CÔNG TY CỔ PHẦN CHỮ KÝ SỐ VI NA
(SMARTSIGN-CA)

QUY CHẾ CHỨNG THỰC
SMARTSIGN-CA

Hồ Chí Minh, 2024

MỤC LỤC

1. Giới thiệu

1.1. Tổng quan

Tài liệu này là quy chế chứng thực chữ ký số của SMARTSIGN-CA. Tài liệu nêu rõ những quy chế của SMARTSIGN-CA sử dụng trong quá trình cung cấp dịch vụ chứng thực 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 Certificate Policy and Certification Practice Statement).

1.2. Tên và dấu hiệu nhận diện tài liệu

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

OID của Quy chế chứng thực này là 1.3.6.1.4.1.30339.1.x

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

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

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 Certification 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 chứng minh nhân 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 cả 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 SMARTSIGN-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 SMARTSIGN-CA.

Các đối tượng khác SMARTSIGN-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 SMARTSIGN-CA và thỏa thuận của thuê bao với SMARTSIGN-CA.

Chứng thư số do SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-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 số 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 dùng cho tổ chức.

- Chứng thư số SSL.
- Chứng thư số Code Signing.

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 SMARTSIGN-CA và thuê bao.

Trong mọi trường hợp, cấm sử dụng chứng thư số do SMARTSIGN-CA cấp phát vào những mục đích liên quan đến an ninh trong 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 cơ quan: Công ty Cổ phần Chữ ký số Vi Na

Địa chỉ: 41A Nguyễn Phi Khanh, Phường Tân Định, Quận 1, Tp Hồ Chí Minh

1.5.2. Liên hệ

Người đứng đầu hệ thống: Nguyễn Hoàng Vũ

- E-mail: vunh@smartsign.com.vn
- Công ty Cổ phần Chữ ký số Vi Na
- Địa chỉ: 41A Nguyễn Phi Khanh, Phường Tân Định, Quận 1, Tp Hồ Chí Minh
- Điện thoại: 08 3820 2261
- E-mail: info@smartsign.com.vn

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

Bộ Thông tin Và Truyền thông và Công ty Cổ phần Chữ ký số Vi Na xác nhận sự phù hợp của quy chế chứng thực này.

1.5.4. Thủ tục phê chuẩn quy chế chứng thực

Công ty Cổ phần Chữ ký số Vi Na 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://smartsign.com.vn/tai-ve/

Các quá trình xem xét và phê duyệt phải đảm bảo rằng 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://smartsign.com.vn/tai-ve/

1.6. Các định nghĩa và viết tắt

1.6.1. Các định nghĩa

Thuật ngữ	**Giải thích**
Chứng thư số SMARTSIGN-CA	Là một dạng chứng thư điện tử do SMARTSIGN-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 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	Certificate Authority
CMS	Cryptographic Message Syntax
CP	Certificate Policy
CPS	Certification Practice Statement
CRLs	Certificate Revocation Lists
CRR	Certificate Revocation Request
CSP	Certification 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 Certificate 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 Telecommunianion Union-T) standard that establishes a distributed, hierarchical directory protocol organized by country, region, Organization, etc.
X.501	The ITU-T (International Telecommunianion Union-T) standard for use of Distinguished Names in an X.500 directory.
X.509	ITU-T standard for Certificates format

2. Trách nhiệm lưu trữ và công bố thông tin

2.1. Lưu trữ

Việc lưu trữ, công bố và tra cứu được thực hiện thông qua giao thức LDAP, danh sách chứng thư số thu hồi (CRL), giao thức kiểm tra tình trạng chứng thư số theo thời gian thực (OCSP) và trang web của SMARTSIGN-CA.

SMARTSIGN-CA có trách nhiệm lưu trữ thông tin, bao gồm:

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

2.2. Công bố thông tin

Khi bàn giao chứng thư số cho khách hàng, SMARTSIGN-CA yêu cầu khách hàng ký biên bản bàn giao chứng thư số, xác nhận thông tin trên chứng thư số là chính xác. Sau đó chứng thư số của khách hàng sẽ được công bố.

SMARTSIGN-CA duy trì và đảm bảo hoạt động của kho lưu trữ cho phép thuê bao và các thành phần tham gia dịch vụ SMARTSIGN-CA khác truy xuất nhằm xác định trạng thái chứng thư số.

Các thông tin cập nhật và công bố bao gồm:

- Chứng thư số của SMARTSIGN-CA;
- Danh sách chứng thư số bị thu hồi (CRL);
- Danh sách CA bị thu hồi (ARL);
- Quy chế của SMARTSIGN-CA, bao gồm các phiên bản;
- Các thông tin liên quan khác.

Công bố danh sách chứng thư số thu hồi (CRL).

- Chứng thư số SMARTSIGN-CA có thời hạn từ ngày 24/02/2023 đến ngày 24/02/2028, sử dụng: http://crl1.smartsign.com.vn;
- Chứng thư số SMARTSIGN-CA có thời hạn từ ngày 19/05/2020 đến ngày 19/05/2025, sử dụng: http://crl256. smartsign.com.vn/.

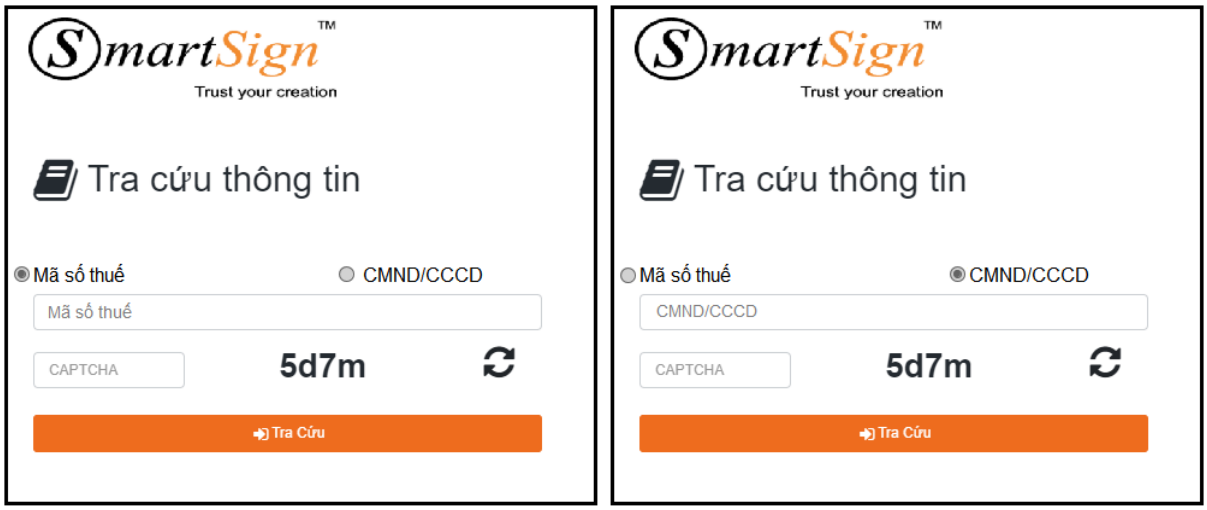
Kiểm tra tình trạng chứng thư số theo thời gian thực (OCSP).

- Chứng thư số SMARTSIGN-CA có thời hạn từ ngày 24/02/2023 đến ngày 24/02/2028, sử dụng: http://ocsp1.smartsign.com.vn;
- Chứng thư số SMARTSIGN-CA có thời hạn từ ngày 19/05/2020 đến ngày 19/05/2025, sử dụng: http://ocsp256.smartsign.com.vn.

Tra cứu tình trạng chứng thư số:

Các thuê bao có chứng thư số được phát hành bởi SMARTSIGN-CA có thể tra cứu tình trạng chứng thư số bằng cách:

Bước 1: Truy cập vào địa chỉ http://tracuu.smartsign.com.vn.

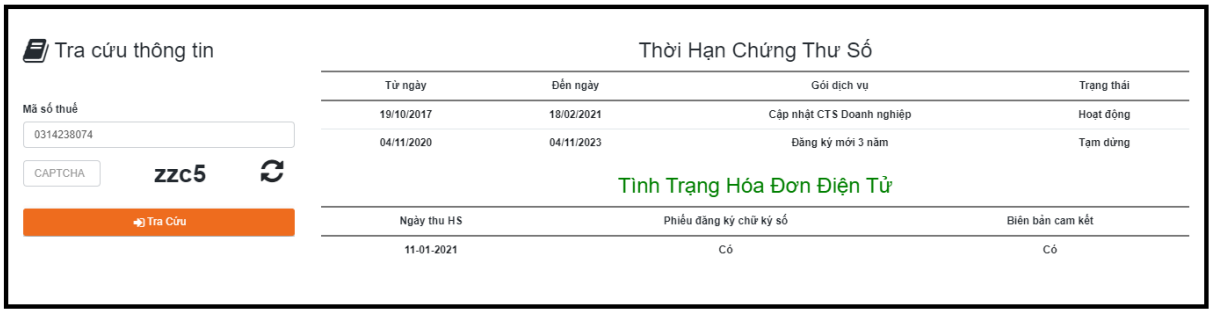


- Thuê bao doanh nghiệp chọn mã số thuế để tra cứu và nhập mã số thuế tại khung nhập Mã số thuế

- Thuê bao cá nhân chọn CMND/CCCD để tra cứu và nhập CMND/CCCD tại khung nhập CMND/CCCD.

- Tại khung nhập CAPTCHA: thuê bao nhập lại mã CAPTCHA được hiển thị bên phải của khung để xác nhận thao tác do người thực hiện.

Bước 2: Tình trạng chứng thư số sẽ được hiển thị như hình dưới:



Vị trí thời hạn chứng thư số: Thông tin của một chứng thư số sẽ được hiển thị bao gồm thời hạn từ ngày, thời hạn đến ngày, gói dịch vụ và trạng thái.

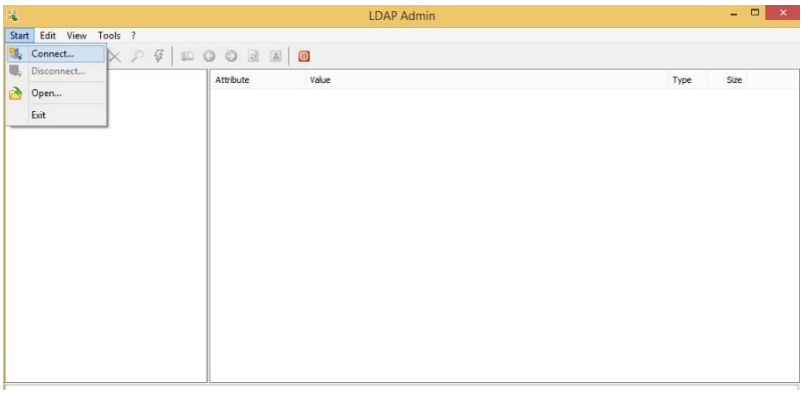
Công bố thông tin chứng thư số (LDAP):

Để đảm bảo an toàn cơ sở dữ liệu LDAP thì SMARTSIGN-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://smartsign.com.vn/tai-ve/

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

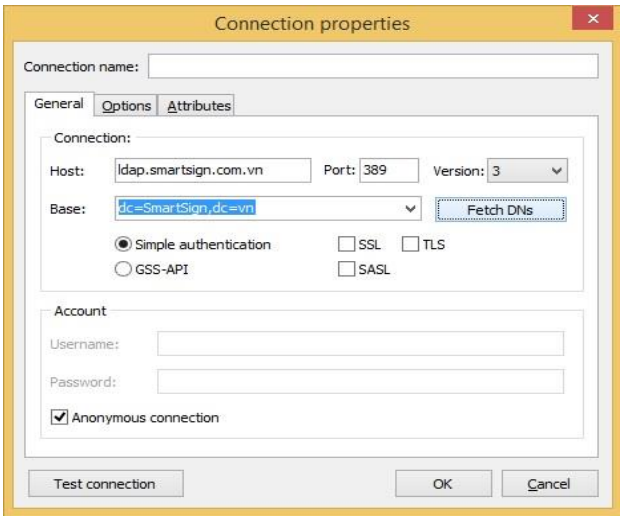


Bước 3 : Chọn new connect và điền các thông số như sau:

Mục host:

- Với chứng thư số SMARTSIGN-CA có thời hạn từ ngày 24/02/2023 đến ngày 24/02/2028 sử dụng địa chỉ: http://ldap1.smartsign.com.vn
- Với chứng thư số SMARTSIGN-CA có thời hạn từ ngày 19/05/2020 đến ngày 19/05/2025 sử dụng địa chỉ: http://ldap256.smartsign.com.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 SMARTSIGN-CA sẽ được công bố ngay sau khi có sự chấp nhận của thuê bao phù hợp với các thủ tục mà SMARTSIGN-CA yêu cầu.

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

Tần số công bố CPS: Một phiên bản mới của 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.

SMARTSIGN-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

SMARTSIGN-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 SMARTSIGN-CA, và các tài liệu (CPS) của SMARTSIGN-CA thông qua địa chỉ công bố truy cập trực tuyến.

SMARTSIGN-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 SMARTSIGN-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 (SMARTSIGN-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=vunh@smartsign.com.com, CN= Nguyễn Hoàng Vũ, L=HCM, OU=BOD, O=SMARTSIGN-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 SMARTSIGN-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.
Quận, huyện (L)	Địa chỉ quận/huyện của thuê bao

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 dinh doanh và một số giấy giờ khác)
Địa chỉ email (E)	Địa chỉ email giao dịch của thuê bao sở hữu chứng thư

- Các thuộc tính trong DN của chứng thư số do SMARTSIGN-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.
Quận, huyện (L)	Địa chỉ quận/huyện của thuê bao
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	CMND: 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 SMARTSIGN-CA cấp cho thuê bao cá nhân được mô tả như sau:

Thuộc tính	**Giá trị**

Quận, huyện (L)	Địa chỉ quận/huyện của thuê bao
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	CMND: Đối với khách hàng cá nhân
Tên thường gọi (CN)	Tên thuê bao sở hữu chứng thư số (Theo như giấy CMND 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 SMARTSIGN-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 kì 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 SMARTSIGN-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 SMARTSIGN-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. SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-CA, SMARTSIGN-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, SMARTSIGN-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

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

a) Tài liệu nhận dạng danh tính

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

Chứng minh thư nhân dân.

Căn cước công dân / Căn cước.

Chứng minh thư quân đội.

Hộ chiếu.

b) Thực hiện nhận dạng cá nhân

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

Tính hợp lệ của thông tin do chủ thể cung cấp.

Thông tin thống nhất trong đơn nộp cấp chứng thư số.

Tổ chức đăng ký chứng thư số hoặc một đại lý tin cậy của RA thực hiện việc nhận dạng cá nhân này. RA tiến hành sẽ so sánh thông tin đăng ký với thông tin thực tế của cá nhân thông qua các tài liệu nhận dạng danh tính.

SMARTSIGN-CA không xác minh những thông tin của thuê bao mà không liên quan đến quy trình quản lý vòng đời chứng thư số. SMARTSIGN-CA không chịu trách nhiệm về những thông tin này.

Hồ sơ xin cấp gồm có:

- Đơn xin cấp chứng thư (theo mẫu của SMARTSIGN-CA)
- Giấy tờ xác thực nhận dạng cá nhân
- Giấy tờ liên quan khác (nếu có)

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

- Người đăng ký nộp hồ sơ cho SMARTSIGN-CA/RA hoặc một đại lý tin cậy.
- SMARTSIGN-CA/RA xác minh thông tin trên hồ sơ với các thông tin trên Giấy tờ xác thực nhận dạng cá nhân.

Nếu thông tin trên hồ sơ không thỏa mãn với các thông tin trên giấy tờ xác thực nhận dạng cá nhân thì đơn xin cấp chứng thư số sẽ không được chấp nhận.

3.2.3. Nhận dạng và xác thực đối với tổ chức

Yêu cầu cấp chứng thư số của một tổ chức có thể được thực hiện qua phương thức điện tử phải bao gồm tên theo pháp luật và địa chỉ của tổ chức. Những yêu cầu tối thiểu Nhận dạng và xác thực về tổ chức đó theo CP đòi hỏi xác nhận rằng:

Tổ chức tồn tại hợp pháp và có địa chỉ kinh doanh theo địa chỉ được nêu ra trong đơn xin cấp chứng thư số.

Thông tin nêu ra trong đơn cấp chứng thư số là chính xác.

Nhận dạng và xác thực được thực hiện bởi RA, thông tin xác định sự tồn tại của tổ chức, gồm có: tên tổ chức, giấy chứng nhận đăng ký kinh doanh hoặc giấy phép hoạt động, địa chỉ.

Bằng chứng chắc chắn đơn vị nộp đơn đang trong thời gian sát nhập hoặc tổ chức.

Thông tin của tổ chức có thể được xác nhận qua sự kiểm tra chéo với thông tin trong cơ sở dữ liệu thông tin của SMARTSIGN-CA, từ một bên thứ ba, hoặc từ một tổ chức tài chính liên quan, và bằng cách gọi điện đến số điện thoại của tổ chức đó. Trong trường hợp điện thoại không liên lạc được, các thông tin về tổ chức đó là sai, không có hiệu lực hoặc bị nghi ngờ thì cần có sự kiểm tra thêm để bảo đảm thông tin. Nếu thông tin tiếp theo không thỏa mãn, hoặc nếu tổ chức nộp đơn từ chối trả lời những thông tin yêu cầu này thì đơn xin cấp chứng thư số sẽ không được chấp nhận. RA có thể tin cậy vào thông tin có được trước đó đối với tổ chức này và sẽ lưu trữ chi tiết thông tin để sử dụng cho xác minh nhận dạng. Quá trình này sẽ không mâu thuẫn với các quy định khác trong CPS.

SMARTSIGN-CA không xác minh những thông tin của thuê bao mà không liên quan đến quy trình quản lý vòng đời chứng thư số. SMARTSIGN-CA không chịu trách nhiệm về những thông tin này.

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 giấy ủy quyền. Trong một số trường hợp cần làm rõ,

SMARTSIGN-CA sẽ xác thực bổ sung bằng cách gọi điện hoặc xác thực trực tiếp tại tổ chức về cá nhân đó.

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 SMARTSIGN-CA có thể yêu cầu phát hành một chứng thư số với một cặp khoá mới. Đề nghị thay đổi cặp khoá trước khi chứng thư số hết hạn được thực hiện bằng cách gửi yêu cầu đề nghị thay đổi cặp khoá dựa trên khoá công khai mới trong một e-mail được ký với khoá bí mật cũ tới RA của SMARTSIGN-CA 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 SMARTSIGN-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 và không thay đổi. Sau khi cấp lại khoá CA hoặc RA của SMARTSIGN-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.

SMARTSIGN-CA hoặc RA có trách nhiệm xác thực yêu cầu cấp lại khóa của thuê bao sau khi nhận đơn đề nghị thay đổi cặp khóa. SMARTSIGN-CA sử dụng một trong hai phương pháp xác thực làm căn cứ để chấp nhận một yêu cầu xin cấp lại khóa.

- Chứng minh quyền sở hữu khóa bí mật: thuê bao sử dụng chứng thư số của mình để gửi yêu cầu đề nghị thay đổi cặp khóa lên SMARTSIGN-CA, khi thuê bao yêu cầu thay đổi cặp khóa chứng thư số yêu cầu này ngay lập tức được SMARTSIGN-CA chấp nhận.
- Sử dụng phương pháp xác thực: thuê bao phải trả lời đúng toàn bộ các câu hỏi xác thực để được SMARTSIGN-CA chấp nhận yêu cầu đề nghị thay đổi cặp khóa.

- Sau khi xác thực, SMARTSIGN-CA ban hành ngay chứng thư số mới cho thuê bao.
- Sau khi ban hành chứng thư số mới cho thuê bao, SMARTSIGN-CA hoặc RA xác minh lại nhận dạng của đối tượng yêu cầu cấp lại khóa và các thông tin liên quan:
- SMARTSIGN-CA hoặc RA liên lạc với thuê bao hoặc đại diện được ủy quyền nếu là tổ chức thông qua điện thoại, email, thư tín hay các phương tiện khác để khẳng định lại chính thuê bao đã yêu cầu làm mới chứng thư số. SMARTSIGN-CA cũng xác minh lại đối tượng yêu cầu làm mới có phải là thành viên của tổ chức như trong thông tin đăng ký ban đầu hay không.

Các đặc trưng (DN) trong chứng thư số tên miền, hoặc sự tồn tại thực sự của tổ chức có thể được kiểm tra bổ sung dựa vào nhà cung cấp tên miền hoặc các đơn vị hữu quan như Cơ quan thuế, Sở kế hoạch Đầu tư.

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 khóa, 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. SMARTSIGN-CA khi gặp phải những yêu cầu như vậy, cần phải có cơ chế xác thực để ngăn chặn các yêu cầu trái phép khi đề nghị thu hồi chứng thư số một cách nhanh chóng. Bởi vậy, trong trường hợp các yêu cầu được gửi điện tử, 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 yêu cầu được ký bởi khóa bí mật tương ứng với khóa công khai của người gửi yêu cầu, yêu cầu này sẽ được chấp nhận xem là có hiệu lực.

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

được lưu giữ bằng văn bản. Khi chứng thư số của thuê bao bị thu hồi, việc thu hồi sẽ được công bố tại CRL thích hợp của SMARTSIGN-CA.

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

Quy trình xác minh đề nghị thu hồi chứng thư số.

Khi có một yêu cầu thu hồi chứng thư số từ thuê bao, SMARTSIGN-CA hoặc RA sẽ tiến hành xác thực thuê bao gửi yêu cầu thu hồi. Thủ tục xác thực yêu cầu có thể sử dụng một trong hai phương pháp sau:

- Sử dụng chữ ký số: SMARTSIGN-CA nhận một thông điệp từ thuê bao yêu cầu thu hồi chứng thư số, yêu cầu thu hồi này được ký bằng chứng thư số đã được cấp. Nếu chữ ký đúng, chứng thư số sẽ bị thu hồi tự động.
- SMARTSIGN-CA sẽ xác nhận lại yêu cầu thu hồi chứng thư số của khách hàng, qua thông tin liên hệ khách hàng đã cung cấp, khi đăng ký cấp chứng thư số.
- Sau khi xác thực, SMARTSIGN-CA sẽ tiến hành xác thực bổ sung bằng cách liên lạc với đối tượng yêu cầu thu hồi để đảm bảo chắc chắn rằng chính thuê bao đã yêu cầu thu hồi chứng thư số. Tùy từng hoàn cảnh, việc liên lạc này có thể thông qua điện thoại, email, thư tín hay thông qua các phương tiện truyền thông.
- RA sử dụng hệ thống quản lý chứng thư số có thể đệ trình nhiều yêu cầu thu hồi tới SMARTSIGN-CA một lúc. Mỗi yêu cầu sẽ được xác thực thông qua chữ ký số của RA.

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. Ai có thể đệ trình đơn xin cấp chứng thư số

Đối tượng được phép yêu cầu cấp chứng thư số gồm:

- Bất cứ cá nhân, tổ chức nào đủ điều kiện theo quy định của pháp luật và quy chế này có nhu cầu sử dụng chứng thư số.
- Đại diện theo pháp luật của tổ chức đủ điều kiện theo quy định của pháp luật và quy chế này có nhu cầu sử dụng chứng thư số.
- Các đại lý đăng ký làm RA cho SMARTSIGN-CA.

4.1.2. Hồ sơ đề nghị cấp chứng thư số

Khách hàng là Tổ chức, doanh nghiệp:

- Hợp đồng, bản khai phải được ký và đóng dấu. Hợp đồng phải đầy đủ các thông tin của khách hàng như: Người đại diện pháp lý ký hợp đồng (trường hợp ủy quyền phải có giấy ủy quyền kèm theo), điện thoại, địa chỉ, tài khoản thanh toán, mã số thuế…
- CMND hoặc Hộ chiếu hoặc Căn cước công dân của người đại diện pháp lý của tổ chức, doanh nghiệp.
- Giấy phép thành lập/Đăng ký kinh doanh.
- Giấy chứng nhận đăng ký thuế của doanh nghiệp (nếu có).

Khách hàng là cá nhân:

- Hợp đồng, bản khai phải được ký và đầy đủ các thông tin của Khách hàng như: Tên khách hàng, Số định danh (hộ chiếu), điện thoại, địa chỉ, tài khoản thanh toán, mã số thuế…
- CMND hoặc Hộ chiếu hoặc Căn cước công dân của cá nhân.
- Giấy ĐKKD hoặc Quyết định thành lập, Giấy phép đầu tư (đối với khách hàng cá nhân thuộc doanh nghiệp).
- CMND hoặc Hộ chiếu hoặc Căn cước công dân hoặc của người đại diện hợp pháp của tổ chức/doanh nghiệp (đối với khách hàng cá nhân thuộc doanh nghiệp).

4.2. Xử lý yêu cầu cấp chứng thư

4.2.1. Nhận dạng và xác thực

SMARTSIGN-CA và SMARTSIGN RA sẽ thực hiện nhận dạng và xác thực mọi thông tin trong yêu cầu cấp chứng thư số được chỉ rõ trong phần 3.2

4.2.2. Duyệt đăng ký cấp chứng thư số

SMARTSIGN-CA và SMARTSIGN RA chấp nhận một đơn đăng ký nếu các điều kiện sau đây thỏa mãn:

- Mọi thông tin cần xác thực được nhận dạng và xác thực đúng.
- Các khoản phí cần thiết đã nhận được từ đối tượng đăng ký.

SMARTSIGN-CA và SMARTSIGN RA không chấp nhận đơn đơn đăng ký nếu:

- Một trong các thông tin cần xác thực được nhận dạng và xác thực sai.
- Người đăng ký không cung cấp đủ tài liệu xác minh thông tin đã kê khai trong đơn đăng ký.
- SMARTSIGN-CA chưa nhận được đầy đủ phí từ người đăng ký
- Chứng thư số có khả năng được sử dụng trong các hoạt động phạm pháp và các hoạt động có thể ảnh hưởng tới uy tín của SMARTSIGN-CA.

4.2.3. Thời gian xử lý yêu cầu cấp chứng thư

SMARTSIGN-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 số trừ khi được đưa ra trong hợp đồng với thuê bao, trong CPS hoặc thoả thuận giữa các bên của dịch vụ SMARTSIGN-CA.

4.3. Cấp chứng thư số

4.3.1. Hoạt động trong suốt quá trình phát hành chứng thư

Khi một đơn xin cấp chứng thư được cấp bởi SMARTSIGN-CA sẽ phải được phê duyệt của đơn xin cấp chứng thư đó.

Chứng thư số sẽ được cấp phát sau khi SMARTSIGN-CA chấp nhận đơn xin cấp chứng thư số.

SMARTSIGN-CA tạo cho thuê bao một chứng thư số dựa vào những thông tin trong đơn xin cấp chứng thư số và yêu cầu cấp chứng thư số.

4.3.2. Thông báo của SMARTSIGN-CA đến người dùng về việc cấp chứng thư

SMARTSIGN-CA cấp phát các chứng thư trực tiếp tới người dùng hoặc thông qua RA. SMARTSIGN-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. Chứng thư có hiệu lực sẽ cho phép người dùng tải về từ website hoặc thông qua LDAP server.

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

- SMARTSIGN-CA tạo chứng thư số và gửi chứng thư số cho Token Manager để cập nhật vào thiết bị token.
- Thuê bao xác nhận các thông tin trong chứng thư số sẽ được cấp là chính xác.
- Quá trình truyền nhận giữa token và server được mã hóa, sử dụng phương thức SSL nhằm đảm bảo tính toàn vẹn và bí mật.

Khi bàn giao chứng thư số, thuê bao có trách nhiệm ký vào bản xác nhận đã nhận đầy đủ chứng thư số của mình và gửi lại cho SMARTSIGN-CA. Bản xác nhận có sự xác nhận thông tin trên chứng thư số phù hợp với thông tin thuê bao. Biên bản giao nhận này được SMARTSIGN-CA lưu trữ.

Nếu thông tin trong chứng thư số không phù hợp, người dùng thông báo lại cho đại lý hoặc RA của SMARTSIGN-CA để được xử lý.

Thông tin tiếp nhận: Công ty Cổ phần Chữ ký số Vi Na

Địa chỉ: 41A Nguyễn Phi Khanh, Phường Tân Định, Quận 1, TP HCM.

Điện thoại: 028 38 202 261

E-mail: info@smartsign.com.vn

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

4.4. Xác nhận và công bố công khai chứng thư

4.4.1. Điều kiện chứng minh việc xác nhận chứng thư

Khi thuê bao nhận chứng thư số và khoá bí mật lưu trong thiết bị lưu trữ (Token) từ thông báo của SMARTSIGN-CA, điều này chứng minh việc chấp thuận của thuê bao đối với thông báo đó.

Trong trường hợp từ chối, thuê bao phải thông báo cho SMARTSIGN-CA từ chối chứng thư và giải thích lý do từ chối. Trong vòng một ngày thuê bao không trả lời thông báo của SMARTSIGN-CA, chứng thư số đó coi như được khách hàng chấp nhận.

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

Sau khi nhận được chấp nhận chứng thư, SMARTSIGN-CA công bố chứng thư số đã phát hành, SMARTSIGN-CA công bố tất cả các chứng thư hợp lệ trong kho lưu trữ trực tuyến trên cả web lẫn kho lưu trữ LDAP.

Chứng thư số được coi là chính thức chấp nhận khi được SMARTSIGN-CA công bố trên website, kho dữ liệu chứng thư số. SMARTSIGN-CA công bố chứng thư số

của thuê bao tại trang web https://smartsign.com.vn/ trong vòng 24 giờ ngay khi nhận được xác nhận của thuê bao về tính chính xác của thông tin.

4.4.3. Thông báo sự phát hành chứng thư đến các đối tượng khác

SMARTSIGN-CA sẽ gửi thông báo về việc phát hành chứng thư đến các RA xử lý yêu cầu của thuê bao.

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 SMARTSIGN-CA và đã chấp nhận chứng thư số được ban hành.

Chứng thư số phát hành bởi SMARTSIGN-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 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 SMARTSIGN-CA, phải kiểm tra chứng thư số hợp lệ bằng cách:

- Kiểm tra có đúng chứng thư số do SMARTSIGN-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 CPS của SMARTSIGN-CA.

4.6. Gia hạn chứng thư

4.6.1. Các trường hợp cần gia hạn chứng thư

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 SMARTSIGN-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 RA thích hợp, SMARTSIGN-CA sẽ chấp nhận và thực hiện yêu cầu gia hạn chứng thư.

4.6.2. Đối tượng yêu cầu gia hạn chứng thư

Chủ sở hữu của chứng thư có thể yêu cầu gia hạn chứng thư trước khi nó hết hạn bằng cách gửi cho RA 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 SMARTSIGN-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

Khi nhận được yêu cầu xác nhận bởi RA, các 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 SMARTSIGN-CA nhận được yêu cầu mà không cần có sự hiện diện vật lý của thuê bao tại SMARTSIGN-CA hoặc RA.

4.6.4. Điều kiện chấp nhận gia hạn chứng thư

Tương tự 4.4.1

4.6.5. Công bố các chứng thư được gia hạn

Tương tự 4.4.2

4.6.6. Thông báo việc cấp chứng thư của SMARTSIGN-CA đến các đối tượng khác

Tương tự 4.4.3

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

Tương tự 4.3.2

4.7.5. Thông báo chấp nhận cấp mới khoá chứng thư

Tương tự 4.4.1

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

Tương tự 4.4.2

4.7.7. Thông báo cấp chứng thư của SMARTSIGN-CA tới các đối tượng khác

Tương tự 4.4.3

4.8. Thay đổi thông tin chứng thư số

Việc sửa đổi giấy chứng nhận có thể được thực hiện bằng cách thu hồi chứng thư và phát hành lại chứng thư số mới cho thuê bao với các khoá được tạo mới (re-key).

4.8.1. Các trường hợp sửa đổi chứng thư

Chứng thư số không được sửa đổi. Chứng thư cũ phải được thu hồi, và một cặp khoá mới phải được tạo ra và yêu cầu sửa đổi các nội dung chứng thư được chấp nhận với cặp khoá mới. Việc thu hồi trên điều kiện phát hành và chấp nhận một chứng thư mới và do đó chứng thư cũ chỉ được thu hồi sau khi một chứng thư mới được chấp nhận.

4.8.2. Đối tượng yêu cầu sửa đổi chứng thư

Không áp dụng

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

Không áp dụng

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

Không áp dụng

4.8.5. Điều kiện chấp nhận sửa đổi thuê bao

Không áp dụng

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

Không áp dụng

4.8.7. Thông báo phát hành chứng thư của SMARTSIGN-CA tới các đối tượng khác

Không áp dụng

4.9. Tạm dừng và thu hồi chứng thư

4.9.1. Các trường hợp thu hồi

Yêu cầu thu hồi chứng thư số sẽ được xử lý khi thuê bao đề nghị, do SMARTSIGN-CA quyết định hoặc theo yêu cầu của pháp luật.

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 SMARTSIGN-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.

- SMARTSIGN-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

Trong trường hợp khẩn cấp, nếu không gửi được e-mail việc thu hồi chứng thư có thể thông báo trực tiếp với RA hoặc CA của SMARTSIGN-CA. Trước khi thu hồi chứng thư SMARTSIGN-CA phải xác nhận nguồn gốc của yêu cầu theo thủ tục được sử dụng cho việc đăng ký ban đầu.

Thu hồi theo yêu cầu: Khi nhận yêu cầu thu hồi từ một thuê bao cho chứng thư số của mình, SMARTSIGN-CA sẽ tạm dừng chứng thư số, và kiểm tra để đảm bảo yêu cầu đó là chính xác. Trong trường hợp thuê bao thông báo khẩn cấp bằng phương tiện liên lạc như điện thoại, thư điện tử,... chỉ khi thuê bao có đơn yêu cầu thu hồi chứng thư số có xác nhận của tổ chức, doanh nghiệp đối với tổ chức doanh nghiệp hoặc chính cá nhân và nêu rõ lý do, SMARTSIGN-CA mới chính thức thu hồi và công bố thông tin thu hồi chứng thư số.

- Xác minh quyết định yêu cầu thu hồi chứng thư số của đơn vị có thẩm quyền.
- Nếu SMARTSIGN-CA có đủ cơ sở để xác minh khách hàng bị lộ khoá bí mật gây mất an toàn, SMARTSIGN-CA có quyền tạm dừng dịch vụ và thông báo cho thuê bao biết để xác nhận thông tin và bảo vệ an toàn thông tin cho thuê bao.

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 SMARTSIGN-CA xử lý yêu cầu thu hồi chứng thư

SMARTSIGN-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. SMARTSIGN-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 SMARTSIGN-CA truy cập qua nền tảng LDAP và web và có thể truy cập qua OCSP. SMARTSIGN-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 SMARTSIGN-CA và được đặt luôn sẵn sàng qua CRL, website, thư mục LDAP và OCSP:

Chứng thư của SMARTSIGN-CA.

Chứng thư cấp bởi SMARTSIGN-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 SMARTSIGN-CA hoặc SMARTSIGN-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

SMARTSIGN-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

5.1.1. Vị trí đặt và xây dựng hệ thống

Hệ thống thiết bị SMARTSIGN-CA được đặt tại hai trung tâm dữ liệu của Viettel và CMC.

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

Việc truy cập vật lý vào hệ thống SMARTSIGN-CA tuân thủ theo quy trình như sau:

Bước 1: Ủy quyền vào Trung tâm dữ liệu;

Bước 2: Bảo vệ lớp ngoài (ra/vào cổng);

Bước 3: Bảo vệ lớp trong (ra/vào tòa nhà);

Bước 4: Giám sát hệ thống;

Bước 5: Truy cập tủ Rack;

Bước 6: Truy cập các thiết bị vật lý.

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 SMARTSIGN-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 SMARTSIGN-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

SMARTSIGN-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, 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 SMARTSIGN-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 SMARTSIGN-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, SMARTSIGN-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 SMARTSIGN-CA phê duyệt và phải có sự chứng kiến của ít nhất 2 cá nhân trong vai trò quản lý khóa CA của SMARTSIGN-CA và việc phá hủy được lưu giữ hồ sơ biên bản của tất cả các bước.

5.1.8. Hệ thống dự phòng

SMARTSIGN-CA đang duy trì hai hệ thống đó là hệ thống SMARTSIGN-CA chính và hệ thống SMARTSIGN-CA dự phòng được đặt tại hai Data Center đạt tiêu chuẩn tương đương tier 3 và có khoảng cách đảm bảo theo quy định. Dữ liệu được đồng bộ realtime giữa hai hệ thống chính và hệ thống dự phòng. Các thiết bị được sử dụng giữa hệ thống chính và hệ thống dự phòng đều có mức độ an ninh giống nhau theo tiêu chuẩn hệ thống CA.

SMARTSIGN-CA đảm bảo hệ thống chính và hệ thống dự phòng luôn luôn hoạt động, luôn luôn trong tình trạng sẵn sàng cao để thay thế, chuyển đổi, đảm bảo thời gian ontime cao nhất.

5.2. Quy trình kiểm soát

5.2.1. Những thành viên được tin cậy

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

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

Người được tin tưởng bao gồm nhưng không giới hạn các đối tượng sau:

- Người đứng đầu hệ thống.
- Người quản trị hệ thống và bộ phận quản trị hệ thống.
- Người phụ trách cấp phát chứng thư số và bộ phận phụ trách cấp phát chứng thư số.

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

5.2.2. Số lượng người yêu cầu cho mỗi công việc

SMARTSIGN-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 SMARTSIGN-CA đều phải được xác minh nhân thân, nhận dạng và trình độ.

SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-CA cũng yêu cầu những nhân viên có xuất thân và lai lịch rõ ràng.

SMARTSIGN-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.

5.3.2. Thủ tục kiểm tra lai lịch

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

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

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

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

5.3.3. Yêu cầu về đào tạo

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

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

- Khái niệm căn bản về PKI;
- Trách nhiệm công việc;
- Các chính sách, quy chế an ninh của nhà nước và của SMARTSIGN-CA;
- Các phiên bản phần cứng phần mềm được sử dụng và các thức vận hành hệ thống CA;
- Báo cáo, chuyển giao các thỏa hiệp và các vấn đề liên quan;
- Xử lý các sự cố;
- Thủ tục khôi phục sau thảm họa và duy trì công việc.

5.3.4. Chu kỳ tái đào tạo

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

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

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

SMARTSIGN-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 SMARTSIGN-CA ở vị trí tương đương.

5.3.7. Cung cấp tài liệu cho nhân viên

SMARTSIGN-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

SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-CA.

Tính toàn vẹn lưu trữ thông tin của SMARTSIGN-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, SMARTSIGN-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 SMARTSIGN-CA ban hành có thời gian sử dụng không quá thời gian sử dụng chứng thư số của SMARTSIGN-CA được dùng để ký lên chứng thư số đó.

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

Trước khi hết hạn chứng thư số của SMARTSIGN-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 SMARTSIGN-CA. Quá trình chuyển tiếp khóa của SMARTSIGN-CA đảm bảo rằng:

- SMARTSIGN-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, theo quy định của pháp luật.
- Khi nhận được yêu cầu ban hành chứng thư số sau thời điểm tạm dừng ban hành chứng thư số trên, SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-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.

SMARTSIGN-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 SMARTSIGN-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

SMARTSIGN-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 SMARTSIGN-CA bị lỗi, các bước sau đây sẽ được thực hiện:

- Tất cả các phần mềm trên SMARTSIGN-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 SMARTSIGN-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 DR của SMARTSIGN-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.

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

SMARTSIGN-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

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

SMARTSIGN-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.

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

Cơ sở dữ liệu của SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-CA sẽ:

- Thông báo với Bộ Thông tin và Truyền thông 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 SMARTSIGN-CA.

Thông báo tạm dừng dịch vụ không ít hơn 60 ngày trong trường hợp chấm dứt bình thường. Các quản lý CA 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 SMARTSIGN-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 đạt chuẩn FIPS 140-2 Level 3 trở lên với thuật toán RSA. Quản lý và bảo mật khóa CA sử dụng mô-đun bảo mật phần cứng (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. SMARTSIGN-CA 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: SMARTSIGN-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 khàng (Bao gồm Thiết bị Token, và giấy chứng nhận).

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

SMARTSIGN-CA có thể xử lý yêu cầu cấp phát chứng thư dựa trên tải yêu cầu theo định dạng PKCS#10. SMARTSIGN-CA cung cấp công cụ để thuê bao truyền các yêu cầu chứng thực, bao gồm khóa công khai, tới SMARTSIGN-CA thông qua các yêu cầu với 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.

6.1.5. Kích thước khoá

Chuẩn hiện tại của dịch vụ SMARTSIGN-CA yêu cầu chiều dài của cặp khoá để đảm bảo mức độ mã hoá đủ mạnh là 1024 hoặc 2048 bits RSA.

Khoá của SMARTSIGN-CA có chiều dài là 2048 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 SMARTSIGN-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 SMARTSIGN-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. SMARTSIGN-CA đang sử dụng cơ chế N = 3;

6.2.3. Lưu trữ khoá bí mật thuê bao

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

6.2.4. Sao lưu, dự phòng khoá bí mật

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

Khi chứng thư của SMARTSIGN-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 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 CPS.

6.2.5. Cách thức sao lưu khoá bí mật

Hiện nay SMARTSIGN-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 SMARTSIGN-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 6.2.2.

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

Đối với thuê bao: khóa bí mật được lưu trong USB token, việc kích hoạt khóa bí mật yêu cầu mật khẩu bảo vệ. Khi không sử dụng, khóa bí mật tồn tại ở dạng mã hóa.

Đối với quản trị hệ thống CA/RA: khóa bí mật được lưu trong USB token, việc kích hoạt khóa bí mật yêu cầu mật khẩu bảo vệ. Khi không sử dụng, khóa bí mật tồn tại ở dạng mã hóa.

Đối với RA: khóa bí mật được lưu trong USB token, việc kích hoạt khóa bí mật yêucầu mật khẩu bảo v. Khi không sử dụng, khóa bí mật tồn tại ở dạng mã hóa.

Đối với SMARTSIGN-CA: 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 6.2.2.

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 SMARTSIGN-CA /RA bị ngừng kích hoạt khi không chứa trong Token Reader (HSM). RA của SMARTSIGN-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

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

SMARTSIGN-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 SMARTSIGN-CA được xác định bởi tài liệu CPS này.

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

Thêm vào đó dịch vụ SMARTSIGN-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 SMARTSIGN-CA được chia thành các mã chia sẻ, các mã chia sẻ này được tạo theo các yêu cầu trong phần 6.2.2 và tuân theo các thủ tục của nghi lễ sinh khóa. Quá trình tạo và phân phối mã chia sẻ được ghi nhật ký.

SMARTSIGN-CA khuyến cáo đối với thuê bao sử dụng mật khẩu đủ mạnh để bảo vệ các khóa bí mật của họ. Mật khẩu để bảo vệ kích hoạt khóa bí mật được đặt theo nguyên tắc mật khẩu mạnh:

- Có ít nhất 8 ký tự;

- Chứa từ 3 trong 4 loại ký tự sau: chữ hoa (A, B, C…), chữ thường (a, b, c), chữ số (0, 1, 2…) và các ký hiệu (!, @, $...);
- Không chứa tất cả hoặc một phần tên tài khoản người dùng tương ứng.

SMARTSIGN-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

SMARTSIGN-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. SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-CA bàn giao mã PIN kích hoạt PKI Token. Sau khi SMARTSIGN-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 SMARTSIGN-CA cấp mã PIN kích hoạt Token sẽ được SMARTSIGN-CA gửi riêng tới thuê bao.

Đối với khóa bí mật của SMARTSIGN-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 SMARTSIGN-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 M x N. Thực hiện sử dụng tối thiểu 2 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

SMARTSIGN-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, SMARTSIGN-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 SMARTSIGN-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

SMARTSIGN-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

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

6.6.3. Kiểm soát về mặt 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: SMARTSIGN-CA phân vai trò, quyền sử dụng phân công trách nhiệm cho từng đối tượng tham gia sử dụng hệ thống
- Bước 2: SMARTSIGN-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: SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-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

SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-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 tối thiểu phải có các nội dung sau:

Tên trường	Giá trị
Serial number	Do SMARTSIGN gán, là định dạng duy nhất của chứng thư số.
Signature algorithm	Số hiệu thuật toán dùng để ký chứng thư số.
Issuer	Bộ TTTT quy định.
Valid from	Thời điểm chứng thư bắt đầu có hiệu lực. Giá trị thời gian được ghi theo định dạng trong RFC 5280.
Valid to	Thời điểm chứng thư hết hiệu lực. Giá trị thời gian được ghi theo định dạng trong RFC 5280.
Subject	Tên của thuê bao (Xem phần 3.1.1).
Public key	Khóa công khai (được mã hóa phù hợp với RFC 5280).
Signature	Chữ ký số được tạo và lưu theo định dạng trong RFC 5280.

7.1.1. Phiên bản

SMARTSIGN-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 SMARTSIGN-CA là:

Chứng thư số dùng cho cá nhân

Basic Constraints	critical, 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 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 CPS này
Issuer Alternative Name	Liên kết (URI) đến chứng thư của SMARTSIGN-CA
CRL Distribution Points	URI của CRL

Chứng thư số dùng cho dịch vụ / Máy chủ

Basic Constraints	critical, ca: false
Subject Key Identifier	hash
Authority Key Identifier	keyid

Key Usage	digitalSignature nonRepudiation keyEncipherment dataEncipherment keyAgreement
Extended Key Usage	clientAuth serverAuth
Certificate Policies	OID của 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 SMARTSIGN-CA
CRL Distribution Points	URI của CRL

7.1.3. Các thuật toán ký

SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-CA và tuân theo cấu trúc được định nghĩa trong tiêu chuẩn ITU-T Standards Recommendation X.501.

7.1.5. Ràng buộc tên

Không có những ràng buộc khác hơn so với quy định tại mục 7.1.4.

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

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

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

Không có ràng buộc nào.

7.1.8. Chính sách hạn định cấu trúc và ngữ nghĩa

Không có quy định.

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

Không có quy định.

7.2. Định dạng danh sách thu hồi chứng thư CRLs

Version	V2
Signature	Sha256WithRSAEncryption
Issuer	SMARTSIGN-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 Certificates	serialNumbers của chứng thư bị thu hồi

Những chứng chỉ đã bị CA thu hồi được ghi vào danh sách. 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

SMARTSIGN-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 CPS được tiến hành ít nhất mỗi năm một lần.

SMARTSIGN-CA tiến hành kiểm tra sự tuân thủ các thủ tục của mỗi RA với 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 SMARTSIGN-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, SMARTSIGN-CA sẽ làm việc với RootCA về những nội dung chưa phù hợp.

- SMARTSIGN-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.
- SMARTSIGN-CA hành động ngay lập tức nếu đánh giá cho thấy một sự vi phạm các quy định trong 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 SMARTSIGN-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 ninh của hệ thống SMARTSIGN-CA.
- SMARTSIGN-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 SMARTSIGN-CA công bố trang web của SMARTSIGN-CA.

Quản lý CA sẽ công bố kết quả trên trang web của SMARTSIGN-CA với thông tin chi tiết về sự vi phạm 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 SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-CA không phải trả phí cho việc phát hành các CRL. Tuy nhiên SMARTSIGN-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: SMARTSIGN-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 là 01 (một) tháng sử dụng.

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 chuẩn sẽ được hoàn trả.

9.2. Trách nhiệm tài chính

9.2.1. Đăng thông tin bảo hiểm

SMARTSIGN-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 SMARTSIGN-CA tiến hành đền bù bảo hiểm

SMARTSIGN-CA tiến hành đền bù bảo hiểm cho các trường hợp sau:

- Lỗi do CA gây ra, bao gồm lỗi kỹ thuật khi phát hành chứng thư theo trách nhiệm của CA.
- Việc đền bù bảo hiểm thực hiện theo đúng hợp đồng với thuê bao.

9.2.3. Các trường hợp không được đền bù bảo hiểm

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

- Các trường hợp sử dụng chứng thư vi phạm điều khoản trong 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.

9.2.4. Các tài sản khác

Không được đề cập.

9.2.5. Trường hợp bị thu hồi giấy phép

SMARTSIGN-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 tiếp nhận và duy trì cơ sở dữ liệu của SMARTSIGN-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 vi 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 SMARTSIGN-CA phát hành không được coi là riêng tư. Khi yêu cầu một chứng thư từ SMARTSIGN-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

SMARTSIGN-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 SMARTSIGN-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

SMARTSIGN-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

SMARTSIGN-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 SMARTSIGN-CA và công bố bất kỳ nào khác có nguồn gốc từ SMARTSIGN-CA bao gồm CPS này.

Các tên phân biệt (DN) của các CA của SMARTSIGN-CA vẫn là tài sản của SMARTSIGN-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 SMARTSIGN-CA

SMARTSIGN-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 SMARTSIGN-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 SMARTSIGN-CA.
- Tuân thủ theo quy trình quản lý vòng đời chứng thư số của SMARTSIGN-CA.

RA có trách nhiệm ký hợp đồng với SMARTSIGN-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 SMARTSIGN-CA đã nhận đầy đủ hồ sơ của thuê bao, và thông tin thuê bao được thẩm định.
- Cam kết của RA với SMARTSIGN-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 SMARTSIGN-CA ban hành.

- Người nhận phải chịu trách nhiệm cho những hành động của mình nếu 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 phần phụ lục.

9.7. Từ chối trách nhiệm

SMARTSIGN-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 SMARTSIGN-CA nếu xuất hiện:

- Những thông tin không hợp lệ do 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 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 SMARTSIGN-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.
- 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 SMARTSIGN-CA. Các điều sửa đổi bổ sung cho 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 việc 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

Trừ khi được quy định rõ ràng, các thành viên SMARTSIGN-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 CPS sẽ được thực hiện bởi Cấp quản lý chính sách có thẩm quyền. 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… SMARTSIGN-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, SMARTSIGN-CA sẽ xem xét yêu cầu thay đổi. Nếu quy chế cần thay đổi, SMARTSIGN-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, SMARTSIGN-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 SMARTSIGN-CA được quyền góp ý cho quy chế chứng thư số trong vòng 15 ngày từ ngày quy chế được công bố.

SMARTSIGN-CA sẽ xem xét mọi góp ý sửa đổi. SMARTSIGN-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 CPS sẽ làm OID thay đổi. Quyết định này được thực hiện bởi quản lý CPS của SMARTSIGN-CA.

9.13. Thủ tục giải quyết tranh chấp

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

- Việc giải quyết tranh chấp giữa SMARTSIGN-CA, cộng tác và thuê bao phải tuân thủ theo các điều khoản được ghi trong hợp đồng.

- Việc giải quyết tranh chấp giữa SMARTSIGN-CA và đại lý phải tuân thủ theo các điều khoản được ghi trong hợp đồng đại lý. Thời gian đàm phán là 60 ngày, 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 2023;
- 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 chứng 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 SMARTSIGN-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 SMARTSIGN-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. SMARTSIGN-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. 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 SMARTSIGN-CA.

9.17. Các điều khoản khác

Không áp dụng.

10.PHỤ LỤC

10.1. Quyền của đại lý

- Được hưởng thù lao đại lý theo quy định được ký kết giữa đại lý và SMARTSIGN-CA.
- Được tham gia các chương trình khuyến mãi, quảng cáo của SMARTSIGN-CA khi cung cấp dịch vụ theo hợp đồng.
- Yêu cầu SMARTSIGN-CA cung cấp các tài liệu và tổ chức tập huấn về dịch vụ, các quy trình, quy định liên quan đến việc cung cấp dịch vụ cho khách hàng và việc thực hiện cho hợp đồng này.
- Chấm dứt hợp đồng khi không có nhu cầu làm đại lý hoặc khi SMARTSIGN-CA vi phạm các điều khoản đã cam kết trong hợp đồng.

10.2. Nghĩa vụ của đại lý

- Không tiết lộ bí mật kinh doanh của SMARTSIGN-CA cho bất kỳ người nào khi chưa được SMARTSIGN-CA cho phép.
- Đại lý có nghĩa vụ phải cung cấp dịch vụ đúng như trong hợp đồng đã ký và theo quy định pháp luật.
- Chịu trách nhiệm bán đúng giá theo bảng giá SMARTSIGN-CA ban hành và không được bán giá cao hơn cho khách hàng.
- Tiếp nhận và bảo quản account truy vấn thông tin hệ thống SMARTSIGN-CA. Đảm bảo bảo mật và chịu hoàn toàn trách nhiệm về các thông tin khai báo do account quản trị này thực hiện trên hệ thống.
- Tiếp nhận mẫu hợp đồng dịch vụ, biên bản bàn giao, nghiệm thu do SMARTSIGN-CA cung cấp để thực hiện thủ tục ký kết hợp đồng và nghiệm thu với khách hàng.

- Bàn giao đầy đủ và đúng hạn các hồ sơ khách hàng cho SMARTSIGN-CA, bao gồm: Hợp đồng và biên bản nghiệm thu với khách hàng và các giấy tờ liên quan đến thủ tục ký kết hợp đồng theo quy định.
- Cung cấp đúng và đầy đủ chính sách giá cước, chính sách dịch vụ cho khách hàng do SMARTSIGN-CA quy định. Không được thu thêm bất kỳ chi phí nào khi giao dịch với khách hàng trong quá trình tiếp xúc giới thiệu, tư vấn, xúc tiến ký kết hợp đồng và cài đặt nghiệm thu dịch vụ.
- Phối hợp với SMARTSIGN-CA thực hiện quảng cáo, tiếp thị, triển khai các đợt khuyến mãi, chăm sóc khách hàng tuỳ theo từng chương trình cụ thể do các bên thoả thuận.
- Tiếp nhận và chuyển các khiếu nại hoặc ý kiến phản hồi của khách hàng cho SMARTSIGN-CA, phối hợp với SMARTSIGN-CA giải quyết và trả lời cho khách hàng.
- Đối soát số liệu hàng tuần/ hàng tháng để làm căn cứ thanh toán tiền thù lao đại lý.
- Khi nhận tiền thù lao đại lý, SMARTSIGN-CA phải xuất hoá đơn tài chính cho đại lý.
- Lắp đặt biển hiệu, tiếp nhận tờ rơi do SMARTSIGN-CA cung cấp để thực hiện công tác quảng bá, tiếp thị dịch vụ cho khách hàng.
- Thông báo cho SMARTSIGN-CA trước 07 ngày khi có sự thay đổi về địa chỉ, số điện thoại, số fax, email hoặc các yêu cầu khác.
- Không được chuyển nhượng hợp đồng đại lý này cho bất kỳ một bên thứ 3 nào khi chưa có sự đồng ý trước bằng văn bản của SMARTSIGN-CA.
- Tự chịu trách nhiệm về các khoản thuế có liên quan theo quy định của pháp luật.

10.3. Các trách nhiệm khác của đại lý

10.3.1. Tiếp thị và giới thiệu dịch vụ chứng thư số của Công Ty Cổ phần Chữ ký số Vi Na

- Đại lý có trách nhiệm chủ động thực hiện các biện pháp tiếp thị (marketing) để tìm kiếm khách hàng trong những quy định về chính sách marketing của SMARTSIGN-CA.

- Đại lý có trách nhiệm giới thiệu đầy đủ, tận tình các dịch vụ giá trị gia tăng của Công Ty Cổ phần Chữ ký số Vi Na cho khách hàng và hướng dẫn khách hàng các thông tin, thủ tục cần thiết để đăng ký và sử dụng các dịch vụ đó.

10.3.2. Kiểm tra điều kiện pháp lý của khách hàng

Đại lý có trách nhiệm kiểm tra điều kiện pháp lý, khả năng tài chính của khách hàng để ký kết hợp đồng sử dụng dịch vụ giá trị gia tăng. Cụ thể:

Khách hàng là Tổ chức, doanh nghiệp:

- Hợp đồng, bản khai phải được ký và đóng dấu. Hợp đồng phải đầy đủ các thông tin của khách hàng như: người đại diện pháp lý ký hợp đồng (trường hợp ủy quyền phải có giấy ủy quyền kèm theo), điện thoại, địa chỉ, tài khoản thanh toán, mã số thuế…
- Bản sao CMND hoặc Hộ chiếu hoặc Căn cước công dân của người đại diện pháp lý của tổ chức, doanh nghiệp có công chứng.
- Bản sao Giấy phép thành lập/Đăng ký kinh doanh có công chứng.
- Bản sao Giấy chứng nhận đăng ký thuế của doanh nghiệp có công chứng (nếu có).

Khách hàng là cá nhân:

- Hợp đồng, bản khai phải được ký và đầy đủ các thông tin của khách hàng như: tên khách hàng, số CMND (CCCD, hộ chiếu), ngày cấp CMND (CCCD, hộ chiếu), điện thoại, địa chỉ, tài khoản thanh toán, mã số thuế…
- Bản sao CMND hoặc Hộ chiếu hoặc Căn cước công dân có công chứng của cá nhân.
- Bản sao có công chứng của cơ quan nhà nước Giấy ĐKKD hoặc Quyết định thành lập, Giấy phép đầu tư (đối với khách hàng cá nhân thuộc doanh nghiệp).
- Bản sao có công chứng của cơ quan nhà nước giấy CMND của người đại diện hợp pháp của tổ chức/doanh nghiệp (đối với khách hàng cá nhân thuộc doanh nghiệp).

10.3.3. Hướng dẫn khách hàng làm Hợp đồng các và thủ tục cần thiết

Nếu khách hàng đủ điều kiện pháp lý và đồng ý sử dụng dịch vụ, đại lý nhận hồ sơ và thẩm định lại trước khi cấp chứng thư số, hướng dẫn khách hàng điền đầy đủ và nộp lại các nội dung vào các mẫu do SMARTSIGN-CA cung cấp sau:

- Giấy đăng ký xin cấp chứng thư số
- Hợp đồng cung cấp và sử dụng dịch vụ chứng thư số.
- Biên bản bàn giao thiết bị, có xác nhận của khách hàng

Đại lý cũng có trách nhiệm hướng dẫn khách hàng thực hiện các nghĩa vụ trong Hợp đồng cung cấp dịch vụ.

10.3.4. Bàn giao Hồ sơ

Đại lý phải đảm bảo thực hiện nhận đầy đủ hồ sơ của thuê bao trước khi cung cấp chứng thư số, và trước ngày mùng 5 hàng tháng đại lý có trách nhiệm bàn giao tất cả các hồ sơ thuê bao cho SMARTSIGN-CA. Cụ thể:

- 01 Giấy đăng ký xin cấp chứng thư số.
- 01 Hợp đồng (bản chính) và các hồ sơ, giấy tờ pháp lý liên quan của khách hàng sử dụng dịch vụ cho SMARTSIGN-CA.
- 01 Biên bản bàn giao thiết bị với khách hàng.
- Bản sao CMND hoặc Hộ chiếu hoặc Căn cước công dân của người đại diện pháp lý của tổ chức, doanh nghiệp có công chứng.
- Bản sao Giấy phép thành lập/Đăng ký kinh doanh có công chứng.

SMARTSIGN-CA có trách nhận tiếp nhận Hồ sơ của khách hàng nhanh chóng và ký Biên bản bàn giao khách hàng với đại lý.

Đại lý bàn giao Hợp đồng dịch vụ cho SMARTSIGN-CA phải đảm bảo hợp đồng có đầy đủ thông tin của nhân viên đại lý trực tiếp tham gia vào quy trình cấp chứng thư số trên cụ thể bao gồm các thông tin sau:

- Họ tên nhân viên:
- Số CMND:
- Điện thoại liên hệ:
- Nếu trong thời gian cung cấp dịch vụ đại lý có thay đổi nhân sự thì phải thông báo bằng văn bản cho SMARTSIGN-CA biết.

10.3.5. Hoàn thành thủ tục thanh toán cho khách hàng và đối soát quyết toán giữa đại lý và SMARTSIGN-CA

Đại lý có trách nhiệm theo dõi việc thực hiện trách nhiệm thanh toán của khách hàng (cước phí cài đặt và duy trì dịch vụ thanh toán lần đầu theo giá trị hợp đồng) đã quy định cụ thể trong Hợp đồng cung cấp dịch vụ cụ thể như sau:

- Đối với hợp đồng hai bên giữa Công ty Cổ phần Chữ ký số Vi Na và khách hàng cuối, khi đại lý nhận thiết bị đã có chữ ký số từ SMARTSIGN-CA, đại lý phải thanh toán cước phí dịch vụ và phí thiết bị (nếu có) cho SMARTSIGN-CA, lấy hoá đơn của SMARTSIGN-CA để giao cho khách hàng. (Công ty Cổ phần Chữ ký số Vi Na không chịu trách nhiệm về số tiền đại lý thu của khách hàng và chưa nộp cho Công ty). Nếu khách hàng thanh toán qua ngân hàng đại lý có trách nhiệm đôn đốc khách hàng đến khi tiền của khách hàng được chuyển về tài khoản của SMARTSIGN-CA và chuyển hoá đơn của SMARTSIGN-CA cho khách hàng.
- Đối với hợp đồng ba bên giữa SMARTSIGN-CA, đại lý và khách hàng cuối, đại lý sẽ thu cước phí dịch vụ và thiết bị từ khách hàng và xuất hóa đơn cho khách hàng. Đối với thiết bị Token trắng, SMARTSIGN-CA sẽ bàn giao trước cho đại lý theo thỏa thuận tại từng thời điểm, và đại lý phải thanh toán cho SMARTSIGN-CA phí thiết bị này. đại lý và Công ty Cổ phần Chữ ký số Vi Na sẽ đối soát một tháng một lần vào từ ngày 01 đến ngày 05 hàng tháng bao gồm cả phí thiết bị.
- Đại lý phải đảm bảo phương thức thanh toán, hoàn thành thủ tục thanh toán và đối soát quyết toán giữa SMARTSIGN-CA và đại lý nhanh chóng, đầy đủ để đảm bảo thuê bao nhận được dịch vụ thông suốt.
- Đại lý có trách nhiệm theo dõi việc thực hiện trách nhiệm thanh toán của khách hàng (cước phí cài đặt và duy trì dịch vụ thanh toán lần đầu theo giá trị hợp đồng) đã quy định cụ thể trong Hợp đồng cung cấp dịch vụ.

10.3.6. Hỗ trợ khách hàng

Đại lý có trách nhiệm tiếp nhận tất cả các yêu cầu hỗ trợ từ phía khách hàng, thực hiện hỗ trợ khách hàng tốt nhất trong khả năng và theo quy trình hướng dẫn của SMARTSIGN-CA đã huấn luyện cho đại lý.

Đại lý có trách nhiệm phối hợp với SMARTSIGN-CA hỗ trợ khách hàng.

10.3.7. Chăm sóc khách hàng

Đại lý có trách nhiệm phối hợp với Công ty Cổ phần Chữ ký số Vi Na thực hiện các hoạt động chăm sóc khách hàng do Công ty Cổ phần Chữ ký số Vi Na đề xuất.

Đại lý có thể chủ động thực hiện các hoạt động chăm sóc đối với khách hàng do đại lý phát triển nhằm tăng uy tín của dịch vụ và không ảnh hưởng đến uy tín của Công ty Cổ phần Chữ ký số Vi Na.

TÀI LIỆU THAM CHIẾU

[1] Luật giao dịch điện tử số 20/2023/QH15 ngày 22/06/2023.

[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] RFC 5280 (https://www.rfc-editor.org/rfc/rfc5280.txt).

[6] 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.