CÔNG TY CỔ PHẦN ICORP

QUY CHẾ CHỨNG THỰC
CHỨNG THƯ CHỮ KÝ SỐ I-CA

Phiên bản: 1.4
OID

Hà Nội, 2025

MỤC LỤC

1. Giới thiệu

1.1. Tổng quan

Tài liệu này là quy chế chứng thực chữ ký số của I-CA. Tài liệu nêu rõ những Quy chế của cơ quan chứng thực I-CA sử dụng trong quá trình cung cấp dịch vụ chứng thư chữ ký số công cộng bao gồm phát hành, quản lý, thu hồi và cấp lại chứng thư số.

Tài liệu này phù hợp với chuẩn RFC 3647 (IETF CertifI-CAte Policy and CertifI-CAtion Practice Statement).

1.2. Tên và dấu hiệu nhận diện tài liệu

- Tên tài liệu: QUY CHẾ CHỨNG THỰC CHỨNG THƯ CHỮ KÝ SỐ I-CA
- Phiên bản: 1.4
- Ban hành: tháng 07/2025

OID: Không quy định

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

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng là các tổ chức cung cấp dịch vụ chứng thực chữ ký số cho cơ quan, tổ chức, cá nhân sử dụng trong các hoạt động công cộng. Hoạt động của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng là hoạt động nhằm mục đích kinh doanh.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng là tổ chức cung cấp dịch vụ chứng thực chữ ký số cho các cơ quan, tổ chức, cá nhân có cùng tính chất hoạt động hoặc mục đích công việc và được liên kết với nhau thông qua điều lệ hoạt động hoặc văn bản quy phạm pháp luật quy định cơ cấu tổ chức chung hoặc hình thức liên kết, hoạt động chung. Hoạt động của tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng là hoạt động nhằm phục vụ nhu cầu giao dịch nội bộ và không nhằm mục đích kinh doanh.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia (Root CertifI-CAtion Authority) là tổ chức cung cấp dịch vụ chứng thực chữ ký số cho các tổ chức cung cấp dịch vụ chữ ký số công cộng. Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia là duy nhất.

Trung tâm Chứng thực chữ ký số quốc gia là đơn vị có chức năng giúp thực hiện công tác quản lý nhà nước về lĩnh vực chứng thực chữ ký số; quản lý các tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng và chuyên dùng; cấp phát chứng thư số cho các tổ chức đăng ký cung cấp dịch vụ chứng thư số công cộng; tổ chức các hoạt động thúc đẩy việc sử dụng chữ ký số trong các ứng dụng công nghệ thông tin phục vụ phát triển kinh tế - xã hội trong phạm vi cả nước. Trung tâm Chứng thực chữ ký số quốc gia vận hành hệ thống tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia.

Tổ chức đăng ký chứng thư số (Registration Authorities hay RA) liên hệ trực tiếp với các thuê bao. Họ thực hiện việc nhận dạng và xác thực dữ liệu của người xin cấp chứng thư số dựa trên các giấy tờ hợp pháp (như căn cước công dân, hộ chiếu...), họ có thể khởi tạo, chấp nhận hoặc huỷ bỏ các yêu cầu thay mặt cho Tổ chức cung cấp dịch vụ chứng thực chữ ký số.

Tổ chức đăng ký chứng thư số thực hiện việc đăng ký các thông tin của thuê bao xin cấp chứng thư số:

- 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 khoá bí mật đang được đăng ký hay không.
- Tạo cặp khoá bí mật/khoá công khai.
- Thay mặt chủ thể thực thể cuối khởi tạo quá trình đăng ký với CA.
- Khởi sinh quá trình khôi phục khoá.
- Phân phối thẻ thông minh chứa khoá bí mật.

Thuê bao là tất các người dùng cuối (tổ chức, cá nhân, máy chủ web, phần mềm,…) nhận được chứng thư từ tổ chức cung cấp dịch vụ chứng thực chữ ký số.

Bên tin tưởng (hay bên nhận) là đối tượng tin tưởng chứng thư số hay chữ ký số được cung cấp bởi I-CA. Phụ thuộc vào quy định sử dụng chứng thư số, bên tin tưởng có thể là thuê bao hoặc không là thuê bao của I-CA.

Các đối tượng khác I-CA không quản lý đối tượng nào khác ngoài thuê bao và các bên tin tưởng.

1.4. Mục đích sử dụng chứng thư số

1.4.1. Mục đích sử dụng chứng thư số

Trong chứng thư số, trường KeyUsage chứa thông tin về mục đích sử dụng chứng thư số. Thuê bao sử dụng chứng thư số vào các mục đích được quy định bởi trường "Mục đích sử dụng" (KeyUsage) trong chứng thư số.

Mục đích sử dụng không bị cấm bởi pháp luật, chính sách chứng thư số của RootCA, chính sách chứng thư số và quy chế chứng thực của I-CA và thỏa thuận của thuê bao với I-CA.

Chứng thư số do I-CA cấp được phân ra các loại sau đây:

- Chứng thư số cho cá nhân: Là chứng thư số cấp cho cá nhân Thuê bao sử dụng chứng thư số này trong việc ký các ứng dụng, ký email, ký các giao dịch điện tử.

Chứng thư số cho cá nhân có thời hạn không quá 5 năm và không được vượt quá thời hạn của chứng thư số I-CA.

- Chứng thư số cho cá nhân thuộc tổ chức doanh nghiệp: Là chứng thư số cấp cho cá nhân, trong chứng thư số có thông tin về tổ chức doanh nghiệp mà thuê bao trực thuộc. Thuê bao sử dụng chứng thư số này trong việc ký các ứng dụng, ký email, ký các giao dịch điện tử.

Chứng thư số cho cá nhân thuộc tổ chức doanh nghiệp có thời hạn không quá 5 năm và không được vượt quá thời hạn của chứng thư số I-CA.

- Chứng thư số cho các tổ chức doanh nghiệp: Thuê bao là tổ chức doanh nghiệp. Thuê bao sử dụng chứng thư số này trong việc ký các ứng dụng, ký email, kê khai thuế điện tử, hải quan điện tử và ký các giao dịch điện tử khác.

Chứng thư số cho tổ chức doanh nghiệp có thời hạn không quá 5 năm và không được vượt quá thời hạn của chứng thư số I-CA.

Khi thuê bao là cá nhân đăng ký xin cấp chứng thư số thì bản thân thuê bao đứng ra thực hiện đăng ký.

Về cơ bản các chứng thư dùng để ký, mã hóa dữ liệu, thực hiện việc xác thực (ví dụ như xác thực máy khách hoặc xác thực máy chủ SSL). Danh sách dưới đây liệt kê tất cả các trường hợp chứng thư dựa trên các thiết lập như sử dụng khoá, chỉ định và giới hạn tính hợp lệ sử dụng một chứng thư số, sử dụng thẻ, tên các thành phần của trường "subject".

- Chứng thư số dùng cho cá nhân.
- Chứng thư số cho cá nhân thuộc tổ chức doanh nghiệp

- Chứng thư số dùng cho tổ chức.
- Chứng thư số dùng cho các dịch vụ.

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

Chứng thư số không được sử dụng cho các mục đích ngoài mục đích đã nêu trong trường KeyUsage và chỉ được sử dụng theo đúng phạm vi quy định trong hợp đồng giữa I-CA và thuê bao.

Trong mọi trường hợp, cấm sử dụng chứng thư số do I-CA cấp phát vào những mục đích đảm bảo an ninh cho lĩnh vực hạt nhân, hệ thống điều khiển vũ khí, trong lĩnh vực an ninh, quân sự, đảm bảo an ninh quốc gia, cho các hoạt động vi phạm pháp luật hoặc làm chứng thư số gốc của CA khác.

1.5. Quản lý quy chế chứng thực

1.5.1. Cơ quan, tổ chức quản lý quy chế chứng thực, thông tin liên hệ

Tên tổ chức: Công ty Cổ phần ICORP

Địa chỉ: Số 32/21 Phố Trương Công Giai, Phường Cầu Giấy, Thành phố Hà Nội, Việt Nam

Điện thoại: 039.239.8888

E-mail: info@icorp.com.vn

Website: https://i-ca.vn/

1.5.2. Công nhận sự phù hợp của quy chế chứng thực

Bộ Khoa học và Công nghệ và Công ty Cổ phần ICORP xác nhận sự phù hợp của quy chế chứng thực này.

1.5.3. Thủ tục phê chuẩn quy chế chứng thực

Công ty Cổ phần ICORP 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://i-ca.vn/cps/version

Các quá trình xem xét và phê duyệt phải đảm bảo rằng việc này CP-CPS tuân thủ RFC 3647 và các quy định có liên quan.

Khi có sự thay đổi thông tin trong quy chế chứng thực, tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng phải có thông báo bằng văn bản đến Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia và phải được sự đồng ý bằng văn bản của tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia đối với các nội dung thay đổi.

Tất cả các phiên bản Quy chế chứng thực dựa trên đó các chứng thư số hợp lệ đang hoặc đã được cấp phát phải được lưu trữ để cung cấp cho các bên tin tưởng khi có yêu cầu. Các phiên bản của Quy chế chứng thực được công bố tại:

https://i-ca.vn/cps/version

1.6. Các định nghĩa và viết tắt

1.6.1. Các định nghĩa

Thuật ngữ	**Giải thích**
Chứng thư số I-CA	Là một dạng chứng thư điện tử do I-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 khoá công khai của người ký có thể xác định được chính xác: a. Việc biến đổi nêu trên được tạo ra bằng đúng khoá bí mật tương ứng với khoá công khai trong cùng một cặp khóa; b. Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.
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: a. Tạo cặp khóa bao gồm khóa công khai và khóa bí mật cho thuê bao; b. Cấp, gia hạn, tạm dừng, phục hồi và thu hồi chứng thư số của thuê bao; c. Duy trì trực tuyến cơ sở dữ liệu về chứng thư số; d. Những dịch vụ khác có liên quan theo quy định.
Hệ thống mật mã không đối xứng	Là hệ thống mật mã có khả năng tạo được cặp khóa bao gồm khoá 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 khoá 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 khoá 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 khoá bí mật tương ứng với khoá 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

ARLs	Authority Revocation Lists
CA	CertifI-CAte Authority
CMS	Cryptographic Message Syntax
CP	CertifI-CAte Policy
CPS	CertifI-CAtion Practice Statement
CRLs	CertifI-CAte Revocation Lists
CRR	CertifI-CAte Revocation Request
CSP	CertifI-CAtion Service Provider
DAP	Directory Access Protocol
DES	Data Encryption Standard
DNS	Domain Name System
HTTPS	Secure Hypertext Transaction Standard
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5 Hash Algorithm
OCSP	Online CertifI-CAte Status Protocol
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Extended Public Key Infrastructure
RA	Registration Authorities
RFC	Request For Comments
RSA	Rivest Shamir Adleman
S/MIME	Secure Multipurpose Internet Mail Extensions
SHA-1	Secure Hash Standard
SSL	Secure Socket Layer
TLS	Transport Layer Security
X.500	X.500 The ITU-T (International TelecommunI-CAtion Union-T) standard that establishes a distributed, hierarchI-CAl directory protocol organized by country, region, Organization, etc.
X.501	The ITU-T (International TelecommunI-CAtion Union-T) standard for use of Distinguished Names in an X.500 directory.
X.509	ITU-T standard for CertifI-CAtes format

2. Trách nhiệm lưu trữ và công bố thông tin

2.1. Lưu trữ

I-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 để cung cấp dữ liệu cần thiết cho người dùng như chứng thư số cấp bởi I-CA hay danh sách thu hồi chứng thư số (CRLs). Các tài liệu liên quan đến dịch vụ của I-CA (CPS) cũng được cung cấp thông qua giao diện web.

I-CA lưu trữ và sử dụng thông tin của thuê bao bí mật, an toàn tại ứng dụng quản lý khách hàng CRM sử dụng khai thác nội bộ và chỉ sử dụng thông tin này vào mục đích liên quan đến chứng thư số.

Các thông tin thuê bao được I-CA 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 là 05 năm kể từ khi chứng thư số hết hiệu lực.

Danh sách các chứng thư số có hiệu lực, tạm dừng và đã hết hiệu lực được lưu trữ đầy đủ, chính xác và cập nhật cho phép, hướng dẫn người sử dụng Internet truy nhập trực tuyến 24 giờ trong ngày và 7 ngày trong tuần qua các đường dẫn được công bố tại mục 2.2. Công bố thông tin.

Toàn bộ các 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 được I-CA lưu trữ 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

I-CA thực hiện lưu trữ trực tuyến an toàn gồm:

Chứng thư số của I-CA.

Danh sách thu hồi chứng thư số.

Chứng thư số do I-CA đã phát hành.

Bản sao CP/CPS của I-CA và các phiên bản trước của các tài liệu này.

Các thông tin liên quan khác.

Các kho lưu trữ trực tuyến được công bố tại địa chỉ URL sau:

http://crl.i-ca.vn

Địa chỉ công bố truy cập trả lời OCSP: http://ocsp.i-ca.vn

LDAP được công bố trên: ldap.i-ca.vn

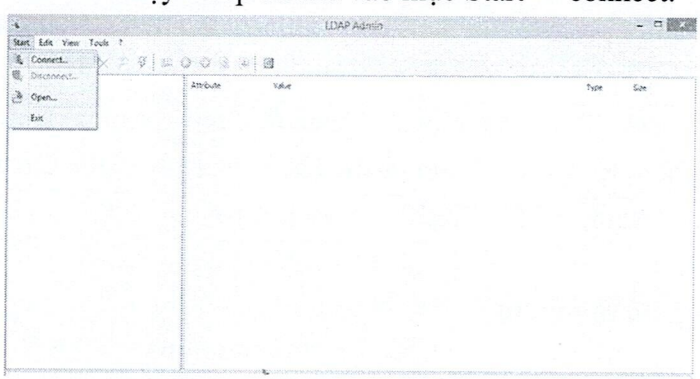
Để đảm bảo an toàn cơ sở dữ liệu LDAP thì I-CA không cho phép truy cập LDAP trên website mà có công cụ để kiểm tra.

Cách kiểm tra như sau:

Bước 1: Download Ldap admin tại:

https://www.i-ca.vn/download/ldapadmin.html

Bước 2: Chạy Ldap admin vào mục Start -> connect.



Bước 3: Chọn new connect và điền các thông số như sau:

Mục host: Ldap.i-ca.vn, ấn nút Fetchs DNs, rồi chọn Base và ấn OK.

Bước 4: chọn Connect tới và xem được thông tin LDAP.

2.3. Thời gian, tần suất công bố thông tin

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

Tần số công bố các dữ liệu thu hồi là: hàng ngày

Tần số 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.

I-CA công bố và duy trì thông tin 24 giờ trong ngày và 7 ngày trong tuần các thông tin quy định tại Mục 2.2 và cập nhật các thông tin này trong vòng 24 giờ khi có thay đổi.

2.4. Kiểm soát truy nhập thông tin

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

I-CA sử dụng biện pháp kỹ thuật để hạn chế những hành động thêm, xóa hay sửa kho lưu trữ. Các hành động truy cập trái phép sẽ bị xử lý theo quy định của công ty và pháp luật.

3. Nhận dạng và xác thực yêu cầu xin cấp chứng thư số

3.1. Đặt tên trong chứng thư số

Chứng thư số chứa một tên dùng để phân biệt với các chứng thư số khác (Distinguished Names – DN) theo chuẩn X.501 trong trường Issuer và Subject. 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:

- EmailAddress (E): Định dạng của thành phần EmailAddress tuân theo chuẩn IETF RFC 2822.
- CommonName (CN): Phân biệt cho mỗi cá nhân, mỗi host, mỗi dịch vụ. Tên đối tượng sở hữu chứng thư số, tên miền nếu là chứng thư số SSL.
- LocalityName (L): Tên khu vực mà đối tượng sở hữu chứng thư số thuộc. Danh sách LocalityName được định nghĩa trước dựa trên các quy định quản trị của I-CA.
- OrganizationalUnitName (OU): Bộ phận thuộc tổ chức (O) mà đối tượng sở hữu chứng thư số thuộc Tên của tổ chức.
- OrganizationName (O): Tên tổ chức mà đối tượng sở hữu chứng thư số thuộc. Giá trị của thành phần OrganizationName được định nghĩa trước (I-CA) và nó cũng là thành phần gốc của LDAP.
- CountryName (C): Hai chữ cái chỉ tên quốc gia theo ISO, Việt Nam được ký hiệu là "VN". 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 cá nhân:

E=tungtv@icorp.com.vn, CN= Trần Văn Tùng, L=Hanoi, OU=Administrator Dept, O=I-CA, C=VN.

3.1.1. Cần thiết cho tên trở nên có ý nghĩa

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 hoặc tên của cá nhân hay tổ chức chịu trách nhiệm.

- Các thuộc tính trong DN của chứng thư số do I-CA cấp cho thuê bao là doanh nghiệp được mô tả như sau:

Thuộc tính	Giá trị
Tổ chức (O)	Tên tổ chức mà thuê bao sở hữu chứng thư số
Bộ phận tổ chức (OU)	Bộ phận thuộc tổ chức (O) mà thuê bao sở hữu chứng thư số trực thuộc.
Tỉnh, thành phố (ST)	Địa chỉ tỉnh, thành phố của thuê bao
Quốc gia (C)	Tên quốc gia của thuê bao
Mã định danh của thuê bao – UID	Mã số Thuế: Đối với khách hàng là tổ chức, doanh nghiệp
Tên thường gọi (CN)	Tên tổ chức, doanh nghiệp (Theo như quyết định thành lập hay giấy đăng ký kinh doanh và một số giấy giờ khác)
Địa chỉ email (E)	Địa chỉ email giao dịch của thuê bao sở hữu chứng thư số

- Các thuộc tính trong DN của chứng thư số do I-CA cấp cho thuê bao là cá nhân thuộc doanh nghiệp được mô tả như sau:

Thuộc tính	Giá trị
Tổ chức (O)	Tên tổ chức mà thuê bao sở hữu chứng thư số
Bộ phận tổ chức (OU)	Bộ phận thuộc tổ chức (O) mà thuê bao sở hữu chứng thư số trực thuộc.
Tỉnh, thành phố (ST)	Địa chỉ tỉnh, thành phố của thuê bao
Quốc gia (C)	Tên quốc gia của thuê bao
Mã định danh của thuê bao – UID	CCCD: Đối với khách hàng cá nhân thuộc tổ chức, doanh nghiệp
Tên thường gọi (CN)	Tên thuê bao sở hữu chứng thư số (Theo như giấy giới thiệu của tổ chức doanh nghiệp, hợp đồng lao động và một số giấy tờ khác)
Địa chỉ email (E)	Địa chỉ email giao dịch của thuê bao sở hữu chứng thư số

- Các thuộc tính trong DN của chứng thư số do I-CA cấp cho thuê bao cá nhân được mô tả như sau:

Thuộc tính	Giá trị
Tỉnh, thành phố (ST)	Địa chỉ tỉnh, thành phố của thuê bao
Quốc gia (C)	Tên quốc gia của thuê bao
Mã định danh của thuê bao – UID	CCCD: Đối với khách hàng cá nhân
Tên thường gọi (CN)	Tên thuê bao sở hữu chứng thư số (Theo như giấy CCCD và một số giấy tờ khác)
Địa chỉ email (E)	Địa chỉ email giao dịch của thuê bao sở hữu chứng thư số

DN trong chứng thư số có thành phần là CN (viết tắt của Common Name – tên thường gọi) và đặt trong trường 'Subject name' của thuê bao. CN trong chứng thư số của thuê bao là tên cá nhân, tổ chức, doanh nghiệp hoặc tên miền, tên thiết bị,… CN được kiểm tra, xác thực trong quá trình cấp chứng thư số.

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

Chứng thư số không được sử dụng biệt hiệu hoặc nặc danh cho tên

Việc sử dụng biệt hiệu hoặc nặc danh cho tên trong chứng thư số chỉ được thực hiện khi có yêu cầu của pháp luật. Khi này, nội dung tên sẽ không phải kiểm tra.

3.1.2. 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.500 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.

Tính duy nhất của tên bao gồm mã định danh thuê bao và số hiệu chứng thư.

Biệt hiệu hay nặc danh: Chứng thư số của các thuê bao không được sử dụng biệt hiệu hoặc nặc danh cho tên. Việc sử dụng biệt hiệu hoặc nặc danh cho tên trong chứng thư số chỉ được chấp nhận khi có yêu cầu của pháp luật và cần có giải trình với I-CA để xem xét.

Chấp nhận, xác thực và vai trò của nhãn hiệu đăng ký (TradeMarks): Thuê bao đăng ký 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 I-CA có quyền thu hồi, tạm dừng chứng thư số hay loại bỏ đơn xin cấp chứng thư số mà không phải chịu trách nhiệm pháp lý.

3.2. Xác minh đề nghị cấp chứng thư số

3.2.1. Phương thức chứng minh sở hữu khóa bí mật

Người đăng ký cấp chứng thư số được yêu cầu phải chứng minh tính sở hữu khóa bí mật của họ thích hợp với khóa công khai trong một yêu cầu chứng thư số thông qua việc ký yêu cầu với khóa bí mật. I-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 tới thuê bao, được coi là sở hữu khóa bí mật tại thời điểm tạo ra hoặc chuyển tiếp. Nếu thuê bao không sở hữu Token khi khóa được tạo ra thì Token sẽ chuyển ngay lập tức đến thuê bao qua một phương pháp tin cậy và có trách nhiệm. Việc chứng minh sự sở hữu khóa bí mật không phải thực hiện khi cặp khóa được I-CA sinh ra trên USB token.

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

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

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

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

Hồ sơ đề nghị cấp chứng thư số của cá nhân được thực hiện bằng phương thức đối chiếu trực tiếp hoặc phương thức điện tử.

I-CA sẽ thực hiện tối thiểu các bước thẩm định bao gồm: thẩm định hồ sơ đáp ứng theo yêu cầu của pháp luật; xác thực chéo với cổng thông tin điện tử của cơ quan quản lý nhà nước hoặc qua kho dữ liệu của I-CA (nếu có).

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

Tên cá nhân;

Địa chỉ theo CCCD/Hộ chiếu hoặc các giấy tờ khác do cơ quan nhà nước cấp;

Số CCCD/Hộ chiếu hoặc các giấy tờ khác do cơ quan nhà nước cấp;

Đơn xin cấp chứng thư số (theo mẫu của I-CA)

Bản sao từ bản gốc/bản sao có chứng thực/bản sao xuất trình bản chính để đối chiếu với một trong các loại giấy tờ: CCCD/Hộ chiếu của cá nhân.

3.2.3. Nhận dạng và xác thực đối với tổ chức

Hồ sơ đề nghị cấp chứng thư số của tổ chức được thực hiện bằng phương thức đối chiếu trực tiếp hoặc phương thức điện tử.

I-CA sẽ thực hiện tối thiểu các bước thẩm định bao gồm: thẩm định hồ sơ đáp ứng theo yêu cầu của pháp luật; xác thực chéo với cổng thông tin điện tử của cơ quan quản lý nhà nước hoặc qua kho dữ liệu của Công ty (nếu có).

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

Tên tổ chức;

Địa chỉ theo đăng ký kinh doanh;

Mã số thuế/mã số tổ chức hợp lệ;

Tên của người đại diện pháp luật;

Đơn xin cấp chứng thư số (theo mẫu của I-CA)

Bản sao từ bản gốc/bản sao có chứng thực/bản sao xuất trình bản chính để đối chiếu với một trong các loại giấy tờ: Đăng ký kinh doanh hoặc Quyết định thành lập/ Giấy phép đầu tư của tổ

chức/quyết định quy định chức năng nhiệm vụ hoặc văn bản xác nhận chức danh của người có thẩm quyền của cơ quan, nhà nước.

Bản sao từ bản gốc/bản sao có chứng thực/bản sao xuất trình bản chính để đối chiếu với một trong các loại giấy tờ: CCCD/Hộ chiếu của người đại diện pháp luật.

Giấy tờ ủy quyền (nếu người ký trên văn bản đăng ký không phải là thông tin của người đại diện pháp luật).

Khi chứng thư số của tổ chức có chứa tên cá nhân làm đại diện, cần thực hiện các thủ tục xác thực sự ủy quyền, các thủ tục xác thực này bao gồm:

- Xác thực sự tồn tại của tổ chức như 3.2.3.
- Xác thực cá nhân như 3.2.2 và xác thực sự ủy quyền của tổ chức đối với cá nhân đó bằng văn bản ủy quyền.

3.3. Xác minh đề nghị thay đổi cặp khóa

Trước khi chứng thư số hết hạn, nếu có nhu cầu thuê bao cần phải đăng ký để có được một chứng thư số mới. Hệ thống cho phép gia hạn (renewal) theo nghĩa sinh một cặp khóa mới thay thế cặp khóa trong chứng thư số đã hết hạn.

3.3.1. Nhận dạng và xác thực trong thủ tục đề nghị thay đổi cặp khóa

Trong thời hạn hiệu lực của chứng thư số thuê bao của I-CA có thể yêu cầu phát hành một chứng thư số với một cặp khoá mới. Việc thay đổi cặp khoá trước khi chứng thư số hết hạn được thực hiện bằng cách gửi yêu cầu dựa trên khoá công khai mới gửi từ Token Manager hoặc nộp đơn đề nghị thay đổi cặp khóa và các giấy tờ chứng minh liên quan khác tại đại lý và điểm giao dịch tin cậy của I-CA. RA đảm bảo rằng cá nhân hay một tổ chức muốn cấp lại khoá cho chứng thư số phải là chủ thuê bao của chứng thư số đó.

Để chấp thuận yêu cầu cấp lại khoá của thuê bao, RA phải nhận dạng và xác nhận các thông tin thuê bao đưa ra là chính xác. Sau khi cấp lại khoá, CA hoặc RA của I-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 thay đổi cặp khóa sau khi đã bị thu hồi

Chứng thư số đã bị thu hồi và hết hạn sử dụng có thể không được thay đổi cặp, làm mới hoặc cập nhật. Việc đề nghị thay đổi cặp 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

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. Thuê bao đưa yêu cầu này có thể được xác thực dựa trên cơ sở chữ ký số được sử dụng khi gửi thông điệp. Nếu chữ ký số đúng, yêu cầu này sẽ được chấp nhận xem là có hiệu lực và thực hiện thu hồi chứng thư số

Tất cả những yêu cầu thu hồi chứng thư số phải được gửi đến I-CA hoặc RA thay mặt cho I-CA, thông qua một quá trình xử lý trực tuyến được chấp nhận hoặc thông qua văn bản.

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 đăng ký

Bất cứ Cá nhân hay tổ chức nào đều có quyền đăng ký xin cấp chứng thư số.

4.1.2. Quy trình đăng ký

Thuê bao phải hoàn thành Phiếu yêu cầu dịch vụ chứng thư số I-CA và phải đảm bảo chính xác thông tin theo mẫu của I-CA.

Thuê bao phải cung cấp các hồ sơ theo yêu cầu của I-CA và đảm bảo tính chính xác của các hồ sơ này.

4.2. Xử lý yêu cầu cấp chứng thư số

4.2.1. Thực hiện chức năng thẩm định

I-CA hoặc RA, đại lý sẽ tổ chức thẩm định theo quy định tại mục 3.2

4.2.2. Chấp thuận (Duyệt) hoặc từ chối

I-CA hoặc RA, đại lý xác thực thông tin đăng ký và trả lời chấp nhận hay từ chối cấp chứng thư số.

- Chấp thuận (Phê duyệt yêu cầu): I-CA hoặc RA, đại lý kiểm tra thông tin yêu cầu cung cấp dịch vụ hợp lệ như yêu cầu tại mục 3.2 thì thực hiện Phê duyệt yêu cầu.
- Từ chối duyệt yêu cầu: Kiểm tra thông tin yêu cầu cung cấp dịch vụ không đúng, không hợp lệ như yêu cầu tại mục 3.2 hoặc không thực hiện theo khung thời gian quy định (nếu có) thì thực hiện Từ chối phê duyệt yêu cầu.

4.2.3. Thời gian xử lý yêu cầu cấp chứng thư số

I-CA có trách nhiệm xử lý các đơn xin cấp chứng thư trong khoảng thời gian phù hợp. Không có quy định thời gian hoàn thành quá trình xử lý một đơn xin cấp chứng thư trừ khi được đưa ra trong hợp đồng với thuê bao, hoặc thoả thuận giữa các bên của dịch vụ I-CA. Thông thường, nếu không có vướng mắc, hệ thống cung cấp dịch vụ I-CA có thể khởi tạo một chứng thư mới tối đa trong 03 ngày.

4.3. Cấp chứng thư số

4.3.1. Quy trình cấp chứng thư số

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

- Tiếp nhận yêu cầu: Bộ phận thẩm định tiếp nhận đăng ký và yêu cầu cấp chứng thư số từ thuê bao, RA.
- Thẩm định: Bộ phận thẩm định tiến hành kiểm tra xác nhận thông tin hồ sơ theo quy định và chuyển yêu cầu cấp đến bộ phận cấp.
- Cấp chứng thư số:Bộ phận cấp chứng thư số tiến hành cấp, quản lý chứng thư số và cập nhật cơ sở dữ liệu ngay khi có phát sinh từ hệ thống.

4.3.2. Thông báo đến người dùng về việc cấp chứng thư số

I-CA cấp phát các chứng thư trực tiếp tới người dùng hoặc thông qua RA. I-CA thông báo cho người dùng rằng chứng thư của họ đã được tạo đồng thời cung cấp cho người dùng quyền truy cập tới chứng thư đó để kiểm tra tính sẵn sàng của chứng thư số. Chứng thư có hiệu lực sẽ cho phép người dùng tải về từ website hoặc thông qua LDAP server.

I-CA gửi email hoặc tin nhắn SMS hoặc điện thoại/fax hoặc phương tiện khác thông báo cho thuê bao về việc yêu cầu cấp chứng thư số của thuê bao đã được phê duyệt.

Thời gian thông báo cho thuê bao sau khi tạo xong chứng thư số tối đa 24h.

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

4.4.1. Điều kiện chứng minh việc xác nhận chứng thư số

Thuê bao xác nhận thông tin chứng thư số là chính xác, hình thức xác nhận bằng phương thức điện tử hoặc văn bản giấy.

- Đối với trường hợp thuê bao xác nhận thông tin bằng phương thức trực tiếp, cụ thể như sau:

Thuê bao thể hiện sự chấp nhận một chứng thư số khi ký vào biên bản giao nhận chứng thư số của I-CA. 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 I-CA lưu trữ.

- Đối với trường hợp thuê bao xác nhận thông tin bằng phương thức điện tử, cụ thể như sau:

Bước 1: Sau khi nhận được chữ ký số từ I-CA, thuê bao cài thiết bị token vào máy tính, hệ thống sẽ hiện lên bảng xác thực bao gồm các thông tin: Tên, Thời hạn, Số Serial chứng thư số

Bước 2: Thuê bao sau khi kiểm tra lại các thông tin trên bảng, nhấn chọn "Chấp nhận" để xác nhận thông tin trên bảng token.

Bước 3: Hệ thống sẽ lưu lại lịch sử xác nhận của khách hàng vào Cơ sở dữ liệu của I-CA

4.4.2. Công bố công khai chứng thư của I-CA

Sau khi nhận được chấp nhận chứng thư, I-CA công bố chứng thư số đã phát hành, I-CA công bố tất cả các chứng thư hợp lệ trong kho lưu trữ trực tuyến trên cả web lẫn kho lưu trữ LDAP. (Xem mục 2.2 Công bố thông tin chứng thư).

Chứng thư số được coi là chính thức chấp nhận khi được I-CA công bố trên website, kho dữ liệu chứng thư số. I-CA công bố chứng thư số của thuê bao tại trang web: https://www.i-ca.vn trong vòng 24h ngay khi nhận được xác nhận của thuê bao về tính chính xác của thông tin.

4.5. Sử dụng cặp khoá và chứng thư số

4.5.1. Sử dụng chứng thư và khoá 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 I-CA và đã chấp nhận chứng thư số được ban hành.

Chứng thư số phát hành bởi I-CA và khoá bí mật tương ứng với khoá công khai trong chứng thư cần 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 khớp với đuôi mở rộng trong trường KeyUsage có trong chứng thư (Trường KeyUsage được định nghĩa trước trong chứng thư và xác định một số chức năng và hoạt động của giao thức như SSL, TLS).

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.

Thuê bao có trách nhiệm bảo vệ khoá bí mật khỏi việc truy cập bất hợp pháp và sẽ không được sử dụng khoá bí mật khi chứng thư hết hạn hay bị thu hồi.

4.5.2. Sử dụng chứng thư và khoá 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 I-CA, phải kiểm tra chứng thư số hợp lệ bằng cách:

- Kiểm tra có đúng chứng thư số do I-CA phát hành;
- Kiểm tra chứng thư số chưa bị thu hồi;
- Chứng thư số được sử dụng theo đúng phần mở rộng của trường KeyUsage và extKeyUsage 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 không bị ngăn cấm hoặc bị giới hạn bởi CP/CPS của I-CA.

4.6. Gia hạn chứng thư số

4.6.1. Các trường hợp cần gia hạn chứng thư số

Gia hạn chứng thư là việc cấp phát chứng thư mới tới thuê bao mà không thay đổi khoá công khai hay bất kỳ một thông tin nào khác trong chứng thư. Nói chung các chứng thư của I-CA sẽ không được gia hạn với cặp khoá tương tự khi chúng sắp hết hạn. Chỉ trong những trường hợp thật cần thiết, và khi việc bảo vệ khóa bí mật có thể được xác định chắc chắn của I-CA hoặc RA/đại lý thích hợp, I-CA sẽ chấp nhận và thực hiện yêu cầu gia hạn chứng thư.

4.6.2. Đối tượng yêu cầu gia hạn chứng thư số

Chủ sở hữu của chứng thư có thể yêu cầu gia hạn chứng thư trước khi nó hết hạn bằng cách gửi cho I-CA hoặc RA/đại lý tương ứng một e-mail ký với khóa bí mật của chứng thư yêu cầu gia hạn hoặc gửi yêu cầu bằng văn bản theo mẫu I-CA công bố trên website có ký xác nhận của chủ thuê bao.

4.6.3. Xử lý các yêu cầu gia hạn chứng thư số

Khi nhận được yêu cầu gia hạn, I-CA sẽ xử lý yêu cầu gia hạn chứng thư như một yêu cầu cấp chứng thư ban đầu.

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

4.6.4. Điều kiện chấp nhận gia hạn chứng thư số

Tuân theo mục 4.4.1

4.6.5. Công bố các chứng thư số được gia hạn

Tuân theo mục 4.4.2

4.7. Thay đổi cặp khóa của thuê bao

Quá trình thay đổi cặp khoá của thuê bao là việc cấp lại một chứng thư mới với cặp khoá mới.

4.7.1. Đối tượng yêu cầu thay đổi khóa

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

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

4.7.2. Trường hợp được thay đổi cặp khóa của thuê bao

Vì lý do an toàn, cấp lại khoá chứng thư được ưu tiên phát hành một chứng thư mới cho một thuê bao có chứng thư sắp hết hạn hoặc những người muốn thay đổi các tham số của chứng thư.

4.7.3. Xử lý các yêu cầu cấp khoá mới cho chứng thư

Khi nhận được yêu cầu xác nhận bởi RA, CA sẽ xử lý yêu cầu thay đổi cặp khóa như một yêu cầu cấp chứng thư ban đầu.

4.7.4. Thông báo phát hành chứng thư mới tới thuê bao

Tuân theo mục 4.3.2

4.7.5. Thông báo chấp nhận cấp mới khoá chứng thư

Tuân theo mục 4.4.1

4.7.6. Phát hành chứng thư đã được cấp mới khoá của I-CA

Tuân theo mục 4.4.2

4.8. Thay đổi thông tin chứng thư số

Việc thay đổi chứng thư số có thể được thực hiện bằng cách thu hồi chứng thư cũ và phát hành lại chứng thư số mới.

4.8.1. Các trường hợp thay đổi thông tin chứng thư số

- Khi thông tin chứng thư số cần thay đổi
- Trừ trường hợp đã nêu tại mục 4.6 và 4.7

4.8.2. Đối tượng yêu cầu thay đổi chứng thư

- Được mô tả tại mục 4.1

4.8.3. Quá trình xử lý yêu cầu thay đổi chứng thư

- I-CA hoặc RA sẽ thực hiện nhận dạng và xác thực mọi thông tin thuê bao được yêu cầu theo mô tả tại ***mục 3.2***

4.8.4. Thông báo phát hành chứng thư mới tới thuê bao

- *Được mô tả tại mục 4.3.2*

4.8.5. Chấp nhận chứng thư số mới được thay đổi

- *Được mô tả tại mục 4.4.1*

4.8.6. Phát hành chứng thư đã được sửa đổi từ I-CA

- *Được mô tả tại mục 4.4.2*

4.9. Tạm dừng và thu hồi chứng thư

4.9.1. Các trường hợp thu hồi

Nếu chứng thư số đã 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 cập nhật vào cơ sở dữ liệu chứng thư số.

Cụ thể chứng thư số bị thu hồi trong các trường hợp sau:

- Thông tin trong chứng thư số được phát hiện sai khác so với thực tế
- Khóa bí mật của thuê bao có chứng thư số bị lộ
- Thuê bao đề nghị thu hồi
- Chứng thư số có tên mạo danh hoặc vi phạm quyền sở hữu trí tuệ
- Chứng thư số sử dụng sai mục đích
- Chứng thư số đã được tạo ra không tuân theo những thủ tục được yêu cầu bởi quy chế chứng thực này
- Có lệnh dừng sử dụng chứng thư số hoặc dừng toàn bộ hệ thống
- Theo quy định của pháp luật hay theo yêu cầu của các cơ quan có thẩm quyền

Khi khóa bí mật của thuê bao bị mất/lộ hoặc nghi ngờ bị mất/lộ, thuê bao phải báo ngay lập tức cho I-CA.

4.9.2. Đối tượng có thể yêu cầu thu hồi

Yêu cầu thu hồi chứng thư được thực hiện bởi:

- Chủ sở hữu khoá của chứng thư.
- I-CA hay bất kỳ một RA đã chứng minh khóa bị lộ.
- Các cơ quan đăng ký có xác nhận của thuê bao chứng thư số.
- Người giữ khoá bí mật.
- Theo yêu cầu của Pháp luật

4.9.3. Quy trình, thủ tục thu hồi chứng thư

Trước khi thu hồi chứng thư số, I-CA xác thực yêu cầu thu hồi:

- Từ thuê bao qua thông điệp ký số yêu cầu thu hồi
- Từ RA.
- Từ các cơ quan quản lý nhà nước hoặc các cơ quan thực thi pháp luật.

RA sử dụng hệ thống quản lý chứng thư số để chuyển các yêu cầu thu hồi tới I-CA.

I-CA tiến hành thu hồi chứng thư số.

I-CA tiến hành cập nhật trạng thái chứng thư số vào các cơ sở dữ liệu xác thực trực tuyến như CRL trong ngày và OCSP ngay lập tức.

4.9.4. Thời gian cho một yêu cầu thu hồi chứng thư

Những yêu cầu thu hồi sẽ được đệ trình ngay khi có thể với thời gian hợp lý.

4.9.5. Thời gian I-CA xử lý yêu cầu thu hồi chứng thư

I-CA sẽ phải xử lý yêu cầu thu hồi chứng thư nhanh nhất có thể. Khi chưa kiểm tra được chính xác danh tính của người yêu cầu thu hồi, chứng thư số sẽ được tạm dừng.

4.9.6. Yêu cầu kiểm tra việc thu hồi cho đối tác tin cậy

Trước khi sử dụng một chứng thư số, bên nhận phải xác nhận CRL gần đây nhất. I-CA sẽ cung cấp các thông tin tìm kiếm CRL thích hợp, kho lưu trữ trên website hay OCSP để kiểm tra trạng thái thu hồi.

4.9.7. Tần số cấp phát CRL

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

4.9.8. Thời gian trễ tối đa cho các CRL

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

4.9.9. Dịch vụ hỗ trợ kiểm tra trạng thái thu hồi trực tuyến

Thông tin trạng thái chứng thư và thông tin thu hồi chứng thư được lưu trữ trực tuyến trên kho của I-CA truy cập qua nền tảng LDAP và web và có thể truy cập qua OCSP. I-CA sẽ cho phép đối tác tin cậy truy vấn trực tuyến các thông tin thu hồi và trạng thái chứng thư.

4.9.10. Những yêu cầu kiểm tra trạng thái chứng thư trực tuyến

Đối tác tin cậy phải kiểm tra CRL trước khi sử dụng và phải tin tưởng chứng thư mong muốn tin cậy.

Không có kiểm soát nào đến khả năng truy cập để kiểm tra CRL.

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 I-CA và được đặt luôn sẵn sàng qua CRL, Website, thư mục LDAP và OCSP:

Chứng thư của I-CA.

Chứng thư cấp bởi I-CA.

Danh sách thu hồi cập nhật mới nhất.

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.

4.10.3. Các tính năng khác

OCSP là dịch vụ tùy chọn, có thể sẽ thu phí.

4.11. Chấm dứt dịch vụ của thuê bao

Chấm dứt dịch vụ của thuê bao có hiệu lực trong các trường hợp sau:

- Có lệnh dừng sử dụng chứng thư số hoặc dừng toàn bộ hệ thống I-CA hoặc I-CA hết thời hạn hoạt động
- Thuê bao đã hết hạn mà không gia hạn
- Thu hồi chứng thư số xảy ra mà không xin cấp một chứng thư số mới

Thời hạn sử dụng của chứng thư số được chỉ rõ trong chứng thư số.

- Thủ tục chấm dứt dịch vụ:

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

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

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

I-CA không cung cấp dịch vụ lưu trữ và phục hồi khoá bí mật của thuê bao. Khóa bí mật được bảo quản bởi chính thuê bao. Chủ sở hữu khoá phải tự thực hiện việc bảo vệ để tránh mất khoá.

Tuy nhiên, cơ chế này hoàn toàn có thể thay đổi, phụ thuộc vào yêu cầu của pháp luật.

5. Kiểm soát, quản lý và vận hành

5.1. Kiểm soát an toàn, an ninh vật lý

I-CA thực hiện các biện pháp kiểm soát và các thủ tục kiểm soát nhằm đảm bảo an ninh vật lý cho toàn bộ hệ thống. Được thể hiện theo các nội dung dưới đây.

5.1.1. Vị trí đặt và xây dựng hệ thống

Hệ thống thiết bị I-CA được đặt tại hai trung tâm dữ liệu là trung tâm chính tại VIETTEL IDC Láng Hòa Lạc và trung tâm dự phòng tại CMC Duy Tân.

Mỗi địa điểm đặt thiết bị được trang bị nhiều lớp bảo vệ khác nhau: bảo vệ vật lý vòng ngoài của tòa nhà, bảo vệ khu đặt thiết bị, bảo vệ tủ đặt thiết bị, bảo vệ chống cháy nổ.

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 khoá bí mật lưu giữ bằng khoá an toàn khi không sử dụng.

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

- Lớp bảo vệ vòng ngoài - bảo vệ tòa nhà
- Lớp bảo vệ khu đặt thiết bị
- Việc truy nhập qua các lớp được được kiểm soát chặt chẽ, chỉ những người có quyền truy cập mới được truy nhập vào các lớp tương ứng. Càng truy nhập vào các lớp quản lý yêu cầu an ninh cao, sự hạn chế càng tăng.
- Tất cả mọi truy nhập đều được ghi nhận.

5.1.3. Điều hoà và nguồn điện

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

Các Server của hệ thống I-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 I-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

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

5.1.6. Phương tiện lưu trữ

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

Các thiết bị và tài liệu nhạy cảm phải được xử lý trước khi bỏ đi.

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 tái sử dụng được.

Các phương pháp phá hủy đảm bảo theo tiêu chuẩn nhà sản xuất trước khi vứt rác và đảm bảo thông tin trên rác thải không thể đọc bằng mọi phương pháp.

Quy trình xử lý rác được thực hiện qua các công đoạn như sau:

Tài liệu có dữ liệu nhạy cảm được I-CA xử lý theo cách an toàn. Các tài liệu và vật liệu nhạy cảm được cắt nhỏ trước khi xử lý. Phương tiện được sử dụng để thu thập hoặc truyền thông tin nhạy cảm không thể đọc được trước khi thải bỏ. Các chất thải khác được xử lý theo các yêu cầu xử lý chất thải thông thường của I-CA. Các thiết bị mật mã, thẻ thông minh và các thiết bị khác có thể chứa khóa cá nhân hoặc tài liệu quan trọng sẽ bị phá hủy vật lý hoặc nghiền vụn nếu thấy cần thiết, I-CA thực hiện hủy theo hướng dẫn của nhà sản xuất trước khi xử lý. Việc phá hủy này cần có sự cho phép để xử lý tất cả các thiết bị lưu trữ có chứa các dữ liệu quan trọng. Việc phá hủy khóa riêng của CA sẽ được lãnh đạo -I-CA phê duyệt và phải có sự chứng kiến của ít nhất 2 cá nhân trong vai trò quản lý khóa CA của I-CA và việc phá hủy được lưu giữ hồ sơ biên bản của tất cả các bước.

5.1.8. Hệ thống dự phòng

I-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 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

I-CA có 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;

(iv)được cung cấp một tài khoản trên hệ thống PKI.

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

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

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. Kinh nghiệm, bằng cấp, chứng chỉ của đội ngũ nhân sự liên quan đến quản lý và vận hành hệ thống

Tất cả các nhân viên của I-CA phải được đào tạo phù hợp có kinh nghiệm về hạ tầng khoá 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 I-CA cũng yêu cầu những nhân sự có xuất thân và lai lịch rõ ràng.

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

Nhân sự quản lý và vận hành hệ thống có bằng đại học trở lên, chuyên ngành an toàn thông tin hoặc công nghệ thông tin hoặc điện tử viễn thông hoặc bằng cấp có liên quan ngành công nghệ thông tin.

5.3.2. Thủ tục kiểm tra lai lịch

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

- Kiểm tra trình độ chuyên môn, bằng cấp liên quan;
- Kiểm tra sơ yếu lý lịch có xác nhận của cơ quan nhà nước; xuất trình CCCD.
- Tham khảo các nguồn thông tin về nhân sự (nếu có);

Các yếu tố trong thủ tục kiểm tra lai lịch được xem là căn cứ để từ chối các ứng viên cho vị trí được tin tưởng, bao gồm:

- Các ứng viên cung cấp sai thông tin;
- Nguồn tham khảo bất lợi hoặc không đáng tin cậy;

5.3.3. Yêu cầu về đào tạo

I-CA tổ chức các chương trình đào tạo cần thiết cho nhân sự 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 quy định đối với mỗi nhân sự phụ trách công việc được giao.

5.3.4. Chu kỳ tái đào tạo

I-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, tối thiểu 1 năm 1 lần

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. Kỷ luật đối với các hoạt động không hợp pháp

I-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 tuỳ thuộc vào mức độ nghiêm trọng của hành động bất hợp pháp.

5.3.6. 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 I-CA ở vị trí tương đương.

5.3.7. Cung cấp tài liệu cho nhân viên

I-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

I-CA ghi nhật ký (log) các sự kiện sau, việc ghi log được thực hiện tự động hay và thủ công tùy vào từng trường hợp:

Trên các máy chủ lưu trữ chứng thư:

- Khởi động và tắt;
- Đăng nhập, đăng xuất;
- Tạo và ký chứng thư;

Trên các máy chủ trực tuyến của I-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.

Mỗi bản ghi nhật ký gồm các thông tin sau:

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

5.4.2. Tần suất xử lý bản ghi sự kiện

Các tập tin log phải được phân tích mỗi tháng một lần, hoặc sau khi vi phạm an ninh do nghi ngờ hoặc biết được.

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 05 năm.

5.4.4. Bảo vệ các bản ghi kiểm định

Bản ghi kiểm định sẽ được bảo vệ bằng hệ thống bản ghi kiểm định điện tử bao gồm các cơ chế bảo vệ bản ghi log khỏi các truy cập, sửa đổi, xoá bỏ hoặc can thiệp bất hợp pháp. Bản ghi kiểm định chỉ được truy cập bởi các điều hành và quản lý CA.

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

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

5.5. Lưu trữ các bản ghi

5.5.1. Các loại hình, thông tin bản ghi nhật ký được lưu trữ

Xem 5.4.1.

5.5.2. Thời gian lưu trữ bản ghi nhật ký

Khoảng thời gian lưu giữ tối thiểu là 05 năm.

5.5.3. Bảo vệ bản ghi nhật ký

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

5.5.4. Thủ tục sao lưu và dự phòng dữ liệu

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

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 tập trung trên hệ thống của I-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 I-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 I-CA.

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

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

5.6. Thay đổi khoá

Trước khi chứng thư số của CA hết hạn, theo quy định, I-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 I-CA ban hành có thời gian sử dụng không quá thời gian sử dụng chứng thư số của I-CA được dùng để ký lên nó.

Cặp khóa của I-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 I-CA có thể được gia hạn (đổi khóa) khi trước khi cặp khóa cũ hết hạn.

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

- I-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, I-CA sử dụng cặp khóa mới để ban hành chứng thư số cho thuê bao.
- CA tiếp tục ký lên CRL bằng cặp khóa cũ đến khi nào hết hạn toàn bộ chứng thư số được ban hành bởi cặp khóa cũ.

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

5.7.1. Các thủ tục xử lý vấn đề lộ khoá và sự cố thảm họa

Nếu các khóa bí mật của một thuê bao bị mất hoặc bị tổn hại, RA của I-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 khoá nên được thông báo của chủ sở hữu khoá.

Nếu khóa bí mật của I-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 khoá và chứng thư của I-CA mới và công bố trong kho lưu trữ;
- Thu hồi tất cả các chứng chỉ hợp lệ ký bởi khoá bị xâm hại;
- Xuất bản danh sách CRL mới trong kho của I-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.

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

Một hệ thống sao lưu đảm bảo phục hồi nguyên trạng I-CA được đặt tại trung tâm dự phòng.

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

I-CA sẽ có những nỗ lực phòng ngừa tốt nhất để giúp phục hồi.

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

- Tất cả các phần mềm trên I-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 I-CA.
- Tất cả các file dữ liệu của các CA hoạt động trong vùng tránh tiếp xúc với internet sẽ được sao lưu trên phương tiện lưu trữ di động sau mỗi lần thay đổi.

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.

Hệ thống sẽ được khởi động lại dựa trên phần cứng dự phòng bằng cách sử dụng phần mềm sao lưu dữ liệu được sao lưu tại DRDC của I-CA, sau đó sẽ được kiểm tra và đưa vào hoạt động trong một điều kiện đảm bảo an toàn.

Hệ thống máy tính bị lỗi sau đó sẽ được phân tích tìm sự cố.

Nếu cần thiết, thêm các biện pháp bảo vệ cũng sẽ đưa ra để ngăn chặn sự xuất hiện của sự cố tương tự trong tương lai.

I-CA có các hợp đồng với các chuyên gia về PKI để phân tích các sự cố này.

I-CA thông báo với Trung tâm Chứng thực điện tử quốc gia về sự cố này không muộn quá 01 ngày làm việc kể từ khi sự cố xảy ra, theo các quy định của Thông tư 06/2015/TT-BTTTT về Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số do Bộ Thông tin truyền thông ban hành.

5.7.3. Khả năng phục hồi hoạt động sau thảm họa

I-CA cần có kế hoạch dự phòng, đảm bảo hoạt động liên tục kể cả có thảm họa hay sự cố lớn. Các kế hoạch này cần được kiểm tra, thử nghiệm và xem xét định kỳ.

I-CA có khả năng phục hồi những hoạt động quan trọng sau đây trong 01 ngày làm việc sau khi một thảm họa xảy ra.

a. Công bố thông tin thu hồi chứng thư số
b. Ban hành chứng thư số
c. Thu hồi chứng thư số

I-CA dự phòng các thiết bị phần cứng và phần mềm cung cấp dịch vụ. Khóa bí mật của I-CA cũng được dự phòng và duy trì phục vụ cho mục đích phục hồi hệ thống như phần VI.2.4.

Cơ sở dữ liệu của I-CA phục hồi thảm họa sẽ được đồng bộ với cơ sở dữ liệu chính trong thời gian phù hợp, ít nhất là một ngày một lần đồng bộ.

Kế hoạch phục hồi của I-CA được thiết kế có khả năng phục hồi hoạt động toàn bộ hệ thống trong vòng một tuần.

5.8. Dừng hoạt động

Trong trường hợp chấm dứt dịch vụ của mình I-CA sẽ:

- Thông báo với Bộ Khoa học và Công nghệ và Trung tâm Chứng thực chữ ký số quốc gia để làm các thủ tục chấm dứt cung cấp dịch vụ;
- Bằng tất cả khả năng có thể để thông báo cho các thuê bao và RA càng sớm càng tốt;

- Thông báo việc chấm dứt trên diện rộng;
- Ngừng cấp chứng thư số;
- Thu hồi tất cả các chứng thư số;
- Tiêu huỷ tất cả các bản sao khóa bí mật của I-CA.

Thông báo tạm dừng dịch vụ không ít hơn 60 ngày trong trường hợp chấm dứt bình thường. Các CA quản lý tại thời điểm chấm dứt có trách nhiệm lưu trữ tất cả các hồ sơ theo yêu cầu trong phần 5.5.2. Thực hiện chuyển giao cần thiết của dịch vụ CA tới các CA đang hoạt động theo thỏa thuận.

6. Đảm bảo an toàn an ninh về kỹ thuật

6.1. Tạo và phân phối cặp khóa

6.1.1. Cách thức tạo cặp khóa, kích thước cặp khóa

Cặp khoá cho I-CA được tạo ra bởi các nhân viên thẩm quyền chứng thực trên máy tính không kết nối vào mạng. Cặp khoá này được sinh trực tiếp bên trong thiết bị HSM của hãng Utimaco đạt chuẩn FIPS 140-2 Level 3 trở lên 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 cặp khoá của thuê bao sinh tại nhà cung cấp dịch vụ. Cơ quan cung cấp dịch vụ chứng thực sử dụng thiết bị chuyên dụng HSM của máy chủ thực hiện khởi tạo và quản lý cặp khoá với thuật toán mã hoá phi đối xứng RSA hoặc cặp khoá được sinh ngay trong phần cứng của thiết bị đầu cuối của thuê bao (eToken) đạt chuẩn FIPS 140-2 Level 2 trở lên. Mỗi cặp khoá đảm bảo được tính duy nhất và không bị suy ra khoá bí mật từ khoá công khai tương ứng. Việc phân phối khoá 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 khoá thuê bao tự sinh: I-CA cung cấp phần mềm để thuê bao sinh cặp khoá theo thuật toán phi đối xứng RSA hoặc thuê bao tự sử dụng chương trình sinh cặp khoá của mình theo thuật toán RSA.

6.1.2. Chuyển giao khoá bí mật cho thuê bao

Thiết bị phần cứng Token sẽ sinh cặp khóa (bao gồm private key và public key). Chứng thư số của thuê bao được tạo ra dựa trên thông tin về public key và các thông tin khác liên quan đến việc xác định của chủ thể (tên doanh nghiệp, mã số thuế, địa chỉ, …). Hệ thống CA sẽ tạo chứng thư số dựa trên các thông tin đó, sau đó ký vào chứng thư đã được tạo và chuyển chứng thư cho Hệ thống RA. Hệ thống RA sẽ trả về chứng thư cho thiết bị Token. Sau đó Thiết bị được bàn giao tới khách hàng (Bao gồm Thiết bị Token, và giấy chứng nhận).

6.1.3. Chuyển giao khoá công khai tới tổ chức ban hành chứng thư

Các RA chứng thực các yêu cầu truyền các yêu cầu xác nhận có chứa khóa công khai trong một e-mail được ký bởi một trong các đại lý của nó.

I-CA có thể xử lý yêu cầu cấp phát chứng thư dựa trên tải yêu cầu theo định dạng PKCS#10.

6.1.4. Chuyển giao khoá công khai của CA tới các đối tác tin cậy

Chứng thư số của CA (có chứa khoá công khai) được chuyển giao cho thuê bao bằng giao dịch trực tuyến từ Server website trực tuyến. Chứng thư của CA cũng có thể tải về từ kho lưu trữ (xem mục 2.1)

6.1.5. Kích thước khoá

Chuẩn hiện tại của dịch vụ I-CA yêu cầu chiều dài tối thiểu của cặp khoá để đảm bảo mức độ mã hoá đủ mạnh là 2048 bits RSA.

Khoá của I-CA có chiều dài là 4096 bits.

6.1.6. Tạo các tham số cho khoá công khai và kiểm tra chất lượng

Quá trình sinh khóa công khai tuân theo chuẩn PKCS #1, đáp ứng theo các tiêu chuẩn trong Thông tư số 6/2015/TT-BTTTT ban hành ngày 23 tháng 3 năm 2015.

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

Khoá 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.

6.2. Kiểm soát và bảo vệ khóa bí mật

6.2.1. Tiêu chuẩn kỹ thuật đối với thiết bị mật mã

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

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

Các thao tác với khoá 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 này tuân theo chuẩn FIPS PUB 140-2 level 3.

Đối với thuê bao PKI Token sử dụng chuẩn FIPS 140-2 Level 2.

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

Cơ chế kiểm soát khóa bí mật được I-CA sử dụng là cơ chế chia sẻ mã. Cơ chế này tách dữ liệu kích hoạt khóa bí mật thành N phần khác nhau, các phần này được giữ bởi các đối tượng khác nhau.

- Với mỗi chức năng nhất định, cần có M phần (M nhỏ hơn hoặc bằng N) mã chia sẻ để kích hoạt chứng năng đó.
- Tại I-CA, N = 3; M=3

Theo nguyên tắc này, khóa MBK sẽ được chia thành 3 mảnh và ghi vào trong 3 smartcard và được phân phối cho 3 nhân sự (n=3) của I-CA. Để có thể sử dụng được khóa này, cần có đủ 3 nhân sự (m=3) sử dụng thẻ để xác thực.

6.2.3. Sao lưu dự phòng khoá bí mật

I-CA không lưu khóa bí mật của thuê bao.

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

6.2.4. Lưu trữ khoá bí mật

Khi chứng thư của I-CA hết hạn, các cặp khoá 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 khoá 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.

6.2.5. Cách thức sao lưu khoá bí mật

Hiện nay I-CA sao lưu khóa từ HSM vào Smartcard chuyên dụng của HSM đó, trong quá trình sao lưu thì HSM đã mã hóa dữ liệu. Khóa từ Smartcard được đưa vào HSM và chỉ có HSM đó mới giải mã được. Thực hiện như vậy sẽ ngăn chặn mất mát, ăn trộm, sửa đổi, tiết lộ và sử dụng trái phép khoá bí mật. Việc chuyển giao này sẽ bị giới hạn để tạo ra các bản sao dự phòng khoá bí mật trên mô đun phần cứng phù hợp với tiêu chuẩn quy định trong chính sách bảo mật của I-CA. Công việc này để đề phòng khi HSM chính bị hư hỏng vật lý, hoặc do thiên tai thảm họa xảy ra thì còn có HSM dự phòng đã được sao lưu khóa bí mật.

6.2.6. Phương thức kích hoạt khoá bí mật

Khoá bí mật của CA được sử dụng HSM để lưu trữ khóa bí mật, việc kích hoạt khóa bí mật yêu cầu các mã chia sẻ theo cơ chế chia sẻ mã trong 5.2.2.

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

6.2.7. Phương thức dừng hiệu lực của một khoá bí mật

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

Khoá 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).

6.2.8. Phương pháp huỷ khoá bí mật

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

6.2.9. Phương pháp ngừng kích hoạt khóa bí mật

- Khóa bí mật của I-CA /RA bị ngừng kích hoạt khi không chứa trong Token Reader (HSM). RA của I-CA được yêu cầu phải đăng xuất khỏi hệ thống khi rời chỗ làm việc.
- Khóa bí mật của quản trị hệ thống, của RA và của thuê bao có thể bị ngừng kích hoạt sau mỗi nhiệm vụ, sau khi đăng xuất hệ thống hoặc sau khi loại bỏ USB Token khỏi máy tính. Trong mọi trường hợp, thuê bao phải có nghĩa vụ thực hiện các biện pháp bảo vệ khóa bí mật của mình.

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

6.3.1. Lưu trữ khoá công khai

I-CA phải lưu trữ tất cả các chứng thư đã phát hành trên máy chủ LDAP Slaver và sao lưu định kỳ theo quy trình sao lưu tập trung của I-CA .

I-CA sẽ lưu khóa công khai của mình và toàn bộ thuê bao.

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

Không có quy định về thời hạn của cặp khoá tạo ra. Chỉ có hiệu lực của chứng thư do I-CA được xác định bởi tài liệu CP/CPS này.

Mặc định thời gian hoạt động chứng thư của thuê bao là 395 ngày (xấp xỉ 01 năm, 01 tháng) và tối đa không quá thời hạn hoạt động của chứng thư số I-CA, thời gian hoạt động chứng thư RA là 03 năm.

Thời gian hoạt động của chứng thư số I-CA là 05 năm.

Thêm vào đó dịch vụ I-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 khởi tạo và cài đặt dữ liệu kích hoạt khóa bí mật

Dữ liệu kích hoạt khóa bí mật của I-CA được chia thành các mã chia sẻ, các mã chia sẻ này được tạo theo các yêu cầu trong phần 5.2.2 và tuân theo các thủ tục của nghi lễ sinh khóa. Quá trình tạo và phân phối mã chia sẻ được ghi nhật ký.

I-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 12 ký tự). I-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

I-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. I-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 I-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.

6.4.4. Quy trình kích hoạt dữ liệu khóa bí mật

Đối với khóa thuê bao: khóa bí mật của thuê bao được tạo trực tiếp PKI Token tiêu chuẩn FIPS 140-2 Level 2. Mã PIN kích hoạt được sinh ngẫu nhiên, và bàn giao tách riêng đến thuê bao. PKI Token được bàn giao cho thuê bao trước khi I-CA bàn giao mã PIN kích hoạt PKI Token. Sau khi I-CA xác nhận việc bàn giao hợp lệ PKI Token tới thuê bao, và sau khi thuê bao đã xác nhận nội dung của chứng thư số do I-CA cấp mã PIN kích hoạt Token sẽ được I-CA gửi riêng tới thuê bao.

Đối với khóa bí mật của I-CA:

Bước 1: Đăng nhập HSM

Thực hiện nhập mật khẩu đăng nhập HSM

Bước 2: Đăng nhập vùng chứa khóa bí mật

Thực hiện nhập mật khẩu xác thực việc đăng nhập vào vùng chứa khóa bí mật.

Bước 3: Kích hoạt khóa bí mật

Hệ thống I-CA được quản lý bảo mật bên trong HSM chuẩn bảo mật 140-2 Level 3 và được kiểm soát bằng bộ thẻ thông minh chuyên dụng theo cơ chế 3 x 5. Thực hiện sử dụng tối thiểu 3 thẻ mật mã để kích hoạt khóa bí mật.

6.5. Kiểm soát an ninh máy tính

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

I-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, I-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, ngoại 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 an ninh hệ thống máy tính

Hệ thống máy chủ cung cấp dịch vụ của I-CA được đánh giá định kỳ 6 tháng một lần.

6.6. Kiểm soát an ninh quy trình sử dụng

6.6.1. Kiểm soát về phát triển hệ thống

I-CA sử dụng các hệ thống có chứng chỉ tiêu chuẩn công nghệ thông tin.

6.6.2. Kiểm soát vấn đề quản lý bảo mật

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

6.6.3. Kiểm soát về măt bảo mật đối với một chu kỳ sống

Không có quy định.

6.6.4. Quy trình, thủ tục giám sát, quản lý giám sát việc triển khai hoạt động của hệ thống

- Bước 1: I-CA phân vai trò, quyền sử dụng phân công trách nhiệm cho từng đối tượng tham gia sử dụng hệ thống
- Bước 2: I-CA sử dụng các phần mềm ứng dụng lưu lại toàn bộ nhật ký trong quá trình sử dụng hệ thống. Đặc biệt đối với những thay đổi liên quan đến dữ liệu hoặc cấu hình gây ảnh hưởng đến an ninh của hoạt động của hệ thống.
- Bước 3: I-CA có hệ thống cảnh báo trong các trường hợp thay đổi dẫn đến ảnh hưởng của hệ thống.
- Bước 4: Đối với việc nâng cấp, thay đổi các chức năng phần mềm, phần cứng thiết bị nằm trên hệ thống I-CA ghi nhận hiện trạng , nhật ký thời gian bắt đầu, kết thúc, nội dung thực hiện, kết quả thực hiện, các lỗi xảy ra trong quá trình thực hiện. Toàn bộ nội dung nhật ký chi tiết được I-CA lưu lại để có thể truy vết hoặc đánh giá nguyên nhân dựa trên nội dung nhật ký.

6.7. Giám sát an ninh hệ thống mạng

I-CA phân đoạn hệ thống cấp chứng thư số thành các vùng mạng dựa trên mối quan hệ chức năng và logic của chúng. Các vùng mạng được thiết lập trong hệ thống CA của I-CA khi lắp đặt được bảo vệ khỏi người dùng trái phép thông qua một loạt tường lửa dựa trên mạng và máy chủ lưu trữ cũng như các hệ thống giám sát và phát hiện khác. Tường lửa được định cấu hình với các quy tắc hỗ trợ các dịch vụ, giao thức, cổng và thông tin liên lạc mà I-CA đã xác định là cần thiết cho hoạt động của hệ thống.

Đánh giá rủi ro định kỳ và phân tích mối đe dọa được thực hiện bởi nhóm Đánh giá Bảo mật để xác định các mối đe dọa và lỗ hổng trong hệ thống CA của I-CA. Quyền truy cập hợp lý vào hệ thống CA bị hạn chế đối với các cá nhân được ủy quyền trong các vai trò đáng tin cậy. Hệ thống CA được định cấu hình bằng cách xóa / vô hiệu hóa các tài khoản, ứng dụng, dịch vụ, giao thức và cổng không được sử dụng trong hoạt động của CA. Phần mềm chống vi-rút và phát hiện phần mềm độc hại được cài đặt trên hệ thống CA của I-CA.

Những chức năng CA và RA được thực hiện dùng mạng được bảo mật đáp ứng phù hợp với những tài liệu chuẩn trong chính sách bảo mật nhằm ngăn chặn sự truy cập trái phép, sự xáo trộn, và tấn công dịch vụ. Sự truyền thông và các thông tin quan trọng sẽ được bảo vệ bằng cách dụng mã hoá điểm - điểm để đảm bảo tính tin cậy và chữ ký số để xác nhận và xác thực.

Máy chủ ký của I-CA được hoạt động trong vùng mạng không có kết nối trực tiếp với Internet.

Tất cả các máy tính CA khác được bảo vệ bằng firewall và Hệ thống phát hiện xâm nhập và phòng chống truy cập trái phép (IDS/IPS) hoặc bằng cách loại bỏ các dịch vụ không cần thiết.

6.8. Dấu thời gian (Time-Stamping)

Các thư số, 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
Phiên bản (Version)		I-CA phát hành chứng thư X.509 phiên bản 3
Số hiệu chứng thư (Serial Number)		Do I-CA gán, là định dạng duy nhất của chứng thư số, số nguyên dương xác định duy nhất một chứng thư số do CA cấp thuê bao, độ dài không quá 20 octet (byte)
Thuật toán ký chứng thư số của CA (Signature)		sha256RSA
Issuer	Tên của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng (commonName)	I-CA
	Tên của tổ chức/doanh nghiệp vận hành CA (organizationName)	I-CA

	Tên nước (countryName)	VN
Validity	Thời điểm chứng thư bắt đầu có hiệu lực (notBefore)	Thời điểm chứng thư bắt đầu có hiệu lực. Được đồng bộ với NTP Server (UTCTime)
	Thời điểm chứng thư hết hiệu lực (notAfter)	Thời điểm chứng thư hết hiệu lực. Được đồng bộ với NTP Server (UTCTime)
Subject	Định danh thuê bao (userID)	MST: [mã số thuế] hoặc MNS: [mã quan hệ ngân sách] hoặc BHXH: [mã số bảo hiểm xã hội] hoặc hoặc HC: [số hộ chiếu] hoặc CCCD: [số thẻ căn cước công dân]
	Tên của thuê bao (commonName)	Tên của thuê bao được cấp chứng thư số
	Tên của tổ chức/đơn vị quản lý thuê bao (organizationName)	Tên của tổ chức quản lý thuê bao (nếu có)
	Tên tỉnh/TP nơi sống/làm việc của thuê bao (stateOrProvinceName)	Tên của tỉnh/TP nơi sống/ làm việc của thuê bao bằng tiếng Việt, có dấu, các chữ cái đầu viết hoa
	Tên nước (countryName)	VN
Subject Public Key Info	Thuật toán sinh khóa (algorithm)	RSA (2048 bits)
	Khóa công khai của thuê bao (subjectPublicKey)	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)		sha256RSA
Chữ ký số của trung tâm chứng thư số (Signature Value)		Chữ ký số của trung tâm chứng thư số I-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

I-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 I-CA là:

Chứng thư số dùng cho cá nhân

Basic Constraints	critI-CAl, ca: false
Subject Key Identifier	hash
Authority Key Identifier	keyid
Key Usage	digitalSignature nonRepudiation keyEncipherment 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 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 I-CA
CRL Distribution Points	URI của CRL

Chứng thư số dùng cho dịch vụ / Máy chủ

Basic Constraints	critI-CAl, ca: false
Subject Key Identifier	hash
Authority Key Identifier	keyid
Key Usage	digitalSignature nonRepudiation keyEncipherment 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 I-CA
CRL Distribution Points	URI của CRL

7.1.3. Các thuật toán ký

I-CA ký lên các chứng thư số, sử dụng một trong các thuật toán sau:

- sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) memberbody(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
- sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) memberbody(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- Thủ tục ký chứng thư số áp dụng lược đồ RSASSA-PSS được quy định trong PKCS#1 phiên bản 2.1
- Phiên bản của I-CA hỗ trợ sử dụng thuật toán mã hóa SHA-256, SHA-384 và SHA-512 trong chứng thư số

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 I-CA và tuân theo cấu trúc được định nghĩa trong tiêu chuẩn ITU-T Standards Recommendation X.501 (Xem mục 3.1.1).

7.1.5. Ràng buộc tên

Không có những ràng buộc khác hơn so với quy định tại mục 7.1.4, và 3.1.1, 3.1.2.

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 I-CA đăng ký với Bộ Khoa học và Công nghệ.

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 CRLs

Version	V2
Signature	sha1WithRSAEncryption
Issuer	I-CA
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 CertifI-CAtes	serialNumbers của chứng thư bị thu hồi

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

I-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. Profile của OCSP

OCSP tuân theo cấu trúc dữ liệu được mô tả trong tiêu chuẩn IETF RFC 6960.

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.

I-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.

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

Người thực hiện kiểm tra kỹ thuật được chỉ định bởi RootCA để thực hiện các cuộc kiểm tra kỹ thuật I-CA.

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

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

- I-CA sẽ nghiên cứu và đề ra và thực hiện phương án xử lý những nội dung chưa phù hợp trong thời gian thống nhất với RootCA.
- I-CA 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.

Dịch vụ của I-CA sẽ bị ngừng trong các tình huống sau:

- Báo cáo kiểm tra kỹ thuật cho thấy có lỗi nghiêm trọng có thể ảnh hưởng ngay lập tức tới an an ninh của hệ thống I-CA.

- I-CA thực hiện kế hoạch xử lý nhưng không có kết quả.

8.5. Công bố kết quả kiểm tra kỹ thuật

Báo cáo kết quả kiểm toán kỹ thuật được I-CA công bố tại https://i-ca.vn.

Quản lý CA sẽ công bố kết quả trên trang web của I-CA với thông tin chi tiết về sự vi phạm CP/CPS.

8.6. Tần suất và các trường hợp đánh giá

Không quy định.

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

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

9. Các nội dung nghiệp vụ và pháp lý khác

9.1. Phí/Giá

9.1.1. Lệ phí cấp chứng thư hoặc gia hạn chứng thư

Khách hàng của dịch vụ I-CA phải trả phí khi xin cấp chứng thư cho nhà cung cấp dịch vụ.

9.1.2. Lệ phí sử dụng chứng thư

Các thuê bao của I-CA và RA không phải trả chi phí để lưu trữ chứng thư trong kho lưu trữ hay dịch vụ cung cấp thông tin chứng thư trực tuyến cho đối tác tin cậy.

9.1.3. Phí truy cập thông tin về trạng thái chứng thư và việc thu hồi chứng thư

Các thành phần tham gia dịch vụ I-CA không phải trả phí cho việc phát hành các CRL. Tuy nhiên I-CA sẽ thu phí khi cung cấp dịch vụ OCSP hoặc các dịch vụ cung cấp thông tin trạng thái khác.

9.1.4. Lệ phí sử dụng cho các dịch vụ khác

Phí cho những dịch vụ khác như là thông tin về chính sách: I-CA, RA và đại lý có thể thiết lập và tính một mức phí hợp lý cho dịch vụ khác.

Phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số theo quy định tại Thông tư số 17/2018/TT-BTC ngày 09/02/2018 của Bộ Tài chính sửa đổi, bổ sung một số điều của Thông tư số 305/2016/TT-BTC và Thông tư số 305/2016/TT-BTC ngày 15/11/2016 của Bộ Tài chính quy định mức thu, chế độ thu, nộp, quản lý và sử dụng phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số. Mức thu phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số: 3000 đồng/chữ ký số/tháng. Chứng thư số phát sinh hiệu lực hoạt động tại bất cứ thời điểm nào của tháng được tính theo quy định.

9.1.5. Chính sách hoàn trả phí

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

9.2. Trách nhiệm tài chính

9.2.1. Thông tin bảo hiểm

I-CA sẽ duy trì tính thương mại hợp lý cho các mức bảo hiểm đối với các lỗi hay thiếu sót, hoặc thông qua các chương trình bảo hiểm lỗi hay thiếu sót với các hãng bảo hiểm hoặc tự cam kết bảo hiểm. Các yêu cầu bảo hiểm này không áp dụng với các tổ chức chính trị.

9.2.2. Các trường hợp I-CA tiến hành bảo hiểm

I-CA tiến hành bảo hiểm dựa trên hợp đồng với đại lý hoặc với thuê bao.

9.2.3. Các trường hợp không được bảo hiểm

I-CA không chịu trách nhiệm trong các trường hợp:

- Các trường hợp sử dụng chứng thư vi phạm điều khoản trong CP/CPS này.
- Các trường hợp sử dụng, cấu hình thiết bị không đúng, không nằm trong trách nhiệm của CA được sử dụng trong quá trình xử lý chứng thư.
- Khoá bí mật bị mất, xâm hại hay bị phá huỷ do khách hàng.
- Đại lý hoặc khách hàng đã ký hợp đồng với I-CA vi phạm điều khoản của hợp đồng.

9.2.4. Các tài sản khác

Không được đề cập.

9.2.5. Trường hợp bị thu hồi giấy phép

I-CA đã thực hiện bảo lãnh thanh toán của một ngân hàng thương mại hoạt động tại Việt Nam không dưới 5 (năm) tỷ đồng, để giải quyết các rủi ro và các khoản đền bù có thể xảy ra trong quá trình cung cấp dịch vụ và thanh toán chi phí duy trì cơ sở dữ liệu của I-CA trong trường hợp bị thu hồi giấy phép.

9.3. Bảo mật các thông tin nghiệp vụ

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

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 khoá 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 mật

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

9.4. Bảo mật thông tin cá nhân

9.4.1. Phạm vị thông tin bí mật cần được bảo vệ

Mọi thông tin thuê bao không được công bố qua nội dung của chứng thư số, dịch vụ Directory và CRL được coi là bí mật.

9.4.2. Thông tin không được coi là riêng tư

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

9.4.3. Trách nhiệm mật thông tin cá nhân

I-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.

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

Trong trường hợp I-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.

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

I-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).

9.4.6. Những trường hợp làm lộ thông tin khác

Không có quy định.

9.5. Quyền sở hữu trí tuệ

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

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

9.6. Tuyên bố và cam kết

9.6.1. Tuyên bố và cam kết của I-CA

I-CA đảm bảo rằng:

- Không thay đổi thông tin đăng ký chứng thư số được cung cấp bởi đối tượng đăng ký.
- Không có lỗi trong quá trình duyệt và ban hành chứng thư số.
- Chứng thư số do I-CA ban hành đáp ứng các yêu cầu trong quy chế này.
- Cung cấp dịch vụ thu hồi và cho phép sử dụng địa chỉ lưu trữ phù hợp với quy chế chứng thực này.
- Chịu trách nhiệm về việc quản lý và xác minh các điều kiện hoạt động của RA theo quy định của pháp luật.

9.6.2. Tuyên bố và cam kết của RA

RA đảm bảo rằng:

- Không thay đổi thông tin đăng ký chứng thư số được cung cấp bởi đối tượng đăng ký.
- Không có lỗi trong quá trình duyệt hồ sơ xin cấp chứng thư số và quá trình gửi thông tin cho I-CA.
- Tuân thủ theo quy trình quản lý vòng đời chứng thư số của I-CA.

RA có trách nhiệm ký hợp đồng với I-CA. Trong hợp đồng có quy định:

- Loại chứng thư số mà RA được phép tham gia cung cấp.
- Các bước trong quy trình cấp phát chứng thư số RA được thực hiện.
- Chứng thư số chỉ được cấp sau khi I-CA đã nhận đầy đủ hồ sơ của thuê bao, và thông tin thuê bao được thẩm định.
- Cam kết của RA với I-CA đúng như trong hợp đồng đã ký và theo quy định của pháp luật.
- Nhân viên RA trực tiếp tham gia vào quy trình cung cấp chứng thư số phải có hiểu biết pháp luật về chữ ký số và dịch vụ chứng thực chữ ký số.

9.6.3. Tuyên bố và cam kết của thuê bao

Thuê bao đảm bảo rằng:

- Khi ký: sử dụng khóa bí mật tương ứng với khóa công khai trong chứng thư số ; tại thời điểm ký, thuê bao chấp nhận chứng thư số và chứng thư số đang có hiệu lực (không hết hạn hoặc bị thu hồi).
- Khóa bí mật của mình được bảo vệ và không cho người khác sử dụng.
- Mọi thông tin cung cấp bởi thuê bao là đúng.
- Sử dụng chứng thư số đúng mục đích của chứng thư số, phù hợp với quy định của pháp luật và quy chế chứng thực này

- Không sử dụng chứng thư số được cấp thực hiện các chức năng của một CA.

Thỏa thuận thuê bao có thể bao gồm thêm những điều khoản khác. Nội dung thỏa thuận thuê bao được trình bày trong phần phụ lục.

9.6.4. Tuyên bố và cam kết của người nhận

Người nhận chịu trách nhiệm về việc tìm hiểu các thông tin trong quy chế chứng thư số, trong thỏa thuận người nhận trước khi quyết định tin tưởng chứng thư số do I-CA ban hành.

- Người nhận phải chịu trách nhiệm cho những hành động của mình do không thực hiện theo các nội dung liên quan được quy định trong thỏa thuận người nhận hoặc quy chế chứng thực này.
- Thỏa thuận thuê bao có thể bao gồm thêm những điều khoản khác. Nội dung thỏa thuận thuê bao được trình bày trong hợp đồng hoặc phụ lục hoặc trên website của I-CA.

9.7. Từ chối trách nhiệm

I-CA không quy định cụ thể về việc từ chối trách nhiệm.

9.8. Giới hạn trách nhiệm

CPS này tùy thuộc vào hệ thống các điều luật, quy tắc, các điều chỉnh, quy định, các sắc lệnh và mệnh lệnh thuộc phạm vi địa phương, bang, quốc gia, nhưng không giới hạn hay hạn chế cho lĩnh vực xuất khẩu phần mềm, phần cứng và các thông tin kỹ thuật.

- Trách nhiệm của các bên được quy định và giới hạn theo hợp đồng đã ký kết
- Các điều khoản có tính độc lập: Trong trường hợp một điều khoản hay sự sửa đổi bổ sung của CPS được giữ lại không thể thi hành được bởi một phiên tòa hay một cuộc xét xử có thẩm quyền, phần còn lại của CPS vẫn có hiệu lực.

9.9. Bồi thường thiệt hại

9.9.1. Vấn đề bồi thường của khách hàng

Khi pháp luật yêu cầu, khách hàng bồi thường cho I-CA nếu xuất hiện:

- Những thông tin không hợp lệ do RA, đại lý, khách hàng cung cấp trên đơn vị cấp chứng thư.
- Lỗi của khách hàng để lộ những nhân tố, yếu tố liên quan đến đơn xin cấp chứng thư, sự bỏ sót do sự cẩu thả hay với mục đích lừa đảo.
- Lỗi của khách hàng trong việc cung cấp các hồ sơ giả mạo để cấp chứng thư số, các hồ sơ này bao gồm: Đơn xin cấp chứng thư số, CCCD/Hộ chiếu, Đăng ký kinh doanh/Quyết định thành lập (đối với Tổ chức/doanh nghiệp/Hộ kinh doanh) và các giấy tờ khác có liên quan.
- Lỗi của khách hàng trong việc bảo vệ khóa bí mật, sử dụng hệ thống không tin cậy, hoặc không thực hiện các biện pháp phòng ngừa cần thiết để tránh gây hậu quả.
- Việc sử dụng tên của khách hàng (kể cả việc không giới hạn tên chung, tên miền, hoặc địa chỉ thư điện tử) vi phạm quyền sở hữu trí tuệ của bên thứ 3.
- Hợp đồng với khách hàng có thể có những bổ sung phù hợp.

9.9.2. Vấn đề bồi thường của đại lý

Khi được pháp luật cho phép, bản thỏa thuận với đại lý sẽ yêu cầu đại lý bồi thường cho I-CA:

- Lỗi của đại lý trong việc thực thi bổn phận của một bên đối tác
- Sự tin cậy của đại lý về một chứng thư số không được đáp ứng trong một số trường hợp.
- Lỗi của đại lý trong việc kiểm tra trạng thái của chứng thư để xác định chứng thư đã hết hạn hay bị thu hồi.

- Lỗi của đại lý liên quan đến việc cung cấp các hồ sơ giả mạo để cấp chứng thư số, các hồ sơ này bao gồm: Đơn xin cấp chứng thư số, CCCD/Hộ chiếu, Đăng ký kinh doanh/Quyết định thành lập (đối với Tổ chức/doanh nghiệp/Hộ kinh doanh) và các giấy tờ khác có liên quan.
- Thỏa thuận với đại lý sẽ bao gồm thêm một số nghĩa vụ khác.

9.10. Hiệu lực của Quy chế chứng thực

9.10.1. Thời hạn bắt đầu có hiệu lực

Tài liệu này có hiệu lực khi được công bố trong kho lưu trữ của dịch vụ I-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. Thời hạn hết hiệu lực

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 quy chế chứng thực hết hiệu lực

Khi quy chế này hết hiệu lực, các điều khoản của nó vẫn được áp dụng cho các chứng thư số được ban hành trong thời hạn của quy chế này cho đến khi chứng thư số hết hạn hoặc bị thu hồi.

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

Tất cả các e-mail liên lạc giữa CA và các RA phải được ký bằng khoá của chứng thư.

Tất cả các e-mail 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.

Trừ khi được quy định rõ ràng, các thành viên I-CA sẽ sử dụng các phương pháp liên lạc hợp lý, tùy thuộc mức độ nguy cấp về nội dung của thông tin cần liên lạc.

9.12. Bổ sung và sửa đổi

9.12.1. Các thủ tục sửa đổi

Những sửa đổi của CP/CPS sẽ được thực hiện bởi Cấp quản lý chính sách có thẩm quyền (xem mục 1.5.4). Nội dung sửa đổi lưu tại https://i-ca.vn Nội dung sửa đổi sẽ thay thế các nội dung trong các điều khoản tương đương

trong phiên bản quy chế chứng thực tương ứng và mọi tài liệu liên quan khác.

Đối với các thay đổi không quan trọng như thay đổi URL, thông tin liên hệ, lỗi in ấn… I-CA PMA có quyền thay đổi quy chế mà không cần thông báo về sự thay đổi.

Đối với các thay đổi theo đề xuất từ các thành viên, I-CA sẽ xem xét yêu cầu thay đổi. Nếu quy chế cần thay đổi, I-CA sẽ đưa ra thông báo về sự thay đổi này.

Trong một số trường hợp đặc biệt, liên quan tới an ninh của hệ thống, I-CA sẽ thực hiện sự thay đổi quy chế này lập tức, sau đó sẽ thông báo cho các thành viên.

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

I-CA sẽ xem xét mọi góp ý sửa đổi. I-CA sẽ thực hiện một trong các tình huống sau:

- Không thay đổi gì góp ý ban đầu; hoặc
- Sửa đổi những góp ý sửa đổi và công bố lại chúng; hoặc
- Hủy bỏ góp ý sửa đổi.

9.12.2. Các trường hợp cần sửa đổi nhận diện đối tượng (OID)

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 I-CA.

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 I-CA.

- Việc giải quyết tranh chấp giữa I-CA, cộng tác và thuê bao phải tuân thủ theo các điều khoản được ghi trong hợp đồng.
- Việc giải quyết tranh chấp giữa I-CA và đại lý phải tuân thủ theo các điều khoản được ghi trong hợp đồng Đại Lý, sau đó có thể được đưa lên tòa án có đủ quyền xử lý.

9.14. Hệ thống pháp lý điều chỉnh

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 06/2015/TT-BTTTT về Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số.
- Thông tư 31/2020/TT-BTTTT ban hành quy chế chức thực của tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia.

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 I-CA phải tuân thủ luật pháp nước CHXHCN Việt Nam.

Nếu có quy định trong quy chế này xung đột với quy định của các văn bản pháp luật, lúc này quy định của văn bản pháp luật sẽ có hiệu lực.

9.16. Các điều khoản chung

9.16.1. Thỏa thuận bao trùm mọi thành viên

Quy chế chứng thực này là thỏa thuận mà mọi thành viên của I-CA phải tuân thủ.

9.16.2. Sự chuyển nhượng

Không có quy định nào cho phép chuyển nhượng quyền sử dụng chứng thư số. I-CA không quy định các trường hợp chuyển nhượng khác.

9.16.3. Tính độc lập của các điều khoản

Nếu như một số điều khoản trong quy chế chứng thực này không hợp pháp các điều khoản đó sẽ không có giá trị, nhưng không ảnh hưởng đến hiệu lực của các điều khoản khác.

9.16.4. Sự ép buộc

Không có sự ép buộc nào đưa đến việc ban hành chứng thư của I-CA

9.16.5. Trường hợp bất khả kháng

Thỏa thuận thuê bao và thỏa thuận người nhận sẽ có điều khoản về trường hợp bất khả kháng để bảo vệ cho I-CA.

9.17. Các điều khoản khác

Không áp dụng.

TÀI LIỆU THAM CHIẾU

[1] Luật giao dịch điện tử số 51/2005/QH11 ngày 29/11/2005.

[2] Nghị định 130/2018/NĐ-CP ngày 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.

[3] Thông tư 06/2015/TT-BTTTT về Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số.

[4] RFC 3647 (https://www.ietf.org/rfc/rfc3647.txt).

[5] Thông tư 31/2020/TT-BTTTT ban hành quy chế chứng thực của tổ chức cung cấp dịch vụ chứng thực chữ ký số Quốc Gia.