơn xin cấp chứng thư. Trình tự xác nhận yêu cầu thu hồi, tạm dừng của thuê bao bao gồm:

- Thuê bao thông báo nội dung yêu cầu chứng thư, chữ ký và chữ ký số liên quan với chứng thư thu hồi, tạm dừng
- Thông báo cho các thuê bao lý do chắc chắn về thu hồi, tạm dừng chứng thư mà cá nhân hay tổ chức yêu cầu. Trên thực tế, việc thông tin với các thuê bao phụ thuộc vào nhiều trường hợp khác nhau nhưng có thể là một trong các cách sau: điện thoại, fax, thư điện tử, thư tín hay các dịch vụ đưa tin khác.
- Thuê bao gửi yêu cầu thu hồi tới E-CA hoặc các RA. E-CA xác nhận nhận dạng của người quản trị thông qua điều khiển truy cập sử dụng SSL và xác thực khách hàng trước khi cho phép họ thực hiện chức năng thu hồi, tạm dừng.
- Sau khi chứng thư số của thuê bao bị tạm dừng/thu hồi, token chứa chứng thư số sẽ bị tạm khóa. Thuê bao không thể sử dụng chứng thư số đã bị tạm dừng/thu hồi.
- Thời gian xử lý yêu cầu tạm dừng, thu hồi: E-CA sẽ xử lý tạm dừng, thu hồi nhanh nhất có thể ngay sau khi nhận được yêu cầu hợp lý về việc tạm dừng, thu hồi và xác nhận thẩm quyền của người yêu cầu.

4.9.4. Thông báo việc thu hồi chứng thư số của thuê bao.

- Ngay sau khi thu hồi chứng thư số, E-CA sẽ cập nhật trực tuyến cơ sở dữ liệu của chứng thư số hoặc CRL (theo mục 2.2)
- Tất cả những yêu cầu tạm dừng, thu hồi và kết quả sẽ được E-CA lưu trữ.
- E-CA gửi thông báo cho thuê bao qua email về việc chứng thư số của thuê bao đã bị tạm dừng/thu hồi.

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

Công bố cập nhật danh sách CTS như mô tả trong Mục 2.2 của tài liệu này.

4.10. Kiểm tra trạng thái chứng thư số.

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

Các chứng thư được lưu trữ trong kho công cộng của E-CA và có thể được kiểm tra qua chức năng tra cứu chứng thư số trên website, tải danh sách chứng thư số bị thu hồi và kiểm tra OCSP

4.10.2. Khả năng sẵn sàng của dịch vụ kiểm tra trạng thái chứng thư số.

Dịch vụ cung cấp trạng thái hoạt động của chứng thư luôn sẵn sàng 24/7, ngoại trừ các hoạt động bảo trì không thể tránh khỏi và do đặc tính tự nhiên của internet (Phụ thuộc vào dịch vụ của các ISP) khi dịch vụ này không thể truy cập được.

Địa chỉ cung cấp dịch vụ:

- Website tra cứu: https://ECA.com.vn/tracuuCTS
- CRL: http://crl.ECA.com.vn/ECA.crl
- OCSP: http://ocsp.ECA.com.vn

4.10.3. Các tính năng khác.

- OCSP là đặc tính dịch vụ kiểm tra trạng thái tuỳ chọn, không sẵn có cho mọi sản phẩm và phải được kích hoạt đối với từng dịch vụ.

4.11. Chấm dứt dịch vụ của thuê bao.

4.11.1. Các trường hợp chấm dứt dịch vụ của thuê bao.

- Trường hợp thuê bao hết hạn theo hiệu lực hợp đồng và không có nhu cầu tiếp tục sử dụng dịch vụ.
- Thu hồi chứng thư số trước khi chứng thư hết hạn mà không thay thế bằng một chứng thư khác.
- Trường hợp thuê bao/E-CA hủy hợp đồng

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

4.12.1. Dịch vụ lưu trữ khóa bí mật của thuê bao.

E-CA không cung cấp dịch vụ cam kết và khôi phục khoá. Chủ sở hữu khóa phải tự thực hiện việc bảo vệ để tránh mất khoá.

4.12.2. Phục hồi khóa bí mật của thuê bao.

E-CA không lưu trữ khóa của thuê bao nên không phát sinh vấn đề khôi phục khóa.

5. KIỂM SOÁT, QUẢN LÝ VÀ VẬN HÀNH.

5.1. Kiểm soát an toàn, an ninh vật lý.

5.1.1. Xác định vị trí đặt hệ thống.

Hoạt động của CA và RA được xây dựng bên trong một môi trường vật lý được bảo vệ nhằm ngăn cản và dò tìm ra các truy cập, sử dụng hoặc phơi bày các thông tin nhạy cảm một cách bất hợp pháp và hệ thống được công khai hay che dấu. RA cũng đồng thời duy trì các biện pháp phòng ngừa thảm họa cho các hoạt động về CA của mình. Các biện pháp phòng ngừa thảm họa được bảo vệ bởi nhiều tầng bảo mật mức vật lý.

5.1.2. Truy cập vật lý.

Các Server của RA và CA được đặt trong một môi trường được kiểm soát, truy cập bị hạn chế bởi quyền truy cập cá nhân. Máy tính đóng vai trò ký của CA và khóa bí mật lưu giữ bằng khóa an toàn khi không sử dụng.

5.1.3. Điều hoà và nguồn điện.

Các Server cung cấp dịch vụ trực tuyến được hoạt động trong môi trường điều hòa thích hợp, và không khởi động lại ngoại trừ việc bảo dưỡng thiết yếu.

Các Server của hệ thống E-CA được bảo vệ bằng hệ thống UPS và máy phát điện dự phòng trong trường hợp mất điện lưới.

5.1.4. Tiếp xúc với nước.

Địa điểm đặt thiết bị hệ thống của E-CA được lựa chọn thích hợp, và xây dựng phương án phòng ngừa để ngăn chặn nước, lụt xâm nhập vào hệ thống.

5.1.5. Phòng cháy chữa cháy.

E-CA thiết kế tuân thủ luật pháp phòng cháy chữa cháy của Việt Nam.

5.1.6. Phương tiện lưu trữ.

Một số các bản sao khóa bí mật của E-CA được lưu giữ trên thiết bị lưu trữ ngoài (USB, CD-ROM) ở vị trí an toàn đảm bảo tránh được những rủi ro bất ngờ (nước, lửa, điện từ trường).

Có phương tiện lưu trữ dữ liệu (máy chủ, hệ thống SAN) được bảo vệ khỏi nước, lửa hay môi trường huỷ hoại và được bảo vệ tránh sử dụng truy cập trái phép hay phá huỷ.

5.1.7. Xử lý rác.

Xử lý rác chứa các dữ liệu được bảo vệ (Các dữ liệu có liên quan đến mã hoá như các khóa bí mật hoặc mật khẩu hoặc dữ liệu cá nhân) sẽ được tiêu hủy một cách để đảm bảo rằng thông tin không thể bị tiết lộ hay tái sử dụng.

5.1.8. Dự phòng từ xa.

E-CA đảm bảo rằng các thiết bị được sử dụng để sao lưu bên ngoài sẽ phải có mức độ an ninh giống như khu vực CA. Hệ thống sao lưu, có khả năng khôi phục khi hệ thống bị hỏng, sẽ được định kỳ thực hiện. Ít nhất một bản sao sẽ được lưu trữ tại một địa điểm bên ngoài (tách biệt với khu vực có thiết bị của CA). Chỉ cần lưu trữ lại lần sao lưu gần nhất. Sao lưu sẽ được lưu trữ tại một địa điểm với các cơ chế và quy trình kiểm soát tương tự như cơ chế và quy trình kiểm soát khi hệ thống hoạt động của hệ thống CA.

5.2. Quy trình kiểm soát.

5.2.1. Những thành viên được tin cậy.

Tất cả các nhân viên có quyền truy cập hoặc điều khiển các hoạt động được mã hóa có thể ảnh hưởng chủ yếu tới việc cấp phát, sử dụng, thu hồi, hủy bỏ/thu hồi chứng thư số, bao gồm cả việc truy cập tới khu vực điều khiển hạn chế của CA.

Những nhân viên này bao gồm nhưng không giới hạn là nhân viên quản trị hệ thống, điều hành, nhân viên kỹ thuật, nhân viên hỗ trợ kỹ thuật, kiểm toán viên, quản trị viên được chỉ định để quản lý hoạt động của CA

5.2.2. Số lượng người yêu cầu cho mỗi công việc

E-CA có các các thủ tục và cơ chế an ninh thích hợp như việc đảm bảo không có một cá nhân nào có thể thực hiện độc lập các hoạt động của CA. Việc áp dụng nguyên tắc này giống như chia sẻ tri thức và cùng điều khiển.

Chính sách và thủ tục được thực hiện để đảm bảo sự phân công nhiệm vụ dựa trên khả năng làm việc. Những công việc mang tính nhạy cảm cao, chẳng hạn truy cập và quản lý hệ thống phần cứng mã hoá và các công việc liên quan đến khoá, yêu cầu nhiều người được tin tưởng tham gia.

Những thủ tục điều khiển ở bên trong được thiết kế để đảm bảo ít nhất 03 cá nhân được tin tưởng cùng tham gia truy cập tới mức vật lý hoặc mức logic của thiết bị truy cập tới phần cứng mã hoá yêu cầu chặt chẽ phải có nhiều người được tin tưởng cùng tham gia toàn bộ quá trình làm việc từ việc nhận và kiểm tra cho tới bước cuối cùng là huỷ về logic hoặc về vật lý.

5.2.3. Nhận dạng và xác thực cho từng thành viên.

Tất cả các nhân viên CA phải được xác minh nhận dạng và xác thực trước khi họ: (i) có trong danh sách truy cập tới các vị trí CA; (ii) có trong danh sách truy cập đến hệ thống CA; (iii) được cung cấp một chứng thư số để thực hiện nhiệm vụ CA; hoặc (iv) được cung cấp một tài khoản trên hệ thống PKI.

5.2.4. Vai trò yêu cầu phân chia trách nhiệm.

Những vai trò yêu cầu phân chia trách nhiệm bao gồm:

- Xác thực thông tin trong đơn xin cấp chứng thư.
- Quá trình chấp nhận, từ chối, hoặc các quá trình khác của đơn xin cấp

chứng thư, yêu cầu thu hồi, cấp mới hay các thông tin đăng ký.

- Quá trình ban hành, thu hồi các chứng thư, bao gồm những cá nhân được truy cập tới những phần hạn chế truy cập của kho lưu trữ.
- Quá trình chuyển giao những thông tin thuê bao hay các yêu cầu từ khách hàng.
- Quá trình tạo, ban hành hay tiêu huỷ chứng thư số.

5.3. Kiểm soát nhân sự.

5.3.1. Năng lực, kinh nghiệm và các yêu cầu khác.

Tất cả các nhân viên của E-CA phải được đào tạo phù hợp có kinh nghiệm về Hạ tầng khóa công khai (PKI) và các hoạt động của nó và những người có năng lực kỹ thuật và chuyên môn có liên quan. Đồng thời E-CA cũng yêu cầu những nhân viên có xuất thân và lai lịch rõ ràng.

5.3.2. Thủ tục kiểm tra lai lịch.

Trước khi nhân viên bắt đầu việc làm trong một vai trò được tin cậy, E-CA tiến hành kiểm tra nền tảng đó bao gồm:

- Xác nhận việc làm trước đó;
- Kiểm tra các nguồn thông tin tham khảo;
- Xác nhận trình độ chuyên môn, bằng cấp liên quan;
- Bản xác minh sơ yếu lý lịch;

Các yếu tố trong thủ tục kiểm tra lai lịch được xem là căn cứ để từ chối các ứng cử viên cho vị trí được tin tưởng hoặc là căn cứ để chống lại những người đã được tin tưởng thường bao gồm:

- Các ứng cử viên hoặc người tin tưởng cung cấp sai thông tin;
- Nguồn tham khảo bất lợi hoặc không đáng tin cậy;
- Có tiền án tiền sự;
- Có vấn đề liên quan đến tài chính.

5.3.3. Yêu cầu về đào tạo.

E-CA tổ chức các chương trình đào tạo cần thiết cho nhân viên để thực hiện nhiệm vụ và công việc của mình một cách phù hợp và chuyên nghiệp. Việc định kỳ đánh giá và tăng cường các chương trình đào tạo này là cần thiết.

Chương trình đào tạo được thiết kế riêng cho nhiệm vụ công việc của nhân viên bao gồm:

- Khái niệm căn bản về PKI;
- Trách nhiệm công việc;
- Các chính sách, quy chế an ninh của nhà nước và của E-CA;
- Các phiên bản phần cứng phần mềm được sử dụng và các thức vận hành hệ

thống CA;

- Báo cáo, chuyển giao các thỏa hiệp và các vấn đề liên quan;
- Thủ tục khôi phục sau thảm hoạ và duy trì công việc.

5.3.4. Chu kỳ tái đào tạo.

E-CA thường xuyên đào tạo lại và cập nhật thông tin cho nhân viên của mình với mức độ và tần suất phù hợp để nhân viên duy trì mức độ tin tưởng và thực hiện tốt công việc của mình.

Việc tổ chức đào tạo lại bắt buộc khi hệ thống sử dụng phần mềm hoặc các tính năng mới cũng như các thủ tục của tổ chức được triển khai.

5.3.5. Tần suất và trình tự luân chuyển công việc.

Không quy định.

5.3.6. Kỷ luật đối với các hoạt động không hợp pháp.

E-CA có quyền truy tố các hành động trái phép theo các quy định của Việt Nam. Các biện pháp kỷ luật hoặc chấm dứt hợp đồng tùy thuộc vào mức độ nghiêm trọng của hành động bất hợp pháp.

5.3.7. Yêu cầu đối với các nhà thầu độc lập.

Các nhà thầu độc lập hoặc tư vấn có thể được coi là đối tượng tin cậy. Bất cứ nhà thầu hoặc tư vấn được coi cùng chức năng và tiêu chuẩn bảo mật tương tự áp dụng cho một nhân viên của E-CA ở vị trí tương đương.

5.3.8. Cung cấp tài liệu cho nhân viên.

E-CA cung cấp tất cả các tài liệu cần thiết để họ hoàn thành tốt công việc của mình.

5.4. Các quy trình ghi nhật ký hệ thống.

5.4.1. Các loại bản ghi sự kiện.

Những sự kiện sau đây được ghi lại:

- Trên các máy chủ lưu trữ chứng thư offline
  - + Khởi động và tắt;
  - + Đăng nhập, đăng xuất;
  - + Tạo và ký chứng thư.
- Trên các máy chủ trực tuyến của E-CA
  - + Nhận yêu cầu chứng thư từ một RA;
  - + Thêm một bản ghi trong cơ sở dữ liệu của CA;
  - + Ghi các yêu cầu cấp chứng thư ra thiết bị lưu trữ ngoài;
  - + Truyền các chứng thư cho yêu cầu bên liên quan;

+ Lưu trữ chứng thư trong kho trực tuyến;
+ Nhận được yêu cầu thu hồi;
+ Phát hành CRL.

5.4.2. Tần suất xử lý bản ghi sự kiện.

Các tập tin log phải được phân tích mỗi quý một lần, hoặc sau khi phát hiện hoặc nghi ngờ có hành vi xâm phạm bất hợp pháp hay sự cố hệ thống.

5.4.3. Thời gian duy trì cho kiểm định bản ghi.

Khoảng thời gian lưu giữ tối thiểu đối với các bản ghi kiểm toán là 07 năm.

5.4.4. Bảo vệ các bản ghi kiểm định.

Bản ghi kiểm định sẽ được phân quyền truy cập, tránh các truy cập, sửa đổi, xoá bỏ hoặc can thiệp bất hợp pháp. Bản ghi kiểm định tại máy chủ local chỉ được truy cập bởi các cán bộ điều hành và quản lý CA. Bản sao của các bản ghi kiểm định lưu tại máy chủ tập trung chỉ được truy cập bởi 2 cán bộ quản lý được cấp đặc quyền truy cập.

5.4.5. Thủ tục sao lưu dự phòng cho các bản ghi kiểm định.

Các bản ghi kiểm định sẽ được lưu trên máy chủ local và máy chủ quản lý log tập trung. Việc sao lưu các bản ghi này thực hiện tự động bằng job backup tự động hằng ngày.

5.4.6. Hệ thống thu thập kiểm định (bên trong và bên ngoài).

Không quy định.

5.4.7. Thông báo về nguyên nhân sự kiện.

Không quy định.

5.4.8. Đánh giá điểm yếu.

Không chỉ định.

5.5. Lưu trữ các bản ghi.

5.5.1. Những kiểu bản ghi được lưu trữ.

Các bản ghi được lưu trữ được liệt kê trong mục 5.4.1.

5.5.2. Thời gian duy trì tài liệu lưu trữ.

Khoảng thời gian lưu giữ tối thiểu là 10 năm.

5.5.3. Bảo mật tài liệu lưu trữ.

Các lưu trữ chỉ được truy cập bởi các nhân viên điều hành và quản lý của E-CA.

5.5.4. Thủ tục sao lưu và dự phòng dữ liệu.

Các bản ghi được sao lưu trên phương tiện lưu trữ di động và được cất giữ trong phòng với truy cập bị hạn chế.

5.5.5. Yêu cầu nhãn thời gian cho dữ liệu.

Tất cả các bản ghi sự kiện phải được đóng dấu thời gian.

5.5.6. Hệ thống thu thập dữ liệu lưu trữ (nội bộ và bên ngoài).

Các lưu trữ sẽ được lưu trữ trên hệ thống trực tuyến chứa kho E-CA và được bảo vệ với mức độ an toàn tốt nhất.

5.5.7. Thủ tục thu thập và kiểm tra thông tin lưu trữ.

Tất cả chứng thư số được cấp bởi E-CA được công bố công khai. Dữ liệu được sử dụng cho việc đăng ký và thẩm định thuê bao chỉ dùng cho nội bộ của E-CA.

Tính toàn vẹn lưu trữ thông tin của E-CA được xác minh:

- Vào thời gian chuẩn bị lưu trữ;
- Vào thời điểm kiểm toán an ninh;
- Bất cứ lúc nào khác khi một kiểm toán an toàn là bắt buộc.

5.6. Thay đổi khóa.

Một thuê bao cần thay đổi khóa sẽ yêu cầu cấp chứng thư số theo quy trình cấp chứng thư số mới. Chi tiết trình bày trong Mục 4.3.

Đối với khóa CA, trong trường hợp cần thay đổi, E-CA sẽ thông báo với cơ quan an ninh liên quan và Trung tâm Chứng thực chữ ký số Quốc gia để phối hợp thực hiện. Khi được Root CA chấp thuận và thống nhất thực hiện, việc thay đổi khóa thực hiện như sau:

- Thực hiện hủy khóa cũ trên hệ thống E-CA.
- Sinh cặp khóa (khoá bí mật và khoá công khai HSM tại E-CA).
- Gửi khóa công khai tới Root CA theo hướng dẫn, cách thức mà Root CA quy định.
- Sau khi Root CA thực hiện cấp phát CTS và truyền lại cho E-CA. CTS này sẽ được import vào HSM để thực hiện các chức năng của mình.
- Root CA, các bên tin tưởng, các CA có liên quan cập nhật thông tin thay đổi.

5.7. Xử lý sự cố, thảm họa và phục hồi.

5.7.1. Các thủ tục xử lý sự cố lộ khóa.

Nếu các khóa bí mật của một thuê bao bị mất hoặc bị tổn hại, RA của E-CA phải thông báo ngay lập tức để yêu cầu thu hồi chứng thư số của họ. Tất cả các bên tin tưởng biết và chấp nhận khóa nên được thông báo của chủ sở hữu khoá.

Nếu khóa bí mật của E-CA bị tổn hại, quản lý CA phải:

- Cố gắng hết sức để thông báo cho các thuê bao và các RA;
- Chấm dứt việc phát hành và phân phối các chứng chỉ và CRLs;

- Yêu cầu thu hồi giấy chứng nhận thỏa hiệp;
- Khởi tạo một cặp khóa và chứng thư của E-CA mới và công bố trong kho lưu trữ;
- Thu hồi tất cả các chứng chỉ hợp lệ ký bởi khóa bị xâm hại;
- Xuất bản danh sách CRL mới trong kho của E-CA;
- Thông báo tới cơ quan an ninh liên quan và Trung tâm Chứng thực chữ ký số Quốc gia;
- Thông báo tới các bên tin tưởng, các CA có liên quan.

5.7.2. Hành vi tiêu cực đối với tài nguyên máy tính, phần mềm và dữ liệu

Các thành phần phần cứng, phần mềm của hệ thống E-CA được xây dựng dựa trên các giải pháp tiêu chuẩn để đảm bảo an toàn thông tin, luôn có phương án dự phòng tại chỗ cũng như từ xa cho mọi tình huống sự cố. Teams Quản Trị Hệ Thống phụ trách việc trực vận hành, sẵn sàng xử lý các tình huống sự cố 24/7.

5.7.3. Xử lý nguy cơ lộ khóa riêng (Private Key)

Nếu E-CA phát hiện thấy nguy cơ lộ khóa riêng (PrivateKey), E-CA sẽ lập tức triệu tập ngay một nhóm phản ứng sự cố khẩn cấp để đánh giá tình hình, xác định mức độ của sự cố và thực hiện hành động thích hợp theo quy định trong kế hoạch ứng phó sự cố bảo mật của E-CA.

5.7.4. Khả năng hoạt động liên tục khi có thảm họa.

E-CA đã thiết kế hệ thống và Thiết lập duy trì khả năng hoạt động liên tục, giải quyết và phục hồi hệ thống trong trường hợp xảy ra thảm họa.

Để có thể tiếp tục phục hồi các hoạt động một cách nhanh nhất sau khi máy tính của E-CA bị lỗi, các bước sau đây sẽ được thực hiện:

- Tất cả các phần mềm trên E-CA sẽ được sao lưu trên phương tiện lưu trữ di động, sau khi cài đặt một phiên bản mới của bất kỳ một thành phần nào của E-CA.
- Tất cả các file dữ liệu của các CA hoạt động offline sẽ được sao lưu trên phương tiện lưu trữ di động sau mỗi lần thay đổi.
- Các thiết bị lưu trữ private key (HSM) dự phòng và lưu trữ dữ liệu backup được lưu trữ tại một cơ sở dự phòng cách xa trên 30km so với cơ sở chính. Tại cơ sở dự phòng luôn luôn duy trì một bản sao hệ thống với các thành phần thiết yếu như hệ thống chính nhằm đảm bảo có thể phục hồi ngay, duy trì tính liên tục của dịch vụ.

Nếu phần cứng hoặc phần mềm của Server ký bị lỗi, trạng thái này sẽ được chẩn đoán và phục hồi kịp thời. Nếu có bất kỳ một nghi ngờ nào về mức độ thiệt hại chưa được khắc phục Server này được cài đặt lại từ đầu bằng cách sử dụng các thiết bị gốc và các phần mềm kèm theo.

Nếu dữ liệu bị lỗi, sẽ được chẩn đoán và phục hồi lại dữ liệu sao lưu gần

nhất.

5.8. Dừng hoạt động.

Việc kết thúc của các tổ chức tham gia dịch vụ sẽ nằm trong thỏa thuận chung, các bên sử dụng áp dụng các biện pháp thương mại hợp lý để đi đến thỏa thuận cho kế hoạch kết thúc nhằm giảm thiểu tối đa tác động tới khách hàng, thuê bao và các đối tác. Kế hoạch kết thúc bao gồm các bước như sau:

- Thông báo với Bộ Thông tin và Truyền thông và Trung tâm Chứng thực quốc gia để làm các thủ tục chấm dứt cung cấp dịch vụ
- Thông báo tới các bên liên quan quá trình chấm dứt hoạt động như thuê bao, các đối tác, khách hàng …
- Ngừng cấp chứng thư số
- Tiếp tục hỗ trợ dịch vụ cho các khách hàng và thuê bao cho tới khi chuyển giao
- Hoàn lại phí (nếu cần) cho những khách hàng, thuê bao có chứng thư chưa hết hạn, chưa bị thu hồi hoặc bị thu hồi trong quá trình chấm dứt hoạt động
- Thực hiện chuyển giao cần thiết của dịch vụ E-CA tới các CA đang hoạt động theo thỏa thuận
- Thông báo và công bố

6. ĐẢM BẢO AN TOÀN AN NINH VỀ KỸ THUẬT.

6.1. Tạo và phân phối cặp khóa.

6.1.1. Tạo cặp khóa.

Cặp khóa cho E-CA được tạo ra bởi các nhân viên thẩm quyền chứng thực trên máy tính không kết nối vào mạng. Cặp khóa này được sinh trực tiếp bên trong thiết bị HSM của hãng Securosys với thuật toán RSA. Quản lý và bảo mật khóa CA sử dụng mô-đun phần cứng bảo mật (HSM) này bảo mật quá trình khởi tạo khóa; phần cứng chuyên nghiệp bảo vệ và quản lý vòng đời khóa bảo mật; gắn kết chính sách bảo mật vào HSM; nâng cao hiệu suất và đảm bảo tính ổn định, sẵn sàng và yêu cầu cao về an toàn bảo mật hệ thống.

Đối với thuê bao, cặp khóa được sinh ngay trong phần cứng của thiết bị đầu cuối của thuê bao (eToken). Mỗi cặp khóa đảm bảo được tính duy nhất và không bị suy ra khóa bí mật từ khóa công khai tương ứng. Việc phân phối khóa đến thuê bao được thực hiện bằng thiết bị lưu trữ thông minh, đảm bảo an toàn bảo mật tuyệt đối trong việc phân phối khoá.

Đối với cặp khóa thuê bao tự sinh: E-CA cung cấp phần mềm để thuê bao sinh cặp khóa theo thuật toán phi đối xứng RSA hoặc thuê bao tự sử dụng chương trình sinh cặp khóa của mình theo thuật toán RSA.

6.1.2. Chuyển giao khóa bí mật cho thuê bao.

Nếu như chính người giữ mô-đun mã hóa tạo khóa thì sẽ không cần chuyển

khóa bí mật.

Nếu khóa không được tạo ra bởi thuê bao thì hệ thống cung cấp dịch vụ của E-CA cung cấp hai phương thức phân phối khóa một cách bảo mật tới thuê bao:

6.1.3. Phân phối khóa trực tiếp tới thuê bao:

- Hệ thống cung cấp dịch vụ của E-CA sinh cặp khóa trong thiết bị phần cứng (PKI Token), ký tạo và cấp chứng thư số cho thuê bao sau đó bàn giao trực tiếp cho người đăng ký.
- Mã PIN của thiết bị được hệ thống E-CA sinh ngẫu nhiên trong quá trình cấp phát chứng thư số và được gửi cho người dùng qua email hoặc bàn giao trực tiếp.
- Người sử dụng phải thực hiện đổi mã PIN trong lần đầu tiên sử dụng để đảm bảo an toàn.
- Đến ngày hẹn trong giấy hẹn hoặc ngay sau khi cấp, thuê bao sẽ được nhận chứng thư số. Nhân viên trung tâm đăng ký thực hiện việc cấp thiết bị eToken đã ghi chứng thư và khóa bí mật, kèm theo biên bản giao chứng thư (trên đó có in đầy đủ các thông tin về thuê bao, khóa công khai của thuê bao, khóa công khai của hệ thống).

6.1.4. Phân phối khóa trực tuyến:

Hệ thống E-CA không phân phối khóa trực tuyến.

6.1.5. Chuyển giao khóa công khai tới tổ chức ban hành chứng thư.

E-CA cung cấp công cụ để thuê bao truyền các yêu cầu chứng thực, bao gồm khóa công khai, tới E-CA thông qua các yêu cầu với định dạng PKCS#10.

6.1.6. Chuyển giao khóa công khai của CA tới các đối tác tin cậy.

Chứng thư số của CA (có chứa khóa công khai) được chuyển giao cho thuê bao bằng giao dịch trực tuyến từ Server website trực tuyến.

6.1.7. Kích thước khoá.

Chuẩn hiện tại của dịch vụ E-CA yêu cầu chiều dài tối thiểu của cặp khóa để đảm bảo mức độ mã hoá đủ mạnh là 2048 bit RSA. Tùy theo gói dịch vụ cung cấp.

6.1.8. Tạo các tham số cho khóa công khai và kiểm tra chất lượng.

Không có quy định.

6.1.9. Mục đích sử dụng khóa (như trong X.509 v3 lĩnh vực sử dụng khoá).

khóa được sử dụng theo mỗi loại chứng thư:

- Với thuê bao:
  - Chứng thực;
  - Chống chối bỏ;

- Mã hoá dữ liệu;
- Thiết lập phiên giao dịch;
- Kiểm tra tính toàn vẹn của dữ liệu.

- Với chứng thư tự ký của CA
  - Ký chứng thư;
  - Ký CRL;
  - Thu hồi chứng thư

6.1.10. Quản lý đại lý và đào tạo đại lý.

- RA (Registration Authority): là một đối tượng, tổ chức được CA tin cậy uỷ quyền để đăng ký và đảm bảo tính đúng đắn nội dung thông tin trong chứng thư số. RA sẽ thu thập thông tin và cung cấp cho CA trực thuộc. RA bao gồm một tập hợp phần cứng máy tính, phần mềm, và những người vận hành. Mỗi RA sẽ thường xuyên vận hành bởi một người, và mỗi CA sẽ quản lý một nhóm RA tin cậy.

- Nhiệm vụ RA:
  - Xác thực nhận dạng đối tượng
  - Xác thực thông tin đối tượng, chủ thể sử dụng CTS và gửi yêu cầu tới CA

- Quản lý đại lý cho phép quản trị viên cấp CA thêm mới đại lý, chỉnh sửa thông tin đại lý, phân quyền gói dịch vụ cho đại lý, thông tin truy cập API

- Đào tạo đại lý: RA sau khi được cấp phép bởi CA, sẽ tiến hành đào tạo theo khung được quy định chi tiết tại NVĐL (nghiệp vụ đại lý) và Hợp đồng đại lý.

6.2. Kiểm soát và bảo vệ khóa bí mật.

6.2.1. Kiểm soát và chuẩn hoá mô đun mã hoá.

Các khóa bí mật được lưu giữ trong môi trường phần cứng an toàn (các khóa ký) và được lưu trữ trong cơ sở dữ liệu của máy chủ (các khóa mã).

Hệ thống CA của E-CA sử dụng thiết bị HSM của hãng Securosys. Các thiết bị này quản lý khóa trên thiết bị phần cứng từ khi sinh khóa quản lý khóa CA, ký chứng thư số, xác nhận, lưu trữ và sao lưu khoá.

Các thao tác với khóa chỉ được thực hiện bên trong thiết bị phần cứng nhằm ngăn chặn những người không có quyền truy cập được phép sử dụng.

Các thiết bị HSM hay USB Token mà E-CA sử dụng đều tuân theo chuẩn FIPS PUB 140-2 level 3.

6.2.2. Đa kiểm soát khóa bí mật.

Để sử dụng được Private Key người dùng cần phải có các điều kiện sau:

- Đối với khóa CA: Sử dụng cơ chế xác thực dựa trên định danh (identity-

based authentication) của thiết bị HSM – đạt tiêu chuẩn FIPS PUB 140 – 2 level 3. E-CA sử dụng cơ chế "m out of n" được cung cấp qua HSM chia key làm 3 phần, yêu cầu phải có 2 trong 3 thành phần mới có thể sử dụng

- Đối với các token cung cấp cho khách hàng (đạt chuẩn FIPS PUB 140-2 Level 3):
    - Phải sở hữu thiết bị.
    - Phải có mã PIN để truy cập thiết bị.

Mã PIN của thiết bị được hệ thống E-CA sinh ngẫu nhiên trong quá trình cấp phát chứng thư số và được gửi cho người dùng qua email hoặc bàn giao trực tiếp.

Người sử dụng token phải thực hiện đổi mã PIN trong lần đầu tiên sử dụng để đảm bảo an toàn.

6.2.3. Bản cam kết khóa bí mật.

Không triển khai dịch vụ cam kết khóa bí mật.

6.2.4. Sao lưu dự phòng khóa bí mật.

Các thuê bao chịu trách nhiệm sao lưu dự phòng khóa bí mật của họ.

Các khóa mã của thuê bao sẽ được sao lưu dự phòng.

E-CA sao lưu các khóa bí mật của CA cho mục đích khôi phục và khắc phục sau thảm họa.

6.2.5. Lưu trữ khóa bí mật.

Khi chứng thư của E-CA hết hạn, các cặp khóa CA gắn với chứng thư đó được lưu trữ trong một thời gian ít nhất là 05 năm trong các mô đun phần cứng có cơ chế mã hoá đáp ứng được các yêu cầu của bản CP/CPS này. Những cặp khóa CA này sẽ không được sử dụng trong bất kỳ chữ ký nào sau khi hết hạn sử dụng trừ khi các chứng thư CA này được khôi phục trong các trường hợp của CP/CPS.

6.2.6. Cách thức khóa bí mật được chuyển đến hoặc đi từ một mô đun mã hoá.

Để thực hiện các hoạt động khóa bí mật chuyển đến hoặc đi từ một mô đun mã hóa khóa bí mật của CA phải được mã hoá trên một máy chủ chứng thực (CA Server) hoạt động offline và chuyển giao chúng vào trong mô đun mã hoá phần cứng khác để ngăn chặn mất mát, ăn trộm, sửa đổi, tiết lộ và sử dụng trái phép khóa bí mật. Việc chuyển giao này sẽ bị giới hạn để tạo ra các bản sao dự phòng khóa bí mật trên mô đun phần cứng phù hợp với tiêu chuẩn quy định trong chính sách bảo mật của E-CA.

6.2.7. Lưu trữ khóa bí mật trên module bảo mật.

khóa bí mật của khách hàng được lưu trữ trên các module bảo mật chuyên dụng PKI Token hoặc PKI smart Card do E-CA cung cấp hoặc khuyến nghị cho khách hàng, đạt tiêu chuẩn bảo mật FIPS PUB 140-2 level 3.

6.2.8. Phương thức kích hoạt khóa bí mật.

Khóa bí mật của CA được bảo vệ bằng thiết bị bảo mật chuyên dụng HSM

và được kích hoạt bằng quy trình điều khiển xác thực đa lớp tới thiết bị. Quản trị viên CA phải có thiết bị kích hoạt là thẻ SmartCard chuyên dụng và sử dụng mật khẩu cá nhân của mình để kích hoạt khóa bí mật.

6.2.9. Phương thức dừng hiệu lực của một khóa bí mật.

khóa bí mật của CA được lưu trữ trong RAM và xoá hoàn toàn khi hoạt động cần thiết của nó kết thúc.

khóa bí mật của thuê bao dừng hiệu lực sau khi hoàn thành hoạt động cần thiết của nó như mỗi khi đăng xuất khỏi hệ thống, hoặc gỡ bỏ thẻ lưu trữ ra khỏi đầu đọc thẻ (phụ thuộc vào loại thiết bị lưu trữ đầu cuối mà thuê bao sử dụng).

6.2.10. Phương thức hủy khóa bí mật.

Quy trình hủy khóa bí mật yêu cầu khóa không thể bị tiết lộ hay tái sử dụng sau khi hủy. Chi tiết mô tả trong *QTHT_M_QT08_Quy trình hủy khóa CA và thuê bao_1.02* của Đề Án Kỹ Thuật.

6.2.11. Mức độ bảo mật của module mã hóa.

Các thiết bị HSM, USB Token được E-CA sử dụng đều đáp ứng chuẩn FIPS PUB 140-2 level 3. Chi tiết trình bày trong Mục *3.1.2. Đáp ứng Chuẩn bảo mật cho HSM và PKI USB TOKEN* của Đề Án Kỹ Thuật

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

6.3.1. Lưu trữ cặp khóa.

E-CA phải lưu trữ tất cả các chứng thư đã phát hành trên thiết bị lưu trữ ngoài và được cất offline ở một nơi an toàn.

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

- Không có quy định về tính hợp lệ của cặp khóa tạo ra. Chỉ có hiệu lực của chứng thư do E-CA được xác định bởi tài liệu CP/CPS này.
- Thời gian hoạt động chứng thư của thuê bao có 3 mức phụ thuộc vào gói dịch vụ E-CA cung cấp và lần lượt là 365 ngày (1 năm), 730 ngày (2 năm), 1095 ngày (3 năm). Thời gian hoạt động chứng thư RA là 3 năm.
- Thời gian hoạt động của chứng thư số E-CA là 5 năm.
- Thêm vào đó dịch vụ E-CA ngưng cấp phát các chứng thư mới trước ngày chứng thư của CA hết hạn nhằm đảm bảo rằng không có một chứng thư nào được cấp phát bởi một CA cấp dưới sẽ bị hết hạn sau khi các chứng thư của các CA cấp trên đó hết hạn sử dụng.

6.4. Kích hoạt dữ liệu

6.4.1. Quá trình tạo và cài đặt dữ liệu kích hoạt.

E-CA khuyến cáo đối với thuê bao sử dụng mật khẩu đủ mạnh để bảo vệ các khóa bí mật của họ (bao gồm ít nhất 8 ký tự). E-CA cũng khuyến nghị sử dụng cơ chế xác thực 2 nhân tố (ví dụ: thẻ và mã nhận dạng cá nhân (PIN), thẻ và sinh trắc học, hay sinh trắc học và mã bảo vệ cá nhân) để kích hoạt khóa bí mật.

6.4.2. Bảo vệ dữ liệu kích hoạt.

E-CA khuyến cáo thuê bao của mình lưu trữ các khóa bí mật của họ ở dạng mã hoá và bảo vệ khóa bí mật của mình thông qua sử dụng thiết bị phần cứng đầu cuối/ hoặc mật khẩu đủ mạnh. E-CA khuyến khích sử dụng cơ chế xác thực hai nhân tố.

Trường hợp chứng thư số được lưu trên token và bảo vệ bằng mật khẩu E-CA khuyến cáo thuê bao định kỳ thay đổi mật khẩu.

Bất kỳ dự phòng của mật khẩu bảo vệ khóa bí mật (trên máy hoặc trên giấy) phải được lưu trữ ở nơi an toàn.

6.4.3. Những khía cạnh khác của dữ liệu kích hoạt.

Không có quy định.

6.5. Kiểm soát an ninh máy tính.

6.5.1. Các yêu cầu về an ninh đối với hệ thống máy tính.

E-CA đảm bảo chắc chắn rằng các hệ thống chứa phần mềm CA và các tệp dữ liệu phải là hệ thống đáng tin cậy chống lại được các truy cập trái phép. Thêm vào đó, E-CA cũng giới hạn tối đa các truy cập đến máy chủ chính với những lý do quyền hạn để truy cập.

Lớp mạng máy tính được phân tách logic thành các phần khác nhau. Phân tách này ngăn chặn truy cập mạng, ngoài trừ thông qua các xử lý ứng dụng đã được xác định. Tất cả các phiên làm việc đều được xác thực bằng mật khẩu hoặc chứng thư proxy để đăng nhập.

6.5.2. Định kỳ đánh giá bảo mật hệ thống máy tính.

Thực hiện đánh giá định kỳ tối thiểu 1 năm 1 lần.

6.6. Kiểm soát an ninh quy trình sử dụng.

6.6.1. Kiểm soát về phát triển hệ thống.

Không có quy định do core ở đây là 1 hệ thống xây dựng dựa trên các thiết bị, giải pháp tiêu chuẩn, khi triển khai chỉ thiết lập các thông số theo công bố và đưa vào vận hành chứ không phát triển thêm.

6.6.2. Kiểm soát vấn đề quản lý bảo mật.

Các vấn đề về quản lý bảo mật được E-CA mô tả trong Mục **3.3. Giải pháp An ninh và bảo mật**, tuân thủ **QTHT_M_QC01_ Quy chế vận hành Trung tâm dữ liệu E-CA** của Đề Án Kỹ Thuật

6.6.3. Kiểm soát chu kỳ bảo mật.

Chu kỳ đánh giá an toàn thông tin được E-CA thực hiện tối thiểu 1 năm 1 lần.

6.7. Giám sát an ninh hệ thống mạng.

- Tất cả các thiết bị hệ thống CA được bảo vệ bằng firewall và Hệ thống phát hiện xâm nhập, phòng chống truy cập trái phép (IDS/IPS) hoặc bằng cách loại bỏ các dịch vụ không cần thiết. Tư tưởng thiết kế hệ thống là giảm thiểu tối đa sự tiếp xúc với môi trường internet; những dịch vụ Frontend, proxy trong vùng DMZ được bảo vệ bởi 1 lớp Firewall, IPS/IDS; những dịch vụ khác đều được bảo vệ bởi 2 lớp Firewall, IPS/IDS.
- Chi tiết mô tả trong Mục **3.3. Giải pháp An ninh và bảo mật** của Đề Án Kỹ Thuật

6.8. Dấu thời gian (Time-Stamping).

- E-CA dự kiến chưa cung cấp dịch vụ TimeStamp.
- Các chứng chỉ, thông tin thu hồi (CLS, OCSP) có chứa thông tin về thời gian và ngày. Các thông tin thời gian cần thiết như trên không được mã hoá.

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

7.1. Định dạng của chứng thư số.

Chứng thư số được định dạng theo chuẩn quốc tế ITU-T X.509v3. Trên mỗi chứng thư số sẽ bao gồm nội dung sau:

Tên trường	Giá trị
Số hiệu chứng thư/ Serial Number	Do E-CA gán, là định dạng duy nhất của chứng thư số.
Tên của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng/ Issuer	E-CA
Thời điểm chứng thư bắt đầu có hiệu lực/ Not Before	Thời điểm chứng thư bắt đầu có hiệu lực. Được đồng bộ với NTP Server.

Thời điểm chứng thư hết hiệu lực/ Not After	Thời điểm chứng thư hết hiệu lực. Được đồng bộ với NTP Server.
Tên của thuê bao/ Subject	Tên của thuê bao
khóa công khai của thuê bao/ Subject Public Key Info	khóa công khai của thuê bao. Được mã hóa theo tiêu chuẩn RFC 3280; Xác định thuật toán RSA được sử dụng cùng với khoá
Thuật toán chữ ký số áp dụng/Signature Algorithm	Thuật toán E-CA sử dụng để ký số chứng thư
Chữ ký số của trung tâm chứng thư số / Signature	Chữ ký số của trung tâm chứng thư số E-CA
Các thông tin khác cho mục đích quản lý, sử dụng, an toàn, bảo mật do tổ chức cung cấp dịch vụ chữ ký số quy định.	

7.1.1. Phiên bản.

E-CA phát hành chứng thư X.509 phiên bản 3.

7.1.2. Phần mở rộng của chứng thư.

Phần mở rộng của chứng thư X.509 v3 được thể hiện trong chứng thư số của E-CA là:

Chứng thư số dùng cho Cá nhân/Tổ chức

Basic Constraints	critical, ca: false
Subject Key Identifier	hash
Authority Key Identifier	keyid
Key Usage	digitalSignature nonRepudiation keyEnciphermnet dataEncipherment keyAgreement
Extended Key Usage	clientAuth codeSigning emailProtection

	timeStamping
Certificate Policies	OID của CP/CPS có hiệu lực tại thời điểm phát hành chứng thư
Subject alternative name	Chứng thư được cấp cho cá nhân/Tổ chức địa chỉ e-mail có liên quan để liên lạc với thuê bao được quy định trong CP/CPS này.
Issuer Alternative Name	Liên kết (URI) đến chứng thư của E-CA
CRL Distribution Points	URI của CRL

Chứng thư số dùng cho dịch vụ / Máy chủ

Basic Constraints	critical, ca: false
Subject Key Identifier	hash
Authority Key Identifier	keyid
Key Usage	digitalSignature nonRepudiation keyEnciphermnet dataEncipherment keyAgreement
Extended Key Usage	clientAuth serverAuth
Certificate Policies	OID của CP/CPS có hiệu lực tại thời điểm phát hành chứng thư
Subject alternative name	Tên miền đầy đủ của máy chủ lưu trữ (DNS:FQDN)
Issuer Alternative Name	Liên kết (URI) đến chứng thư của E-CA
CRL Distribution Points	URI của CRL

7.1.3. Thuật toán nhận biết đối tượng.

Các OID cho các thuật toán được sử dụng cho chữ ký của chứng thư phát hành bởi E-CA theo:

- hash function: id-sha1 — 1.3.14.3.2.26 hoặc id-sha2:

- encryption: rsaEncryption — 1.2.840.113549.1.1.1

- signature: sha-1WithRSAEncryption —1.2.840.113549.1.1.5 hoặc sha256WithRSAEncryption: —1.2.840.113549.1.1.11

7.1.4. Cấu trúc tên.

Mỗi chứng thư có một tên duy nhất và rõ ràng Tên phân biệt trong tất cả các chứng thư phát hành bởi E-CA và tuân theo cấu trúc được định nghĩa trong tiêu chuẩn ITU-T Standards Recommendation X.501 (Xem mục III.1.2).

7.1.5. Ràng buộc tên.

Không có những ràng buộc khác hơn so với quy định tại mục VII.1.4, và III.1.2 III.1.5.

7.1.6. Chính sách nhận biết đối tượng.

OID của Quy chế chứng thực này là 1.3.6.1.4.1.30339.1.x.3

Trong đó, x được xác định khi E-CA đăng ký với Bộ Thông tin và Truyền thông.

7.1.7. Cách dùng của sự mở rộng chính sách ràng buộc.

Không có ràng buộc nào.

7.1.8. Chính sách hạn định cấu trúc và ngữ nghĩa.

Không có quy định.

7.1.9. Xử lý ngữ nghĩa cho phần mở rộng của các chứng thư quan trọng

Không có quy định.

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

E-CA sẽ tạo và xuất bản danh sách thu hồi chứng thư CRL X.509 phiên bản 2.

Version	V2
Signature	Sha256RSA
Issuer	CN = E-CA O = THAISONSOFT C = VN
This Update	Chỉ ra ngày và thời gian CRL được công bố
Next Update	Chỉ ra ngày và thời gian danh sách thu hồi kế tiếp được cấp.
Revoked Certificates	serialNumbers của chứng thư bị thu hồi

Những chứng chỉ đã bị CA thu hồi được ghi vào danh sách theo thứ tự của

revokedCertificates. Mỗi đầu vào nhận biết chứng chỉ thông qua số serial và ngày thu hồi trên đó có ghi rõ thời gian và ngày khi chứng chỉ bị CA thu hồi.

7.2.1. Phiên bản.

E-CA sẽ tạo và xuất bản danh sách thu hồi chứng thư CRL X.509 phiên bản 2.

7.2.2. CRL và phần mở rộng đầu vào CRL.

Không có quy định.

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

OCSP tuân theo cấu trúc dữ liệu được mô tả trong tiêu chuẩn IETF RFC 5280

Version	V1
Responder ID	Tên của OCSP yêu cầu
Produced At	Ngày tháng phát hành
Responses	Mã trạng thái (tốt, thu hồi, không biết) của yêu cầu

7.3.1. Phiên bản.

Profile của OCSP sử dụng phiên bản 1 trong các yêu cầu và các hồi đáp.

7.3.2. Phần mở rộng của OCSP.

Chưa được xác định.

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

8.1. Tần suất và các tình huống kiểm tra kỹ thuật

- Các cuộc kiểm tra sự tuân thủ điều khoản CP/CPS được tiến hành ít nhất mỗi năm một lần.
- E-CA tiến hành kiểm tra sự tuân thủ các thủ tục của mỗi RA với CP/CPS có hiệu lực ít nhất mỗi năm một lần.
- Quy định việc kiểm tra kỹ thuật cho hệ thống chứng thực chữ ký số: kiểm tra định kỳ, đột xuất.

8.2. Đơn vị, người thực hiện kiểm tra kỹ thuật

Trung tâm vận hành hệ thống E-CA. Bộ phận quản trị hệ thống.

8.3. Các nội dung kiểm tra kỹ thuật

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

- Hạ tầng hệ thống.

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

8.4. Xử lý khi phát hiện sai sót

E-CA phải hành động ngay lập tức nếu đánh giá cho thấy một sự vi phạm các quy định trong CP/CPS. Nếu phát hiện vi phạm trực tiếp tới sự tin cậy của chứng thư, Chứng thư được phát hành vi phạm sẽ bị thu hồi ngay lập tức.

Khi phát hiện có sự cố, Bộ phận vận hành thực hiện các biện pháp cô lập và xác định nguyên nhân xảy ra sự cố theo nguyên tắc hạn chế tối đa ảnh hưởng tới hoạt động của hệ thống; đồng thời phải thông báo cho bộ phận sử dụng và các cá nhân, tổ chức có liên quan về tình hình sự cố. Tùy thuộc vào mức độ ảnh hưởng của sự cố, đánh giá và phân loại theo 03 mức: sự cố thông thường, sự cố nghiêm trọng và sự cố đặc biệt nghiêm trọng:

- Đối với các sự cố thông thường (không gây ảnh hưởng đến hoạt động của Trung tâm dữ liệu), Bộ phận vận hành nhanh chóng xử lý sự cố. Trường hợp không xử lý được, thông báo quản lý để phối hợp giải quyết.
- Đối với các sự cố nghiêm trọng (các sự cố liên quan đến thiết bị mạng, thiết bị bảo mật, máy chủ, đường truyền dữ liệu, cơ sở dữ liệu, các sự cố liên quan đến an ninh thông tin, mất mát dữ liệu, gây ảnh hưởng trực tiếp đến hoạt động của Trung tâm dữ liệu), ngay sau khi phát hiện sự cố Bộ phận vận hành cần đánh giá ảnh hưởng của sự cố và thực hiện báo cáo quản lý để được xây dựng phương án xử lý.
- Đối với các sự cố đặc biệt nghiêm trọng (gây ngưng trệ đến toàn bộ hoạt động của Trung tâm dữ liệu), Bộ phận vận hành và quản lý phải có đánh giá ảnh hưởng của sự cố và thực hiện báo cáo ngay tới lãnh đạo công ty để có chỉ đạo xử lý kịp thời.

8.5. Công bố kết quả kiểm tra kỹ thuật

Công bố bằng Biên bản kiểm tra kỹ thuật tại địa điểm kiểm tra.

8.6. Tần suất và các trường hợp đánh giá

Được mô tả tại mục 8.1 và 8.3.

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

Chưa được xác định.

9. CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC

9.1. Phí/Giá.

- Phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số theo quy định tại Thông tư số 19/2022/TT-BTC ngày 23/03/2022 của Bộ Tài chính quy định mức thu, chế độ thu, nộp, quản lý và sử dụng phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số.

- Giá cấp, gia hạn, thu hồi chứng thư số. (Có Phụ lục bảng giá cung cấp kèm theo)
- Các loại chi phí khác (nếu có).

9.2. Trách nhiệm tài chính.

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

Tổ chức cung cấp dịch vụ CTS sẽ nộp phí theo hướng dẫn của ~~Thông tư số~~ Thông tư số 19/2022/TT-BTC ngày 23/03/2022 của Bộ Tài chính quy định mức thu, chế độ thu, nộp, quản lý và sử dụng phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số.

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

Tuân thủ theo hướng dẫn tại Điều 18 của Nghị định 130/2018/NĐ-CP ngày 27 tháng 9 năm 2018 của Chính phủ quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số

- Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng bị thu hồi giấy phép có trách nhiệm thỏa thuận để bàn giao các cơ sở dữ liệu, hồ sơ có liên quan đến hoạt động cung cấp dịch vụ và đảm bảo quyền lợi sử dụng dịch vụ của các thuê bao cho tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng khác đang hoạt động trong thời hạn không quá 30 ngày, kể từ ngày nhận được thông báo bị thu hồi giấy phép.
- Bộ Thông tin và Truyền thông giám sát và hướng dẫn việc bàn giao giữa các tổ chức cung cấp dịch vụ chứng thực chữ ký số để đảm bảo việc sử dụng dịch vụ không bị gián đoạn của các thuê bao.
- Trong trường hợp không thỏa thuận được với các tổ chức khác về việc bàn giao các cơ sở dữ liệu, hồ sơ có liên quan đến hoạt động cung cấp dịch vụ và đảm bảo việc sử dụng dịch vụ của các thuê bao, Bộ Thông tin và Truyền thông chỉ định một hoặc một số tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng thực hiện điều này. Tổ chức tiếp nhận thực hiện tiếp quyền và nghĩa vụ đối với các thuê bao và người nhận theo hợp đồng đã ký giữa thuê bao và tổ chức bị thu hồi giấy phép.
- Chi phí tiếp nhận, duy trì cơ sở dữ liệu, hồ sơ liên quan và đảm bảo việc sử dụng dịch vụ của thuê bao được lấy từ tiền ký quỹ tại ngân hàng của tổ chức cung cấp dịch vụ chứng thực chữ ký số bị thu hồi giấy phép.

9.3. Bảo mật các thông tin nghiệp vụ.

9.3.1. Phạm vi của thông tin cần bảo mật.

Những dữ liệu sau của thuê bao sẽ được đảm bảo tính bí mật và riêng tư:

- Các dữ liệu CA, được phê chuẩn hoặc không phê chuẩn;

- Các dữ liệu về đơn xin cấp chứng thư;
- Các khóa bí mật của thuê bao;
- Các dữ liệu kiểm toán.

9.3.2. Thông tin không nằm trong phạm vi của quá trình đảm bảo tính bảo mật.

Các thông tin đã được ban hành trong chứng thư số và CRL không được coi là bí mật.

9.3.3. Trách nhiệm bảo mật thông tin bí mật.

Tất cả các thành phần tham gia trong hệ thống E-CA và khách hàng có trách nhiệm bảo mật các thông tin bí mật được chia sẻ. Không được để lộ hoặc tiết lộ cho bên thứ ba.

9.4. Bảo mật thông tin cá nhân.

9.4.1. Kế hoạch đảm bảo tính riêng tư.

Không có quy định.

9.4.2. Những thông tin được coi là riêng tư.

Tất cả các thông tin về người đăng ký mà không được trích trong chứng thư và CRL được coi là riêng tư và không được công khai với bên ngoài CA và RA thực thi việc đăng ký.

9.4.3. Thông tin không được coi là riêng tư.

Thông tin có trong chứng thư và các CRL do E-CA phát hành không được coi là riêng tư. Khi yêu cầu một chứng thư từ E-CA các thuê bao đã đồng ý bao gồm các thông tin này như một phần của chứng thư được công bố.

9.4.4. Trách nhiệm bảo vệ thông tin riêng tư.

E-CA và các RA được công nhận của nó có trách nhiệm bảo vệ thông tin riêng tư của các thuê bao và phải tuân theo những luật riêng tư trong phạm vi quyền hạn của mình.

9.4.5. Thông báo và cho phép sử dụng thông tin bí mật.

Trong trường hợp E-CA hoặc bất kỳ một RA của nó muốn sử dụng thông tin riêng tư của thuê bao phải được các thuê bao đồng ý bằng văn bản.

9.4.6. Cung cấp thông tin riêng theo yêu cầu của pháp luật hay cho quá trình quản trị.

E-CA có trách nhiệm cung cấp thông tin riêng tư nếu:

- Khi có yêu cầu của cơ quan pháp luật có thẩm quyền hoặc các quá trình liên quan đến luật pháp đã được quy định.
- Khi có yêu cầu truy cập thông tin để phục vụ cho quản trị (yêu cầu xác nhận, yêu cầu cho quá trình tạo tài liệu).

9.4.7. Những trường hợp làm lộ thông tin khác.

Không có quy định.

9.5. Quyền sở hữu trí tuệ.

E-CA sở hữu và đăng ký quyền sở hữu trí tuệ liên quan đến tất cả các cơ sở dữ liệu, các trang web, chứng thư số của E-CA và công bố bất kỳ nào khác có nguồn gốc từ E-CA bao gồm CP/CPS này.

Các tên phân biệt (DN) của các CA của E-CA vẫn là tài sản của E-CA và tuân theo những quyền sở hữu này.

9.6. Tuyên bố và cam kết.

9.6.1. Đại diện của CA và vấn đề bảo lãnh.

Các thông tin được công bố trong chứng thư, CRLs và OCSP đáp ứng một cách chính xác khả năng cung cấp tốt nhất của E-CA. Không bảo lãnh khác được đưa ra.

9.6.2. Đại diện của RA và vấn đề bảo lãnh.

Tất cả các RA thực hiện nhiệm vụ của họ về nhận dạng và xác thực của các bên yêu cầu như được mô tả trong 3.2.2 và 3.2.3 với trách nhiệm và khả năng tốt nhất. Không có bảo lãnh khác được đưa ra.

9.6.3. Đại diện của khách hàng và sự bảo lãnh.

Khi yêu cầu E-CA cấp chứng thư khách hàng đã chấp nhận sử dụng và bảo vệ chứng thư và khóa của chứng thư tuân theo quy định trong CP/CPS có hiệu lực tại thời điểm nhận phát hành chứng thư. Tuy nhiên thuê bao có thể áp dụng những quy tắc nghiêm ngặt hơn.

Cụ thể là các thuê bao sẽ thông báo ngày cho E-CA nếu khóa bí mật của chứng thư bị mất hoặc bị xâm hại để CA thu hồi chứng chỉ đó và các bên tin tưởng từ chối chấp nhận chứng thư đó.

Trong trường hợp vi phạm quy định của CP/CPS các thuê bao đã đồng ý theo yêu cầu thu hồi chứng thư của E-CA. Không có một bảo lãnh thêm được yêu cầu từ các thuê bao.

9.6.4. Đại diện các đối tác tin cậy và vấn đề bảo lãnh

Thoả thuận với đối tác tin cậy yêu cầu đối tác tin cậy phải có đủ thông tin để đưa ra một quyết định dựa vào các thông tin trong chứng thư. Họ có trách nhiệm quyết định tin tưởng hay không vào các thông tin trong chứng thư. Các đối tác tin cậy sẽ chịu trách nhiệm pháp lý nếu vi phạm các điều khoản về nghĩa vụ của đối tác tin cậy có trong CP/CPS.

9.6.5. Đại diện cho các bên liên quan khác và vấn đề bảo lãnh.

Không có quy định.

9.7. Từ chối trách nhiệm.

Trong giới hạn cho phép của pháp luật, hợp đồng thuê bao và hợp đồng đối tác tin cậy có thể từ chối sự bảo lãnh của E-CA.

9.8. Giới hạn trách nhiệm.

Trong giới hạn của pháp luật, hợp đồng thuê bao và hợp đồng đối tác tin cậy có thể giới hạn khả năng trách nhiệm pháp lý của E-CA. Việc giới hạn trách nhiệm pháp lý bao gồm cả việc loại bỏ các thiệt hại ngẫu nhiên hay gián tiếp, những thiệt hại nặng nề.

9.9. Bồi thường thiệt hại.

Khi pháp luật yêu cầu, thuê bao sử dụng phải bồi thường cho E-CA nếu xuất hiện:

- Những thông tin sai lạc hoặc xuyên tạc sự thật do thuê bao cung cấp trên chứng thư số
- Lỗi của thuê bao để lộ những nhân tố, yếu tố liên quan đến dịch vụ chứng thư, sự bỏ xót hay làm sai lạc do sự cẩu thả hay với mục đích lừa đảo.
- Lỗi của thuê bao trong việc bảo vệ khóa riêng, sử dụng hệ thống tin cậy, hoặc không thực hiện các biện pháp phòng ngừa cần thiết để tránh gây hậu quả.
- Việc thuê bao sử dụng một tên (kể cả việc không giới hạn bên trong một tên phổ biến, tên miền, thư điện tử) vi phạm quyền sở hữu trí tuệ của một bên thứ ba.
- Hợp đồng với thuê bao tương ứng có thể có một số nghĩa vụ khác.

9.10. Hiệu lực của Quy chế chứng thực.

9.10.1. Thời hạn.

Tài liệu này có hiệu lực khi được công bố trong kho lưu trữ của dịch vụ E-CA. Các điều sửa đổi bổ sung cho CP/CPS này cũng bắt đầu có hiệu lực khi có sự công bố từ kho lưu trữ.

9.10.2. Kết thúc.

Tài liệu này có hiệu lực cho đến khi nó được thay thế bởi một phiên bản mới hơn.

9.10.3. Ảnh hưởng của sự kết thúc và những tổn hại.

Khi CP/CPS hết hiệu lực, các thành phần của dịch vụ E-CA sẽ không bị giới hạn bởi các điều khoản còn hiệu lực của chứng thư đã được ban hành.

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

- Tất cả các email liên lạc giữa CA và các RA phải được ký bằng khóa của chứng thư.
- Tất cả các email liên lạc giữa CA hoặc RA và thuê bao phải được ký điện

tử để làm bằng chứng. Mọi yêu cầu bất kỳ đều phải ký điện tử.

9.12. Bổ sung và sửa đổi.

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

Thay đổi đáng kể điều mục trong CP/CPS sẽ làm OID thay đổi. Quyết định này được thực hiện bởi quản lý CP/CPS của E-CA.

9.12.2. Quy trình sửa đổi, bổ sung quy chế

Những sửa đổi của CP/CPS sẽ được thực hiện bởi cấp quản lý chính sách có thẩm quyền (xem mục 1.5.4).

9.13. Thủ tục giải quyết tranh chấp.

Tranh chấp phát sinh từ CP/CPS sẽ được giải quyết bởi quản lý CP/CPS của E-CA.

9.14. Hệ thống pháp lý điều chỉnh.

Hoạt động của E-CA phải tuân theo luật của nước CHXHCN Việt Nam và luật Thương mại điện tử của Việt Nam. Tất cả các tranh chấp phát sinh từ điều khoản của CP/CPS này, các hoạt động của CA, RA, việc sử dụng các dịch vụ của họ, việc sử dụng và chấp nhận bất kỳ chứng thư được phát hành bởi E-CA được xử lý theo luật của nước CHXHCN Việt Nam.

Tài liệu Quy chế chứng thực của các tổ chức cung cấp dịch vụ chứng thực chữ ký số được điều chỉnh bởi các văn bản quy phạm pháp luật, bao gồm:

- Luật giao dịch điện tử năm 2005;

- Nghị định số 130/2018/NĐ-CP ngày 27/9/2020 của Chính phủ quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số;

- Thông tư số 31/2020/TT-BTTTT ngày 30/10/2020 của Bộ trưởng Bộ Thông tin và Truyền thông.

9.15. Phù hợp với pháp luật hiện hành.

Mọi hoạt động liên quan đến yêu cầu, phát hành, sử dụng hoặc chấp nhận của một chứng thư E-CA phải tuân thủ luật pháp nước CHXHCN Việt Nam.

9.16. Các điều khoản chung.

CP/CPS này sẽ ràng buộc đối với tất cả các bên tham gia. Nếu bất kỳ điều khoản nào của CP/CPS này được phát hiện là không thể thực thi, các điều khoản còn lại sẽ được giải thích để thực hiện thống nhất hợp lý hành động của các bên. Chúng tôi đồng ý rõ ràng rằng mọi điều khoản của CP/CPS này quy định giới hạn trách nhiệm pháp lý hoặc loại trừ thiệt hại, từ chối trách nhiệm hoặc hạn chế bất kỳ bảo đảm, lời hứa hoặc nghĩa vụ nào khác, đều có tính chất quan trọng và độc lập với bất kỳ điều khoản nào khác. CP/CPS này sẽ được giải thích phù hợp với những gì hợp lý về mặt thương mại trong các trường hợp và xem xét phạm vi Việt Nam và ứng dụng thống nhất của nó. Việc bất kỳ ai thi hành một điều khoản của

CP/CPS này sẽ không được coi là sự khước từ việc thực thi trong tương lai đối với điều khoản đó hoặc bất kỳ điều khoản nào khác. Bất kỳ thông báo hoặc yêu cầu nào liên quan đến CP/CPS này sẽ được truyền đạt bằng cách sử dụng các thông điệp được ký điện tử phù hợp với CP/CPS này hoặc bằng văn bản. Thông tin liên lạc điện tử sẽ có hiệu lực khi nhận được bởi người có trách nhiệm.

9.16.1. Sự thừa nhận toàn bộ.

Xem 9.16

9.16.2. Điều khoản chuyển giao.

Xem 9.16

9.16.3. Tính độc lập của các điều khoản.

Xem 9.16

9.16.4. Bắt buộc thực thi.

Xem 9.16

9.16.5. Bất khả kháng.

Xem 9.16

9.17. Các điều khoản khác.

Không áp dụng

PHỤ LỤC I.

HỢP ĐỒNG MẪU GIỮA TỔ CHỨC CUNG CẤP DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG E-CA VÀ THUÊ BAO

(Theo Thông tư số 31/2020/TT-BTTTT ngày 30 tháng 10 năm 2020 của Bộ trưởng Bộ Thông tin và Truyền thông).

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

HỢP ĐỒNG

CUNG CẤP VÀ SỬ DỤNG DỊCH VỤ
CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG

Số:.....

[PHẦN 1. CÁC CĂN CỨ]

Căn cứ Bộ Luật Dân sự ngày 24 tháng 11 năm 2015;

Căn cứ Luật Thương mại ngày 14 tháng 6 năm 2005;

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Nghị định số 130/2018/NĐ-CP ngày 27 tháng 9 năm 2018 của Chính phủ quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số;

Các căn cứ pháp lý khác có liên quan;

[PHẦN 2. NỘI DUNG BẮT BUỘC]

I. THÔNG TIN CÁC BÊN

1. Bên sử dụng dịch vụ (Bên A):

1.1. Đối với tổ chức

Người đại diện:..... Chức vụ:.....

Địa chỉ:.....

Điện thoại:..... Fax:.....

Tài khoản:.....

Mã số thuế:.....

Các thông tin khác (nếu có).

1.2. Đối với cá nhân

Họ và tên:.....

CMND/Hộ chiếu/Căn cước công dân: .....

Địa chỉ:.....

Điện thoại:..... Fax:.....

Tài khoản:.....

Mã số thuế:.....

Các thông tin khác (nếu có).

2. Bên cung cấp dịch vụ (Bên B):

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.....

Người đại diện theo pháp luật:.....

Địa chỉ:.....

Điện thoại:..... Fax:.....

Tài khoản:.....

Mã số thuế:.....

Các thông tin khác (nếu có).

Hợp đồng đại lý được lập thành văn bản với các nội dung được các bên thống nhất...

Sau khi thỏa thuận, các bên thống nhất ký kết hợp đồng cung cấp và sử dụng dịch vụ chứng thực chữ ký số công cộng với các nội dung sau:

II. NỘI DUNG HỢP ĐỒNG

Điều. Phạm vi, giới hạn sử dụng

(áp dụng đối với dịch vụ chứng thực chữ ký số)

Điều. Mức độ bảo mật

- Hệ thống phân phối khóa cho thuê bao (Bên A) phải đảm bảo sự toàn vẹn và bảo mật của cặp khóa. Trong trường hợp phân phối khóa thông qua môi trường mạng máy tính thì hệ thống phân phối khóa phải sử dụng các giao thức bảo mật đảm bảo không lộ thông tin trên đường truyền.

- Bên A có trách nhiệm lưu trữ và sử dụng khóa bí mật của mình một cách an toàn, bí mật trong suốt thời gian chứng thư số của mình có hiệu lực và bị tạm dừng.

Điều. Điều kiện đảm bảo an toàn cho chữ ký số

- Chữ ký số được tạo ra trong thời gian chứng thư số có hiệu lực và kiểm tra được bằng khóa công khai ghi trên chứng thư số đó;

- Chữ ký số được tạo ra bằng việc sử dụng khóa bí mật tương ứng với khóa công khai ghi trên chứng thư số do Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng cấp;

- khóa bí mật chỉ thuộc sự kiểm soát của người ký tại thời điểm ký.

Điều. Chi phí liên quan đến việc cấp và sử dụng chứng thư số của thuê bao

(Chi phí liên quan đến việc cấp và sử dụng chứng thư số của thuê bao do hai bên thỏa thuận)

Điều. Tạm dừng, thu hồi chứng thư số của thuê bao

(Nội dung liên quan đến tạm dựng, thu hồi chứng thư số của thuê bao theo quy định tại Điều 28, 29 Nghị định số 130/2018/NĐ-CP)

Điều. Quyền và nghĩa vụ

1. Quyền và nghĩa vụ của bên A

a) Nhận thức đầy đủ quyền và trách nhiệm khi thực hiện giao dịch sử dụng dịch vụ trên đây, đồng thời chịu trách nhiệm đảm bảo sự an toàn trong lưu trữ và sử dụng khóa bí mật.

b) Cung cấp đầy đủ hồ sơ đề nghị cấp chứng thư số bao gồm:

- Đơn cấp chứng thư số theo mẫu của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.

- Giấy tờ kèm theo:

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

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

c) Có quyền yêu cầu tổ chức cung cấp dịch vụ chứng thực chữ ký số của mình tạm dừng, thu hồi chứng thư số đã cấp và tự chịu trách nhiệm về yêu cầu đó.

d) Cung cấp thông tin theo quy định một cách trung thực, chính xác cho tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.

đ) Trường hợp tự tạo cặp khóa cho mình, thuê bao phải đảm bảo thiết bị tạo cặp khóa sử dụng đúng quy chuẩn kỹ thuật và tiêu chuẩn bắt buộc áp dụng. Quy định này không áp dụng cho trường hợp thuê bao thuê thiết bị tạo cặp khóa của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.

e) Lưu trữ và sử dụng khóa bí mật của mình một cách an toàn, bí mật trong suốt thời gian chứng thư số của mình có hiệu lực và bị tạm dừng.

g) Thông báo trong thời gian 24 giờ cho tổ chức cung cấp dịch vụ chứng thực chữ ký số của mình nếu phát hiện thấy dấu hiệu khóa bí mật của mình đã bị lộ, bị đánh cắp hoặc sử dụng trái phép để có các biện pháp xử lý.

2. Quyền và nghĩa vụ của bên B

a) Đảm bảo cung cấp cho Bên A dịch vụ chứng thực chữ ký số... (loại chứng thư số) sau khi kiểm tra thông tin trong hồ sơ đề nghị cấp chứng thư số của thuê bao là chính xác;

b) Đảm bảo cung cấp dịch vụ chứng thực chữ ký số cho Bên A đáp ứng các điều kiện an toàn cho chữ ký số theo Quy định tại Điều 9 Nghị định số 130/2018/NĐ-CP.

c) Tạo khóa và phân phối khóa cho thuê bao

- Tổ chức, cá nhân đề nghị cấp chứng thư số có thể tự tạo cặp khóa hoặc yêu cầu bằng văn bản tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng tạo cặp khóa cho mình.

- Đảm bảo sử dụng các phương thức an toàn để chuyển giao khóa bí mật đến thuê bao và chỉ được lưu bản sao của khóa bí mật khi tổ chức, cá nhân đề nghị cấp chứng thư số có yêu cầu bằng văn bản.

- Đảm bảo an toàn trong suốt quá trình tạo và chuyển giao chứng thư số cho thuê bao.

- Sử dụng thiết bị, phần mềm theo đúng tiêu chuẩn quy định để khởi tạo và lưu trữ cặp khóa.

d) Đảm bảo việc sử dụng dịch vụ của thuê bao liên tục, không bị gián đoạn trong suốt thời gian hiệu lực của chứng thư số và việc kiểm tra trạng thái chứng thư số của thuê bao là liên tục.

đ) Giải quyết các rủi ro và các khoản đền bù xảy ra cho thuê bao và người nhận trong trường hợp lỗi được xác định của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.

e) Đảm bảo an toàn thông tin riêng, thông tin cá nhân và thiết bị lưu trữ chứng thư số cho thuê bao theo quy định của pháp luật về an toàn thông tin và pháp luật khác có liên quan.

g) Tiếp nhận thông tin:

Đảm bảo kênh tiếp nhận thông tin hoạt động 24 giờ trong ngày và 7 ngày trong tuần từ thuê bao liên quan đến việc sử dụng chứng thư số.

h) Liên quan đến hoạt động quản lý khóa:

- Thông báo ngay cho thuê bao, đồng thời áp dụng những biện pháp ngăn chặn và khắc phục kịp thời trong trường hợp phát hiện thấy dấu hiệu khóa bí mật của thuê bao đã bị lộ, không còn toàn vẹn hoặc bất cứ sự sai sót nào khác có nguy cơ ảnh hưởng xấu đến quyền lợi của thuê bao;

- Khuyến cáo cho thuê bao việc thay đổi cặp khóa khi cần thiết nhằm đảm bảo tính tin cậy và an toàn cao nhất cho cặp khóa.

i) Trong trường hợp phải tạm dừng cấp chứng thư số mới:

Trong thời gian tạm dừng, tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng có trách nhiệm duy trì hệ thống cơ sở dữ liệu liên quan đến chứng thư số đã cấp.

k) Khi bị thu hồi giấy phép, tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng phải thông báo ngay cho thuê bao về việc ngừng cung cấp dịch vụ của mình và thông tin về tổ chức tiếp nhận cơ sở dữ liệu của mình để đảm bảo quyền lợi sử dụng dịch vụ của thuê bao.

Điều. Thủ tục khiếu nại và giải quyết tranh chấp

(Hai bên tự thỏa thuận đảm bảo tuân thủ pháp luật về thương mại và dân sự)

[PHẦN 3. NHỮNG THỎA THUẬN KHÁC (phù hợp với các quy định của pháp luật về dân sự, thương mại)]

….....

.....

ĐẠI DIỆN BÊN A	**ĐẠI DIỆN BÊN B**
(Ký, ghi rõ họ tên và đóng dấu)	*(Ký, ghi rõ họ tên và đóng dấu)*

PHỤ LỤC II. BẢNG GIÁ DỰ KIẾN PHÍ DỊCH VỤ

Gói chứng thư số CA	Thời hạn sử dụng	Dự kiến chi phí (VNĐ)
Dành cho tổ chức, doanh nghiệp		
E-CA1	1 năm	1,826,000
E-CA2	2 năm	2,739,000
E-CA3	3 năm	3,113,000
Dành cho các cá nhân		
E-CA P1	1 năm	1,490,000
E-CA P1	2 năm	2,260,000
E-CA P1	3 năm	2.660,000
Dành cho máy chủ (Server)		
E-CA S1	1 năm	9,590,000
E- CA S2	2 năm	14,590,000
E- CA S3	3 năm	22,590,000
Dành cho HSM *(Hardware Security Module)*		
E- CA H1	1 năm	14,590,000
E- CA H2	2 năm	24,590,000
E-CA H3	3 năm	33,590,000