NG TY CỔ PHẦN CHỮ KÝ SỐ VI NA (SMARTSIGN)

QUY CHẾ CHỨNG THỰC SMARTSIGN

OID: 1.3.6.1.4.1.30339.1.7

Hồ Chí Minh, 2026

MỤC LỤC

1. Giới thiệu

1.1. Tổng quan

Tài liệu này là quy chế chứng thực chữ ký số của SMARTSIGN. Tài liệu nêu rõ những quy chế của SMARTSIGN sử dụng trong quá trình cung cấp dịch vụ chứng thực chữ ký số công cộng bao gồm phát hành, quản lý, tạm dừng, thu hồi và cấp lại chứng thư chữ ký 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 1.3.6.1.4.1.30339.1.7

OID này được xác định khi SMARTSIGN đăng ký với Bộ Khoa học và Công nghệ.

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

1.3.1. Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia (Trung tâm Chứng thực điện tử quốc gia)

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.

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

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng (CA công cộng) là doanh nghiệp được cấp phép cung cấp dịch vụ chứng thực chữ ký số cho cơ quan, tổ chức, và cá nhân

1.3.3. Thuê bao

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.

1.3.4. Bên tin cậy

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

1.3.5. Các bên khác

Các bên khác SMARTSIGN không quản lý đối tượng nào khác ngoài thuê bao và các bên tin cậy.

1.4. Mục đích sử dụng chứng thư chữ ký số

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

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

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

Chứng thư chữ ký số do SMARTSIGN cấp được phân ra các loại sau đây:

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

Chứng thư chữ ký số cho cá nhân có thời hạn tối đa 03 năm (theo Điều 7 Nghị định 23/2025/NĐ-CP) và không được vượt quá thời hạn của chứng thư chữ ký số SMARTSIGN.

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

Chứng thư chữ ký số cho cá nhân thuộc tổ chức doanh nghiệp có thời hạn tối đa 03 năm (theo Điều 7 Nghị định 23/2025/NĐ-CP) và không được vượt quá thời hạn của chứng thư chữ ký số SMARTSIGN.

- Chứng thư chữ ký số cho các tổ chức doanh nghiệp: thuê bao là tổ chức doanh nghiệp. Thuê bao sử dụng chứng thư chữ ký 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 chữ ký số cho tổ chức doanh nghiệp có thời hạn tối đa 03 năm (theo Điều 7 Nghị định 23/2025/NĐ-CP) và không được vượt quá thời hạn của chứng thư chữ ký số SMARTSIGN.

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

Về cơ bản các chứng thư chữ ký 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 khóa, chỉ định và giới hạn tính hợp lệ sử dụng một chứng thư chữ ký số, sử dụng thẻ, tên các thành phần của trường "subject".

- Chứng thư chữ ký số dùng cho cá nhân.
- Chứng thư chữ ký số dùng cho tổ chức.
- Chứng thư chữ ký số SSL.
- Chứng thư chữ ký số Code Signing.

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

Chứng thư chữ ký 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 và thuê bao.

Trong mọi trường hợp, cấm sử dụng chứng thư chữ ký số do SMARTSIGN phát hành 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 chữ ký số gốc của CA khác.

1.5. Quản lý quy chế chứng thực

1.5.1. Tổ chức quản lý quy chế chứng thực

Tên cơ quan: Công ty Cổ phần Chữ Ký Số Vi Na

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

1.5.2. Thông tin 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, Tp Hồ Chí Minh
- Điện thoại: 028 3820 2261
- E-mail: info@smartsign.com.vn

1.5.3. Cơ quan, tổ chức đánh giá sự phù hợp của quy chế chứng thực với pháp luật

Bộ Khoa học Công nghệ 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 duyệt, ban hành 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/ho-tro/tien-ich/

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 chữ ký số hợp lệ đang hoặc đã được phát hành phải được lưu trữ để cung cấp cho các bên tin cậy khi có yêu cầu. Các phiên bản của Quy chế chứng thực được công bố tại: https://smartsign.com.vn/ho-tro/tien-ich/

1.6. Các định nghĩa và từ viết tắt

1.6.1. Các định nghĩa

Thuật ngữ	**Giải thích**
Chứng thư chữ ký số SMARTSIGN	Là một dạng chứng thư điện tử do SMARTSIGN số cấp.
Chứng thư chữ ký số có hiệu lực	Là chứng thư chữ ký 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 phi đối xứng theo đó người có được thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định được chính xác: a. Việc biến đổi nêu trên được tạo ra bằng đúng khóa bí mật tương ứng với khóa 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 chữ ký số của thuê bao; c. Duy trì trực tuyến cơ sở dữ liệu về chứng thư chữ ký 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 khóa bí mật và khóa công khai.
Khoá	Là một chuỗi các số nhị phân (0 và 1) dùng trong các hệ thống mật mã.
Khóa bí mật	Là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được dùng để tạo chữ ký số.
Khóa công khai	Là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được sử dụng để kiểm tra chữ ký số được tạo bởi khóa bí mật tương ứng trong cặp khóa.
Ký số	Là việc đưa khóa bí mật vào một chương trình phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu.
Người ký	Là thuê bao dùng đúng khóa bí mật của mình để ký số vào một thông điệp dữ liệu dưới tên của mình.
Người nhận	Là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng chứng thư chữ ký 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 chữ ký số,

	chấp nhận chứng thư chữ ký số và giữ khóa bí mật tương ứng với khóa công khai ghi trên chứng thư chữ ký số được cấp đó.
Tạm dừng chứng thư chữ ký số	Là làm mất hiệu lực của chứng thư chữ ký số một cách tạm thời từ một thời điểm xác định.
Thu hồi chứng thư chữ ký số	Là làm mất hiệu lực của chứng thư chữ ký 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	Hypertext Transaction Standard Secure
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-256	Secure Hash Algorithm 256-bit
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 chữ ký số thu hồi (CRL), giao thức kiểm tra tình trạng chứng thư chữ ký số theo thời gian thực (OCSP) và trang web của SMARTSIGN.

SMARTSIGN 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 chữ ký số.

- Lưu trữ đầy đủ, chính xác và cập nhật thông tin của thuê bao phục vụ việc cấp chứng thư chữ ký số trong suốt thời gian chứng thư chữ ký số có hiệu lực và trong thời gian ít nhất 05 năm, kể từ khi chứng thư chữ ký 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 chữ ký 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 chữ ký số cho khách hàng, SMARTSIGN yêu cầu khách hàng ký biên bản bàn giao chứng thư chữ ký số, xác nhận thông tin trên chứng thư chữ ký số là chính xác. Sau đó chứng thư chữ ký số của khách hàng sẽ được công bố.

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

Các thông tin cập nhật và công bố bao gồm:

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

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

- Chứng thư chữ ký số SMARTSIGN có thời hạn từ ngày 24/02/2023 đến ngày 24/02/2028, sử dụng: http://crl1.smartsign.com.vn;

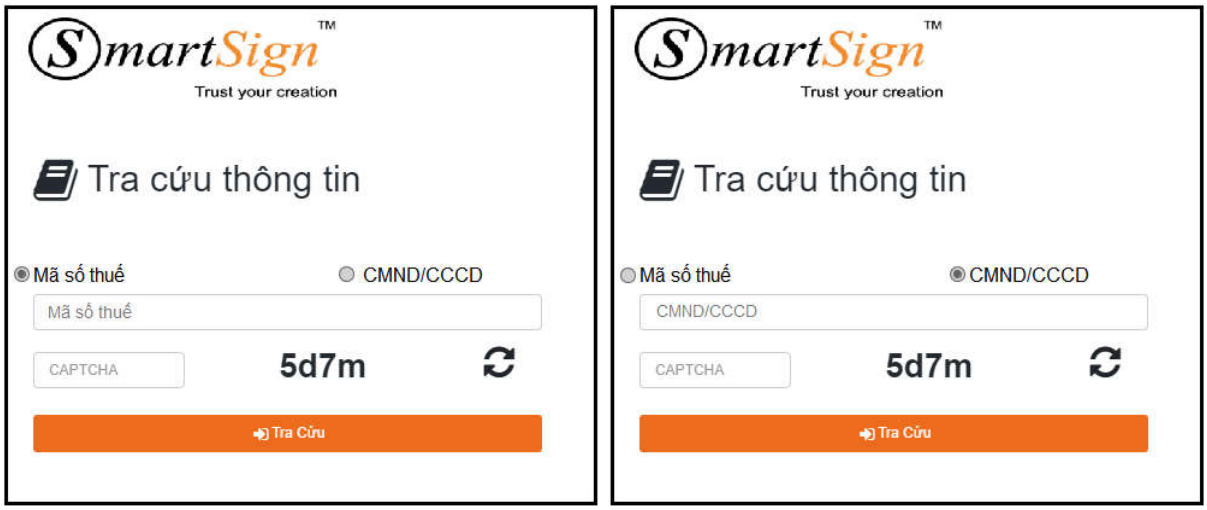
Kiểm tra tình trạng chứng thư chữ ký số theo thời gian thực (OCSP).

- Chứng thư chữ ký số SMARTSIGN có thời hạn từ ngày 24/02/2023 đến ngày 24/02/2028, sử dụng: http://ocsp1.smartsign.com.vn;

Tra cứu tình trạng chứng thư chữ ký số:

Các thuê bao có chứng thư chữ ký số được phát hành bởi SMARTSIGN có thể tra cứu tình trạng chứng thư chữ ký 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 chữ ký số sẽ được hiển thị như hình dưới:

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

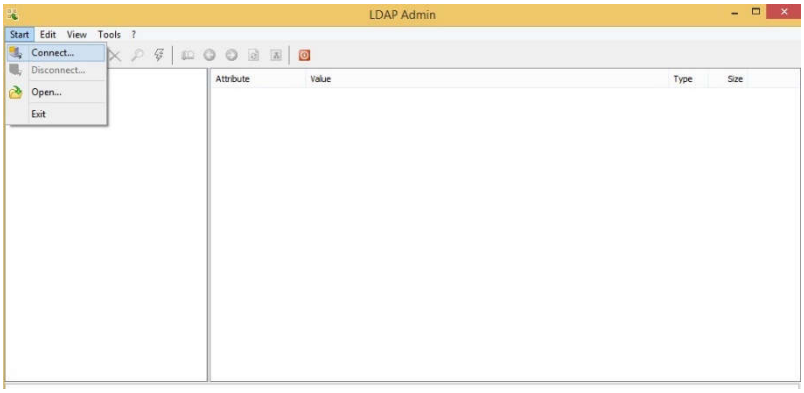
Công bố thông tin chứng thư chữ ký số (LDAP):

Để đảm bảo an toàn cơ sở dữ liệu LDAP thì SMARTSIGN 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/ho-tro/tien-ich/

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

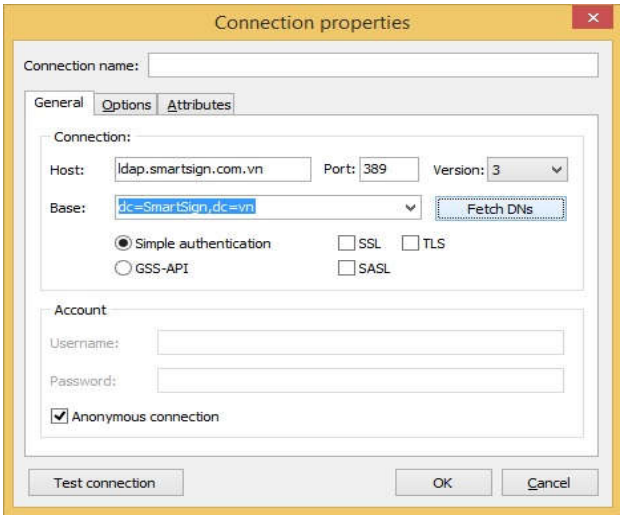


Bước 3 : Chọn new connect và điền các thông số như sau:

Mục host:

- Với chứng thư chữ ký số SMARTSIGN có thời hạn từ ngày 24/02/2023 đến ngày 24/02/2028 sử dụng địa chỉ: ldap1.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 chữ ký số SMARTSIGN sẽ được công bố ngay sau khi có sự chấp nhận của thuê bao phù hợp với các thủ tục mà SMARTSIGN 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 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 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 chữ ký số của SMARTSIGN, và các tài liệu (CPS) của SMARTSIGN thông qua địa chỉ công bố truy cập trực tuyến.

SMARTSIGN 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. Định danh và xác thực yêu cầu đề nghị phát hành chứng thư chữ ký số

3.1. Đặt tên

3.1.1. Các kiểu tên

Chứng thư chữ ký số chứa một tên dùng để phân biệt với các chứng thư chữ ký số khác (Distinguished Names – DN) theo chuẩn X.501 trong trường Issuer và Subject. Trường "subject" của chứng thư chữ ký số tuân theo chuẩn X.509 v3. Nội dung của trường "subject" của chứng thư chữ ký 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 chữ ký số, tên miền nếu là chứng thư chữ ký số SSL.

- OrganizationalUnitName (OU): Bộ phận thuộc tổ chức (O) mà đối tượng sở hữu chứng thư chữ ký số thuộc. Tên của tổ chức.

- OrganizationName (O): Tên tổ chức mà đối tượng sở hữu chứng thư chữ ký số thuộc. Giá trị của thành phần OrganizationName được định nghĩa trước (SMARTSIGN) và nó cũng là thành phần gốc của LDAP.

- State or Province (S): Thuộc tính chứa tên tỉnh/ thành phố, được sử dụng để định danh địa điểm địa lý của chủ thể chứng chỉ.

- 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 chữ ký số cấp cho cá nhân nội dung trường "subject" phải bao gồm Họ và tên của thuê bao.

- Trong trường hợp chứng thư chữ ký số cấp cho host/server nội dung trường "subject" phải bao gồm FQDN (Fully Qualified Domain Name) của host/server.

Minh họa đầy đủ nội dung của trường "subject" của một chứng thư chữ ký số cấp cho cá nhân:

E=vunh@smartsign.com.vn, CN=Nguyễn Hoàng Vũ, O=Công ty Cổ phần Chữ ký số Vi Na, S=Hồ Chí Minh, C=VN.

3.1.2. Cần tên có ý nghĩa

Nội dung của chứng thư chữ ký 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 chữ ký 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 chữ ký số được phát hành 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 chữ ký số do SMARTSIGN 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 chữ ký số
Bộ phận tổ chức (OU)	Bộ phận thuộc tổ chức (O) mà thuê bao sở hữu chứng thư số trực thuộc.
Tỉnh, thành phố (S)	Địa chỉ tỉnh, thành phố của thuê bao
Quốc gia (C)	Tên quốc gia của thuê bao
Mã định danh của thuê	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 chữ ký số do SMARTSIGN 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 chữ ký số
Bộ phận tổ chức (OU)	Bộ phận thuộc tổ chức (O) mà thuê bao sở hữu chứng thư chữ ký số trực thuộc.
Tỉnh, thành phố (S)	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 chữ ký 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 chữ ký số

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

Thuộc tính	**Giá trị**
Tỉnh, thành phố (S)	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 chữ ký 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 chữ ký số

DN trong chứng thư chữ ký 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 chữ ký 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 chữ ký số.

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

Chứng thư chữ ký 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 chữ ký số chỉ được thực hiện khi có yêu cầu của pháp luật. Khi này, nội dung tên sẽ không phải kiểm tra.

3.1.3. Ẩn danh hoặc bút danh

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

3.1.4. Quy tắc diễn giải các hình thức tên khác nhau

Không quy định.

3.1.5. Tính duy nhất của tên

Tên thuê bao được nêu ra trong chứng thư chữ ký số phải rõ ràng và duy nhất với toàn bộ các chứng thư chữ ký số do CA phát hành phát hành, 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 chữ ký 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 chữ ký 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 chữ ký số chỉ được chấp nhận khi có yêu cầu của pháp luật và cần có giải trình với SMARTSIGN để xem xét.

Chấp nhận, xác thực và vai trò của nhãn hiệu đăng ký (TradeMarks): thuê bao đăng ký xin cấp chứng thư chữ ký 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 có quyền thu hồi, tạm dừng chứng thư chữ ký số hay loại bỏ hồ sơ đề nghị phát hành chứng thư chữ ký số mà không phải chịu trách nhiệm pháp lý.

3.1.6. Nhận diện, xác thực và vai trò của nhãn hiệu

Đối tượng đăng ký chứng thư chữ ký số không được sử dụng các tên đã được bảo hộ quyền sở hữu trí tuệ cho đối tượng khác theo quy định của pháp luật về sở hữu trí tuệ.

SMARTSIGN không chịu trách nhiệm về mọi tranh chấp về quyền sở hữu trí tuệ phát sinh liên quan đến việc sử dụng tên của đối tượng đăng ký chứng thư chữ ký số.

3.2. Xác minh đề nghị phát hành chứng thư chữ ký số

3.2.1. Phương thức chứng minh quyền sở hữu khóa bí mật

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

Tệp tin đề nghị cấp chứng thư chữ ký số mã hóa theo chuẩn PKCS#10 sinh thiết bị phần cứng đạt chuẩn FIPS 140-2 Level 2 trở lên, hoặc tương đương do thuê bao thực hiện;

Hoặc thuê bao ủy quyền cho SMARTSIGN, SMARTSIGN sinh khóa theo ủy quyền của thuê bao sử dụng thiết bị phần cứng đạt chuẩn FIPS 140-2 Level 2 trở

lên. Theo quy trình, SMARTSIGN 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. Xác minh danh tính đối với tổ chức

Khi có một đề nghị cấp chứng thư chữ ký số nhận dạng cho tổ chức, thông tin nhận dạng của tổ chức đó được SMARTSIGN xác minh các thông tin bắt buộc dựa trên hồ sơ đề nghị phát hành chứng thư chữ ký số công cộng theo quy định pháp luật như sau:

- Giấy đề nghị phát hành chứng thư chữ ký số công cộng dưới dạng bản giấy hoặc điện tử theo mẫu của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.

- Tài liệu kèm theo bao gồm: quyết định thành lập hoặc quyết định quy định về chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức hoặc giấy chứng nhận đăng ký doanh nghiệp hoặc giấy chứng nhận đầu tư hoặc giấy chứng nhận đăng ký hộ kinh doanh và giấy tờ tùy thân của người đại diện theo pháp luật của tổ chức, bao gôm thẻ căn cước công dân hoặc thẻ căn cước hoặc giấy chứng nhận căn cước hoặc tài khoản định danh điện tử mức độ 2 hoặc hộ chiếu; hoặc tài khoản định danh điện tử của tổ chức.

Tổ chức có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc nộp bản sao kèm bản chính để đối chiếu hoặc sử dụng tài khoản định danh điện tử mức độ 2 theo quy định của pháp luật về định danh và xác thực điện tử.

Thuê bao có thể thực hiện cung cấp giấy tờ theo 02 phương thức gồm:

- Hồ sơ giấy: Thuê bao đến trực tiếp làm thủ tục tại các địa điểm cung cấp dịch vụ của Công ty hoặc Nhân viên thuộc các kênh bán hàng hợp pháp của Công ty đến địa điểm của Thuê bao thu hồ sơ. Đối với các giấy tờ kèm theo, thuê bao có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc nộp bản sao xuất trình kèm bản chính để đối chiếu.

- Hồ sơ điện tử: Thuê bao thực hiện quy trình đăng ký và xác thực theo Quy trình và giải pháp cấp chứng thư chữ ký số bằng phương thức điện tử do Công ty cung cấp.

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

3.2.3. Xác minh danh tính đối với cá nhân

Khi có một đề nghị cấp chứng thư chữ ký số nhận dạng cho cá nhân, thông tin nhận dạng của cá nhân sẽ được SMARTSIGN xác minh các thông tin bắt buộc dựa trên hồ sơ đề nghị phát hành chứng thư chữ ký số công cộng theo quy định pháp luật như sau:

- Giấy đề nghị phát hành chứng thư chữ ký số công cộng dưới dạng bản giấy hoặc điện tử theo mẫu của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.

- Thẻ căn cước công dân hoặc thẻ căn cước hoặc căn cước điện tử hoặc giấy chứng nhận căn cước hoặc tài khoản định danh điện tử mức độ 2 hoặc hộ chiếu còn thời hạn; thị thực nhập cảnh còn thời hạn hoặc giấy tờ chứng minh được miễn thị thực nhập cảnh (đối với cá nhân là người nước ngoài).

Thuê bao có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc nộp bản sao kèm bản chính để đối chiếu hoặc sử dụng tài khoản định danh điện tử mức độ 2 theo quy định của pháp luật về định danh và xác thực điện tử.

Thuê bao có thể thực hiện cung cấp giấy tờ theo 02 phương thức gồm:

- Hồ sơ giấy: Thuê bao đến trực tiếp làm thủ tục tại các địa điểm cung cấp dịch vụ của Công ty hoặc Nhân viên thuộc các kênh bán hàng hợp pháp của Công ty đến địa điểm của Thuê bao thu hồ sơ. Đối với các giấy tờ kèm theo, thuê bao có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc nộp bản sao xuất trình kèm bản chính để đối chiếu.

- Hồ sơ điện tử: Thuê bao thực hiện quy trình đăng ký và xác thực theo Quy trình và giải pháp cấp chứng thư chữ ký số bằng phương thức điện tử do Công ty cung cấp.

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

3.2.4. Thông tin không được xác minh

Không quy định.

3.2.5. Xác minh thẩm quyền

Khi chứng thư chữ ký 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 3.2.2.

- Xác thực cá nhân như 3.2.3 và xác thực sự ủy quyền của tổ chức đối với cá nhân đó bằng giấy ủy quyền. Trong một số trường hợp cần làm rõ, SMARTSIGN sẽ xác thực bổ sung bằng cách gọi điện hoặc xác thực trực tiếp tại tổ chức về cá nhân đó.

3.2.6. Tiêu chí liên thông

Không quy định.

3.3. Xác minh đề nghị thay đổi cặp khóa

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

3.3.1. Xác minh danh tính và xác thực đối với yêu cầu thay đổi cặp khóa định kỳ

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

Để chấp thuận yêu cầu thay đổi cặp khóa của thuê bao, RA phải nhận dạng và xác nhận các thông tin thuê bao đưa ra là chính xác và không thay đổi. Sau khi cấp lại khóa CA hoặc RA của SMARTSIGN sẽ xác nhận lại việc nhận dạng và xác thực thuê bao sao cho phù hợp với các yêu cầu của hồ sơ đề nghị phát hành chứng thư chữ ký số ban đầu.

SMARTSIGN hoặc RA có trách nhiệm xác thực yêu cầu thay đổi cặp khóa của thuê bao sau khi nhận đơn đề nghị thay đổi cặp khóa. SMARTSIGN 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 chữ ký số của mình để gửi yêu cầu đề nghị thay đổi cặp khóa lên SMARTSIGN, khi thuê

bao yêu cầu thay đổi cặp khóa chứng thư chữ ký số yêu cầu này ngay lập tức được SMARTSIGN chấp nhận.

- Sử dụng phương pháp xác thực: thuê bao phải trả lời đúng toàn bộ các câu hỏi xác thực để được SMARTSIGN chấp nhận yêu cầu đề nghị thay đổi cặp khóa.

Sau khi xác thực, SMARTSIGN ban hành ngay chứng thư chữ ký số mới cho thuê bao.

Sau khi ban hành chứng thư chữ ký số mới cho thuê bao, SMARTSIGN hoặc RA xác minh lại nhận dạng của đối tượng yêu cầu thay đổi cặp khóa và các thông tin liên quan:

SMARTSIGN 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 chữ ký số. SMARTSIGN 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.

3.3.2. Xác minh danh tính và xác thực đối với yêu cầu thay đổi cặp khóa sau khi thu hồi

Chứng thư chữ ký 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 chữ ký số

SMARTSIGN tiến hành kiểm tra và xác thực lại yêu cầu thu hồi chứng thư chữ ký số như sau. Quy trình xác thực bao gồm:

- Tiếp nhận yêu cầu thu hồi thông qua các kênh liên lạc hoặc gặp trực tiếp.
- Thông báo cho thuê bao về lý do thu hồi. Nếu yêu cầu thu hồi từ cơ quan có thẩm quyền thì đính kèm văn bản thông báo.
- Kiểm tra xác nhận khách hàng sau đó tiến hành thu hồi chứng thư.

4. Các yêu cầu đối với vòng đời hoạt động của chứng thư chữ ký số

4.1. Yêu cầu đề nghị phát hành chứng thư chữ ký số

4.1.1. Đối tượng đề nghị phát hành chứng thư chữ ký số

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

- 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 chữ ký 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 chữ ký số.

- Các đại lý đăng ký làm RA cho SMARTSIGN.

4.1.2. Trách nhiệm và quy trình đăng ký

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 đề nghị phát hành chứng thư chữ ký số

4.2.1. Thực hiện chức năng xác minh danh tính và xác thực

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

4.2.2. Phê duyệt hoặc từ chối hồ sơ đề nghị phát hành chứng thư chữ ký số

SMARTSIGN 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 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 chưa nhận được đầy đủ phí từ người đăng ký

- Chứng thư chữ ký 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.

4.2.3. Thời gian xử lý hồ sơ đề nghị phát hành chứng thư chữ ký số

SMARTSIGN có trách nhiệm xử lý các hồ sơ đề nghị phát hành chứng thư chữ ký số trong khoảng thời gian phù hợp. Không có quy định thời gian hoàn thành quá trình xử lý một hồ sơ đề nghị phát hành chứng thư chữ ký số trừ khi được đưa ra trong hợp đồng với thuê bao hoặc thỏa thuận giữa các bên.

4.3. Phát hành chứng thư chữ ký số

4.3.1. Quy trình phát hành chứng thư chữ ký số

Hồ sơ đề nghị phát hành chứng thư chữ ký số phải được SMARTSIGN phê duyệt trước khi phát hành chứng thư chữ ký số.

Chứng thư chữ ký số sẽ được phát hành sau khi SMARTSIGN chấp nhận hồ sơ đề nghị phát hành chứng thư chữ ký số.

SMARTSIGN tạo cho thuê bao một chứng thư chữ ký số dựa vào những thông tin trong hồ sơ đề nghị phát hành chứng thư chữ ký số và yêu cầu cấp chứng thư chữ ký số.

4.3.2. Thông báo việc phát hành chứng thư chữ ký số

SMARTSIGN phát hành chứng thư chữ ký số trực tiếp tới thuê bao hoặc thông qua RA. SMARTSIGN thông báo cho thuê bao rằng chứng thư chữ ký số của họ đã được tạo đồng thời cung cấp cho thuê bao quyền truy cập tới chứng thư đó để kiểm tra tính sẵn sàng của chứng thư. Chứng thư có hiệu lực sẽ cho phép thuê bao tải về từ website hoặc thông qua LDAP server.

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

SMARTSIGN tạo chứng thư chữ ký số và gửi chứng thư chữ ký số cho Token Manager để cập nhật vào thiết bị Token.

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

Nếu thông tin trong chứng thư chữ ký số không phù hợp, người dùng thông báo lại cho đại lý hoặc RA của SMARTSIGN 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, 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 chữ ký số tối đa 24 giờ.

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

4.4.1. Xác nhận các thông tin trên chứng thư chữ ký số được cấp là chính xác

Khi thuê bao nhận chứng thư chữ ký số và khóa bí mật lưu trong thiết bị lưu trữ (Token) từ thông báo của SMARTSIGN, 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 từ chối chứng thư và giải thích lý do từ chối. Trong vòng một ngày thuê bao không trả lời thông báo của SMARTSIGN, chứng thư chữ ký số đó coi như được khách hàng chấp nhận.

4.4.2. Công bố chứng thư chữ ký số theo quy định

Sau khi nhận được chấp nhận chứng thư, SMARTSIGN công bố chứng thư chữ ký số đã phát hành, SMARTSIGN 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 chữ ký số được coi là chính thức chấp nhận khi được SMARTSIGN công bố trên website, kho dữ liệu chứng thư chữ ký số. SMARTSIGN công bố chứng thư chữ ký 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 đến các đối tượng khác về việc phát hành chứng thư chữ ký số

SMARTSIGN 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 khóa và chứng thư chữ ký số

4.5.1. Sử dụng khóa bí mật và chứng thư chữ ký số

Chứng thư chữ ký số và khóa bí mật tương ứng được phép sử dụng nếu thuê bao đã đồng ý thỏa thuận với SMARTSIGN và đã chấp nhận chứng thư chữ ký số được ban hành.

Chứng thư chữ ký số phát hành bởi SMARTSIGN và khóa bí mật tương ứng với khóa công khai trong chứng thư cần được sử dụng hợp pháp theo bản thỏa 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 chữ ký số phải nhất quán với phạm vi sử dụng được phép của chứng thư chữ ký số đó (quy định trong trường KeyUsage trong chứng thư chữ ký số). Ví dụ, nếu không có chức năng "Digital Signature" thì chứng thư chữ ký số đó không được sử dụng để ký điện tử.

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

4.5.2. Sử dụng khóa công khai và chứng thư chữ ký số bởi các bên tin cậy

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

- Kiểm tra có đúng chứng thư chữ ký số do SMARTSIGN phát hành;
- Kiểm tra chứng thư chữ ký số chưa bị thu hồi;
- Chứng thư chữ ký 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.

4.6. Gia hạn chứng thư chữ ký số

4.6.1. Các trường hợp được gia hạn chứng thư chữ ký số

Gia hạn chứng thư là việc phát hành chứng thư chữ ký số mới tới thuê bao mà không thay đổi khóa công khai hay bất kỳ một thông tin nào khác trong chứng

thư. Các chứng thư của SMARTSIGN sẽ không được gia hạn với cặp khóa tương tự khi chúng sắp hết hạn.

4.6.2. Đối tượng có thể yêu cầu gia hạn chứng thư chữ ký số

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 công bố trên website có ký xác nhận của chủ thuê bao.

4.6.3. Xử lý yêu cầu gia hạn chứng thư chữ ký số

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 chữ ký số mới của thuê bao sẽ được ban hành ngay sau khi SMARTSIGN nhận được yêu cầu mà không cần có sự hiện diện vật lý của thuê bao tại SMARTSIGN hoặc RA.

4.6.4. Thông báo việc gia hạn chứng thư chữ ký số

Tương tự 4.3

4.6.5. Xác nhận đối với chứng thư chữ ký số được gia hạn

Tương tự 4.4.1

4.6.6. Công bố chứng thư chữ ký số đã được gia hạn

Tương tự 4.4.2

4.6.7. Thông báo chứng thư chữ ký số được gia hạn đến các đối tượng khác

Tương tự 4.4.3

4.7. Thay đổi cặp khóa

4.7.1. Các trường hợp được thay đổi cặp khóa

- Thuê bao có nhu cầu có thể yêu cầu thay đổi cặp khóa

- SMARTSIGN khi phát hiện dấu hiệu nghi ngờ bị lộ cặp khóa sẽ đề nghị thuê bao thay đổi cặp khóa.

4.7.2. Đối tượng được gửi yêu cầu thay đổi cặp khóa

Chủ sở hữu chứng thư chữ ký số mới có quyền gửi yêu cầu thay đổi cặp khóa.

4.7.3. Xử lý yêu cầu thay đổi cặp khóa

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 chữ ký số mới.

4.7.4. Thông báo cập nhật chứng thư chữ ký số sau khi thay đổi cặp khóa

Tương tự 4.3.2

4.7.5. Xác nhận đối với chứng thư chữ ký số được cập nhật

Tương tự 4.4.1

4.7.6. Công bố chứng thư chữ ký số được cập nhật sau khi thay đổi cặp khóa

Tương tự 4.4.2

4.7.7. Thông báo chứng thư chữ ký số được cập nhật sau khi thay đổi cặp khóa đến các đối tượng khác

Tương tự 4.4.3

4.8. Thay đổi thông tin chứng thư chữ ký số

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

Khi thông tin chứng thư chữ ký số cần thay đổi, trừ những trường hợp đã nêu trong 4.6 và 4.7.

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

- Thay đổi tên chủ thể trên thuê bao chứng thư chữ ký số được xác nhận bởi cơ quan chức nâng.

Thay đổi tỉnh/thành phố nơi ở, trụ sở đăng ký.

- Thay đổi loại mã, mã thuê bao

Sáp nhập tổ chức, mã căn cước với chủ thể là cá nhân.

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

4.8.2. Đối tượng được gửi yêu cầu thay đổi thông tin chứng thư chữ ký số

Chủ thế chứng thư chữ ký số.

Đại diện của tổ chức trên chứng thư chữ ký số.

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

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

4.8.4. Thông báo cập nhật chứng thư chữ ký số

Tương tự 4.3

4.8.5. Xác nhận đối với chứng thư chữ ký số được cập nhật

Tương tự 4.4.1

4.8.6. Công bố chứng thư chữ ký số được cập nhật sau khi thay đổi thông tin

Tương tự 4.4.2

4.8.7. Thông báo chứng thư chữ ký số được cập nhật sau khi thay đổi thông tin đến các đối tượng khác

Tương tự 4.4.3

4.9. Tạm dừng, phục hồi và thu hồi chứng thư chữ ký số

4.9.1. Các trường hợp được phép thu hồi chứng thư chữ ký số

- Khi thuê bao yêu cầu bằng văn bản và yêu cầu này được SMARTSIGN xác minh là chính xác.

- Khi SMARTSIGN có căn cứ khẳng định chứng thư chữ ký số được cấp không tuân theo các quy định trong quy chế chứng thực SMARTSIGN đưa ra hoặc khi phát hiện sai sót có ảnh hưởng tới quyền lợi của Thuê Bao và người nhận.

- Theo điều kiện thu hồi chứng thư chữ ký số được quy định trong hợp đồng giữa thuê bao và SMARTSIGN.

- Khi thuê bao là cá nhân đã chết hoặc mất tích theo tuyên bố của tòa án hoặc thuê bao là tổ chức giải thế hoặc phá sản theo quy định của pháp luật.

- Khóa bí mật của thuê bao có chứng thư chữ ký số bị lộ.

- Chứng thư chữ ký số đã được tạo ra không tuân theo những thủ tục được yêu cầu bởi quy chế chứng thực này

- Chứng thư chữ ký số được sử dụng sai mục đích, với mục đích bị cấm hoặc với các mục đích gây ảnh hưởng không tốt tới SMARTSIGN-CA.

- Khi có yêu cầu của cơ quan tiến hành tố tụng, cơ quan công an hoặc Bộ Khoa học và Công nghệ.

4.9.2. Đối tượng được phép yêu cầu thu hồi chứng thư chữ ký số

- Chủ sở hữu chứng thư chữ ký số.

- SMARTSIGN hay bất kỳ một RA đã chứng minh khóa bị lộ.

- Các cơ quan có thẩm quyền.

- Theo yêu cầu của Pháp luật.

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

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. Trước khi thu hồi chứng thư SMARTSIGN 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 chữ ký số của mình, SMARTSIGN sẽ tạm dừng chứng thư chữ ký 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 chữ ký 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 mới chính thức thu hồi và công bố thông tin thu hồi chứng thư chữ ký số.

- Xác minh quyết định yêu cầu thu hồi chứng thư chữ ký số của đơn vị có thẩm quyền.

- Nếu SMARTSIGN có đủ cơ sở để xác minh khách hàng bị lộ khóa bí mật gây mất an toàn, SMARTSIGN 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 hạn gia hạn yêu cầu thu hồi chứng thư chữ ký số

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

4.9.5. Thời gian phải xử lý yêu cầu thu hồi chứng thư chữ ký số

SMARTSIGN sẽ 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 chữ ký số sẽ được tạm dừng.

4.9.6. Yêu cầu kiểm tra trạng thái thu hồi chứng thư chữ ký số đối với các bên tin cậy

Trước khi sử dụng một chứng thư chữ ký số, bên nhận phải xác nhận CRL gần đây nhất. SMARTSIGN 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 suất công bố danh sách thu hồi chứng thư chữ ký số (CRL) (nếu áp dụng)

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

4.9.8. Độ trễ công bố CRL (nếu áp dụng)

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

4.9.9. Kiểm tra trạng thái/thu hồi chứng thư chữ ký số trực tuyến

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

4.9.10. Yêu cầu kiểm tra trạng thái thu hồi chứng thư chữ ký số trực tuyến

Thông qua OCSP Response.

4.9.11. Các hình thức thông báo thu hồi khác

Không sử dụng.

4.9.12. Yêu cầu đặc biệt liên quan đến thay đổi cặp khóa

Không quy định.

4.9.13. Các trường hợp được phép tạm dừng, phục hồi chứng thư chữ ký số

- Khi thuê bao yêu cầu bằng văn bản và yêu cầu này đã được tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng xác minh là chính xác;

- Khi phát hiện có rủi ro, sai lệch hoặc có dấu hiệu bất thường giữa các thông tin nhận biết tổ chức, cá nhân với các yếu tố sinh trắc học của tổ chức, cá nhân hoặc phát hiện giao dịch đáng ngờ trong quá trình ký số hoặc khi phát hiện ra bất cứ sai sót nào có ảnh hưởng đến quyền lợi của thuê bao và người nhận;

- Khi thuê bao là tổ chức tạm ngừng toàn bộ hoạt động kinh doanh;

- Khi có yêu cầu bằng văn bản của cơ quan tiến hành tố tụng, cơ quan công an hoặc Bộ Khoa học và Công nghệ;

- Theo điều kiện tạm dừng chứng thư chữ ký số công cộng đã được quy định trong hợp đồng giữa thuê bao và tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.

4.9.14. Đối tượng được phép yêu cầu tạm dừng, phục hồi chứng thư chữ ký số

- Chủ sở hữu chứng thư chữ ký số.

- SMARTSIGN hay bất kỳ một RA đã chứng minh khóa bị lộ.

- Các cơ quan có thẩm quyền.

- Theo yêu cầu của Pháp luật.

4.9.15. Quy trình, thủ tục yêu cầu tạm dừng, phục hồi chứng thư chữ ký số

Trường hợp thuê bao yêu cầu tạm dừng:

- Thuê bao: Ký phiếu đề nghị tạm dừng chứng thư tới nhà cung cấp dịch vụ với chữ ký hoặc con dấu hợp pháp của chủ thể.

- SMARTSIGN và SMARTSIGN-RA: Tiếp nhận và tạo phiếu yêu cầu tạm dừng.

- SMARTSIGN Thực hiện kiểm tra và duyệt phiếu yêu cầu tạm dừng chứng thư chữ ký số của thuê bao. Nếu hợp lệ, SMARTSIGN sẽ tiến hành tạm dừng chứng thư của thuê bao.

- SMARTSIGN có trách nhiệm cập nhật thông tin trên kho lưu trữ của dịch vụ về chứng thư đã bị tạm dừng.

- SMARTSIGN gửi thông báo về việc tạm dừng trực tiếp cho thuê bao hoặc thông qua SMARTSIGN-RA quản lý trực tiếp.

Trường hợp SMARTSIGN hoặc Cơ quan quản lý nhà nước có thẩm quyền yêu cầu tạm dừng:

- SMARTSIGN và SMARTSIGN-RA: Tiếp nhận và tạo phiếu yêu cầu tạm dừng.

- SMARTSIGN tiến hành xác minh và xác thực chính xác thông tin yêu cầu tạm dừng chứng thư từ phía đối tượng gửi đơn tạm dừng. Nếu hợp lệ, SMARTSIGN sẽ tiến hành tạm dừng chứng thư của thuê bao.

- SMARTSIGN có trách nhiệm cập nhật thông tin trên kho lưu trữ của dịch vụ về chứng thư đã bị tạm dừng.

- SMARTSIGN gửi thông báo về việc tạm dừng trực tiếp cho thuê bao hoặc thông qua SMARTSIGN-RA quản lý trực tiếp.

4.9.16. Giới hạn thời gian tạm dừng, phục hồi chứng thư chữ ký số

Ngay sau khi kết thúc thẩm định yêu cầu.

4.10. Kiểm tra trạng thái chứng thư chữ ký số

4.10.1. Các hình thức kiểm tra trạng thái chứng thư chữ ký số

Các chứng thư được lưu trữ trong kho công cộng của SMARTSIGN và được đặt luôn sẵn sàng qua CRL, website, thư mục LDAP và OCSP:

- Chứng thư của SMARTSIGN.

- Chứng thư cấp bởi SMARTSIGN.

- Danh sách thu hồi cập nhật mới nhất.

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

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

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

Thời hạn sử dụng của chứng thư chữ ký số được chỉ rõ trong chứng thư chữ ký 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 chữ ký số hết hạn mà không gia hạn;
- Yêu cầu thu hồi trước thời hạn.

4.12. Lưu trữ và phục hồi khóa

4.12.1. Chính sách và thực tiễn việc lưu trữ và phục hồi khóa

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

4.12.2. Chính sách và thực tiễn việc mã hóa và phục hồi khóa phiên

Không quy định.

5. Kiểm soát, quản lý và vận hành

5.1. Kiểm soát an toàn, an ninh vật lý

5.1.1. Vị trí đặt và xây dựng hệ thống

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

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 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 hòa 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 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 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 ngừa và bảo vệ chống cháy

SMARTSIGN 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. Xử lý rác

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

5.1.8. Hệ thống dự phòng

SMARTSIGN đang duy trì hai hệ thống đó là hệ thống SMARTSIGN chính và hệ thống SMARTSIGN 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 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. Kiểm soát quy trình

5.2.1. Các vai trò 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 hồ sơ đề nghị phát hành chứng thư chữ ký số.
- Việc chấp nhận, loại bỏ, hay các xử lý khác đối với hồ sơ đề nghị phát hành chứng thư chữ ký số, yêu cầu thu hồi, làm mới, hay thông tin đăng ký.
- Việc ban hành, thu hồi chứng thư chữ ký 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 phát hành chứng thư chữ ký số và bộ phận phụ trách phát hành chứng thư chữ ký 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 cần thiết cho mỗi công việc

SMARTSIGN 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 khóa, 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. Định danh 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:

- Có trong danh sách truy cập tới các vị trí CA;
- Có trong danh sách truy cập đến hệ thống CA;
- Được cung cấp một chứng thư chữ ký số để thực hiện nhiệm vụ CA;
- 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 đều phải được xác minh nhân thân, nhận dạng và trình độ.

SMARTSIGN 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, trách nhiệm của từng thành viên

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

- Xác thực thông tin trong hồ sơ đề nghị phát hành chứng thư chữ ký số.

- Quá trình chấp nhận, từ chối, hoặc các quá trình khác của hồ sơ đề nghị phát hành chứng thư chữ ký số, 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 chữ ký số.

5.3. Kiểm soát nhân sự

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

SMARTSIGN 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 có kinh nghiệm tối thiểu 02 năm tương ứng với ngành được đào tạo.

5.3.2. Quy trình kiểm tra lý lịch

Trước khi nhân viên bắt đầu việc làm trong một vai trò được tin cậy, SMARTSIGN 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 cho cán bộ vận hành, quản lý hệ thống

SMARTSIGN 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;

- Các phiên bản phần cứng phần mềm được sử dụng và các thức vận hành hệ thống CA;

Báo cáo, chuyển giao các thỏa hiệp và các vấn đề liên quan;

Thủ tục khôi phục sau thảm họa và duy trì công việc.

5.3.4. Tần suất và yêu cầu đào tạo lại

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

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

5.3.5. Tần suất và trình tự luân chuyển công việc

Không quy định cụ thể về tần suất luân chuyển công việc

5.3.6. Các hình thức xử lý đối với hành động không được phép

SMARTSIGN 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.

5.3.7. Yêu cầu đối với 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 ở vị trí tương đương.

5.3.8. Cung cấp tài liệu cho nhân sự

SMARTSIGN 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 sự kiện được ghi lại

SMARTSIGN 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 tất cả các máy chủ (CA, RA, OCSP, CRL, LDAP, cơ sở dữ liệu):

- Hành động truy cập, đăng nhập, đăng xuất;
- Tạo, xóa mật khẩu hoặc thay đổi đặc quyền người dùng; bật/tắt hệ thống và ứng dụng; lỗi ứng dụng, dịch vụ; bảo trì, thay đổi cấu hình hệ thống;

Bổ sung riêng theo từng loại máy chủ:

- Máy chủ CA: tạo khóa CA, thay đổi khóa CA; các sự kiện liên quan đến cấp chứng thư chữ ký số;
- Máy chủ RA: lỗi đọc/ghi chứng thư và kho lưu trữ; các sự kiện vòng đời chứng thư (cấp mới, gia hạn, thu hồi);
- Máy chủ OCSP: sự kiện kiểm tra trạng thái chứng thư chữ ký số; Máy chủ LDAP: sự kiện cấp chứng thư chữ ký số mới.

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 nhật ký hệ thống

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 lưu giữ nhật ký hệ thống

Khoảng thời gian lưu giữ tối thiểu đối với các bản ghi kiểm toán là 05 năm.

5.4.4. Bảo vệ nhật ký hệ thống

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. Quy trình sao lưu nhật ký hệ thống

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

5.4.6. Hệ thống thu thập nhật ký hệ thống (nội bộ so với bên ngoài)

SMARTSIGN triển khai hệ thống giám sát và thu thập nhật ký tập trung (hệ thống giám sát Zabbix) để thu thập nhật ký và các chỉ số hoạt động từ toàn bộ máy chủ (CA, RA, OCSP, CRL, LDAP, cơ sở dữ liệu) và thiết bị mạng thông qua các agent giám sát cài đặt trên từng máy chủ. Toàn bộ nhật ký được thu thập, lưu trữ tập trung trên hệ thống nội bộ, tách biệt với máy chủ vận hành, không chia sẻ hay chuyển giao cho bên ngoài, trừ trường hợp có yêu cầu bằng văn bản của cơ quan nhà nước có thẩm quyền theo quy định pháp luật.

5.4.7. Thông báo cho đối tượng gây ra sự kiện

Khi hệ thống giám sát phát hiện sự kiện bất thường mang tính kỹ thuật (vượt ngưỡng lưu lượng mạng, lỗi thiết bị, lỗi cơ sở dữ liệu, sự cố phần cứng...), hệ thống tự động gửi cảnh báo qua email đến quản trị viên phụ trách để xử lý kịp thời, không cần thông báo cho đối tượng bên ngoài gây ra sự kiện. Đối với sự kiện phát sinh từ hành vi vi phạm của một đối tượng cụ thể (thuê bao, đại lý, nhân viên), SMARTSIGN thông báo trực tiếp bằng văn bản hoặc qua kênh liên lạc đã đăng ký, yêu cầu giải trình trong thời hạn phù hợp trước khi áp dụng biện pháp xử lý tương ứng (tạm dừng, thu hồi quyền truy cập, chấm dứt hợp đồng...).

5.4.8. Đánh giá lỗ hổng bảo mật

SMARTSIGN triển khai hệ thống tường lửa (Firewall) phân vùng mạng theo chức năng (vùng DMZ cho các dịch vụ công khai như OCSP, LDAP; vùng CA Zone được cách ly, chặn toàn bộ truy cập trực tiếp từ bên ngoài) kết hợp hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS) để giám sát liên tục, phát hiện sớm các dấu hiệu tấn công, xâm nhập trái phép hoặc lỗ hổng có thể bị khai thác. SMARTSIGN định kỳ rà soát, đánh giá rủi ro an toàn thông tin đối với hạ tầng, phần mềm CA/RA/OCSP/CRL/LDAP và cơ sở dữ liệu; kết quả đánh giá là căn cứ xây dựng phương án khắc phục, vá lỗi và cập nhật hệ thống kịp thời.

5.5. Lưu trữ các bản ghi

5.5.1. Các loại bản ghi được lưu trữ

Xem 5.4.1.

5.5.2. Thời hạn lưu trữ bản ghi

Khoảng thời gian lưu giữ tối thiểu là 05 năm.

5.5.3. Bảo vệ bản ghi

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

5.5.4. Quy trình sao lưu bản ghi

Dữ liệu lưu trữ được backup theo chế độ backup chung của SMARTSIGN

5.5.5. Yêu cầu về gắn dấu thời gian cho bản ghi

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

5.5.6. Hệ thống thu thập bản ghi (nội bộ so với bên ngoài)

Các lưu trữ sẽ được lưu trữ tập trung trên hệ thống của SMARTSIGN và được bảo vệ với mức độ an toàn tốt nhất.

5.5.7. Quy trình truy cập và xác minh thông tin bản ghi

Tất cả chứng thư chữ ký số được cấp bởi SMARTSIGN 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.

Tính toàn vẹn lưu trữ thông tin của SMARTSIGN 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 cặp khóa

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

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

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

Trước khi hết hạn chứng thư chữ ký số của SMARTSIGN, 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. Quá trình chuyển tiếp khóa của SMARTSIGN đảm bảo rằng:

- SMARTSIGN chỉ ban hành chứng thư chữ ký 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 chữ ký số, theo quy định của pháp luật.

- Khi nhận được yêu cầu ban hành chứng thư chữ ký số sau thời điểm tạm dừng ban hành chứng thư chữ ký số trên, SMARTSIGN sử dụng cặp khóa mới để ban hành chứng thư chữ ký số cho thuê bao.

- CA tiếp tục ký lên CRL bằng cặp khóa cũ đến khi nào hết hạn toàn bộ chứng thư chữ ký số được ban hành bởi cặp khóa cũ.

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

5.7.1. Quy trình xử lý sự cố và thảm họa

Khi có sự cố, các dữ liệu được phục hồi theo các thủ tục được ban hành. Các dữ liệu bao gồm:

- Dữ liệu về thủ tục cấp chứng thư chữ ký số.
- Dữ liệu về nhật ký.
- Các bản ghi chứng thư chữ ký số được tạo ra.

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

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

- Tất cả các phần mềm trên SMARTSIGN 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.

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

SMARTSIGN 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 số 50/2025/TT-BKHCN và QCVN 137:2025/BKHCN về Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số do Bộ Khoa học và Công nghệ ban hành.

5.7.3. Quy trình xử lý khóa bí mật bị xâm phạm

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

Nều khóa bí mật của SMARTSIGN 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 chứng thư của khóa bị xâm hại;
- Khởi tạo một cặp khóa và chứng thư của SMARTSIGN mở và công bố trong kho lưu trữ;
- Thu hồi tất cả các chứng chỉ hợp lệ ký bởi khóa bị xâm hại;

Xuất bản danh sách CRL mới trong kho của SMARTSIGN;

- Thông báo tới cơ quan an ninh liên quan và Trung tâm Chứng thực điện tử Quốc gia;
- Thông báo tới các bên tin cậy, các CA có liên quan.

Khi có sự cố xảy ra, dữ liệu được khôi phục theo đúng các thủ tục đã ban hành. Dữ liệu được khôi phục bao gồm:

- Dữ liệu về thủ tục cấp chứng thư chữ ký số
- Dữ liệu về nhật ký

- Các bản ghi chứng thư chữ ký số được tạo ra

5.7.4. Khả năng phục hồi hoạt động sau thảm họa

SMARTSIGN 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 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 chữ ký số.

b. Ban hành chứng thư chữ ký số.

c. Thu hồi chứng thư chữ ký số.

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

Cơ sở dữ liệu của SMARTSIGN 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 được thiết kế có khả năng phục hồi hoạt động toàn bộ hệ thống trong vòng một tuần.

5.8. Dừng hoạt động cung cấp dịch vụ

Trong trường hợp chấm dứt dịch vụ của mình SMARTSIGN sẽ:

- Thông báo với Bộ Khoa học và Công nghệ và Trung tâm Chứng thực chữ ký số quốc gia để làm các thủ tục chấm dứt cung cấp dịch vụ;
- Bằng tất cả khả năng có thể để thông báo cho các thuê bao và RA càng sớm càng tốt;
- Thông báo việc chấm dứt trên diện rộng;
- Ngừng cấp chứng thư chữ ký số;
- Thu hồi tất cả các chứng thư chữ ký số;
- Tiêu huỷ tất cả các bản sao khóa bí mật của SMARTSIGN.

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

Cặp khóa cho SMARTSIGN được tạo ra bởi các nhân viên thẩm quyền chứng thực trên máy tính không kết nối vào mạng. Cặp khóa này được sinh trực tiếp bên trong thiết bị HSM đạt chuẩn FIPS 140-2 Level 3 và có chứng nhận hợp quy theo QCVN 137:2025/BKHCN 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.

Việc tạo cặp khóa CA được thực hiện trực tiếp trên thiết bị HSM với sự tham gia đồng thời của tối thiểu hai quản trị viên hệ thống, sau khi thực hiện đầy đủ quy trình kiểm soát truy cập vật lý và truy cập quản trị HSM. Quản trị viên sử dụng công cụ quản lý khóa chuyên dụng của nền tảng CA (PKCS11 HSM Key Tool) để sinh cặp khóa theo thuật toán RSA, bao gồm khóa mặc định (2048 bit) và khóa ký (2048 bit) phục vụ hoạt động ký số của hệ thống.

Đối với cặp khóa của thuê bao sinh tại nhà cung cấp dịch vụ. SMARTSIGN sử dụng thiết bị chuyên dụng HSM của máy chủ thực hiện khởi tạo và quản lý cặp khóa với thuật toán mã hoá phi đối xứng RSA hoặc cặp khóa được sinh ngay trong phần cứng của thiết bị đầu cuối của thuê bao (Token) đạt chuẩn FIPS 140-2 Level 2 trở lên. Mỗi cặp khóa đảm bảo được tính duy nhất và không bị suy ra khóa bí mật từ khóa công khai tương ứng. Việc phân phối khóa đến thuê bao được thực hiện bằng thiết bị lưu trữ thông minh, đảm bảo an toàn bảo mật tuyệt đối trong việc phân phối khóa.

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

6.1.2. Chuyển giao khóa bí mật

Thiết bị phần cứng Token sẽ sinh cặp khóa (bao gồm private key và public key). Chứng thư chữ ký 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 chữ ký 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 khóa công khai cho tổ chức phát hành chứng thư chữ ký số

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

6.1.4. Chuyển giao khóa công khai của tổ chức phát hành chứng thư chữ ký số cho bên tin cậy

Chứng thư chữ ký số của CA (có chứa khóa 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 khóa

Chuẩn hiện tại của dịch vụ SMARTSIGN yêu cầu chiều dài của cặp khóa để đảm bảo mức độ mã hoá đủ mạnh là tối thiểu 2048 bits RSA (theo QCVN 137:2025/BKHCN).

Khoá của SMARTSIGN có chiều dài là 2048 bits.

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

Không quy định.

6.1.7. Mục đích sử dụng khóa

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, mô-đun mật mã

6.2.1. Tiêu chuẩn và kiểm soát đối với mô-đun mật mã

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

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

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

Các thiết bị HSM này tuân theo chuẩn FIPS PUB 140-2 level 3.

Đối với thuê bao thiết bị phần cứng sử dụng chuẩn FIPS 140-2 Level 2.

6.2.2. Kiểm soát đa bên đối với khóa bí mật (n out of m)

Cơ chế kiểm soát khóa bí mật được SMARTSIGN 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 đang sử dụng cơ chế N = 3;

6.2.3. Chuyển giao khóa bí mật

Khóa bí mật của CA không được phép chuyển giao.

6.2.4. Dự phòng khóa bí mật

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

Các thuê bao chịu trách nhiệm sao lưu dự phòng khóa bí mật của họ. SMARTSIGN không sao lưu khóa bí mật của thuê bao trừ các tường hợp có văn bản ủy quyền giữa thuê bào và SMARTSIGN..

6.2.5. Lưu trữ khóa bí mật

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

6.2.6. Chuyển khóa bí mật vào hoặc ra khỏi mô-đun mật mã

Hiện nay SMARTSIGN sao lưu khóa từ HSM vào thiết bị lưu khóa chuyên dụng của HSM đó, trong quá trình sao lưu thì HSM đã mã hóa dữ liệu. Khóa từ

thiết bị lưu khóa chuyên dụng 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 khóa bí mật. Việc chuyền giao này sẽ bị giới hạn để tạo ra các bản sao dự phòng khóa bí mật trên mô đun phần cứng phù hợp với tiêu chuẩn quy định trong chính sách bảo mật của SMARTSIGN. Công việc này để đề phòng khi HSM chính bị hư hỏng vật lý, hoặc do thiên tai thảm họa sảy ra thì còn có HSM dự phòng hoặc thiết bị lưu khóa chuyên dụng đã được sao lưu khóa bí mật.

Với khóa thuê bao, khóa dược lưu trên Token không có cơ chế export hoặc nhân bản đến mô đun mã hóa khác. Thiết bị được chuyển đến khách hàng theo 3 cách:

- Dịch vụ chuyển phát đảm bảo của đại lý trong trường hợp khách hàng ở xa. Khách hàng ký xác nhận với dịch vụ chuyển phát. Sau đó, đại lý gọi điện khách hàng xác minh.

- Khách hàng đến tận đại lý lấy, khách hàng ký biên bản xác nhận nhận thiết bị.

- Nhân viên đại lý giao tận tay cho khách hàng, ký biên bản xác nhận nhận thiết bị.

6.2.7. Lưu trữ khóa bí mật trên mô-đun mật mã

Hiện nay SMARTSIGN sao lưu khóa từ HSM vào Smartcard chuyên dụng của HSM đó, trong quá trình sao lưu thì HSM đã mã hóa dữ liệu.

6.2.8. Phương thức kích hoạt khóa 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 thiết bị phần cứng 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.

6.2.9. Phương thức vô hiệu hóa khóa bí mật

Đối với thuê bao: khóa bí mật được lưu trong 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 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 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 SMARTSIGN: 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.

6.2.10. Phương pháp huỷ khóa 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 Token được xóa bằng phần mềm quản trị 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.

6.2.11. Đánh giá mô-đun mật mã

Áp dụng chuẩn đánh giá mô-đun mật mã quy định tại 6.2.1.

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

6.3.1. Lưu trữ khóa công khai

SMARTSIGN 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.

SMARTSIGN sẽ lưu khóa công khai của mình và toàn bộ thuê bao.

6.3.2. Thời hạn sử dụng chứng thư chữ ký số và thời hạn sử dụng cặp khóa

Không có quy định về thời hạn của cặp khóa tạo ra. Chỉ có hiệu lực của chứng thư do SMARTSIGN được xác định bởi tài liệu CPS này.

Thời gian hoạt động của chứng thư chữ ký số SMARTSIGN là tối đa 10 năm (theo Nghị định 23/2025/NĐ-CP).

Thêm vào đó dịch vụ SMARTSIGN ngưng phát hành các chứng thư chữ ký số mới trước ngày chứng thư của CA hết hạn nhằm đảm bảo rằng không có một chứng thư nào được phát hành 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. Khởi tạo và cài đặt dữ liệu kích hoạt

Dữ liệu kích hoạt khóa bí mật của SMARTSIGN 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 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 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 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 khuyến khích sử dụng cơ chế xác thực hai nhân tố.

Trường hợp chứng thư chữ ký số được lưu trên Token và bảo vệ bằng mật khẩu SMARTSIGN 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. Các khía cạnh khác của dữ liệu kích hoạt

Không có quy định.

6.5. Kiểm soát an ninh máy tính

6.5.1. Các yêu cầu kỹ thuật cụ thể về an ninh máy tính

SMARTSIGN 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 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.

Ở mức hệ điều hành, mỗi máy chủ được bảo vệ bằng tường lửa nội tại (FirewallD/Iptables) kiểm soát truy cập ra/vào, kết hợp cơ chế kiểm soát truy cập

bắt buộc (SELinux) để chỉ cho phép các tiến trình hợp lệ được thực thi; toàn bộ truy cập được xác thực bằng tài khoản, mật khẩu, mã hóa và ghi nhật ký. Ở mức cơ sở dữ liệu, hệ thống áp dụng đồng thời ba lớp xác thực (tường lửa, hệ điều hành, cơ sở dữ liệu); tài khoản truy cập cơ sở dữ liệu được tách biệt hoàn toàn với tài khoản hệ điều hành nhằm ngăn chặn truy cập trái phép.

6.5.2. Định kỳ đánh giá an ninh hệ thống máy tính

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

6.6. Kiểm soát vòng đời kỹ thuật

6.6.1. Kiểm soát phát triển hệ thống

SMARTSIGN sử dụng các hệ thống có chứng chỉ tiêu chuẩn công nghệ thông tin.

6.6.2. Kiểm soát quản lý an ninh

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

6.6.3. Kiểm soát vòng đời hệ thống

Không có quy định.

6.7. Giám sát an ninh hệ thống mạng

SMARTSIGN phân đoạn hệ thống cấp chứng thư chữ ký 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 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 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. 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.

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 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)

SMARTSIGN cung cấp dịch vụ cấp dấu thời gian (Timestamp) và dịch vụ chứng thực thông điệp dữ liệu, tuân thủ các quy định tại Nghị định 23/2025/NĐ-CP và QCVN 138:2025/BKHCN, QCVN 139:2025/BKHCN..

7. Định dạng chứng thư chữ ký số, danh sách thu hồi chứng thư chữ ký số (CRL), giao thức kiểm tra trạng thái chứng thư chữ ký số trực tuyến (OCSP)

7.1. Định dạng của chứng thư chữ ký số

Chứng thư chữ ký số được định dạng theo chuẩn quốc tế ITU-T X.509v3. Trên mỗi chứng thư chữ ký 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 chữ ký số.
Signature algorithm	Số hiệu thuật toán dùng để ký chứng thư chữ ký số.
Issuer	Bộ KHCN 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 phát hành chứng thư X.509 phiên bản 3.

7.1.2. Các trường mở rộng

Phần mở rộng của chứng thư X.509 v3 được thể hiện trong chứng thư chữ ký số của SMARTSIGN là:

Chứng thư chữ ký 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
CRL Distribution Points	URI của CRL

Chứng thư chữ ký 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
CRL Distribution Points	URI của CRL

7.1.3. Định danh thuật toán

SMARTSIGN ký lên các chứng thư chữ ký số, sử dụng một trong các thuật toán sau:

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

Thủ tục ký chứng thư chữ ký số áp dụng lược đồ RSASSA-PSS được quy định trong PKCS#1 phiên bản 2.1

Phiên bản của SMARTSIGN hỗ trợ sử dụng thuật toán mã hóa SHA-256, SHA-384 và SHA-512 trong chứng thư chữ ký số

7.1.4. Định dạng 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 và tuân theo cấu trúc được định nghĩa trong tiêu chuẩn ITU-T Standards Recommendation X.501.

7.1.5. Các ràng buộc, hạn chế về tên

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

7.1.6. Định danh quy chế chứng thực

Theo mục 1.2

7.1.7. Sử dụng trường mở rộng Policy Constraint

Không có ràng buộc nào.

7.1.8. Cú pháp và ngữ nghĩa trong quy chế chứng thực

Không có quy định.

7.1.9. Xử lý ngữ nghĩa cho trường mở rộng quan trọng Certificate Policies

Không có quy định.

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

Version	V2
Signature	Sha256WithRSAEncryption
Issuer	SMARTSIGN
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. Số phiên bản của CRL

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

7.2.2. CRL và phần mở rộng đầu vào CRL

Không có quy định.

7.3. Định dạng giao thức kiểm tra trạng thái chứng thư chữ ký số trực tuyến (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. Số phiên bản của OCSP

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

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

8.3. Tính độc lập của bên đánh giá đối với tổ chức được đánh giá

Chuyên gia đánh giá độc lập (bên thứ ba) phải là đơn vị kiểm toán/đánh giá độc lập, có thẩm quyền và chứng chỉ hành nghề hợp pháp theo quy định của pháp luật.

8.4. Xử lý khi phát hiện sai sót

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

SMARTSIGN 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 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 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.

SMARTSIGN 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 công bố trang web của SMARTSIGN.

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

8.6. Tần suất và các trường hợp đánh giá

Không quy định.

9. Các nội dung nghiệp vụ và pháp lý khác

9.1. Phí, giá

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

Phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư chữ ký số theo quy định tại Thông tư số 13/2025/TT-BTC ngày 19 tháng 3 năm 2025 của Bộ trưởng 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 chữ ký số.

9.1.2. Giá

Bảng giá dịch vụ chứng thực chữ ký số công cộng được công bố trên website của SMARTSIGN. Ngoài phí sử dụng dịch vụ, thuê bao có thể phải hoàn thành các chi phí sau:

Giá phát hành hoặc gia hạn chứng thư chữ ký số.

Giá truy cập chứng thư chữ ký số: Thuê bao không phải trả chi phí khi truy cập kho chứng thư chữ ký số hay dịch vụ cung cấp thông tin chứng thư chữ ký số trực tuyến cho người nhận.

Giá truy cập thông tin thu hồi hoặc trạng thái chứng thư chữ ký số: SMARTSIGN không thu phí này

Chính sách hoàn tiền: Theo thỏa thuận sử dụng/hợp đồng ký kết giữa SMARTSIGN và thuê bao..

9.1.3. Các loại chi phí khác

Theo quy định của pháp luật và chính sách bán hàng của SMARTSIGN..

9.2. Trách nhiệm tài chính

9.2.1. Phạm vi bảo hiểm

SMARTSIGN 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.

9.2.2. Các tài sản khác

Không được đề cập.

9.2.3. Phạm vi bảo hiểm hoặc bảo hành cho người dùng cuối

SMARTSIGN 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 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 mật

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

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

Các dữ liệu về hồ sơ đề nghị phát hành chứng thư chữ ký số;

Các khóa bí mật của thuê bao;

Các dữ liệu kiểm toán.

9.3.2. Thông tin nằm ngoài phạm vi bảo mật

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

9.3.3. Trách nhiệm bảo mật thông tin nghiệp vụ

Các thông tin đã được ban hành trong chứng thư chữ ký số và CRL không được coi là bí mậ SMARTSIGN và các RA được công nhận của nó có trách nhiệm bảo vệ thông tin.

9.4. Bảo vệ dữ liệu cá nhân

9.4.1. Biện pháp bảo vệ dữ liệu cá nhân

SMARTSIGN áp dụng các biện pháp bảo vệ dữ liệu cá nhân theo quy định tại Nghị định số 13/2023/NĐ-CP và Nghị định số 23/2025/NĐ-CP, bao gồm:

Biện pháp quản lý: ban hành quy chế, quy trình nội bộ về thu thập, xử lý, lưu trữ dữ liệu cá nhân; phân quyền truy cập theo nguyên tắc chỉ cấp quyền tối thiểu cần thiết cho từng vị trí công việc; ký cam kết bảo mật đối với cán bộ, nhân viên và các bên thứ ba có liên quan (RA, đại lý) khi tiếp cận dữ liệu cá nhân của thuê bao;

Biện pháp kỹ thuật: mã hóa dữ liệu cá nhân khi lưu trữ và truyền tải; kiểm soát truy cập bằng xác thực đa yếu tố đối với hệ thống lưu trữ hồ sơ thuê bao; ghi nhật ký (log) toàn bộ hoạt động truy cập, chỉnh sửa dữ liệu cá nhân để phục vụ truy vết khi cần thiết; sao lưu dự phòng định kỳ nhằm chống mất mát dữ liệu;

Biện pháp vật lý: kiểm soát ra vào khu vực đặt máy chủ, kho lưu trữ hồ sơ giấy có chứa dữ liệu cá nhân của thuê bao;

Biện pháp ứng phó sự cố: xây dựng quy trình phát hiện, xử lý và thông báo khi xảy ra sự cố lộ, mất dữ liệu cá nhân theo quy định của pháp luật về bảo vệ dữ liệu cá nhân.

9.4.2. Phạm vi bảo vệ dữ liệu cá nhân

Phạm vi dữ liệu cá nhân được SMARTSIGN bảo vệ bao gồm toàn bộ thông tin cá nhân của thuê bao, người đại diện theo pháp luật của thuê bao là tổ chức, và các cá nhân có liên quan mà SMARTSIGN thu thập, xử lý trong quá trình cung cấp dịch vụ chứng thực chữ ký số, cụ thể:

Thông tin nhận dạng cá nhân: họ tên, ngày sinh, số định danh cá nhân/số Căn cước công dân/Hộ chiếu, quốc tịch, địa chỉ thường trú;

Thông tin liên hệ: số điện thoại, địa chỉ email, địa chỉ nhận thông báo;

Thông tin xác thực: hình ảnh, dữ liệu sinh trắc học (nếu có thu thập để phục vụ định danh điện tử theo quy định);

Dữ liệu khóa bí mật, dữ liệu kích hoạt khóa bí mật của thuê bao;

Các hồ sơ, tài liệu, giấy tờ chứng minh nhân thân do thuê bao cung cấp trong quá trình đăng ký, gia hạn, thay đổi thông tin chứng thư chữ ký số.

9.4.3. Những thông tin cá nhân ngoài phạm vi bảo vệ

Thông tin cá nhân đã được chính chủ thể dữ liệu tự công khai hoặc đồng ý cho phép công khai;

Thông tin cá nhân được thuê bao đồng ý đưa vào nội dung chứng thư chữ ký số, danh sách chứng thư bị thu hồi (CRL) hoặc công bố công khai theo quy định tại Quy chế chứng thực này để phục vụ mục đích xác thực, kiểm tra hiệu lực chứng thư;

Thông tin cá nhân đã được tổng hợp, thống kê dưới dạng ẩn danh, không còn khả năng xác định hoặc liên kết tới một cá nhân cụ thể;

Thông tin cá nhân phải cung cấp cho cơ quan nhà nước có thẩm quyền theo quy định của pháp luật về an ninh, quốc phòng, phòng chống tội phạm hoặc theo yêu cầu của cơ quan tiến hành tố tụng;

Thông tin cá nhân đã được công khai hợp pháp trên các phương tiện thông tin đại chúng, cơ sở dữ liệu quốc gia hoặc nguồn khác theo quy định của pháp luật.

9.4.4. Trách nhiệm bảo vệ dữ liệu cá nhân

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

9.4.5. Thông báo và cho phép sử dụng dữ liệu cá nhân

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

9.4.6. Cung cấp thông tin theo yêu cầu của cơ quan quản lý

SMARTSIGN có trách nhiệm cung cấp thông tin riêng tư nếu:

Khi có yêu cầu của cơ quan pháp luật có thẩm quyền hoặc các quá trình liên quan đến luật pháp đã được quy định.

Khi có yêu cầu truy cập thông tin để phục vụ cho quản trị (yêu cầu xác nhận, yêu cầu cho quá trình tạo tài liệu).

9.4.7. Các tình huống cung cấp thông tin khác

Không có quy định.

9.5. Quyền sở hữu trí tuệ

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

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

9.6. Tuyên bố và cam kết

9.6.1. Tuyên bố và cam kết của tổ chức phát hành chứng thư chữ ký số

SMARTSIGN đảm bảo rằng:

Không thay đổi thông tin đăng ký chứng thư chữ ký số được cung cấp bởi đối tượng đăng ký.

Không có lỗi trong quá trình duyệt và ban hành chứng thư chữ ký số.

Chứng thư chữ ký số do SMARTSIGN 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 thuê bao

Thuê bao đảm bảo rằng:

Khi ký: sử dụng khóa bí mật tương ứng với khóa công khai trong chứng thư chữ ký số; tại thời điểm ký, thuê bao chấp nhận chứng thư chữ ký số và chứng thư chữ ký 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 chữ ký số đúng mục đích của chứng thư chữ ký số, phù hợp với quy định của pháp luật và quy chế chứng thực này

Không sử dụng chứng thư chữ ký 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.

9.6.3. Tuyên bố và cam kết của bên tin cậy

Người nhận chịu trách nhiệm về việc tìm hiểu các thông tin trong quy chế chứng thư chữ ký số, trong thỏa thuận người nhận trước khi quyết định tin tưởng chứng thư chữ ký số do SMARTSIGN 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.

9.6.4. Tuyên bố và cam kết của các bên liên quan khác

RA đảm bảo rằng:

Không thay đổi thông tin đăng ký chứng thư chữ ký số được cung cấp bởi đối tượng đăng ký.

Không có lỗi trong quá trình duyệt hồ sơ xin cấp chứng thư chữ ký số và quá trình gửi thông tin cho SMARTSIGN.

Tuân thủ theo quy trình quản lý vòng đời chứng thư chữ ký số của SMARTSIGN.

RA có trách nhiệm ký hợp đồng với SMARTSIGN. Trong hợp đồng có quy định:

Loại chứng thư chữ ký số mà RA được phép tham gia cung cấp.

Các bước trong quy trình phát hành chứng thư chữ ký số do RA thực hiện.

Chứng thư chữ ký số chỉ được cấp sau khi SMARTSIGN đã nhận đầy đủ hồ sơ của thuê bao, và thông tin thuê bao được thẩm định.

Cam kết của RA với SMARTSIGN 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 chữ ký số phải có hiểu biết pháp luật về chữ ký số và dịch vụ chứng thực chữ ký số.

9.7. Từ chối bảo hành

SMARTSIGN 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

Khi pháp luật yêu cầu, khách hàng bồi thường cho SMARTSIGN 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 hồ sơ đề nghị phát hành chứng thư chữ ký số, 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.

9.10. Hiệu lực của quy chế chứng thực

9.10.1. Thời hạn

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

SMARTSIGN sẽ cung cấp dịch vụ theo CPS này kể từ khi CPS này bắt đầu có hiệu lực.

9.10.2. Chấm dứt 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 chấm dứt hiệu lực

Khi quy chế này hết hiệu lực, các điều khoản của nó vẫn được áp dụng cho các chứng thư chữ ký số được ban hành trong thời hạn của quy chế này cho đến khi chứng thư chữ ký 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 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. Quy trình 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 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 sẽ xem xét yêu cầu thay đổi. Nếu quy chế cần thay đổi, SMARTSIGN 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 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 được quyền góp ý cho quy chế chứng thư chữ ký số trong vòng 15 ngày từ ngày quy chế được công bố.

SMARTSIGN sẽ xem xét mọi góp ý sửa đổi. SMARTSIGN 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. Cơ chế và thời hạn thông báo

Không quy định

9.12.3. Các trường hợp cần thay đổi 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.

9.13. Thủ tục giải quyết khiếu nại

Tranh chấp phát sinh từ Quy chế chứng thực này sẽ do quản lý CPS của SMARTSIGN giải quyết.

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

Việc giải quyết tranh chấp giữa SMARTSIGN 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 căn cứ pháp lý

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 số 20/2023/QH15 ngày 22/06/2023;

- Nghị định số 23/2025/NĐ-CP ngày 21/02/2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ tin cậy;

- Thông tư số 50/2025/TT-BKHCN ngày 31/12/2025 của Bộ Khoa học và Công nghệ ban hành các Quy chuẩn kỹ thuật quốc gia về dịch vụ tin cậy;

- QCVN 137:2025/BKHCN: Quy chuẩn kỹ thuật quốc gia về yêu cầu đối với dịch vụ chứng thực chữ ký số công cộng;

- Chuẩn RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

- Thông tư số 16/2025/TT-BKHCN ngày 20/08/2025 của Bộ Khoa học và Công nghệ quy định quy chế chứng thực mẫu ban hành quy chế chứng thực của tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia;

- QCVN 139:2025/BKHCN: Quy chuẩn kỹ thuật quốc gia về yêu cầu đối với dịch vụ chứng thực thông điệp dữ liệu;

- QCVN 138:2025/BKHCN: Quy chuẩn kỹ thuật quốc gia về yêu cầu đối với dịch vụ cấp dấu thời gian;

9.15. Tuân thủ quy định pháp luật hiện hành

Mọi hoạt động liên quan đến yêu cầu, phát hành, sử dụng hoặc chấp nhận của một chứng thư SMARTSIGN 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 toàn bộ

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

9.16.2. Chuyển nhượng

Không có quy định nào cho phép chuyển nhượng quyền sử dụng chứng thư chữ ký số. SMARTSIGN không quy định các trường hợp chuyển nhượng khác.

9.16.3. Tính độc lập của các điều khoản

9.16.4. Sự thực thi

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.

9.16.5. Sự kiện 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.

9.17. Các điều khoản khác

Không áp dụng.

10. Phụ lục quy định về đại lý

10.1. Quyền của đại lý

a) Được áp dụng bảng giá đại lý và tham gia các chương trình khuyến mãi, quảng cáo của SMARTSIGN khi cung cấp dịch vụ theo hợp đồng đại lý.
b) Yêu cầu SMARTSIGN cung cấp 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.

c) Chấm dứt hợp đồng khi không có nhu cầu làm đại lý hoặc khi SMARTSIGN vi phạm các điều khoản đã cam kết, với thông báo bằng văn bản trước ít nhất 15 ngày.

10.2. Nghĩa vụ của đại lý

a) Thực hiện toàn bộ quy trình tư vấn, tiếp nhận, xác minh thông tin, đăng ký khách hàng theo Quy chế chứng thực (CP/CPS) của SMARTSIGN và các quy trình nội bộ do SMARTSIGN ban hành; tư vấn đầy đủ, trung thực cho khách hàng về sản phẩm dịch vụ của SMARTSIGN.

b) Niêm yết quy trình phát hành chứng thư chữ ký số tại trụ sở đại lý (không bắt buộc, khuyến khích thực hiện).

c) Tiếp nhận yêu cầu từ khách hàng 24 giờ/ngày, 7 ngày/tuần.

d) Chịu trách nhiệm báo cáo khi có yêu cầu của cơ quan chức năng nhằm phục vụ công tác quản lý nhà nước về dịch vụ chứng thực chữ ký số.

đ) Phối hợp với SMARTSIGN cung cấp hồ sơ, giải trình, tạo điều kiện cho Bộ Khoa học và Công nghệ hoặc Trung tâm Chứng thực điện tử quốc gia (NEAC) thanh tra, kiểm tra khi được yêu cầu.

e) Bán đúng giá theo bảng giá SMARTSIGN ban hành; không thu thêm bất kỳ khoản phí nào ngoài quy định.

g) Tiếp nhận và bảo quản tài khoản RA truy cập hệ thống SMARTSIGN; đảm bảo bảo mật và chịu hoàn toàn trách nhiệm về mọi thao tác thực hiện thông qua tài khoản này.

h) Bàn giao đầy đủ và đúng hạn hồ sơ khách hàng cho SMARTSIGN, bao gồm: Hợp đồng dịch vụ, Giấy xác nhận thông tin chứng thư chữ ký số (mẫu BG026) và các giấy tờ liên quan theo quy định.

i) Tiếp nhận và chuyển khiếu nại, phản hồi của khách hàng cho SMARTSIGN; phối hợp giải quyết và trả lời khách hàng.

k) Đối soát số liệu hàng tháng làm căn cứ thanh toán (chốt ngày 07 hàng tháng).

l) Lắp đặt biển hiệu, sử dụng tờ rơi do SMARTSIGN cung cấp để quảng bá dịch vụ (không bắt buộc).

m) Phối hợp với SMARTSIGN thực hiện các đợt khuyến mãi, chăm sóc khách hàng theo từng chương trình cụ thể do hai bên thỏa thuận (không bắt buộc).

n) Thông báo cho SMARTSIGN trước 07 ngày khi có thay đổi về tên công ty, địa chỉ, điện thoại, email hoặc thông tin ngân hàng.

o) Không chuyển nhượng hợp đồng đại lý cho bất kỳ bên thứ ba nào khi chưa có sự đồng ý bằng văn bản của SMARTSIGN.

p) Không tiết lộ bí mật kinh doanh của SMARTSIGN cho bất kỳ bên nào khi chưa được SMARTSIGN cho phép.

q) Tự chịu trách nhiệm về các khoản thuế liên quan theo quy định của pháp luật.

r) Liên đới chịu trách nhiệm về chất lượng dịch vụ trong trường hợp có lỗi do đại lý gây ra; chịu trách nhiệm hoàn toàn trước pháp luật khi các vi phạm của đại lý gây hậu quả nghiêm trọng, ảnh hưởng đến quyền lợi của thuê bao hoặc uy tín của SMARTSIGN.

s) Chịu trách nhiệm trước khách hàng và SMARTSIGN trong trường hợp chứng thư chữ ký số của thuê bao bị tạm dừng, thu hồi hoặc khóa thiết bị lưu khóa bí mật do lỗi của đại lý trong quá trình xác minh hồ sơ hoặc thực hiện quy trình.

t) Khi có khiếu nại từ khách hàng, đại lý có nghĩa vụ giải trình trước SMARTSIGN; trường hợp xác định lỗi thuộc về đại lý, đại lý phải bồi hoàn đầy đủ các khoản chi phí đã thu từ khách hàng và bồi thường toàn bộ thiệt hại gây ra cho khách hàng và SMARTSIGN.

u) Ngay khi nhận bàn giao chứng thư chữ ký số từ SMARTSIGN, đại lý cam kết và chịu hoàn toàn trách nhiệm đảm bảo sự toàn vẹn và bảo mật của chứng thư chữ ký số; mọi rủi ro về việc khóa bí mật của khách hàng bị lộ hoặc không còn toàn vẹn do lỗi của đại lý, đại lý chịu trách nhiệm hoàn toàn trước khách hàng và pháp luật.

v) Chỉ sử dụng dữ liệu cá nhân của khách hàng thu thập trong quá trình thực hiện hợp đồng vào đúng mục đích cung cấp dịch vụ; không chia sẻ, tiết lộ hoặc sử dụng cho mục đích khác khi chưa có sự đồng ý của chủ thể dữ liệu, trừ trường hợp pháp luật yêu cầu; tuân thủ Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân.

10.3. Quy trình phối hợp cung cấp dịch vụ giữa SMARTSIGN và đại lý

I. Tài khoản RA và điều khoản bảo mật

1. Hệ thống RA là hệ thống tiếp nhận yêu cầu và phát hành chứng thư chữ ký số cho khách hàng. SMARTSIGN cấp cho đại lý tài khoản RA để thực hiện các công việc theo hợp đồng đại lý.
2. Mỗi nhân viên sử dụng một tài khoản riêng; nghiêm cấm dùng chung hoặc chia sẻ tài khoản giữa các cá nhân.
3. Tài khoản bị khóa ngay trong ngày cuối cùng làm việc của nhân viên khi nhân viên đó nghỉ việc hoặc không còn tham gia quy trình phát hành chứng thư chữ ký số.
4. SMARTSIGN có trách nhiệm hướng dẫn, đào tạo, tập huấn, cung cấp tài liệu sử dụng và cấp quyền truy cập phù hợp cho đại lý.

5. Mỗi bên có trách nhiệm giữ bí mật thông tin được bên kia cung cấp và không tiết lộ cho bất kỳ bên thứ ba nào khi chưa có sự đồng ý bằng văn bản của bên kia. Thông tin bảo mật bao gồm toàn bộ nội dung và thông tin về khách hàng, thông tin kinh doanh và thông tin kỹ thuật liên quan đến việc thực hiện hợp đồng đại lý.
6. Đại lý chỉ sử dụng dữ liệu cá nhân của khách hàng vào đúng mục đích cung cấp dịch vụ theo quy định tại Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân.

II. Danh sách nhân viên đại lý tham gia quy trình phát hành chứng thư chữ ký số

Chỉ những nhân viên có tên trong danh sách do đại lý đăng ký với SMARTSIGN mới được phép thực hiện các thao tác trên hệ thống RA và tiếp nhận, xác minh hồ sơ khách hàng. Trường hợp có thay đổi nhân sự, đại lý phải thông báo bằng văn bản cho SMARTSIGN trước khi thực hiện.

III. Hồ sơ đề nghị phát hành chứng thư chữ ký số công cộng

Khi nhận được hồ sơ đề nghị phát hành chứng thư chữ ký số công cộng của tổ chức, cá nhân, đại lý phải tiến hành kiểm tra, đối chiếu các giấy tờ trong hồ sơ đề nghị phát hành, xác minh thông tin nhận biết tổ chức, cá nhân.

Hồ sơ đề nghị phát hành chứng thư chữ ký số công cộng bao gồm:

1. Giấy đề nghị phát hành chứng thư chữ ký số công cộng dưới dạng bản giấy theo mẫu của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.
2. Tài liệu kèm theo bao gồm:
   a) Đối với cá nhân: giấy tờ tùy thân bao gồm thẻ căn cước công dân hoặc thẻ căn cước hoặc giấy chứng nhận căn cước hoặc hộ chiếu còn thời hạn; thị thực nhập cảnh còn thời hạn hoặc giấy tờ chứng minh được miễn thị thực nhập cảnh (đối với cá nhân là người nước ngoài);
   b) Đối với tổ chức: quyết định thành lập hoặc quyết định quy định về chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức hoặc giấy chứng nhận đăng ký doanh nghiệp hoặc giấy chứng nhận đầu tư hoặc giấy chứng nhận đăng ký hộ kinh doanh; và giấy tờ tùy thân của người đại diện theo pháp luật của tổ chức, bao gồm thẻ căn cước công dân hoặc thẻ căn cước hoặc giấy chứng nhận căn cước hoặc hộ chiếu.
3. Cá nhân, tổ chức có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc nộp bản sao kèm bản chính để đối chiếu theo quy định của pháp luật.

Đối với trường hợp xuất trình bản chính để đối chiếu, đại lý phải xác nhận vào bản sao và chịu trách nhiệm về tính chính xác của bản sao so với bản chính.

IV. Quy trình đại lý thực hiện trên hệ thống RA

Bước 1: Thu thập bộ hồ sơ giấy từ khách hàng theo đúng danh mục quy định tại Mục III.

Bước 2: Thực hiện scan toàn bộ hồ sơ thành 01 tệp tài liệu số.

Bước 3: Tải tệp hồ sơ scan lên hệ thống RA của SMARTSIGN.

Bước 4: Nhân viên đại lý ký số tệp hồ sơ trên hệ thống RA bằng chứng thư chữ ký số hợp lệ. Chữ ký số xác nhận đại lý đã: (i) xác minh thông tin nhận biết khách hàng theo quy định tại Mục III; (ii) đối chiếu bản sao với bản chính các giấy tờ trong hồ sơ; (iii) xác nhận tệp scan trung thực, đầy đủ, không chỉnh sửa so với hồ sơ giấy gốc. Nhân viên ký số chịu trách nhiệm pháp lý về tính chính xác của hồ sơ đã xác nhận.

Bước 5: Hệ thống RA tự động kiểm tra chữ ký số và phê duyệt nếu chữ ký số hợp lệ.

Bước 6: Ghi chứng thư chữ ký số vào thiết bị lưu khóa bí mật và bàn giao cho khách hàng; khách hàng ký Giấy xác nhận thông tin chứng thư chữ ký số (mẫu BG026).

V. Bàn giao hồ sơ về SMARTSIGN

Đại lý bàn giao đầy đủ và đúng hạn hồ sơ khách hàng về SMARTSIGN, tối đa không quá 30 ngày kể từ ngày phát hành chứng thư chữ ký số, bao gồm: Giấy đăng ký/Hợp đồng cung cấp và sử dụng dịch vụ, Giấy xác nhận thông tin chứng thư chữ ký số (mẫu BG026) và các giấy tờ kèm theo quy định tại Mục III.

Đại lý cam kết cung cấp dịch vụ đúng như trong hợp đồng đại lý đã ký và theo quy định của pháp luật.

VI. Thanh toán và đối soát

1. Đại lý thu cước phí dịch vụ từ khách hàng và xuất hóa đơn giá trị gia tăng cho khách hàng.
2. Đại lý và SMARTSIGN đối soát vào ngày 01 đến ngày 07 hàng tháng hoặc theo thỏa thuận khác nếu có.
3. SMARTSIGN xuất hóa đơn giá trị gia tăng cho đại lý sau khi đối soát hoàn tất.

VII. Hỗ trợ khách hàng

1. Đại lý tiếp nhận toàn bộ yêu cầu hỗ trợ từ khách hàng và thực hiện hỗ trợ trong phạm vi năng lực, theo quy trình hướng dẫn của SMARTSIGN.
2. Đại lý phối hợp với SMARTSIGN để hỗ trợ khách hàng trong các trường hợp vượt quá phạm vi xử lý của đại lý.