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

QUY CHẾ VÀ CHÍNH SÁCH CHỨNG THƯ SỐ

SMARTSIGN

01/09/2021

MỤC LỤC

1. GIỚI THIỆU

1.1. Tổng quan

SmartSign là tên gọi của dịch vụ chứng thực chữ ký số công cộng do Công Ty Cổ Phần Chữ Ký Số Vi Na cung cấp. Các quy định về chính sách chứng thư số của dịch vụ SmartSign được trình bày trong tài liệu này bao gồm phát hành, quản lý, thu hồi và cấp lại chứng thư số.

Bản quy chế chứng thực mô tả các thủ tục và cơ chế thực thi của nhà cung cấp chứng thư số của hệ thống SmartSign. Quy chế chứng thực mô tả các điều khoản và điều kiện thực hiện của nó nhằm cung cấp tới các cơ quan quản lý cũng như người sử dụng những mô tả rõ ràng về các dịch vụ của hệ thống và các điều kiện để sử dụng chúng. Ngoài ra, nó cũng đưa ra những đảm bảo về mặt an toàn bảo mật và an toàn thông tin của hệ thống SmartSign và các dịch vụ chứng thực chữ ký số cung cấp cho khách hàng.

Hệ thống SmartSign tuân thủ theo Nghị định số 130/2018/NĐ-CP ngày 27 tháng 9 năm 2018 của Chính phủ quy định chi tiết thi hành luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số, Thông tư số 31/2020/TT-BTTTT ngày 30 tháng 10 năm 2020.

Mục tiêu của văn bản này là:

- SmartSign với tư cách là nhà cung cấp dịch vụ chứng thực chữ ký số công cộng hoạt động trên cơ sở quy chế chứng thực và tuân thủ theo các yêu cầu trong quy chế này;
- Cung cấp cho người sử dụng dịch vụ SmartSign các quy trình liên quan đến cấp phát, quản lý, sử dụng, thu hồi và cấp lại chứng thư số trong hệ thống SmartSign cũng như trách nhiệm của họ trong khi tham gia vào các quá trình này;
- Cung cấp thông tin cho bên tin tưởng về mức độ bảo đảm của các chứng thư số mà SmartSign cung cấp cho người sử dụng.

1.2. Tên tài liệu và nhận dạng

Tài liệu này được gọi là quy chế chứng thực của nhà cung cấp dịch vụ chứng thư số SmartSign. Bản quy chế này được chấp nhận bởi đơn vị quản lý của Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia (RootCA) là Trung tâm Chứng thực điện tử Quốc gia, Bộ thông tin và truyền thông. Các chứng thư số do SmartSign phát hành có số Object Identifier (OID), do Trung tâm CTĐTQG cấp để chỉ ra đường dẫn của bản quy chế này.

1.3. Đối tượng tham gia

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng SmartSign là Công ty Cổ phần Chữ ký số Vi Na.

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. Trung tâm Chứng thực chữ ký số quốc gia vận hành hệ thống tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia.

Tổ chức đăng ký chứng thư số (SmartSign RA) là tổ chức được SmartSign tin cậy, uỷ quyền để tiếp nhận yêu cầu cung cấp dịch vụ và xác thực thông tin của thuê bao nhằm đảm bảo tính chính xác của thông tin thuê bao trên toàn hệ thống. SmartSign RA là toàn bộ các đại lý có ký kết hợp đồng đại lý, có trách nhiệm, khả năng kiểm tra, xác thực định danh các thuê bao. SmartSign RA thực hiện việc đăng ký các thông tin của thuê bao xin cấp chứng thư số:

- Xác thực cá nhân chủ thể đăng ký chứng thư số.
- Kiểm tra tính hợp lệ của thông tin do chủ thể cung cấp.
- Xác nhận quyền của chủ thể đối với những thuộc tính chứng thư số yêu cầu.
- Kiểm tra xem chủ thể có thực sự sở hữu khoá bí mật đang được đăng ký hay không.
- Thay mặt chủ thể thuê bao khởi tạo quá trình đăng ký với CA.
- Phân phối USB Token và PKI Card chứa khoá bí mật.

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

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

Các đối tượng khác: SmartSign không quản lý đối tượng nào khác ngoài thuê bao và các bên tin tưởng.

1.4. Mục đích sử dụng chứng thư số

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

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

1.5. Quản lý quy chế chứng thực

1.5.1 Tổ chức quản lý tài liệu

Tên cơ quan: Công Ty Cổ Phần Chữ Ký Số Vi Na

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

1.5.2 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, Quận 1, Tp Hồ Chí Minh
- Điện thoại: 08 3820 2261
- E-mail: info@smartsign.com.vn

1.5.3 Công nhận sự phù hợp của quy chế

Bộ Thông tin và Truyền Thông và Công Ty Cổ Phần Chữ Ký Số Vi Na xác nhận sự phù hợp của quy chế chứng thực này.

1.5.4 Thủ tục phê chuẩn quy chế

Công Ty Cổ Phần Chữ Ký Số Vi Na sẽ phê chuẩn quy chế và phát hành quy chế trên website. Các thay đổi, cập nhật của quy chế được ghi trong một tài liệu chứa các sửa đổi của quy chế hay các thông tin về quá trình cập nhật và được công bố tại https://smartsign.com.vn/downloads/CP-CPS.pdf

1.6. Các định nghĩa và viết tắt

1.6.1 Các định nghĩa

Thuật ngữ	Giải thích
Chứng thư số SmartSign	Là một dạng chứng thư điện tử do SmartSign số cấp.
Chứng thư số có hiệu lực	Là chứng thư số chưa hết hạn, không bị tạm dừng hoặc bị thu hồi.
Chữ ký số	Là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng theo đó người có được thông điệp dữ liệu ban đầu và khoá công khai của người ký có thể xác định được chính xác: a. Việc biến đổi nêu trên được tạo ra bằng đúng khoá bí mật tương ứng với khoá công khai trong cùng một cặp khóa; b. Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.
Dịch vụ chứng thực chữ ký số	Là một loại hình dịch vụ chứng thực chữ ký điện tử, do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp. Dịch vụ chứng thực chữ ký số bao gồm:

	a. Tạo cặp khóa bao gồm khóa công khai và khóa bí mật cho thuê bao; b. Cấp, gia hạn, tạm dừng, phục hồi và thu hồi chứng thư số của thuê bao; c. Duy trì trực tuyến cơ sở dữ liệu về chứng thư số; d. Những dịch vụ khác có liên quan theo quy định.
Hệ thống mật mã không đối xứng	Là hệ thống mật mã có khả năng tạo được cặp khóa bao gồm khoá bí mật và khóa công khai.
Khoá	Là một chuỗi các số nhị phân (0 và 1) dùng trong các hệ thống mật mã.
Khóa bí mật	Là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được dùng để tạo chữ ký số.
Khóa công khai	Là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được sử dụng để kiểm tra chữ ký số được tạo bởi khoá bí mật tương ứng trong cặp khoá.
Ký số	Là việc đưa khóa bí mật vào một chương trình phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu.
Người ký	Là thuê bao dùng đúng khoá bí mật của mình để ký số vào một thông điệp dữ liệu dưới tên của mình.
Người nhận	Là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng chứng thư số của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.
Thuê bao	Là tổ chức, cá nhân được cấp chứng thư số, chấp nhận chứng thư số và giữ khoá bí mật tương ứng với khoá công khai ghi trên chứng thư số được cấp đó.
Tạm dừng chứng thư số	Là làm mất hiệu lực của chứng thư số một cách tạm thời từ một thời điểm xác định.
Thu hồi chứng thư số	Là làm mất hiệu lực của chứng thư số một cách vĩnh viễn từ một thời điểm xác định.

1.6.2 Từ viết tắt

ARL	Authority Revocation List
CA	Certificate Authority
CMS	Cryptographic Message Syntax
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CRR	Certificate Revocation Request
CSP	Certification Service Provider
DAP	Directory Access Protocol
DES	Data Encryption Standard
DNS	Domain Name System
HTTPS	Secure Hypertext Transaction Standard

LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5 Hash Algorithm
OCSP	Online Certificate Status Protocol
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Extended Public Key Infrastructure
RA	Registration Authorities
RFC	Request For Comments
RSA	Rivest Shamir Adleman
S/MIME	Secure Multipurpose Internet Mail Extensions
SHA	Secure Hash Standard
SSL	Secure Socket Layer
TLS	Transport Layer Security
X.500	X.500 The ITU-T (International Telecommunication Union-T) standard that establishes a distributed, hierarchical directory protocol organized by country, region, Organization, etc.
X.501	The ITU-T (International TelecommuniCAtion Union-T) standard for use of Distinguished Names in an X.500 directory.
X.509	ITU-T standard for Certificates format

2. TRÁCH NHIỆM LƯU TRỮ VÀ CÔNG BỐ THÔNG TIN

2.1. Lưu trữ

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

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

2.2. Công bố thông tin

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

SmartSign 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 số.

Các thông tin cập nhật và công bố bao gồm:

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

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

- Chứng thư số SmartSign có thời hạn từ ngày 26/11/2012 đến ngày 26/11/2017 sử dụng: http://crl.smartsign.com.vn;
- Chứng thư số SmartSign có thời hạn từ ngày 24/07/2017 đến ngày 24/07/2022 sử dụng: http://crl1.smartsign.com.vn;
- Chứng thư số SmartSign có thời hạn từ ngày 19/05/2020 đến ngày 19/05/2025 sử dụng: http://crl256. smartsign.com.vn/.

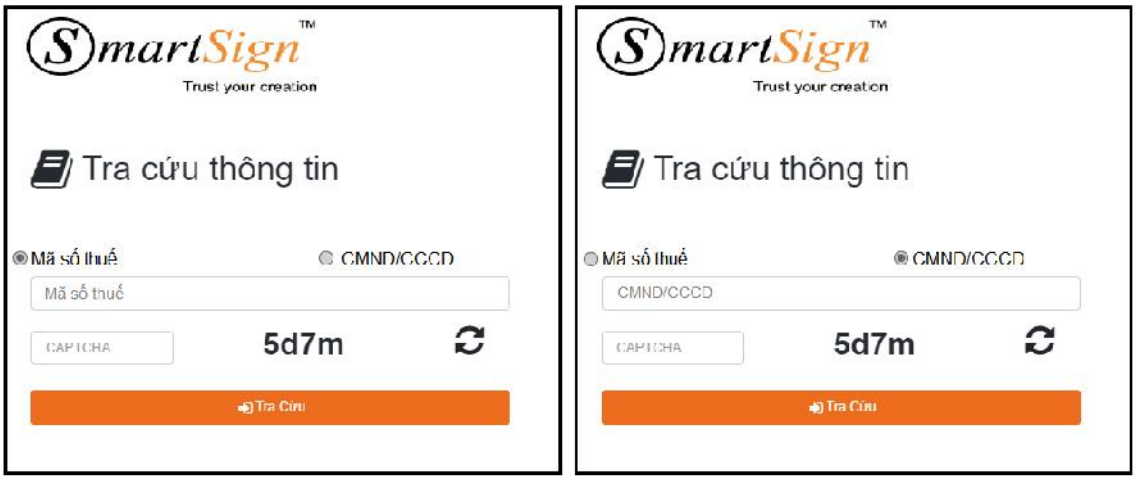
Kiểm tra tình trạng chứng thư số theo thời gian thực (OCSP).

- Chứng thư số SmartSign có thời hạn từ ngày 26/11/2012 đến ngày 26/11/2017 sử dụng: http://ocsp.smartsign.com.vn/;
- Chứng thư số SmartSign có thời hạn từ ngày 24/07/2017 đến ngày 24/07/2022 sử dụng: http://ocsp1.smartsign.com.vn;
- Chứng thư số SmartSign có thời hạn từ ngày 19/05/2020 đến ngày 19/05/2025 sử dụng: http://ocsp256.smartsign.com.vn.

Tra cứu tình trạng chứng thư số:

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

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



- Thuê bao doanh nghiệp chọn mã số thuế để tra cứu và nhập mã số thuế tại khung nhập Mã số thuế
- Thuê bao cá nhân chọn CMND/CCCD để tra cứu và nhập CMND/CCCD tại khung nhập CMND/CCCD.
- Tại khung nhập CAPTCHA: Thuê bao nhập lại mã CAPTCHA được hiển thị bên phải của khung để xác nhận thao tác do người thực hiện.

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

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

Công bố thông tin chứng thư số (LDAP):

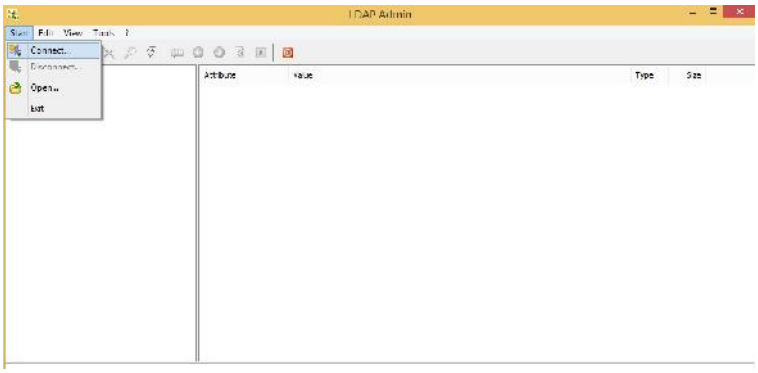
Để đảm bảo an toàn cơ sở dữ liệu LDAP thì SmartSign không cho phép truy cập LDAP trên website mà có công cụ để kiểm tra.

Cách kiểm tra như sau :

Bước 1 : Download Ldap admin tại:

http://www.ldapadmin.org/download/ldapadmin.html

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

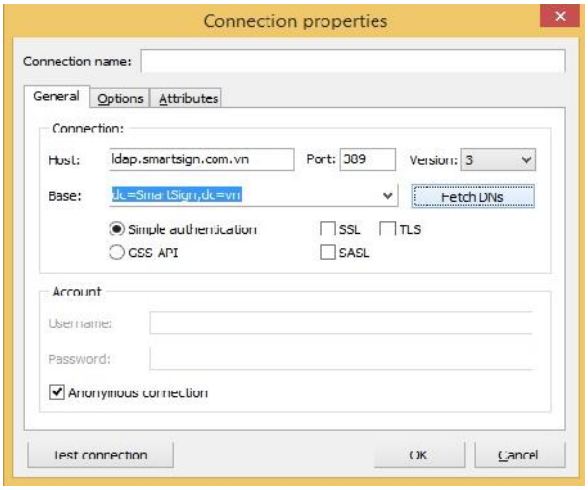


Bước 3 : Chọn new connect và điền các thông số như sau:

Mục host:

- Với chứng thư số SmartSign có thời hạn từ ngày 26/11/2012 đến ngày 26/11/2017 sử dụng địa chỉ: http://ldap.smartsign.com.vn
- Với chứng thư số SmartSign có thời hạn từ ngày 24/07/2017 đến ngày 24/07/2022 sử dụng địa chỉ: http://ldap1.smartsign.com.vn
- Với chứng thư số SmartSign có thời hạn từ ngày 19/05/2020 đến ngày 19/05/2025 sử dụng địa chỉ: http://ldap256.smartsign.com.vn

Ấn nút Fetchs DNs, rồi chọn Base và ấn ok



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

2.3. Thời gian, tần suất công bố thông tin

Chứng thư số SmartSign 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: 01 ngày.

Tần số công bố quy chế: Một phiên bản mới của quy chế sẽ được công bố ngay sau khi được phê chuẩn và phiên bản cũ sẽ được lưu trữ tron g kho lưu trữ một cách an toàn.

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 số của SmartSign, và các tài liệu (quy chế) của SmartSign thông qua địa chỉ công bố truy cập trực tuyến.

SmartSign được quyền kiểm soát việc truy nhập các thông tin được công bố trên trang thông tin điện tử như quy chế chứng thực, danh sách các chứng thư số có hiệu lực, bị thu hồi.

3. NHẬN DẠNG VÀ XÁC THỰC

3.1. Đặt tên trong chứng thư số

Chứng thư số chứa một tên dùng để phân biệt với các chứng thư số khác theo chuẩn X.501 trong trường Issuer và Subject.

- Đối với chứng thư số cho cá nhân, thành phần UID của đối tượng phân biệt định danh duy nhất thuê bao như sau:
  - CN = Họ và Tên
  - C = VN
  - S = Tên Tỉnh / Thành phố
  - UID = CMND/CCCD
  - Email = Địa chỉ email
- Đối với chứng thư số cho tổ chức, thành phần UID của đối tượng phân biệt định danh duy nhất thuê bao như sau:
  - CN = Tên tổ chức
  - C = VN
  - S = Tên Tỉnh / Thành phố
  - UID = MST
  - Email = Địa chỉ email
- Đối với chứng thư số cho dịch vụ, SSL, mail:
  - CN = Domain name
  - C = VN
  - S = Tên Tỉnh / Thành phố
  - Email = Địa chỉ email
- Đối với các chứng thư số khác (codesigning,…) theo quy định của Bộ Thông tin và Truyền thông.

3.1.2. Quy định tính duy nhất của tên

Tên thuê bao của dịch vụ SmartSign sẽ là duy nhất gắn với một cấp chứng thư số xác định trong miền của dịch vụ SmartSign. Một thuê bao có thể có hai hoặc nhiều chứng thư số có cùng tên.

3.1.3. Nhận dạng, xác thực và vai trò của thương hiệu

Đối tượng đăng ký chứng thư số không được sử dụng các tên đã được sở hữu và đăng ký bởi tổ chức, cá nhân theo quy định của pháp luật.

Trong trường hợp cần thiết, SmartSign có thể yêu cầu thuê bao cung cấp bằng chứng, tài liệu chứng minh quyền sở hữu đối với tên đăng ký.

SmartSign không chịu trách nhiệm trong mọi tranh chấp về tên của đối tượng đăng ký. SmartSign có quyền chấm dứt hoặc tạm dừng chứng thư số của thuê bao trong trường hợp có tranh chấp xảy ra.

3.2. Xác minh đề nghị cấp chứng thư số

3.2.1. Cách thức chứng minh sở hữu khóa bí mật

Đối tượng đăng ký chứng thư số phải chứng minh đang sở hữu khóa bí mật tương ứng với khóa công khai được ghi trong chứng thư số. Phương pháp chứng minh sở hữu khóa bí mật tuân theo chuẩn PKCS#10 hoặc một phương pháp mật mã tương ứng, hoặc phương pháp khác được SmartSign công nhận. Điều kiện này không áp dụng khi cặp khóa được CA sinh ra trên USB Token.

3.2.2. Nhận dạng và xác thực đối với cá nhân

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

a) Tài liệu nhận dạng danh tính

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

- Chứng minh nhân dân.
- Căn cước công dân.
- Hộ chiếu.

b) Thực hiện nhận dạng cá nhân

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

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

3.2.3 Nhận dạng và xác thực đối với tổ chức

Việc cấp phát chứng thư số cho tổ chức hoặc chứng thư số cá nhân trong tổ chức, SmartSign cần phải thực hiện xác thực tính định danh của tổ chức nhằm đảm bảo:

- Tổ chức có tên đề cập hiện có mặt tại địa điểm được ghi trong chứng thư số, bao gồm: quốc gia, tỉnh/thành phố, quận/huyện/thị xã, xã/phường/thị trấn;
- Trong trường hợp tổ chức có hiện diện tại địa điểm đó, SmartSign cần yêu cầu các tài liệu và văn bản chứng minh như: Quyết định thành lập; Điều lệ tổ chức và hoạt động; Giấy phép kinh doanh hoặc Chứng nhận đăng ký kinh doanh; Thông tin về website, quyền sở hữu tên miền (dùng cho việc cấp chứng thư số SSL); Quyết định bổ nhiệm; Thông tin về người sử dụng chứng thư số.

3.2.4 Thông tin thuê bao không xác minh

Thông tin của thuê bao không được xác thực gồm có:

- Các đơn vị, phòng ban thuộc tổ chức (Organization Unit)
- Bất kì một thông tin nào được coi là không cần xác thực trong chứng thư.

3.2.5 Xác thực thẩm quyền

Khi tên của cá nhân trong chứng thư số có liên quan tới một tổ chức, cần thực hiện:

- Xác định sự tồn tại của tổ chức thông qua ít nhất một bên thứ ba;
- Xác thực các thông tin ghi trong Phiếu yêu cầu cấp chứng thư số thông qua các tài liệu cần thiết và có thể thu thập;
- Xác định danh tính và vị trí của cá nhân trong tổ chức có tương ứng với các thông tin đã đăng ký hay không.

3.3. Xác minh đề nghị thay đổi cặp khóa

Trong thời hạn hiệu lực của chứng thư số, thuê bao có thể yêu cầu phát hành một chứng thư số mới với một cặp khoá mới. Việc yêu cầu phát hành một chứng thư số mới được thực hiện bằng cách gửi yêu cầu phát hành và khoá công khai mới được ký bằng khoá bí mật cũ tới SmartSign RA. Ngoài ra, thuê bao cần phải cung cấp đầy đủ các thông tin cần thiết sao cho khớp với thông tin đăng ký sử dụng chứng thư số gốc.

3.4. Quy trình nhận diện và xác thực thủ tục cấp lại khoá

Thủ tục thay đổi cặp khóa đảm bảo rằng cá nhân hay một tổ chức muốn cấp lại khóa cho chứng thư là chủ thuê bao của chứng thư đó.

Khi thuê bao có yêu cầu tiếp tục sử dụng chứng thư số thì chứng thư mới sẽ được tự động cấp phát. Sau khi cấp lại khoá, SmartSign RA sẽ xác nhận lại việc định danh của thuê bao sao cho phù hợp với các yêu cầu xác thực và định danh của đơn xin cấp chứng thư ban đầu.

3.5. Nhận diện và xác thực việc cấp lại khoá sau khi đã bị thu hồi

Các trường hợp không được cấp lại khoá sau khi bị thu hồi.

- Chứng thư số vi phạm hợp đồng giữa thuê bao với SmartSign.
- Phát hiện có sự thiếu sót trong việc thẩm định các giấy tờ khi đăng ký chứng thư số (Chứng minh thư hoặc hộ chiếu giả, hộ khẩu không hợp lệ…)
- Chứng thư bị thu hồi vì đã sử dụng vào các mục đích trái pháp luật…

Chứng thư của một tổ chức được khôi phục sẽ chứa cùng các thông tin đặc trưng như của chứng thư cũ. Việc khôi phục chứng thư của một cá nhân bị thu hồi chứng thư cũng cần đảm bảo rằng người đang yêu cầu được khôi phục chính là khách hàng đang sử dụng chứng thư đó.

3.6. Xác minh đề nghị thu hồi chứng thư số

Chỉ có người đứng tên thuê bao mới được phép thực hiện yêu cầu thu hồi chứng thư số. Để yêu cầu thu hồi chứng thư số, thuê bao cần liên hệ với SmartSign RA thông qua phương tiện liên lạc thích hợp bao gồm điện thoại, thư điện tử, giao dịch trực tiếp để chỉ định rõ chứng thư số cụ thể nào cần thu hồi.

Sau khi nhận được yêu cầu thu hồi, SmartSign sẽ tiến hành xác minh bằng phương thức thích hợp và gửi xác nhận lại cho thuê bao một lần nữa. Chỉ sau khi thuê bao xác nhận lại, SmartSign mới thực hiện thu hồi chưng thư số và công bố danh sách chứng thư số thu hồi lên phương tiện công bố thích hợp. Thông báo thu hồi sẽ được gửi cho thuê bao và đến đụa chỉ của các đối tượng được chỉ định từ trước.

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

4.1. Yêu cầu cấp chứng thư số

4.1.1. Đối tượng được phép yêu cầu chấp chứng thư số

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

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

4.1.2. Đăng ký cấp chứng thư số và trách nhiệm của các bên

Tất cả thuê bao đều phải ký Hợp đồng dịch vụ với SmartSign hoặc SmartSign RA được đề cập trong mục 9.6.3, sau khi thực hiện quy trình đăng ký bao gồm:

- Hoàn thành bảng kê khai, hồ sơ đăng ký cấp chứng thư số và cung cấp các thông tin đúng, chính xác;
- Sinh một cặp khóa hoặc ủy thác sinh một cặp khóa;
- Gửi khóa công khai đến SmartSign và chứng minh quyền sở hữu khóa bí mật tương ứng với khóa công khai đã gửi đến SmartSign (đối với trường hợp tự sinh cặp khóa);
- SmartSign sẽ tiến hành xác thực thông tin đã kê khai theo mục 3.2.

4.2. Thủ tục xử lý yêu cầu cấp chứng thư số

4.2.1. Thực hiện xác thực định danh

SmartSign hoặc SmartSign RA tiến hành xác thực định danh tất cả các thông tin của đối tượng yêu cầu cấp chứng thư số theo mục 3.2.

4.2.2. Chấp nhận hoặc từ chối cấp chứng thư số

SmartSign hoặc SmartSign RA chỉ chấp nhận yêu cầu cấp chứng thư số nếu thỏa mãn tất cả các điều kiện: Thực hiện xác thực định danh thành công tất cả các thông tin về đối tượng yêu cầu cấp chứng thư số theo mục 3.2; Đối tượng yêu cầu cấp chứng thư số nộp đầy đủ phí dịch vụ cấp chứng thư số cho SmartSign hoặc SmartSign RA.

SmartSign hoặc SmartSign RA từ chối yêu cầu cấp chứng thư số trong các trường hợp sau:

- Xác thực định danh không thành công ít nhất một trong các thông tin về đối tượng yêu cầu cấp chứng thư số theo phần mục 3.2;
- Đối tượng yêu cầu cấp chứng thư số không cung cấp đủ tài liệu theo yêu cầu;

- Đối tượng yêu cầu cấp chứng thư số không trả lời yêu cầu liên lạc trong hạn thời gian xác định;
- Đối tượng yêu cầu cấp chứng thư số chưa thanh toán phí dịch vụ cấp chứng thư số;
- Có căn cứ cho rằng việc SmartSign cấp chứng thư số cho đối tượng yêu cầu có thể ảnh hưởng tới uy tín và độ tin cậy của SmartSign.

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

SmartSign hoặc SmartSign RA có trách nhiệm xử lý yêu cầu cấp chứng thư số trong một khoảng thời gian phù hợp. Không quy định thời gian hoàn thành quá trình xử lý một yêu cầu cấp chứng thư số trừ khi có thỏa thuận trong Hợp đồng dịch vụ hoặc quy chế, tuy nhiên thời gian tối đa là 5 ngày làm việc. Yêu cầu cấp chứng thư số sẽ ở trạng thái có hiệu lực cho tới khi bị SmartSign từ chối.

4.3. Phát hành chứng thư số

4.3.1. Hoạt động của SmartSign khi phát hành chứng thư số

Chứng thư số được tạo và phát hành dựa trên kết quả chấp nhận yêu cầu cấp chứng thư số. SmartSign tạo và phát hành chứng thư số theo các thông tin trong bản yêu cầu cấp chứng thư số đã được xác thực định danh .

4.3.2. Thông báo cho đối tượng yêu cầu về phát hành chứng thư số

SmartSign thông báo cho thuê bao về việc phát hành chứng thư số (trực tiếp hoặc gián tiếp thông qua SmartSign RA). Thuê bao có thể lấy được chứng thư số bằng cách:

- Nhận qua USB Token.
- Tải về từ trang Web của SmartSign.

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

4.4.1. Cách thức thể hiện sự chấp nhận một chứng thư số của thuê bao

Thuê bao thể hiện sự chấp nhận một chứng thư số khi ký vào biên bản giao nhận chứng thư số của SmartSign. Biên bản giao nhận có sự xác nhận thông tin trên chứng thư số phù hợp với thông tin thuê bao. Biên bản giao nhận này được SmartSign lưu trữ.

4.4.2. SmartSign công bố chứng thư số

Sau khi thuê bao chấp nhận chứng thư số (4.4.1), SmartSign sẽ công bố chứng thư số của thuê bao.

Chứng thư số sau khi được ban hành sẽ được công bố trên Web của SmartSign và cơ sở dữ liệu LDAP.

4.4.3. Thông báo sự ban hành chứng thư số cho các đối tượng khác

SmartSign sẽ thông báo về việc chứng thư số được ban hành cho SmartSign RA đã chấp nhận đơn xin cấp chứng thư số tương ứng.

4.5. Sử dụng cặp khóa và chứng thư số

4.5.1. Cách sử dụng chứng thư số và khóa bí mật của thuê bao

Việc sử dụng khóa bí mật tương ứng với khoá công khai trong chứng thư số chỉ được cho phép khi thuê bao chấp nhận chứng thư số. Chứng thư số sẽ được sử dụng hợp pháp dựa trên các điều khoản của Hợp đồng dịch vụ, các điều khoản trong quy chế này cũng như quy định của pháp luật.

Cách sử dụng chứng thư số phải tương ứng với giá trị quy định của trường KeyUsage bên trong chứng thư số (Ví dụ nếu giá trị Digital Signature không có trong trường KeyUsage thì chứng thư số này không thể được dùng để ký điện tử).

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

4.5.2. Cách sử dụng chứng thư số và khóa công khai của người nhận

Người nhận sẽ được SmartSign đảm bảo các điều khoản về độ tin cậy của chứng thư số. Độ tin cậy của chứng thư số được xác định dựa vào từng hoàn cảnh cụ thể. Nếu hoàn cảnh chỉ ra rằng cần phải thêm sự bảo đảm, thì người nhận phải đạt được sự bảo đảm mà nó cần phải có. Trước khi được tin cậy, người nhận sẽ được đánh giá một cách độc lập các yếu tố sau:

- Chứng thư số được sử dụng vào các mục đích phù hợp và xác định rằng các mục đích đó không bị cấm hoặc bị giới hạn bởi SmartSign, quy chế hay các quy định của pháp luật. SmartSign không có trách nhiệm kiểm tra và đánh giá việc sử dụng chứng thư số của người nhận;
- Chứng thư số được sử dụng theo đúng phần mở rộng của trường KeyUsage trong chứng thư số (Ví dụ: chữ ký số mà không có hiệu lực thì chứng thư số không được tin cậy cho tính xác thực chữ ký của thuê bao);
- Kiểm tra trạng thái của chứng thư số và tất cả các CA trong chuỗi tham gia phát hành chứng thư số. Nếu bất cứ một chứng thư số nào trong chuỗi bị thu hồi, người nhận phải chịu trách nhiệm xem xét độ tin cậy của chữ ký số do thuê bao thực hiện tại thời điểm trước khi bị thu hồi có đúng đắn không. Bất cứ tin cậy nào đưa ra đều có thể gây rủi ro tới người nhận.
- Khi sử dụng chứng thư số hợp lý, người nhận cần sử dụng phương tiện phần mềm, phần cứng hợp lý nhằm tiến hành xác minh chữ ký số hoặc các thao tác mật mã cần thiết khác. Các thao tác này bao gồm cả việc xác định chuỗi chứng thư số và kiểm tra các chữ ký số trên tất cả chứng thư số trong chuỗi.

4.6. Gia hạn chứng thư số

Gia hạn chứng thư số là việc phát hành chứng thư số mới cho thuê bao. Việc gia hạn chứng thư số mới này khách hàng có thể yêu cầu giữ nguyên khóa cũ hoặc tạo cặp khóa mới, mà không thay đổi bất cứ thông tin nào khác trên chứng thư số nếu khách hàng không có yêu cầu thay đổi thông tin. Tuy nhiên SmartSign vẫn khuyến cáo các khách hàng sử dụng chứng thư số với thời hạn lớn hơn 3 năm, nên tạo khóa mới để đảm bảo an toàn khóa.

4.6.1. Điều kiện gia hạn

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

4.6.2. Đối tượng được phép yêu cầu gia hạn

Chỉ có thuê bao cá nhân hoặc đại diện theo pháp luật của tổ chức đối với thuê bao tổ chức mới được phép yêu cầu gia hạn chứng thư số.

4.6.3. Xử lý yêu cầu gia hạn chứng thư số

Thuê bao cần tiến hành các thủ tục đã đề cập trong mục 4.1.2 trong Phiếu yêu cầu gia hạn chứng thư số theo mẫu do SmartSign ban hành.

SmartSign RA tiến hành xác thực thông tin của thuê bao trong Phiếu yêu cầu gia hạn chứng thư số theo mục 3.2. Nếu thông tin xác thực, việc gia hạn được tiến hành. Nếu thông tin sai lệch, yêu cầu bị từ chối.

4.6.4. Thông báo cho thuê bao về việc phát hành chứng thư số mới

Việc thông báo cho thuê bao về việc phát hành chứng thư số mới tuân theo quy định ghi tại mục 4.3.2.

4.6.5. Điều khoản chấp nhận gia hạn chứng thư số

Tương tự 4.4.1.

4.6.6. Công bố chứng thư số được gia hạn

Tương tự 4.4.2.

4.6.7. Thông báo đến các đối tượng khác về việc gia hạn chứng thư số

Tương tự 4.4.3.

4.7. Khôi phục chứng thư số

4.7.1. Trường hợp khi cần khôi phục chứng thư

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

4.7.2. Đối tượng yêu cầu khôi phục chứng thư

Chủ sơ hữu của chứng thư có thể yêu cầu khôi phục chứng thư trước khi nó hết hạn bằng cách gửi cho SmartSign RA tương ứng một e-mail ký với khóa bí mật của chứng thư yêu cầu khôi phục.

4.7.3. Quy trình xử lý các yêu cầu khôi phục chứng thư

Khi nhận được yêu cầu xác nhận bởi SmartSign RA, SmartSign sẽ xử lý yêu cầu khôi phục chứng thư như một yêu cầu cấp chứng thư ban đầu.

4.7.4. Điều kiện chấp nhận khôi phục chứng thư

Tương tự 4.4.1.

4.7.5. Công bố các chứng thư được khôi phục

Tương tự 4.4.2.

4.7.6. Thông báo việc cấp chứng thư của SmartSign đến các đối tượng khác

Tương tự 4.4.3.

4.8. Thay đổi thông tin chứng thư số

Sửa đổi chứng thư số là việc SmartSign phát hành chứng thư số mới cho thuê bao thay đổi các thông tin trong chứng thư số ngoại trừ khóa công khai.

4.9.1. Điều kiện sửa đổi chứng thư số

Sửa đổi chứng thư số được xem như yêu cầu cấp chứng thư số theo phần 4.1.

4.9.2. Đối tượng được phép yêu cầu sửa đổi chứng thư số

Tương tự 4.1.1.

4.9.3. Xử lý yêu cầu sửa đổi chứng thư số

SmartSign tiến hành xác thực định danh thông tin của thuê bao theo phần 3.2.

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

Tương tự 4.3.2.

4.9.5. Điều khoản chấp nhận sửa đổi chứng thư số

Tương tự 4.4.1

4.9.6. Công bố chứng thư số đã sửa đổi

Tương tự 4.4.2.

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

Xem phần 4.4.3.

4.10. Tạm dừng và thu hồi chứng thư số

4.10.1. Các trường hợp thu hồi chứng thư số

Một chứng thư được thu hồi trong những trường hợp sau đây:

- Thuê bao đã ngừng hoặc thôi đại diện cho một tổ chức;
- Thuê bao yêu cầu không sử dụng chứng thư;
- Khoá của chứng thư bị mất hoặc bị xâm hại;
- Những thông tin trong chứng thư sai hoặc không chính xác;
- Hệ thống được cấp chứng thư đã dừng;
- Thuê bao không thực hiện đúng các quy tắc của chính sách này.
- Thuê bao là cá nhân đã chết hoặc mất tích theo tuyên bố của tòa án hoặc thuê bao là tổ chức giải thể hoặc phá sản theo quy định của pháp luật hoặc khi có yêu cầu của cơ quan tiến hành tố tụng, cơ quan an ninh hoặc Bộ Thông tin và Truyền thông.

4.10.2. Đối tượng có thể yêu cầu thu hồi

Yêu cầu thu hồi chứng thư được thực hiện bởi:

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

4.10.3. Thủ tục yêu cầu thu hồi chứng thư

Thuê bao chứng thư số gửi một e-mail ký với khóa bí mật của chứng thư (chưa hết hạn) yêu cầu thu hồi.

Trong trường hợp khẩn cấp, nếu không gửi được e-mail việc thu hồi chứng thư có thể thông báo trực tiếp với 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.

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

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

4.10.5. Thời gian SmartSign xử lý yêu cầu thu hồi chứng thư

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

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

Trước khi sử dụng một chứng thư số, bên nhận phải xác nhận CRL gần đây nhất. SmartSign 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.

4.10.7. Tần số cấp phát CRL

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

4.10.8. Thời gian trễ tối đã cho các CRL

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

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

Thông tin trạng thái chứng thư và thông tin thu hồi chứng thư được lưu trữ trực tuyến trên kho của SmartSign 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.

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

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

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

4.11. Kiểm tra trạng thái chứng thư số

4.11.1. Các đặc tính hoạt động

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

- Chứng thư của SmartSign.
- Chứng thư cấp bởi SmartSign.
- Danh sách thu hồi cập nhật mới nhất.

4.11.2. Tính sẵn sàng của dịch vụ

Dịch vụ cung cấp trạng thái hoạt động của chứng thư luôn sẵn sàng 24/7.

4.11.3. Các đặc tính tuỳ chọn

OCSP có thể sẽ thu phí.

4.12. Chấm dứt dịch vụ của thuê bao

Thuê bao có thể kết thúc hợp đồng sử dụng dịch vụ chứng thư của SmartSign khi:

- Chứng thư hết hạn sử dụng mà không gia hạn.
- Thu hồi chứng thư trước khi chứng thư hết hạn mà không thay thế bằng một chứng thư khác.

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

4.13.1. Chính sách và thực hiện cam kết khôi phục khoá

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

4.13.2. Chính sách và thực hiện phục hồi khóa

Xem mục 4.12.

5. KIỂM SOÁT, QUẢN LÝ VÀ VẬN HÀNH

5.1. Kiểm soát an toàn, an ninh vật lý

5.1.1 Vị trí

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

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 hoà và nguồn điện

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

Các Server của hệ thống SmartSign 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 cháy chữa cháy

SmartSign thiết kế tuân thủ luật pháp phòng cháy chữa cháy của Việt Nam.

5.1.6 Phương tiện lưu trữ

Phương tiện lưu trữ dữ liệu của SmartSign được bảo vệ tương đương với mức độ quan trong của dữ liệu mà hệ thống đó lưu trữ.

Phương tiện lưu trữ dữ liệu backup cũng được bảo vệ tương tự như hệ thống chính.

5.1.7 Xử lý rác

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

5.1.8 Dự phòng từ xa

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 cách nhau >30km. 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. Quy trình kiểm soát

5.2.1 Những thành viên được tin cậy

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

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

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

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

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

5.2.2 Số lượng người yêu cầu cho mỗi công việc

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

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

Những thủ tục điều khiển ở bên trong được thiết kế để đảm bảo ít nhất 02 cá nhân được tin tưởng cùng tham gia truy cập tới mức vật lý hoặc mức logic của thiết bị truy cập tới phần cứng mã hoá yêu cầu chặt chẽ phải có nhiều người được tin tưởng cùng tham gia toàn bộ quá trình làm việc từ việc nhận và kiểm tra cho tới bước cuối cùng là huỷ về logic hoặc về vật lý.

5.2.3 Nhận dạng và xác thực cho từng thành viên

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. Quá trình nhận dạng được trình bày trong phần 5.3.1.

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 yêu cầu phân chia trách nhiệm

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

- Xác thực thông tin trong đơn xin cấp chứng thư.
- Quá trình chấp nhận, từ chối, hoặc các quá trình khác của đơn xin cấp chứng thư, yêu cầu thu hồi, cấp mới hay các thông tin đăng ký.
- Quá trình ban hành, thu hồi các chứng thư, bao gồm những cá nhân được truy cập tới những phần hạn chế truy cập của kho lưu trữ.
- Quá trình chuyển giao những thông tin thuê bao hay các yêu cầu từ khách hàng.
- Quá trình tạo, ban hành hay tiêu huỷ chứng thư số.

5.3. Kiểm soát nhân sự

5.3.1 Năng lực, kinh nghiệm và các yêu cầu khác

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

5.3.2 Thủ tục kiểm tra lai lịch

Trước khi nhân viên bắt đầu việc làm trong một vai trò được tin cậy, 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

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 thoả hiệp và các vấn đề liên quan;
- Thủ tục khôi phục sau thảm hoạ và duy trì công việc.

5.3.4 Chu kỳ tái đào tạo

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 là bắt buộc khi hệ thống sử dụng phần mềm hoặc các tính năng mới cũng như khi có các thủ tục mới được triển khai.

5.3.5 Kỷ luật đối với các hoạt động không hợp pháp

SmartSign thiết lập, duy trì và áp đặt các chính sách đối với hành động bất hợp pháp. Các biện pháp kỷ luật có thể bao gồm đánh giá, và có thể chấm dứt hợp đồng phụ thuộc vào tần suất và mức độ nghiêm trọng của các hành động bất hợp pháp.

5.3.6 Yêu cầu đối với các nhà thầu độc lập

Các SmartSign RA và các nhà thầu hay nhà tư vấn độc lập cần sự tin tưởng của SmartSign. Những người này cũng phải tuân theo các tiêu chuẩn an ninh như nhân viên của SmartSign. Nếu những người này không đáp ứng đủ các tiêu chí trong 5.3.2, họ chỉ được phép thực hiện công việc khi có sự giám sát của người được tin tưởng của SmartSign.

5.3.7 Cung cấp tài liệu cho nhân viên

SmartSign cung cấp các tài liệu cần thiết để nhân viên có thể hoàn thành tốt công việc của mình.

5.4. Các quy trình ghi nhật ký hệ thống

5.4.1 Các loại bản ghi sự kiện

Những sự kiện sau đây được ghi lại:

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

5.4.2 Tần suất xử lý bản ghi sự kiện

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

5.4.3 Thời gian duy trì cho bản ghi

Khoảng thời gian lưu giữ tối thiểu đối với các bản ghi là 02 tháng sau khi xử lý và sau đó được chuyển sang khu vực lưu trữ (phần 5.5.2).

5.4.4 Bảo vệ các bản ghi

Bản ghi sẽ được bảo vệ bằng hệ thống bản ghi kiểm định điện tử bao gồm các cơ chế bảo vệ bản ghi log trước các truy cập, sửa đổi, xoá bỏ hoặc can thiệp bất hợp pháp. Bản ghi kiểm định chỉ được truy cập bởi các người quản trị hệ thống và bảo đảm an toàn an ninh hệ thống.

5.4.5 Thủ tục sao lưu dự phòng cho các bản ghi

Các bản ghi được dự phòng theo chế độ lưu trữ và dự phòng chung của SmartSign.

5.4.6 Hệ thống thu thập bản ghi

Các log ứng dụng, hệ điều hành và mạng được ghi lại tự động.

Một số log được ghi bằng tay bởi nhân viên.

5.4.7 Thông báo về nguyên nhân sự kiện

Khi một sự kiện được ghi nhật ký, không có thông báo cho đối tượng gây ra sự kiện đó.

5.4.8 Đánh giá điểm yếu

Không quy định.

5.5. Lưu trữ các bản ghi

5.5.1 Những kiểu bản ghi được lưu trữ

Xem 5.4.1.

5.5.2 Thời gian duy trì tài liệu lưu trữ

Khoảng thời gian lưu giữ tối thiểu là 10 năm.

5.5.3 Bảo mật tài liệu lưu trữ

Các lưu trữ chỉ được truy cập bởi các nhân viên được phép của SmartSign. Dữ liệu lưu trữ được bảo vệ theo các phương pháp cần thiết, chống lại việc xem, thay đổi, xóa hay các thao tác khác không được cho phép.

Hệ thống chứa dữ liệu lưu trữ và ứng dụng xử lý dữ liệu lưu trữ được duy trì để đảm bảo dữ liệu lưu trữ có thể được truy nhập trong khoảng thời gian được quy định trong quy chế chứng thực này .

5.5.4 Thủ tục sao lưu và dự phòng dữ liệu

Dữ liệu được dự phòng theo chế độ dự phòng chung của SmartSign.

5.5.5 Yêu cầu nhãn thời gian cho dữ liệu

Tất cả các bản ghi sự kiện đều chứa thời gian, ngày, tháng, năm.

5.5.6 Hệ thống lưu trữ

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

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

Chỉ những người được cấp quyền mới được phép truy nhập tới thông tin lưu trữ.

Thông tin lưu trữ sẽ được kiểm tra tính toàn vẹn khi được lấy ra .

5.6. Chuyển tiếp khóa

Chứng thư số của SmartSign có thể được Bộ Thông tin và Truyền thông gia hạn, cấp mới với điều kiện thời gian hiệu lực còn lại của chứng thư số SmartSign lớn hơn thời gian hiệu lực của chứng thư số cấp cho thuê bao là 90 ngày.

Quy trình và thủ tục thay đổi cặp khóa được tuân theo nội dung nghị định 130/2018/NĐ-CP.

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

5.7.1 Các thủ tục kiểm soát sự cố và thảm họa

- Các thông tin sau được dự phòng đề phòng có sự cố và thảm họa: dữ liệu về đơn xin cấp chứng thư số, dữ liệu nhật ký, và các bản ghi chứng thư số được tạo ra.
- Khi có sự cố, các dữ liệu được phục hồi theo các thủ tục đã có.

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

Khi có các sự cố về máy tính, phần mềm và dữ liệu, các thủ tục xử lý sự cố được thực hiện. Mỗi sự cố sẽ có các quy trình xử lý khác nhau. Nếu sự cố nghiêm trọng, các thủ tục phục hồi sẽ được thực hiện

5.7.3 Thủ tục xử lý vấn đề lộ khoá và sự cố

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

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

- Thông báo tới cơ quan an ninh liên quan và Trung tâm Chứng thực chữ ký số Quốc gia;

5.7.4 Khả năng phục hồi hoạt động sau thảm họa

SmartSign thực hiện khôi phục hoạt động sau thảm họa theo kế hoạch dự phòng. Hệ thống dự phòng sẽ được kích hoạt trong vòng 60 phút đảm bảo việc cung cấp dịch vụ không bị gián đoạn. Quy trình kích hoạt hệ thống dự phòng được thực hiện như sau:

- Nhận thông báo sự cố của hệ thống từ Trung tâm dữ liệu chính;
- Quản trị hệ thống đánh giá sự cố và nếu cần thiết ra lệnh kích hoạt trung tâm dự phòng;
- Phụ trách an toàn thông tin truy cập hệ thống dự phòng và tiến hành khôi phục dữ liệu từ Backup Database vào các server chức năng (CA, RA, LDAP, OCSP, CRL);
- Phụ trách an toàn thông tin truy cập hệ thống quản lý domain;
- Phụ trách an toàn thông tin chuyển hướng DNS dịch vụ về hệ thống dự phòng;

Sau khi sự cố được khắc phục thì hệ thống chính và hệ thống dự phòng sẽ trở lại như cũ.

5.8. Dừng hoạt động

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

- Thông báo với Bộ Thông tin và Truyền thông và Trung tâm Chứng thực chữ ký số quốc gia để làm các thủ tục chấm dứt cung cấp dịch vụ;
- Bằng tất cả khả năng có thể để thông báo cho các thuê bao và RA càng sớm càng tốt;
- Thông báo việc chấm dứt trên diện rộng;
- Ngừng cấp chứng thư số;
- Thu hồi tất cả các chứng thư số;
- Tiêu huỷ tất cả các bản sao khóa bí mật của SmartSign.
- Thực hiện các thủ tục chuẩn bị trước khi chuyển các dịch vụ chứng thực sang cho CA khác.

6. ĐẢM BẢO AN TOÀN AN NINH VỀ KỸ THUẬT

6.1. Tạo và phân phối cặp khoá

6.1.1 Tạo cặp khoá

Cặp khoá cho SmartSign được sinh ra trong thiết bị phần cứng đạt chuẩn FIPS 140-2 level 3.

Cặp khóa của thuê bao được tạo bên phía thuê bao hoặc trên USB Token / PKI Card trong trường hợp thuê bao có thỏa thuận cho phép tạo khóa phía SmartSign.

6.1.2 Chuyển giao khoá bí mật cho thuê bao

Quy trình bàn giao USB Token / PKI Card và khóa bí mật cho thuê bao như sau:

Đến ngày hẹn, SmartSign hoặc SmartSign RA sẽ liên hệ và giao trực tiếp USB Token / PKI Card đã có cặp khóa và chứng thư số cho khách hàng. Đồng thời làm biên bản bàn giao chứng thư số, trên đó ghi thông tin của thuê bao và thông tin chứng thư số. Chứng thư số sẽ được công bố trong vòng 24 giờ sau khi bàn giao cho thuê bao.

Nếu khách hàng ở xa, USB Token / PKI Card sẽ được chuyển đến tận tay khách hàng bằng dịch vụ chuyển phát bảo đảm. SmartSign hoặc SmartSign RA sẽ hướng dẫn cho khách hàng:

- Kiểm tra thông tin CTS, hướng dẫn sử dụng và bàn giao các giấy tờ liên quan;
- Hướng dẫn khách hàng kiểm tra USB Token / PKI Card và tự đổi, kiểm tra mật khẩu mới.

6.1.3 Chuyển giao khoá công khai tới SmartSign

Khóa công khai được thuê bao gửi cho SmartSign thông qua thông điệp dạng PKCS#10. Nếu cặp khóa được tạo bên phía SmartSign, việc gửi khóa cho CA là không cần thiết.

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

Người nhận có thể tải về khóa công khai của SmartSign và RootCA từ trang Web của SmartSign.

Việc gửi khóa này cũng thông qua một phiên SSL để đảm bảo an ninh.

6.1.5 Kích thước khoá

Chuẩn hiện tại của dịch vụ SmartSign yêu cầu chiều dài tối thiểu của cặp khoá để đảm bảo mức độ mã hoá đủ mạnh là 1024 bits RSA.

Khoá của SmartSign có chiều dài là 2048 bits.

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

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

6.1.7 Mục đích sử dụng khoá (như trong X.509 v3 trường Key Usage)

Khoá được sử dụng theo mỗi loại chứng thư:

- Với thuê bao:
  - Chứng thực;
  - Chống chối bỏ;
  - Mã hoá dữ liệu;
  - Thiết lập phiên giao dịch;
  - Kiểm tra tính toàn vẹn của dữ liệu.
- Với chứng thư tự ký của CA
  - Ký chứng thư;
  - Ký CRL;
  - Thu hồi chứng thư.

6.2. Kiểm soát và bảo vệ khóa bí mật

6.2.1 Tiêu chuẩn hoá mô đun mã hoá

Hệ thống SmartSign sử dụng thiết bị HSM UTIMACO SAFEGUARD CRYPOSERVER SE10 LAN với các tính năng sau:

a) Tiêu chuẩn bảo mật

- FIPS 140-2 Level 3
- PCI HSM
- CE, FCC Class B
- UL, IEC/EN 60950-1
- CB certificate
- RoHS II, WEEE

b) Các chức năng

- Lưu trữ và xử lý khóa một cách bảo mật
- Lưu trữ khóa trong thiết bị hoặc lưu trữ file chứa khóa được mã hóa.
- Xác thực truy cập bằng smart card theo phương thức n/m

c) Thuật toán mã hóa

- RSA
- ECDSA, NIST and Brainpool curves
- DSA.

6.2.2 Cơ chế kiểm soát khoá bí mật

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 Lưu giữ ngoài khóa bí mật của thuê bao

Lưu giữ ngoài khóa bí mật của thuê bao được trình bày trong phần 4.12.

6.2.4 Sao lưu dự phòng khoá bí mật

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

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

6.2.5 Lưu trữ khoá bí mật

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

6.2.6 Cách thức sao lưu khoá bí mật

SmartSign giữ khóa trên một HSM và một bản sao khóa để dự phòng phục vụ cho trường hợp phục hồi hệ thống trên một HSM khác. Khóa bí mật sẽ được mã hóa trong quá trình chuyển giữa 2 HSM. Công việc này để đề phòng khi HSM chính bị hư hỏng vật lý, hoặc do thiên tai thảm họa xảy ra thì kích hoạt HSM dự phòng đã được sao lưu khóa bí mật.

6.2.7 Lưu trữ khóa bí mật trong HSM

SmartSign giữ khóa bí mật trong các HSM, khóa bí mật được lưu dưới dạng được mã hóa.

6.2.8 Phương thức huỷ khoá bí mật

Việc xóa khóa bí mật được thực hiện theo phương pháp an toàn, đảm bảo không thể phục hồi lại khóa đã xóa.

- Khóa bí mật lưu trên USB Token được xóa bằng phần mềm quản trị USB Token
- Khóa bí mật lưu trên HSM được xóa bằng chức năng xóa khóa của HSM
- Các hoạt động hủy bỏ khóa bí mật được ghi nhật ký.

6.2.9 Phương thức kích hoạt khoá bí mật

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

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

Đối với 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 n/m.

6.2.10 Phương thức ngừng kích hoạt khoá bí mật

Khóa bí mật của SmartSign bị ngừng kích hoạt khi không chứa trong HSM.

Khóa bí mật của thuê bao bị ngừng khi ngưng kết nối USB Token khỏi máy tính. Trong mọi trường hợp, thuê bao phải có nghĩa vụ thực hiện các biện pháp bảo vệ khóa bí mật của mình.

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

6.3.1 Lưu trữ khoá công khai

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

6.3.2 Thời gian hoạt động của chứng thư và của cặp khoá

Thời hạn sử dụng của chứng thư số sẽ kết thúc khi chứng thư số đó hết hạn hoặc bị thu hồi.

Thời hạn sử dụng cặp khóa của thuê bao giống như thời hạn sử dụng của chứng thư số, ngoại trừ chức năng giải mã và kiểm tra chữ ký sau khi chứng thư số hết hạn.

SmartSign không ban hành các chứng thư số có thời hạn sử dụng vượt quá thời hạn sử dụng chứng thư số của CA.

Chứng thư số mà SmartSign cung cấp cho thuê bao tùy thuộc vào thỏa thuận với thuê bao, thông thường là 1 năm. Chứng thư số cũng có thể kéo dài đến 2 năm hoặc hơn với các điều kiện sau:

- Thuê bao được yêu cầu thực hiện lại các thủ tục xác thực ít nhất 12 tháng một lần (phần 3.2.3).
- Thuê bao phải chứng minh quyền sở hữu khóa bí mật ít nhất 12 tháng một lần.

Nếu điều kiện trên không được thực hiện, SmartSign sẽ tự động thu hồi chứng thư số thuê bao.

6.4. Kích hoạt dữ liệu

6.4.1 Quá trình tạo và cài đặt dữ liệu kích hoạt

SmartSign quy định 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.

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 .

6.4.2 Bảo vệ dữ liệu kích hoạt

Người giữ mã chia sẻ của SmartSign được yêu cầu bảo vệ an toàn mã chia sẻ của họ. Những người này phải ký một thỏa thuận với SmartSign về việc đảm bảo trách nhiệm trong việc bảo vệ mã chia sẻ mà họ giữ.

Thuê bao của SmartSign được yêu cầu lưu trữ các khóa bí mật của họ ở dạng mã hoá sử dụng USB Token và mật khẩu đủ mạnh. SmartSign khuyến cáo thuê bao định kỳ thay đổi mật khẩu.

6.4.3 Những khía cạnh khác của dữ liệu kích hoạt.

Không có quy định.

6.5. Kiểm soát an ninh máy tính

6.5.1 Các yêu cầu về kỹ thuật bảo mật máy tính

SmartSign đảm bảo rằng các máy chủ cài đặt hệ thống CA và dữ liệu được bảo vệ trước các truy nhập không được phép. SmartSign giới hạn quyền truy nhập tới CA

server theo vai trò của quản trị. Trên các máy chủ cài đặt hệ thống CA, không có ứng dụng nào khác được cài đặt thêm.

Hệ thống mạng của SmartSign được cách ly với các thành phần khác, bảo vệ khỏi sự truy cập bất hợp pháp. Sự cách ly này được thực hiện bằng hệ thống tường lửa đa lớp. Lớp tường lửa bên ngoài bảo vệ cả hệ thống khỏi các truy nhập từ ngoài. Lớp tường lửa bên trong cách ly các server CA ra khỏi hệ thống mạng chung của SmartSign. Các quản trị viên của SmartSign chỉ truy nhập và quản trị hệ thống thông qua một số giới hạn các máy tính quản trị được xác định sẵn.

SmartSign yêu cầu sử dụng mật khẩu theo các tiêu chí trong phần 6.4.1, mật khẩu được định kỳ được thay đổi.

Việc truy nhập trực tiếp dữ liệu của CA chỉ được giới hạn cho những người có quyền và nhiệp vụ phù hợp.

6.5.2 Đánh giá bảo mật máy tính

Nhân viên quản lý an ninh hoặc bên thứ ba sẽ đánh giá dựa theo quy trình quản lý rủi ro và an toàn hệ thống thông tin định kỳ 06 tháng một lần.

6.6 Kiểm soát vòng đời

6.6.1 Giám sát triển khai triển khai hệ thống

Các ứng dụng được phát triển và triển khai sử dụng trong SmartSign tuân theo các tiêu chuẩn thiết kế, phát triển và triển khai phần mềm của SmartSign.SmartSign cũng cung cấp phần mềm cho các SmartSign RA.

Phần mềm được SmartSign phát triển sẽ được ký số đảm bảo trong quá trình phân phối không bị thay đổi nội dung hoặc phiên bản. Chữ ký trên phần mềm sẽ được kiểm tra khi phần mềm được cài đặt.

6.6.2 Giám sát quản lý an ninh

SmartSign có các thủ tục và biện pháp kiểm soát an ninh trong quá trình thiết lập hệ thống. Các thủ tục và biện pháp này tuân theo tiêu chuẩn quản lý theo Phương án Kỹ thuật.

6.6.3 Giám sát an ninh vòng đời

SmartSign không quy định cụ thể quy trình giám sát an ninh vòng đời phát triển, triển khai và vận hành hệ thống cung cấp dịch vụ của SmartSign.

6.6. Giám sát an ninh hệ thống mạng

Hệ thống SmartSign thực hiện các chức năng trong vùng mạng đảm bảo an ninh. Mọi thông tin nhạy cảm sẽ được mã hóa và ký số.

6.7. Dấu thời gian (Time-Stamping)

Các chứng chỉ, thông tin thu hồi (CLS, OCSP) có chứa thông tin về thời gian và ngày. Các thông tin thời gian cần thiết như trên không được mã hoá.

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

7.1. Định dạng của chứng thư số

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

Tên trường	Giá trị
Số hiệu chứng thư/ Serial Number	Do SmartSign gán, là định dang duy nhất của chứng thư số
Tên của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng/ Issuer	SmartSign
Thời điểm chứng thư bắt đầu có hiệu lực/ Not Before	Thời điểm chứng thư bắt đầu có hiệu lực. Sử dụng UTCTime.
Thời điểm chứng thư hết hiệu lực/ Not After	Thời điểm chứng thư hết hiệu lực. Sử dụng UTCTime.
Tên của thuê bao/ Subject	Tên của thuê bao
Khóa công khai của thuê bao/ Subject Public Key Info	RSA (2048 bits)
Thuật toán chữ ký số áp dụng/Signature Algorithm	SHA256RSA
Chữ ký số của trung tâm chứng thư số / Signature	Chữ ký số của trung tâm chứng thư số SmartSign
Các thông tin khác cho mục đích quản lý, sử dụng, an toàn, bảo mật do tổ chức cung cấp dịch vụ chữ ký số quy định.	

7.1.1 Phiên bản

SmartSign phát hành chứng thư X.509 phiên bản 3.

7.1.2 Phần mở rộng của chứng thư

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

Chứng thư số dùng cho cá nhân, tổ chức

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

	keyEnciphermnet dataEncipherment keyAgreement
Extended Key Usage	clientAuth codeSigning emailProtection timeStamping
Certificate Policies	OID của quy chế 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 quy chế này.
Issuer Alternative Name	Liên kết (URL) đến chứng thư của SmartSign
CRL Distribution Points	URL của CRL

Chứng thư số dùng cho dịch vụ / Máy chủ

Basic Constraints	critical, ca: false
Subject Key Identifier	hash
Authority Key Identifier	keyid
Key Usage	digitalSignature nonRepudiation keyEnciphermnet dataEncipherment keyAgreement
Extended Key Usage	clientAuth serverAuth
Certificate Policies	OID của quy chế 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 (URL) đến chứng thư của SmartSign
CRL Distribution Points	URL của CRL

7.1.3 Thuật toán ký

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

- sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
- sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- Thủ tục ký chứng thư số áp dụng lược đồ RSASSA -PSS được quy định trong PKCS #1 phiên bản 2.1

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

7.1.4 Cấu trúc tên

Mỗi chứng thư có một tên duy nhất và rõ ràng tên phân biệt trong tất cả các chứng thư phát hành bởi SmartSign và tuân theo cấu trúc được định nghĩa trong tiêu chuẩn ITU-T Standards Recommendation X.501.

7.1.5 Ràng buộc tên

Không có những ràng buộc khác hơn so với quy định tại mục 0, và **Error! Reference source not found.**.

7.1.6 Định danh chính sách và quy chế chứng thư số

Không có ràng buộc nào.

7.1.7 Sử dụng ràng buộc mở rộng chính sách chứng thư số

Không có ràng buộc nào.

7.1.8 Cú pháp và ngữ nghĩa của chính sách phân loại

Không có quy định.

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

Không có quy định.

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

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

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

7.2.1 Phiên bản

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 số trực tuyến (OCSP)

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

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

7.3.1 Phiên bản

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

7.3.2 Phần mở rộng của OCSP

Không quy định.

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

8.1. Tần suất và tình huống kiểm tra kỹ thuật

Các cuộc kiểm tra sự tuân thủ điều khoản quy chế được tiến hành ít nhất mỗi năm một lần.

SmartSign tiến hành kiểm tra sự tuân thủ các thủ tục của mỗi RA với quy chế có hiệu lực ít nhất mỗi năm một lần.

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

Đơn vi, người kiểm tra sẽ được nhân viên quản lý an ninh xác định dựa theo quy trình quản lý rủi ro và an toàn hệ thống thông tin hồ sơ kỹ thuật hoặc hợp đồng với bên thứ ba.Các nội dung kiểm tra kỹ thuật.

8.3. Mối quan hệ của người kiểm tra kỹ thuật với đối tượng được kiểm tra

Kiểm tra kỹ thuật được thực hiện bởi những người không phụ thuộc vào SmartSign.

8.4. Các nội dung kiểm tra kỹ thuật

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

- Hạ tầng hệ thống.
- Các quy trình quản lý khóa.
- Quy trình vận hành hệ thống.

Các nội dung khác theo yêu cầu của đơn vị kiểm tra kỹ thuật.

8.5. Xử lý khi phát hiện sai sót

Khi phát hiện sai sót, sự cố, SmartSign sẽ dựa theo quy trình quản lý rủi ro, sự cố an toàn thông tin và cải tiến hệ thống trong phương án kỹ thuật của SmartSign.

8.6. Công bố kết quả kiểm tra kỹ thuật

SmartSign sẽ công bố kết quả trên trang web của SmartSign với thông tin chi tiết về sự vi phạm quy chế.

8.7. Tần suất và các trường hợp đánh giá

SmartSign phải hành động ngay lập tức nếu đánh giá cho thấy một sự vi phạm các quy định trong quy chế. 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.

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

Danh tính và khả năng của đơn vi, người kiểm tra sẽ được nhân viên quản lý an ninh xác định dựa theo quy trình quản lý rủi ro và an toàn hệ thống thô ng tin trong phương án kỹ thuật, hồ sơ nhân sự hoặc hợp đồng với bên thứ ba.

9. CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC

9.1. Phí/Giá

9.1.1 Lệ phí cấp Chứng thư hoặc gia hạn chứng thư

Khách hàng của dịch vụ SmartSign phải trả phí cho việc ban hành, quản lý, và gia hạn chứng thư số. Mức phí sẽ tùy thuộc vào hợp đồng với từng thuê bao.

9.1.2 Lệ phí sử dụng chứng thư

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

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

SmartSign không thu phí cho việc phát hành các CRL. Tuy nhiên SmartSign sẽ thu phí khi cung cấp dịch vụ OCSP hoặc các dịch vụ cung cấp thông tin trạng thái khác.

9.1.4 Lệ phí sử dụng cho các dịch vụ khác

Không quy định.

9.1.5 Chính sách hoàn trả phí

SmartSign sẽ thực hiện việc hoàn phí cho thuê bao theo các điều khoản thỏa thuận với thuê bao.

9.2. Trách nhiệm tài chính

9.2.1 Đăng thông tin bảo hiểm

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

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.

9.2.2 Các trường hợp SmartSign tiến hành đền bù bảo hiểm

SmartSign tiến hành đền bù bảo hiểm cho các trường hợp sau:

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

9.2.3 Các trường hợp không được đền bù bảo hiểm

SmartSign không chịu trách nhiệm trong các trường hợp:

- Các trường hợp sử dụng chứng thư vi phạm điều khoản trong quy chế này.
- Các trường hợp sử dụng, cấu hình thiết bị không đúng, không nằm trong trách nhiệm của CA được sử dụng trong quá trình xử lý chứng thư.
- Khoá bí mật bị mất, xâm hại hay bị phá huỷ do khách hàng.

9.2.4 Các tài sản khác

Không quy định.

9.3. Bảo mật các thông tin nghiệp vụ

9.3.1 Phạm vi của thông tin cần bảo mật

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

- Các thông tin được yêu cầu bởi pháp luật.
- Hồ sơ đăng ký cấp chứng thư số.
- Biên bản giao dịch.
- Nhật ký kiểm tra SmartSign.
- Báo cáo kiểm tra SmartSign.
- Kế hoạch đối phó với sự cố và kế hoạch khôi phục lại sau thảm họa.
- Phương pháp điều khiển hoạt động các thành phần SmartSign: phần cứng, phần mềm và quản trị của dịch vụ của SmartSign, dữ liệu CA, được phê chuẩn hoặc không phê chuẩn;
- Các khoá bí mật của thuê bao;
- Các dữ liệu kiểm toán.

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

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

9.3.3 Trách nhiệm bảo vệ các thông tin bí mật

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

9.4. Bảo mật thông tin cá nhân

9.4.1 Kế hoạch đảm bảo tính bảo mật

Thông tin của khách hàng, doanh nghiệp được SmartSign phân thành dữ liệu cơ bản và dữ liệu nhạy cảm. Trong đó dữ liệu cơ bản gồm tên, mã số thuế, ngày cấp, và các thông tin được ghi trên chứng thư số sẽ được công khai trên LDAP và chứng thư số. Và dữ liệu nhạy cảm gồm thông tin đăng ký, gia hạn, và các thông tin được sử dụng nhằm đăng ký, gia hạn chứng thư số sẽ được SmartSign lưu trữ trong khu vực bảo mật cao.

9.4.2 Những thông tin được coi là bảo mật

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

9.4.3 Thông tin không được coi là bảo mật

Thông tin có trong chứng thư và các CRL do SmartSign phát hành không được coi là bảo mật. Khi yêu cầu một chứng thư từ SmartSign, các thuê bao đã đồng ý bao gồm các thông tin này như một phần của chứng thư được công bố.

9.4.4 Trách nhiệm bảo vệ thông tin riêng tư

SmartSign RA có trách nhiệm bảo vệ thông tin bảo mật của các thuê bao và phải tuân theo những luật bảo mật trong phạm vi quyền hạn của mình.

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

Trong trường hợp SmartSign RA muốn sử dụng thông tin bảo mật của thuê bao phải được các thuê bao đồng ý bằng văn bản.

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

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.

9.4.7 Những trường hợp làm lộ thông tin khác

Không quy định.

9.5. Quyền sở hữu trí tuệ

SmartSign sở hữu và đăng ký quyền sở hữu trí tuệ liên quan đến tất cả các cơ sở dữ liệu, các trang web, chứng thư số của SmartSign và công bố bất kỳ nào khác có nguồn gốc từ SmartSign bao gồm quy chế 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 SmartSign

SmartSign đảm bảo rằng:

- Không thay đổi thông tin đăng ký chứng thư số được cung cấp bởi đối tượng đăng ký.
- Không có lỗi trong quá trình duyệt và ban hành chứng thư số.
- Chứng thư số do SmartSign 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 SmartSign RA theo quy định của pháp luật..

9.6.2 Tuyên bố và cam kết của SmartSign RA

SmartSign RA đảm bảo rằng:

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

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

- Loại chứng thư số mà SmartSign RA được phép tham gia cung cấp.
- Các bước trong quy trình cấp phát chứng thư số SmartSign RA được thực hiện.
- Chứng thư 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 SmartSign RA với SmartSign đúng như trong hợp đồng đã ký và theo quy định của pháp luật.
- Nhân viên SmartSign RA trực tiếp tham gia vào quy trình cung cấp chứng thư số phải có hiểu biết pháp luật về chữ ký số và dịch vụ chứng thực chữ ký số.

9.6.3 Tuyên bố và cam kết của thuê bao

Thuê bao đảm bảo rằng:

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

- Sử dụng chứng thư số đúng mục đích của chứng thư số, phù hợp với quy định của pháp luật và quy chế chứng thực này
- Không sử dụng chứng thư số được cấp thực hiện các chức năng của một CA.

Thỏa thuận thuê bao có thể bao gồm thêm những điều khoản khác.

9.6.4 Tuyên bố và cam kết của người nhận

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

Người nhận phải chịu trách nhiệm cho những hành động của mình do không thực hiện theo các nội dung liên quan được quy định trong thỏa thuận người nhận hoặc quy chế chứng thực này.

Thỏa thuận thuê bao có thể bao gồm thêm những điều khoản khác.

9.6.5 Tuyên bố và cam kết của các đối tượng khác

Không quy định.

9.7. Từ chối trách nhiệm

Không quy định.

9.8. Giới hạn trách nhiệm pháp lý

- 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 quy chế được giữ lại không thể thi hành được bởi một phiên toà hay một cuộc xét xử có thẩm quyền, phần còn lại của quy chế vẫn có hiệu lực.

9.9. Bồi thường thiệt hại

9.9.1 Vấn đề bồi thường của khách hàng

Khi pháp luật yêu cầu, khách hàng bồi thường cho SmartSign nếu xuất hiện:

- Những thông tin không hợp lệ do khách hàng cung cấp trên đơn vị cấp chứng thư.
- Lỗi của khách hàng để lộ những nhân tố, yếu tố liên quan đến đơn xin cấp chứng thư, sự bỏ sót do sự cẩu tha hay với mục đích lừa đảo.
- Lỗi của khách hàng trong việc bảo vệ khóa bí mật, sử dụng hệ thống tin cậy, hoặc không thực hiện các biện pháp phòng ngừa cần thiết để tránh gây hậu quả.
- Việc sử dụng tên của khách hàng (kể cả việc không giới hạn tên chung, tên miền, hoặc địa chỉ thư điện tử) vi phạm quyền sở hữu trí tuệ của bên thứ 3.
- Hợp đồng với khách hàng có thể có những bổ sung phù hợp.

9.9.2 Vấn đề bồi thường của đại lý

Khi được pháp luật cho phép, thỏa thuận với SmartSign RA sẽ yêu cầu SmartSign RA bồi thường cho SmartSign:

- Lỗi của SmartSign RA trong việc thực thi nghĩa vụ của SmartSign RA.
- Sự tin cậy của SmartSign RA về một chứng thư số không được đáp ứng trong một số trường hợp.
- Lỗi của SmartSign RA trong việc kiểm tra trạng thái của chứng thư để xác định chứng thư đã hết hạn hay bị thu hồi .
- Thỏa thuận với SmartSign RA sẽ bao gồm thêm một số nghĩa vụ khác.

9.10. Hiệu lực của Quy chế chứng thực

9.10.1 Thời hạn

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

9.10.2 Kết thúc

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

9.10.3 Ảnh hưởng của sự kết thúc và những tổn hại

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

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

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

9.12. Bổ sung và sửa đổi

9.12.1 Các thủ tục sửa đổi

Những sửa đổi của quy chế này sẽ được thực hiện bởi Cấp quản lý chính sách có thẩm quyền (xem mục 1.5.4).

9.12.2 Cơ chế và thời hạn thông báo

Đối với các thay đổi không quan trong 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.

9.13. Thủ tục giải quyết tranh chấp

Tranh chấp giữa SmartSign với SmartSign RA sẽ được giải quyết theo các điều khoản được ghi trong hợp đồng.

Tranh chấp giữa SmartSign với thuê bao sẽ được giải quyết theo các điều khoản được ghi trong hợp đồng.

9.14. Pháp luật

Pháp luật Việt Nam sẽ được sử dụng trong mọi trường hợp, kể cả có liên quan đến các yếu tố nước ngoài..

9.15. Phù hợp với pháp luật hiện hành

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

Không quy định.

9.17. Các điều khoản khác

Không quy định.

10. PHỤ LỤC

10.1. Quyền của Đại Lý

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

10.2. Nghĩa vụ của Đại Lý

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

10.3. Các trách nhiệm khác của Đại Lý

10.3.1 Tiếp thị và giới thiệu dịch vụ chứng thư số của Công Ty CP Chữ Ký Số Vi Na

- Đại Lý có trách nhiệm chủ động thực hiện các biện pháp marketing tiếp thị để tìm kiếm khách hàng trong những quy định về chính sách marketing của SmartSign.
- Đại Lý có trách nhiệm giới thiệu đầy đủ, tận tình các dịch vụ giá trị gia tăng của Công Ty CP Chữ Ký Số Vi Na cho khách hàng và hướng dẫn khách hàng các thông tin, thủ tục cần thiết để đăng ký và sử dụng các dịch vụ đó.

10.3.2 Kiểm tra điều kiện pháp lý của khách hàng

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

Khách hàng là Tổ chức, doanh nghiệp:

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

Khách hàng là cá nhân:

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

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

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

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

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

10.3.4 Bàn giao Hồ sơ

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

- 01 Giấy đăng ký xin cấp chứng thư số

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

SmartSign có trách nhận tiếp nhận Hồ sơ của khách hàng nhanh chóng và ký Biên bản bàn giao khách hàng với Đại Lý.

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

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

10.3.5 Hoàn thành thủ tục thanh toán cho khách hàng và đối soát quyết toán giữa Đại Lý và SmartSign

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

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

10.3.6 Hỗ trợ khách hàng

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

10.3.7 Chăm sóc khách hàng

- Đại lý có trách nhiệm phối hợp với Công ty CP Chữ ký Số Vi Na thực hiện các hoạt động chăm sóc khách hàng do Công ty CP Chữ ký Số Vi Na đề xuất.
- Đại lý có thể chủ động thực hiện các hoạt động chăm sóc đối với khách hàng do Đại lý phát triển nhằm tăng uy tín của dịch vụ và không ảnh hưởng đến uy tín của Công ty CP Chữ ký Số Vi Na.