TẬP ĐOÀN BƯU CHÍNH VIỄN THÔNG VIỆT NAM

QUY CHẾ CHỨNG THỰC

DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG
(VNPT-CA)

Hà nội, năm 2019

MỤC LỤC

Lời giới thiệu

Văn bản này là một bộ quy chế chứng thực (CPS) tuyên bố về mặt nguyên tắc các chính sách quản trị của VNPT-CAtrong quá trình cung cấp dịch vụ chứng thực chữ ký số. Bản CPS đưa ra các yêu cầu luật pháp, các yêu cầu về kỹ thuật, cũng như yêu cầu kinh doanh cho quá trình chấp thuận, cấp phát, quản lý, sử dụng, thu hồi và cấp lại chứng thư số trong hệ thống VNPT-CA. Các yêu cầu của CPS đảm bảo tính bảo mật và toàn vẹn cho dịch vụ VNPT-CA, được áp dụng cho tất cả các thành phần tham gia dịch vụ chứng thực chữ ký số VNPT-CA. Bản CPS này không phải thỏa thuận về mặt luật pháp giữa VNPT-CAvà các thực thể sử dụng dịch vụ chứng thực chữ ký số công cộng.

Mục tiêu của văn bản này là:

- Nhà cung cấp dịch vụ VNPT-CA hoạt động với quy chế chứng thực chứng thực số và tuân thủ theo các yêu cầu trong bản CPS này.

- Cung cấp cho khách hàng sử dụng dịch vụ VNPT-CA về quá trình xác thực và trách nhiệm của họ.

- Cung cấp thông tin cho đối tác tin cậy (Relying party) về mức độ đảm bảo mà chứng thư VNPT-CAcung cấp.

- Bản CPS này tuân theo luật pháp Việt Nam cũng như tuân theo các chính sách, quy chế ban hành bởi cơ quan chức năng nhà nước Bộ Thông tin và các cơ quan chức năng có liên quan khác.

1. THÔNG TIN CHUNG

1.1. Tổng quan

VNPT-CA là tên gọi của dịch vụ chứng thực chữ ký số công cộng do Tập đoàn Bưu chính Viễn thông Việt Nam cung cấp. Các quy định về chính sách chứng thư số của dịch vụ VNPT-CA được trình bày trong tài liệu này gồm có: phát hành chứng thư, quản lý, thu hồi và cấp lại chứng thư số cho các thuê bao đầu cuối.

1.2. Nhận biết

Văn bản này là một bộ quy chế chứng thực (CPS) tuyên bố về mặt nguyên tắc các chính sách quản trị của VNPT-CA trong quá trình cung cấp dịch vụ chứng thực chữ ký số. Bản CPS đưa ra các yêu cầu luật pháp, các yêu cầu về kỹ thuật, cũng như yêu cầu kinh doanh cho quá trình chấp thuận, cấp phát, quản lý, sử dụng, thu hồi và cấp lại chứng thư số trong hệ thống VNPT-CA. Các yêu cầu của CPS đảm bảo tính bảo mật và toàn vẹn cho dịch vụ VNPT-CA, được áp dụng cho tất cả các thành phần tham gia dịch vụ chứng thực chữ ký số VNPT-CA. Bản CPS này không phải thỏa thuận về mặt luật pháp giữa VNPT-CAvà các thực thể sử dụng dịch vụ chứng thực chữ ký số công cộng.

Mục tiêu của văn bản này là:

- Nhà cung cấp dịch vụ VNPT-CA hoạt động với quy chế chứng thực chứng thực số và tuân thủ theo các yêu cầu trong bản CPS này.
- Cung cấp cho khách hàng sử dụng dịch vụ VNPT-CA về quá trình xác thực và trách nhiệm của họ.
- Cung cấp thông tin cho đối tác tin cậy (Relying party) về mức độ đảm bảo mà chứng thư VNPT-CAcung cấp.
- Bản CPS này tuân theo luật pháp Việt Nam cũng như tuân theo các chính sách, quy chế ban hành bởi cơ quan chức năng nhà nước Bộ Thông tin và các cơ quan chức năng có liên quan khác.

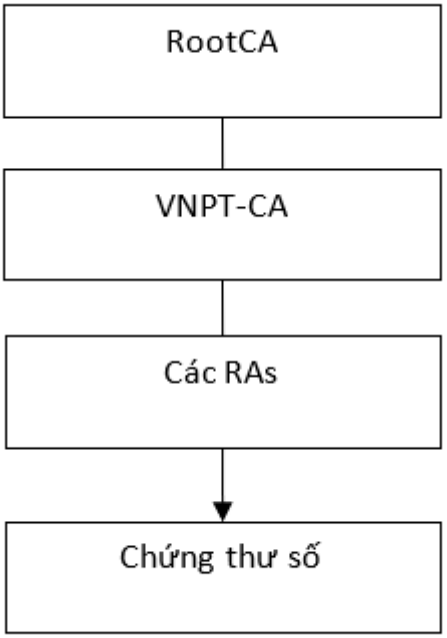
1.3. Thành phần tham gia dịch vụ VNPT-CA.

1.3.1. Thành phần Certification Authorities (CA)

Cấu trúc tổng quan dịch vụ VNPT-CA được trình bày ở Sơ đồ dưới. Tại đỉnh của sự phân cấp chính là RootCA, đơn vị cấp phép cho VNPT-CA trở thành nhà cung cấp dịch vụ chứng thực chữ ký số. RootCA đồng thời cũng là đơn vị điều tiết và quản lý nội dung chính sách và quy chế chứng thực của dịch vụ phải tuân theo.

VNPT-CA là đơn vị dưới quyền quản lý của Bộ Thông tin và Truyền thông được phép cung cấp trực tiếp cho người dùng cuối trong mạng tin cậy này.

Registration Authorities (RA) là những thực thể có nhiệm vụ xác thực thông tin và thẩm định các yêu cầu trong dịch vụ VNPT-CA. Các RA của dịch vụ VNPT-CA chịu trách nhiệm xác thực thông tin về các đối tượng muốn đăng ký sử dụng dịch vụ chứng thực. Chứng thư của thuê bao có thể cấp từ VNPT-CA hoặc qua các đơn vị RA quản lý.



Quyền của CA:

CA là đơn vị cung cấp chứng thư số. Trong mô hình tổ chức của VNPT-CA cho dịch vụ này, các VNPT-CA không có SUB-CA để cấp phát chứng thư số nhưng có các đơn vị RA làm nhiệm vụ cấp chứng thư cho người dùng cuối.

CA có nghĩa vụ sau:

- Không cung cấp những thông tin sai lệch so với thực tế trong chứng thư biết đến hay khởi đầu từ thực thể phê chuẩn chứng thư hoặc ban hành chứng thư.

- Không mắc lỗi ở các thông tin trong chứng thư được đưa ra bởi thực thể phê chuẩn chứng thư hoặc ban hành chứng thư do lỗi gây ảnh hưởng tới khả năng chăm sóc trong việc quản lý ứng dụng chứng thư.

- Đảm bảo cho chứng thư số của người sử dụng đầu cuối đạt tiêu chuẩn theo CPS.

- Đảm bảo nơi lưu trữ CA phù hợp với tiêu chuẩn trong CPS, đảm bảo cho dịch vụ thu hồi và sử dụng chứng thư số.

1.3.2. Thành phần Registration Authorities (RA)

Quyền của RA:

- Nhận, kiểm tra, chấp thuận hoặc từ chối yêu cầu đăng kí dịch vụ VNPT-CA.

- Đăng kí dịch vụ VNPT-CA cho thuê bao.

Nghĩa vụ của RA:

- Cung cấp các thông tin chính xác về dịch vụ VNPT-CA cho khách hàng và đại lý cung cấp dịch vụ VNPT-CA.

- Nhận các đơn yêu cầu cung cấp chứng thư số thư số của khách hàng theo quy chế CPS của VNPT-CA.

- Gửi các đơn yêu cầu cung cấp chứng thư số thư số lên VNPT-CA.

- Cung cấp chứng thư số trực tiếp tới thuê bao.

- Ký các giấy tờ và biên bản bàn giao giữa hai bên.

1.3.3. Thuê bao

Quyền của thuê bao:

- Chứng thư số được cấp phát trực tiếp tới thuê bao theo đúng loại chứng thư số mà thuê bao đã yêu cầu.

- Chứng thư số của thuê bao được chấp nhận và hoạt động trong thời gian có hiệu lực của chứng thư số.

- Khóa bí mật chỉ có bên thuê bao nắm giữ, được bảo vệ trong thiết bị chuyên biệt của thuê bao.

- Thuê bao có quyền đăng ký nhà cung cấp lưu trữ lại khóa đảm bảo trong trường hợp mất, hoặc hỏng thiết bị chuyên biệt vẫn còn cần dùng lại cặp khóa thì có thể phục hồi.

- Thuê bao có quyền yêu cầu gia hạn, thu hồi cặp chứng thư số của mình. Trong trường hợp đăng ký dịch vụ phục hồi khóa thì khách hàng có quyền yêu cầu khôi phục lại cặp khóa.

Nghĩa vụ của thuê bao:

- Mọi cam kết của thuê bao trong ứng dụng chứng thư số thuê bao trình lên là đúng sự thật.

- Tất cả các thông tin cung cấp bởi thuê bao và chứa bên trong chứng thư số là đúng sự thật.

- Chứng thư số phải được sử dụng cho các mục đích hợp pháp và tuân theo những yêu cầu trong CPS.

- Thuê bao có nghĩa vụ bảo mật cặp khóa riêng, sử dụng hệ thống tin cậy. Ngăn chặn việc mất cắp, lộ thông tin, hay sửa đổi, phá hủy khóa bí mật. Phải thông báo tới RA ngay khi khóa bí mật bị lộ hay sửa đổi, phá hủy.

- Không được giả mạo chứng thư số của VNPT.

- Nếu có bất kỳ sự thay đổi thông tin nào, đều phải thông báo tới VNPT.

- Nết có bất kỳ một ứng dụng hay thiết bị lưu trữ chứng thư số nào của khách hàng bị cài sai, phải hủy bỏ chứng thư số của VNPT-CA cung cấp.

- Yêu cầu thu hồi chứng thư số trong trường hợp có lỗi mà lỗi này có thể làm ảnh hưởng tới toàn bộ chứng thư số của VNPT.

1.3.4. Thành phần người nhận

Quyền của người nhận:

- Người nhận là một cá nhân hay một tập thể được tin tưởng, kiểm tra chứng thư số thư số của đối tác theo thỏa thuận và cam kết giữa hai bên.

- Người nhận có quyền xác nhận các thông tin của thuê bao trong chứng thư số là đúng sự thật.

- Người nhận dựa vào các thông tin trong chứng thư số là chính xác và các thông tin trong CPS để đưa ra quyết định thực hiện thỏa thuận và cam kết giữa hai bên.

- Người nhận phải là chủ thể của chứng thư số được cấp hoặc phải có giấy ủy quyền hợp pháp của chủ thể.

Nghĩa vụ của người nhận

- Nhận các thông báo của VNPT-CA về các điều kiện hợp tác đối với bên thứ 3.

- Chỉ tin tưởng chứng thư số do VNPT-CA cung cấp nếu khi kiểm tra thấy hợp lệ và cập nhật thường xuyên.

- Chỉ tin tưởng vào chứng thư số nếu nó chưa bị thu hồi.

- Phải thông báo cho RA ngay lập tức, nếu nghi ngờ rằng khóa bí mật bị lộ, mất cắp hay sửa đổi, phá hủy.

1.3.5. Thành phần khác

Không có

1.4. Sử dụng chứng thư số

1.4.1. Chứng thư số hợp pháp

Tất cả chứng thư số đều phải sử dụng theo quy định của pháp luật và CPS này

1.4.2. Chứng thư số không hợp pháp

Không có

1.5. Chi tiết liên lạc

1.5.1. Tổ chức quản lý

Tập đoàn bưu chính viễn thông Việt Nam (VNPT).

Tòa nhà VNPT, số 57 Huỳnh Thúc Kháng, Quận Đống Đa, Hà Nội, Việt Nam.

1.5.2. Liên hệ

Công ty công nghệ thông tin VNPT-CA(VNPT-CAIT).

Tòa nhà VNPT, số 57 Huỳnh Thúc Kháng, Quận Đống Đa, Hà Nội, Việt Nam.

Và

VNPT-CAVinaphone

Tòa nhà VNPT, số 57 Huỳnh Thúc Kháng, Quận Đống Đa, Hà Nội, Việt Nam.

1.5.3. Đơn vị quyết tịnh tính hợp pháp của CPS

CPS này được xây dựng phù hợp với quy định của pháp luật cũng như danh mục các tiêu chuẩn bắt buộc áp dụng trong lĩnh vực chữ ký số của Bộ Thông tin và truyền thông. VNPT-CA chịu trách nhiệm trước pháp luật về tính hợp pháp của CPS này.

1.5.4. Thủ tục phê duyệt CPS

VNPT-CAIT là đơn vị có thẩm quyền phê duyệt CPS này và những thay đổi liên quan trong quá trình hoạt động của VNPT-CA. Các thay đổi phải được phê duyệt bởi lãnh đạo trung tâm. Tất cả những phiên bản đã sửa đổi hoặc cập nhật thông tin được công bố tại đại chỉ https://vnpt-ca.vn/download-page.

1.6. Định nghĩa và tên viết tắt

Thuật ngữ	**Giải thích**
CA	Certificate Authority – Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.
CP	Certificate Policies – Chính sách chứng thư
CPS	Certification Practice Statement – Quy chế chứng thực
CRL	Certificate Revocation List – Danh sách chứng thư số bị thu hồi
OCSP	Online Certificate Status Protocol - là giao thức cho phép kiểm tra trạng thái chứng thư số trực tuyến
RA	Registration Authority – Tổ chức tiếp nhận đăng ký và xác thực thông tin của người sử dụng dịch vụ.

2. CÔNG BỐ VÀ LƯU TRỮ THÔNG TIN THUÊ BAO

2.1. Lưu trữ

VNPT-CA lưu trữ thông tin chứng thư số của thuê bao trên hệ quản trị cơ sở dữ liệu Oracle, MySQL và LDAP.

Việc lưu trữ, cập nhật danh sách các chứng thư số có hiệu lực và đã hết hiệu lực công khai trên internet cho phép truy cập 24/7 được VNPT-CA thực hiện bởi các server chức năng: CRL server, LDAP server , OCSP server. Các máy chủ này được VNPT-CA xây dựng nằm trong phân đoạn mạng công cộng có băng thông rộng, nằm trong datacenter của VNPT, với đường truyền internet ổn định, tốc độ cao, điều kiện môi trường, nguồn điện ổn định, có đội ngũ kỹ thuật duy trì hệ thống 24/7 đảm bảo tính liên tục cung cấp dịch vụ và tính sẵn sàng của hệ thống cung cấp dịch vụ.

Danh sách chứng thư số bị thu hồi CRL là danh sách các số serial của các chứng thư số đã bị thu hồi do nhà cung cấp dịch vụ công bố, các bên tham gia giao dịch (relying party) cần kiểm tra các chứng thư và từ chối tin tưởng các chứng thư này. Một CRL lưu ở thư mục công cộng của nhà cung cấp dịch vụ, nó được tạo định kỳ theo một chu kỳ thời gian hoặc ngay sau khi có một chứng thư số bị thu hồi hoặc tam ngưng. Hệ thống cung cấp dịch vụ VNPT-CA lưu trữ và tự động cập nhật định kỳ liên tục các thông tin về danh sách các chứng thư số có hiệu lực và đã hết hiệu lực. Danh sách các chứng thư số thu hồi CRL được đặt trên CRL server để đảm bảo khả năng truy cập trực tuyến của người dùng 24/7, giao thức truy cập để lấy CRL có thể là HTTP hoặc FTP.

2.2. Công bố thông tin thuê bao

Hệ thống VNPT-CA công bố công khai chứng thư số của khách hàng qua website dịch vụ https://vnpt-ca.vn, kênh này được công khai để các khách hàng của VNPT-CA có thể truy cập lấy thông tin chứng thư số của mình từ internet.

Đối với khách hàng tự tra cứu thông tin qua website của dịch vụ https://vnpt-ca.vn/khach-hang/tai-lieu khách hàng cần cung cấp các thông tin sau để có thể thực hiện tìm kiếm thông tin:

- Mã số thuê bao (Serial Number)
- Tên đầy đủ của chủ thuê bao (CN)
- Quận/Huyện (L)
- Tỉnh/Thành Phố (ST)

Khách hàng nhập các thông tin này ngay trên website của dịch vụ.

2.3. Thời gian công bố

Hệ thống tự động và liên tục cập nhật các thông tin về danh sách các chứng thư số có hiệu lực và đã hết hiệu lực trong hệ thống cơ sở dữ liệu và hệ thống danh bạ. Đồng thời, việc truy cập để xác định tính hiệu lực (vadility) của các chứng thư thông qua hai dịch vụ OCSP và CRL được đảm bảo liên tục và trực tuyến qua mạng Internet 24h trong một ngày và 7 ngày trong tuần.

2.4. Quản lý truy cập kho lưu trữ

CPS được công bố công khai nhưng không cho phép sửa đổi hoặc thay thế tại địa chỉ https://vnpt-ca.vn/download-page.

Cập nhật CRL được thực hiện tự động bởi hệ thống VNPT-CA.

Mọi thay đổi của CPS chỉ được phép thực hiện bởi cấp có thẩm quyền của VNPT.

Đối với khách hàng tự tra cứu thông tin qua website của dịch vụ https://vnpt-ca.vn/khach-hang/tai-lieu khách hàng cần cung cấp các thông tin sau để có thể thực hiện tìm kiếm thông tin:

- Mã số thuê bao (Serial Number)
- Tên đầy đủ của chủ thuê bao (CN)
- Quận/Huyện (L)
- Tỉnh/Thành Phố (ST)

Khách hàng nhập các thông tin này ngay trên website của dịch vụ.

3. Định danh và xác thực

3.1. Đặt tên

3.1.1. Các thuộc tính

Các chứng thư của VNPT-CAtuân theo chuẩn ITU-T X.509 và các quy định trong RFC5280: Internet X.509 Public Key Infastructure Certificate and CRL Profile (“RFC5280”).

Các chứng thư số tuân theo chuẩn X.509 V3 bao gồm các trường cơ bản và các giá trị bắt buộc chỉ ra hoặc tuân theo các ràng buộc trong bảng dưới đây:

Tên trường	**Giá trị hoặc những ràng buộc**
Serial Number	Duy nhất cho một Issuer

Signature Algorithm	Thuật toán Hash: SHA2, Thuật toán ký: RSA
Issuer	Thông tin về người phát hành chứng thư
Valid from	Thời gian bắt đầu có hiệu lực của chứng thư số. Được đồng bộ với Master Clock của U.S.Naval Observatory.
Valid to	Thời gian kết thúc hiệu lực của chứng thưu số. Được đồng bộ với U.S.Naval Observatory.
Subject	Thông tin về người nhận chứng thư số
Public Key	Được mã hóa theo tiêu chuẩn RFC5280 Mã hóa RSA 2048 bit

3.1.2. Tính rõ ràng và ý nghĩa của tên trong chứng thư

Tên miền không cần có nghĩa hoặc có tính duy nhất, nhưng cần phải tương ứng với tên miền cấp hai được đăng ký với InterNIC (tên miền cấp ba được đăng ký với VNNIC).

3.1.3. Trường hợp thuê bao sử dụng tên ẩn danh hay bút danh

Thuê bao không được phép sử dụng tên ẩn danh hoặc bút danh khác với tên thật của mình.

3.1.4. Quy tắc diễn giải các mẫu tên

Không có quy định.

3.1.5. Tính duy nhất của tên thuê bao

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

3.1.6. 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 bảo hộ quyền sở hữu trí tuệ cho đối tượng khác theo quy định của pháp luật về sở hữu trí tuệ.

Trong trường hợp cần thiết, VNPT-CA sẽ yêu cầu đối tượng đăng ký chứng thư số cung cấp các tài liệu chứng minh quyền sở hữu trí tuệ đối với tên đăng ký.

Tuy nhiên, VNPT-CA 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 số.

Trường hợp cần thiết, VNPT-CA có quyền chấm dứt hoặc tạm dừng bất cứ chứng thư số nào liên quan đến các tranh chấp đã nêu.

3.2. Xác thực định danh ban đầu

3.2.1. Phương pháp 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 sẽ tuân theo chuẩn PKCS#10 hoặc một phương pháp mật mã tương ứng, hoặc phương pháp khác được VNPT-CA công nhận.

3.2.2. Xác minh định danh tổ chức

Nội dung xác thực thông tin thuê bao là tổ chức gồm có:

- Tên tổ chức.
- Địa chỉ.
- Ngành nghề: giấy phép kinh doanh, giấy phép thành lập (bản chính hoặc bản sao có công chứng thư số).
- Thông tin về website, tên miền của tổ chức (sử dụng cho chứng thư SSL).
- Thông tin về người sử dụng chứng thư.

3.2.3. Xác minh định danh cá nhân

Nội dung xác thực thông tin thuê bao là cá nhân gồm có:

- Địa chỉ.
- Bản sao hợp lệ CMTND hoặc hộ chiếu.
- Thông tin sở hữu tên miền (sử dụng cho chứng thư SSL).

3.2.4. Thông tin thuê bao không xác minh

Không có quy định.

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.

3.2.6. Các tiêu chuẩn thực hiện liên hoạt

Không có quy định.

3.3. Xác thực với yêu cầu thay đổi khóa

Thuê bao muốn thay đổi cặp khóa phải đưa ra hợp đồng đăng ký sử dụng chứng thư số đã ký nhằm chứng thư số minh có quyền yêu cầu. Trong trường hợp mất hợp đồng, thuê bao phải cung cấp đầy đủ các thông tin cần thiết sao cho khớp với thông tin đăng ký sử dụng chứng thư số gốc bao gồm:

Đối với tổ chức

- Tên tổ chức.

- Địa chỉ.

- Ngành nghề: giấy phép kinh doanh, giấy phép thành lập (bản chính hoặc bản sao có công chứng thư số).

- Thông tin về website, tên miền của tổ chức (sử dụng cho chứng thư SSL).

- Thông tin về người sử dụng chứng thư.

Đối với cá nhân

- Địa chỉ.

- Bản sao hợp lệ CMTND hoặc hộ chiếu.

- Thông tin sở hữu tên miền (sử dụng cho chứng thư SSL).

3.4. Xác thực với yêu cầu thu hồi

Chỉ trong các tình huống được liệt kê dưới đây, chứng thư số của thuê bao sẽ bị VNPT-CA thu hồi và được công bố trên CRL.

Một chứng thư số thư của thuê bao sẽ bị thu hồi nếu rơi vào trong một số tình huống sau:

- VNPT-CA hoặc RA, thuê bao có lý do để tin rằng hoặc nghi ngờ về sự tổn hại của khóa bí mật của chứng thư số.

- VNPT-CA hoặc RA có lý so để tin rằng thuê bao vi phạm nghĩa vụ trách nhiệm đối với hợp đồng hoặc các thỏa thuận đã cam kết của thuê bao.

- VNPT-CA hoặc một thuê bao có lý do để tin rằng Chứng thư số được ban hành không phù hợp với quy định trong CPS. Chứng thư số tạo cho cho cá nhân không có tên như trong giấy Chứng nhận sử dụng chứng thư số.

- Thông tin trong Chứng thư không chính xác.

- Việc tiếp tục sử dụng chứng thư số này gây nguy hại cho VNPT-CA.

Khi xem xét việc sử dụng chứng thư số có gây nguy hại cho VNPT-CA hay không, VNPT-CA xem xét giữa các yếu tố sau :

- Nguồn gốc và tên của các khiếu nại nhận được.

- Xác nhận người khiếu nại.

- Cưỡng chế theo luật.

- Trả lời cho việc sử dụng gây nguy hại của người đăng ký.

VNPT-CA có thể thu hồi chứng thư số quản trị nếu thẩm quyền của người quản trị kết thúc.

Thỏa thuận giữa VNPT-CAvà thuê bao yêu cầu thuê bao này phải thông báo kịp thời cho VNPT-CAvề nguy cơ bị lộ khóa bí mật của chứng thư số của thuê bao.

4. CÁC QUY ĐỊNH VỀ VIỆC QUẢN LÝ VÒNG ĐỜI CỦA CHỨNG THƯ SỐ

4.1. Đơn xin Cấp chứng thư số

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

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

- Bất cứ cá nhân, tổ chức nào đủ điều kiện theo quy định của pháp luật và CPS 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 CPS này có nhu cầu sử dụng chứng thư số.

Một chứng thư số được xây dựng ban hành theo sự chấp thuận đơn xin chứng thư số của VNPT-CA hoặc nhận được yêu cầu của RA để ban hành giấy chứng thư số. VNPT-CA xây dựng và ban hành tới người xin cấp chứng thư số một chứng thư số trên cơ sở thông tin về đơn xin cấp chứng thư số sau khi được chấp thuận.

4.1.2. Quy trình xử lý đơn xin cấp chứng thư số

Thuê bao muốn đăng ký sử dụng chứng thư số cần đến các điểm đăng ký bao gồm các bưu điện Tỉnh thành trên cả nước, hoặc trực tiếp giao dịch đăng ký tại trụ sở và các chi nhánh của VNPT.

Thuê bao cần khai báo thông tin cần thiết trên Mẫu kê khai thông tin chuẩn của dịch vụ do VNPT-CAban hành. Sau đó chuyển lại cho RA và chờ thông tin xác thực phản hồi.

Các RA tiền hành xác thực thông tin thuê bao đã kê khai và tiến hành xác thực thông tin thuê bao. Trong trường hợp xác thực thông tin được chấp nhận hay không chấp nhận thì các RA có trách nhiệm gửi phiếu kết quả thông báo về việc xác thực thông tin tới thuê bao đăng ký.

RA có trách nhiệm tiến hành làm hợp đồng đăng ký sử dụng chứng thư số với thuê bao đăng ký trong trường hợp thông tin xác thực được chấp nhận.

4.2. Xử lý đơn xin cấp chứng thư số

4.2.1. Xác thực định danh

VNPT-CA tiến hành xác thực định danh tất cả các thông tin của đối tượng yêu cầu cấp chứng thư số theo phần 3.2.

4.2.2. Chấp nhận hoặc từ chối cấp chứng thư số

VNP-CA 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 phần 3.2.

Đối tượng yêu cầu cấp chứng thư số nộp đầy đủ phí dịch vụ cấp chứng thư số cho VNPT-CA.

VNPT-CA 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 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 VNPT-CA cấp chứng thư số cho đối tượng yêu cầu có thể ảnh hưởng tới uy tín và độ tin cậy của VNPT-CA.

4.2.3. Thời gian xử lý yêu cầu

VNPT-CA 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 CPS, tuy nhiên thời gian tối đa là 3 ngày làm việc. Yêu cầu cấp chứng thư số sẽ ở trạng thái có hiệu lực cho tới khi bị VNPT-CA từ chối.

4.3. Phát hành chứng thư số

4.3.1. Hoạt động CA trong phát hành chứng thứ số

Chứng thư số được tạo và phát hành dựa trên kết quả chấp nhận yêu cầu cấp chứng thư số. VNPT-CA 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 tới thuê bao

VNPT-CA sẽ trực tiếp hoặc thông là thông qua một RA để thông báo cho các thuê bao rằng chứng thư số của họ vừa được cấp.

4.4. Chứng nhận chứng thư số

4.4.1. Điều kiện chứng minh việc chấp nhận chứng thư sô

Khi nhận được chứng thư số, thuê bao cần ký xác nhận các thủ tục bàn giao khóa và chứng thư số.

4.4.2. Công bố chứng thư số

VNPT-CA công bố công khai chứng thư số đã phát hành trên kho lưu trữ công khai theo phần 2.

Khi thuê bao xác nhận bàn giao khóa và chứng thư số, khi đó chứng thư số mới bắt đầu có hiệu lực.

4.4.3. Thông báo đến các đối tượng khác về việc phát hành chứng thư số

VNPT-CA sẽ trực tiếp hoặc thông là thông qua một RA để thông báo cho các thuê bao rằng chứng thư số của họ vừa được gia hạn.

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 CPS 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.

Các chứng thư X.509 phiên bản 3 được tạo ra phù hợp với RFC5280. Việc mở rộng sử dụng khóa đối với chứng thư X.509 phiên bản 3 nói chung được cấu hình như việc thiết lập và hủy bỏ các phần nhỏ và các trường quan trọng phù hợp với bảng dưới đây. Các trường quan trọng trong việc mở rộng sử dụng khóa nói chung được thiết lập là TRUE cho các chứng thư và có thể thiết lập là TRUE hoặc FALSE cho các chứng thư người đăng ký sử dụng đầu cuối.

		CAs	Chứng thư số cá nhân, tổ chức	Chứng thư số SSL	Chứng thư số Code Signning
Criticality		TRUE	FALSE	FALSE	FALSE
0	digitalSingnature	Clear	Set	Set	Set
1	nonRepudiation	Clear	Set	Clear	Set
2	keyEncipherment	Clear	Set	Set	Clear
3	dataEncipherment	Clear	Set	Clear	Set
4	keyAgreement	Clear	Clear	Clear	Clear
5	keyCertSign	Set	Clear	Clear	Clear
6	CRLSign	Set	Clear	Clear	Clear
7	encipherOnly	Clear	Clear	Clear	Set
8	decipherOnly	Clear	Clear	Clear	Set

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

Người nhận sẽ được VNPT-CA 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 VNPT-CA, CPS hay các quy định của pháp luật.

- VNPT-CA không có trách nhiệm kiểm tra và đánh 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

4.6.1. Điều kiện gia hạn

- Thuê bao đưa ra yêu cầu gia hạn chứng thư số trong vòng trước 90 ngày trước ngày hết hạn sử dụng của chứng thư đó.

- Chỉ những thuê bao với chứng thư số cá nhân hoặc một đại diện hợp pháp mới có thể yêu cầu gia hạn chứng thư số.

- Hoàn tất chi phí dịch vụ gia hạn chứng thư số.

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 phần 4.1.2 và điền đủ thông tin yêu cầu trong Phiếu yêu cầu gia hạn chứng thư số theo mẫu do VNPT-CA ban hành. RA tiến hành xác thực thông tin của thuê bao trong Phiếu yêu cầu gia hạn chứng thư số theo phần 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 phần 4.2.2.

4.6.5. Điều khoản chấp nhận gia hạn chứng thư sô

Điều kiện cấu thành điều khoản gia hạn chứng thư số tuân theo phần 4.3.1.

4.6.6. Công bố chứng thư số được gia hạn

VNPT-CA có trách nhiệm công bố chứng thư số được gia hạn trên kho lưu trữ công khai theo phần 2.

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

VNPT-CA có trách nhiệm thông báo cho RA về việc gia hạn chứng thư số do họ xác thực định danh.

4.7. Thay đổi cặp khóa

4.7.1. Điều kiện thay đổi

Thuê bao muốn thay đổi cặp khóa phải xuất trình Hợp đồng dịch vụ để chứng minh quyền yêu cầu. Trong trường hợp mất hợp đồng, thuê bao phải cung cấp đầy đủ các thông tin cần thiết đúng với với thông tin đã đăng ký sử dụng chứng thư số gốc theo quy định trong phần 3.2.

4.7.2. Đối tượng được phép yêu cầu thay đổi khóa

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 thay đổi khóa chứng thư số.

4.7.3. Xử lý yêu cầu thay đổi khóa

Thuê bao cần tiến hành các thủ tục theo phần 4.1.2 và điền đủ thông tin yêu cầu trong bản Phiếu yêu cầu thay đổi khóa theo mẫu do VNPT-CA ban hành. VNPT-CA hoặc RA tiến hành xác thực thông tin cung cấp của thuê bao theo phần 3.2. Nếu thông tin xác thực, việc thay khóa được tiến hành. Nếu thông tin sai lệch, yêu cầu bị từ chối.

4.7.4. Thông báo cho thuê bao về việc thay khóa chứng thư số

VNPT-CA có trách nhiệm thông báo cho RA về việc gia hạn chứng thư số do họ xác thực định danh.

4.7.5. Điều khoản chấp nhận thay khóa chứng thư sô

Điều khoản chấp nhận thay khóa chứng thư số theo phần 4.3.1.

4.7.6. Công bố chứng thư số đã thay khóa

VNPT-CA có trách nhiệm công bố chứng thư số được thay khóa trên kho lưu trữ công khai theo phần 2.

4.7.7. Thông báo đến các đối tượng khác về việc thay khóa chứng thư sô

VNPT-CA có trách nhiệm thông báo cho RA về việc thay khóa chứng thư số do họ xác thực định danh.

4.8. Thay đổi chứng thư số

4.8.1. Điều kiện thay đổi

Thuê bao muốn thay đổi chứng thư số phải xuất trình Hợp đồng dịch vụ để chứng minh quyền yêu cầu. Trong trường hợp mất hợp đồng, thuê bao phải cung cấp đầy đủ các thông tin cần thiết đúng với với thông tin đã đăng ký sử dụng chứng thư số gốc theo quy định trong phần 3.2.

4.7.2. Đối tượng được phép yêu cầu thay đổi khóa

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 thay đổi khóa chứng thư số.

4.7.3. Xử lý yêu cầu thay đổi khóa

Thuê bao cần tiến hành các thủ tục theo phần 4.1.2 và điền đủ thông tin yêu cầu trong bản Phiếu yêu cầu thay đổi khóa theo mẫu do VNPT-CA ban hành. VNPT-CA hoặc RA tiến hành xác thực thông tin cung cấp của thuê bao theo phần 3.2. Nếu thông tin xác thực, việc thay khóa được tiến hành. Nếu thông tin sai lệch, yêu cầu bị từ chối.

4.7.4. Thông báo cho thuê bao về việc thay khóa chứng thư số

VNPT-CA có trách nhiệm thông báo cho RA về việc gia hạn chứng thư số do họ xác thực định danh.

4.7.5. Điều khoản chấp nhận thay khóa chứng thư sô

Điều khoản chấp nhận thay khóa chứng thư số theo phần 4.3.1.

4.7.6. Công bố chứng thư số đã thay khóa

VNPT-CA có trách nhiệm công bố chứng thư số được thay khóa trên kho lưu trữ công khai theo phần 2.

4.7.7. Thông báo đến các đối tượng khác về việc thay khóa chứng thư sô

VNPT-CA có trách nhiệm thông báo cho RA về việc thay khóa chứng thư số do họ xác thực định danh.

4.9. Tạm dừng và Thu hồi chứng thư số

4.9.1. Các trường hợp thu hồi chứng thư số

Chỉ trong các tình huống được liệt kê dưới đây, chứng thư số của thuê bao sẽ bị VNPT-CA thu hồi và được công bố trên CRL.

Một chứng thư số thư của thuê bao sẽ bị thu hồi nếu rơi vào trong một số tình huống sau:

- VNPT-CA hoặc RA, thuê bao có lý do để tin rằng hoặc nghi ngờ về sự tổn hại của khóa bí mật của chứng thư số.

- VNPT-CA hoặc RA có lý so để tin rằng Thuê bao vi phạm nghĩa vụ trách nhiệm đối với hợp đồng hoặc các thỏa thuận đã cam kết của thuê bao.

- VNPT-CA hoặc một thuê bao có lý do để tin rằng Chứng thư số được ban hành không phù hợp với quy định trong CPS. Chứng thư số tạo cho cho cá nhân không có tên như trong giấy Chứng nhận sử dụng chứng thư số.

- Thông tin trong Chứng thưkhông chính xác.

- Việc tiếp tục sử dụng chứng thư số này gây nguy hại cho VNPT-CA.

Khi xem xét việc sử dụng chứng thư số có gây nguy hại cho VNPT-CA hay không, VNPT-CA xem xét giữa các yếu tố sau :

- Nguồn gốc và tên của các khiếu nại nhận được.

- Xác nhận người khiếu nại.

- Cưỡng chế theo luật.

- Trả lời cho việc sử dụng gây nguy hại của người đăng ký.

VNPT-CA có thể thu hồi chứng thư số quản trị nếu thẩm quyền của người quản trị kết thúc.

Thỏa thuận giữa VNPT-CAvà thuê bao yêu cầu thuê bao này phải thông báo kịp thời cho VNPT-CAvề nguy cơ bị lộ khóa bí mật của chứng thư số của thuê bao.

4.9.2. Đối tượng yêu cầu thu hồi

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 thay đổi khóa chứng thư số.

4.9.3. Thủ tục yêu cầu thu hồi

Thuê bao/RA/RP:

- Gửi đơn yêu cầu thu hồi chứng thư tới nhà cung cấp dịch vụ với chữ ký hoặc con dấu hợp pháp của chủ thể.

RA:

- Tiến hành xác minh và xác thực chính xác thông tin yêu cầu thu hồi chứng thư từ phía đối tượng gửi đơn thu hồi.

- Trường hợp thông tin không đủ hợp lệ thu hồi, RA tự động hủy bỏ yêu cầu đồng thời có trách nhiệm thông báo từ chối tới đối tượng nộp đơn yêu cầu.

- Trường hợp thông tin là hợp lệ để thu hồi, RA gửi báo cáo thông tin xác thực kèm theo đề nghị thu hồi chứng thư tới VNPT-CAlàm có cơ sở thực hiện yêu cầu.

VNPT-CA:

- VNPT-CA xác thực RA và các thông tin RA gửi, nếu hợp lệ, VNPT-CA sẽ tiến hành thu hồi chứng thư của thuê bao.

- VNPT-CA trách nhiệm cập nhật thông tin trên kho lưu trữ của dịch vụ về chứng thư đã bị thu hồi.

- VNPT-CA gửi thông báo về việc thu hồi trực tiếp cho thuê bao hoặc thông qua RA quản lý trực tiếp.

4.9.4. Thời gian xử lý yêu cầu thu hồi

Thời gian cho việc thu hồi chứng thư và thông báo cần phải được xử lý sớm nhất có thể.

4.9.5. Thời gian xử lý đề nghị thu hồi

Thời gian cho việc thu hồi chứng thư và thông báo cần phải được xử lý sớm nhất có thể.

4.9.6. Yêu cầu kiểm tra thu hồi cho người nhận

Kiểm tra trạng thái chứng thư số tại các địa chỉ:

- Chuẩn hàm băm SHA-1 với đường dẫn OCSP là http://ocsp.vnpt-ca.vn/responder và CRL là http://crl.vnpt-ca.vn/vnptca.crl.

- Chuẩn hàm băm SHA-256 với đường dẫn OCSP là http://ocsp-sha256.vnpt-ca.vn/responder và CRL là http://crl-sha256.vnpt-ca.vn/vnptca-sha256.crl.

4.9.7. Tần suất phát hành chứng thư số bị thu hồi

Đối với CRL là 1 giờ, OCSP là ngay lập tức khi có yêu cầu thu hồi.

4.9.8. Thời gian trễ lớn nhất của CRL

Thời gian trễ lớn nhất để hệ thống tự động cập nhật là 24h.

4.9.9. Hỗ trợ kiểm tra trực tuyến trạng thái chứng thư số bị thu hồi

Kiểm tra trạng thái chứng thư số tại các địa chỉ:

- Chuẩn hàm băm SHA-1 với đường dẫn OCSP là http://ocsp.vnpt-ca.vn/responder và CRL là http://crl.vnpt-ca.vn/vnptca.crl.

- Chuẩn hàm băm SHA-256 với đường dẫn OCSP là http://ocsp-sha256.vnpt-ca.vn/responder và CRL là http://crl-sha256.vnpt-ca.vn/vnptca-sha256.crl.

4.9.10. Điều kiện kiểm tra trực tuyến chứng thư số bị thu hồi

Người nhận phải kiểm tra trạng thái chứng thư số trước khi tin tưởng.

4.9.11. Mẫu quảng bá chứng thư số bị thu hồi khác

Không có

4.9.12. Các điều kiện đặc biệt khi khóa bị xâm phạm

VNPT– CA sẽ sử dụng phương tiện hợp lý để thông báo cho người nhận nếu phát hiện ra, hoặc có lý do để tin rằng khóa bí mật của một trong các CA hoặc RA của VNPT– CA bị xâm phạm.

4.9.13. Các trường hợp tạm dừng

Không có quy định

4.9.14. Đối tượng được phép yêu cầu tạm dừng

Không có quy định.

4.9.15. Thủ tục yêu cầu tạm dừng

Không có quy định.

4.9.16. Giới hạn thời gian tạm dừng

Không có quy định.

4.10. Dịch vụ kiểm tra trạng thái chứng thư sô

4.10.1. Đặc tính hoạt động

Trạng thái chứng thư số được kiểm tra thông qua CRL, OCSP.

4.10.2. Tính sẵn sàng của dịch vụ

Dịch vụ kiểm tra trạng thái chứng thư số luôn sẵn sàng 24 x 7 và không bị gián đoạn.

4.10.3. Các đặc tính tùy chọn

Không có quy định

4.10.4. Kết thúc thuê bao

Thuê bao sẽ chấm dứt quá trình sử dụng chứng thư số trong một trong các trường hợp sau:

- Chứng thư số hết hạn và không đề nghị gia hạn.

- Chứng thư số bị thu hồi trước khi hết hạn và không thay thế bằng chứng thư số mới.

4.10.5. Ủy thác giữ và phục hồi khóa

Trường hợp thuê bao ủy thác cho đơn vị hoặc cá nhân khác giữ khóa phải có văn bản ký kết giữa bên ủy thác và bên được ủy thác.

5. Đảm bảo an toàn, an ninh cơ sở vật chất, quy chế làm việc và nhân sự của CA

5.1.Thiết bị, máy móc, nguồn điện, trụ sở và các yếu tố cần thiết khác

5.1.1 Ví trí xây dựng

Hoạt động của VNPT-CAvà RA được xây dựng bên trong một môi trường vật lý được bảo vệ nhằm ngăn cản và dò tìm ra các truy cập, sử dụng hoặc phơi bày các thông tin nhạy cảm một cách bất hợp pháp và hệ thống được công khai hay che dấu.

VNPT-CAcũng đồng thời duy trì các biện pháp phòng ngừa thảm họa cho các hoạt động về CA của mình. Các biện pháp phòng ngừa thảm họa được bảo vệ bởi nhiều tầng bảo mật mức vật lý.

5.1.2. Truy cập vật lý

Đơn vi chủ quản dịch vụ chứng thực chữ ký số VNPT-CA đòi hỏi tất cả phải có thẻ nhân viên. Trong trường hợp khách đến cơ quan giao dịch, khách cần xuất trình chứng minh thư nhân dân hoặc hộ chiếu. các giấy tờ này sẽ được lưu lại tại trụ sở của bảo vệ cơ quan và khách sẽ được cấp thẻ khách đi lại trong cơ quan.

Quyền ra vào nơi đặt thiết bị phục vụ việc cung cấp dịch vụ chứng thực chữ ký số được kiểm soát bởi hệ thông kiểm tra dấu vân tay và nhân viên bảo vệ. Bản thân nhân viên bảo vệ không có quyền ra vào nơi đặt thiết bị. Nhân viên này có nhiệm vụ ngăn chặn những cố gắng xâm nhập của người lạ, không có thẩm quyền. Những người có thể vào nơi đặt thiết bị phải là những người mà nhân viên bảo vệ biết trước là có quyền hạn và trách nhiệm đi vào khu vực này, đồng thời phải xác thực và cho phép của hệ thống nhận dạng vân tay. Mặt khác, nơi đặt thiết bị có camera theo dõi liên tục (24/7).

Quyền truy cập hệ thống chỉ được trao cho những người có trách nhiệm quản trị và theo dõi hệ thống. Do đó, những người không đủ thẩm quyền, nếu có vượt qua được hệ thống bảo vệ và kiểm soát vân tay cũng không có khả năng truy cập vào hệ thống.

5.1.3. Điều kiện nguồn điện

Hệ thống cung cấp dịch vụ VNPT-CA được nối qua hệ thống UPS, có khả năng cung cấp điện trong thời gian khoảng 30 phút. Đồng thời hệ thống phát điện của tòa nhà có hệ thống

máy phát, sẽ được kích hoạt sau khi mất điện khoảng 4 phút. Điều này đảm bảo nguồn điện cung cấp cho hệ thống là liên tục.

5.1.4. Phòng chống nước

VNPT-CA cần có phương án phòng ngừa để hạn chế đến mức tối thiểu vấn đề nước xâm nhập vào hệ thống của mình.

5.1.5. Phòng cháy chữa cháy

VNPT-CA có phương án phòng ngừa để ngăn chặn và dập tắt lửa hay các thảm họa khác có thể gây cháy hay khói. Hệ thống phòng cháy chữa cháy của VNPT-CA cần được thiết kế để phù hợp với tiêu chuẩn phòng cháy chữa cháy.

5.1.6. Phương tiện lưu trữ

Tất cả các sản phẩm lưu trữ thông tin về phần mềm và dữ liệu, kiểm toán, tư liệu hay thông tin dự phòng được lưu trữ trong phương tiện của VNPT-CA hoặc phương tiện lưu trữ đảm bảo an ninh với việc triển khai các phương tiện vật lý và các điều khiển truy cập để hạn chế các truy cập tới các công việc có tính thẩm quyền, và bảo vệ các phương tiện lưu trữ không bị phá hủy (do nước, do lửa, do điện từ trường …).

5.1.7. Tiêu hủy rác

Các tài liệu và tài nguyên nhạy cảm cần được cắt thành từng miếng vụn trước khi hủy. Các phương tiện thu thập hay truyền các thông tin nhạy cảm cần được làm cho không thể truy cập được trước khu tiêu hủy. Các loại rác khác được tiêu hủy đạt yêu cầu về tiêu hủy rác thông thường của VNPT.

5.1.8. Hệ thống dự phòng

Hệ thống chính của dịch vụ VNPT-CA được đặt tại IDC Internet: Lô 2A Làng Quốc tế Thăng Long, Nguyễn Phong Sắc, Cầu Giấy, Hà Nội.

Hệ thống dự phòng (back up) cho dịch vụ VNPT-CA cũng được xây dựng về mặt chức năng giống hệt hệ thống chính thức và được đặt tại IDC Tân Thuận: Lô Va.02c-03a, đường 24, khu chế xuất Tân Thuận, phường Tân Thuận Đông, quận 7, Thành phố Hồ Chí Minh.

5.2. Kiểm soát thủ tục

5.2.1. Vai trò tin cây

Nhân viên đều phải được xem xét trước khi trở thành người tin cậy làm việc tại vị trí được tin cậy của VNPT-CA. Những người được chọn là người tin cậy làm việc tại vị trí tin cậy đáp ứng yêu cầu của VNPT-CA. Người tin cậy bao gồm tất cả các nhân viên, kỹ sư, nhân viên tư vấn có truy cập hay điều khiển quá trình xác thực hoặc mã hóa có thể gây ảnh hưởng lớn tới:

- Quá trình kiểm tra thông tin trong ứng dụng chứng thư số.

- Quá trình cung cấp dịch vụ chứng thực chữ ký số.

- Ban hành, thu hồi quyền truy cập tới các phần bị hạn chế của hệ thống.

- Chuyển giao thông tin hoặc yêu cầu của thuê bao.

- Người tin cậy bao gồm, nhưng không giới hạn bởi các thành phần sau:

- Nhân viên giao dịch, nhân viên chăm sóc khách hàng.
- Nhân viên điều hành công việc mã hóa.
- Nhân viên an ninh.
- Nhân viên bảo mật hệ thống.
- Các kỹ sư thiết kế.

5.2.2. Số lượng người tin cậy yêu cầu cho mỗi công việc

VNPT-CAđã thiết lập, duy trì và có các yêu cầu nghiêm ngặt về thủ tục điều khiển để đảm bảo sự phân công nhiệm vụ dựa trên khả năng làm việc và đã chỉ ra rằng nhiều người được tin tưởng sẽ cùng thực hiện các công việc có tính chất nhạy cảm.

5.2.3. Xác thực định danh các vai trò

Với tất cả những người muốn được trở thành người được tin tưởng, quá trình phê chuẩn nhận dạng được thực hiện qua sự hiện diện về mặt con người (hay vật lí) của những người này trước khi những người được tin tưởng thực hiện hay các thủ tục an ninh và một quá trình kiểm tra thông thường(như hộ chiếu hay giấy phép lái xe). Thủ tục nhận dạng sẽ được tiến hành sâu thêm một mức nữa thông qua thủ tục kiểm tra lai lịch.

VNPT-CAđảm bảo những nhân viên đạt được vị trí tin tưởng và bộ phận phê chuẩn được giao trước khi những nhân viên này :

- Được cấp phép truy cập tới các tiện nghi cần thiết.

- Được cấp các tài liệu điện tử để có thể truy cập đến và thực hiện một số chức năng trên VNPT, RA hay các hệ thống IT khác.

5.2.4. Phân chia trách nhiệm giữa các vị trí

Những vai trò yêu cầu phân chia trách nhiệm bao gồm nhưng ko giới hạn:

- Xác nhận thông tin trong đơn đăng ký chứng thư số.

- Quá trình chấp nhận, từ chối, hoặc các quá trình khác của ứng dụng chứng thư số, yêu cầu thu hồi, cấp mới hay các thông tin đăng ký.

- Quá trình ban hành, thu hồi các chứng thư số, 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 hủy một chứng thư số.

5.3. Kiểm soát nhân sự

5.3.1. Yêu cầu phẩm chất, kinh nghiệm và tin tưởng

Tất cả các đối tượng muốn trở thành người tin cậy và làm việc tại các vị trí tin cậy hệ thống của VNPT-CA cần phải chứng minh mình có lý lịch phù hợp, có phẩm chất tốt và kinh nghiệm cần thiết để thực hiện tốt các yêu cầu công việc trong tương lai, cũng như việc được tin tưởng (nếu có), cần thiết để thực hiện các dịch vụ về chứng thư số theo hợp đồng quản lý. Quá trình kiểm tra lý lịch được thực hiện lặp đi lặp lại với tần suất 1 lần/năm với những nhân viên có vị trí được tin cậy.

5.3.2. Thủ tục kiểm tra lý lịch

Trước khi chứng nhận vai trò được tin cậy cho một nhân viên, VNPT-CA thực hiện việc kiểm tra lý lịch gồm các yếu tố sau:

- Giấy xác nhận của địa phương về cá nhân, gia đình.
- Xác nhận của đơn vị công tác trước đó.
- Kiểm tra, tham khảo từ các đồng nghiệp.
- Xác nhận cấp đào tạo cao nhất đã đạt được.
- Kiểm tra các tiền án, tiền sự ở địa phương cũng như cấp quốc gia.
- Kiểm tra thông tin về tài chính.
- Xác nhận đáp ứng các điều kiện về chính trị và an ninh của cơ quan chính trị và bảo vệ an ninh của VNPT. Khi một trong các yếu tố bắt buộc này không thể đạt được do luật pháp hoặc hoàn cảnh nào đó, VNPT-CA sẽ sử dụng kỹ thuật đánh giá thay thế khác được luật pháp cho phép.

Các yếu tố phát hiện được trong quá trình kiểm tra lý lịch có thể dùng để loại bỏ ứng viên thông thường là:

- Thông tin do ứng viên hoặc người tin cậy cung cấp không trung thực.
- Mức độ không tán thành hay tin tưởng cao của người tin cậy.
- Tiền án tiền sự.
- Thiếu khả năng hoặc có dấu hiệu không minh bạch về về tài chính. Báo cáo bao gồm các thông tin trên được bộ phận quản trị nguồn nhân lực và các nhân viên an ninh đánh giá, từ đó đưa ra các biện pháp thích hợp cho mỗi tình huống. Các biện pháp này có thể bao gồm việc kiểm tra và loại bỏ ứng viên khỏi vị trí được tin cậy hoặc chấm dứt công việc của ứng viên. Việc sử dụng các thông tin thu thập được từ trong quá trình kiểm tra lý lịch phải phù hợp với luật pháp và chính sách của nhà nước.

5.3.3. Yêu cầu đào tạo

VNPT-CA đào tạo nhân viên sau tuyển dụng cũng như trong quá trình làm việc để đảm bảo nhân viên có thể hoàn thành công việc của mình. VNPT-CA sẽ lưu giữ các tư liệu của những lần đào tạo này đồng thời thường xuyên xem xét lại và nâng cấp các chương trình đào tạo khi thấy cần thiết. Chương trình đào tạo của VNPT-CA thích hợp cho mỗi công việc riêng lẻ và thường liên quan tới:

- Các vấn đề cơ bản của hạ tầng khóa công khai.
- Yêu cầu công việc.
- Chính sách, thủ tục an ninh và các hoạt động của VNPT-CA.
- Sử dụng và điều hành các thiết bị phần cứng, phần mềm đã triển khai.
- Báo cáo, chuyển giao các thỏa ước và các vấn đề liên quan.
- Thủ tục khôi phục sau thảm họa và duy trì công việc. Chương trình đào tạo của VNPT-CA được thiết kế tương thích với chương trình đào tạo về chữ ký số và chứng thực chữ ký số do Trung tâm Chứng thực điện tử quốc gia (NEAC) cung cấp.

5.3.4. Yêu cầu đào tạo lại thường xuyên

Trong quá trình làm việc, các nhân viên trong hệ thống VNPT-CA sẽ thường xuyên được đào tạo nâng cao chuyên môn. Thời gian đào tạo do đơn vị quản lý quyết định dựa theo yêu cầu để mỗi nhân viên cần để duy trì mức độ tin tưởng và thực hiện tốt các công việc của bản thân.

5.3.5. Tần suất luân chuyển công tác

Không có quy định

5.3.6. Kỉ luật đối với các hành vi vi phạm

Các biện pháp kỉ luật phù hợp được thi hành đối với các hành vi bất hợp pháp hay các hành vi vi phạm chính sách, quy định của VNPT-CA. Các biện pháp kỉ luật có thể bao gồm việc sa thải tùy thuộc vào tần suất và mức độ nghiêm trọng của các hành vi nêu trên.

5.3.7. Các yêu cầu ký kết độc lập

Trong một số trường hợp nhất định, các nhân viên triển khai hay tư vấn độc lập được sử dụng vào các vị trí tin cậy. Những nhân viên này có cùng chức năng và vai trò an ninh như các nhân viên VNPT-CA ở vị trí tương ứng. Các đối tượng trên phải là người đã hoàn thành hay vượt qua thủ tục kiểm tra lý lịch và được phép truy cập tới các phương tiện được bảo mật của dịch vụ VNPT-CA trong phạm vi quyền hạn của họ.

5.3.8. Cung cấp tài liệu cho nhân viên

VNPT-CA có nhiệm vụ cung cấp cho nhân viên chương trình đào tạo và tài liệu cần thiết để họ hoàn thành tốt công việc của mình.

5.4 .Thủ tục kiểm tra

5.4.1. Các sự kiện VNPT-CA cần ghi nhận

Các sự kiện có thể kiểm định phải được ghi lại bởi VNPT-CA và các RA. Mọi bản ghi điện tử hay bằng tay, chứa thời gian của sự kiện, và nhận dạng của đơn vị thực hiện. VNPT-CA đưa ra các loại bản ghi sự kiện trong CPS này.

Các dạng sự kiện có thể kiểm định bao gồm:

- Tạo khóa CA.
- Bật tắt các hệ thống và ứng dụng.
- Thay đổi khóa CA.
- Quá trình xử lý dữ liệu kích hoạt cho khóa bí mật của CA.
- Các bản ghi truy cập vật lý.
- Các sự kiện về vòng đời của chứng thư số, bao gồm: phát hành, cấp lại, cấp mới, thu hồi, tạm dừng.
- Sự kiện lên quan tới người tin cậy, bao gồm: hành động truy cập hay thoát ra; tạo và xóa bỏ mật khẩu hay thay đổi đặc quyền của người sử dụng; thay đổi nhân sự; - Báo cáo về việc truy nhập vào mạng và các hệ thống không được cấp quyền.
- Lỗi trong việc đọc và ghi chứng thư số và kho lưu trữ; - Thay đổi chính sách tạo chứng thư số, thời gian hợp lệ; - Lỗi phát sinh liên quan đến chứng thư số và dịch vụ chứng thực chữ ký số do thuê bao thông báo hoặc do VNPTphát hiện.

5.4.2. Tần suất xử lý bản ghi kiểm tra

Các bản ghi kiểm tra được xử lý tối thiểu hàng tuần đối với các sự kiện an ninh và vận hành quan trọng. Ngoài ra, VNPT-CA sẽ tiến hành kiểm tra bất thường dựa theo các cảnh báo và hiện tượng của hệ thống.

5.4.3. Thời gian lưu trữ bản ghi kiểm tra

Bản ghi kiểm tra phải được lưu trữ theo phần 5.5.2.

5.4.4. Bảo vệ bản ghi kiểm tra

Bản ghi kiểm tra sẽ được bảo vệ bằng hệ thống bản ghi kiểm tra điện tử bao gồm các cơ chế bảo vệ các bàn ghi log khỏi các truy nhập, sửa đổi, xóa bỏ hoặc can thiệp bất hợp pháp.

5.4.5. Thủ tục sao lưu bản ghi kiểm tra

Hàng ngày, các bản ghi kiểm tra sẽ được sao lưu những phần thay đổi, bổ sung; và hàng tuần sẽ được sao lưu dự phòng toàn bộ.

5.4.6. Hệ thống kiểm tra

Kiểm tra hệ thống tự động được thực hiện ở mức ứng dụng, mạng và hệ điều hành. Nhân viên chuyên trách của VNPT-CA sẽ thực hiện thao tác kiểm tra thủ công.

5.5. Lưu trữ hồ sơ

5.5.1. Các loại hồ sơ cần lưu trữ

VNPT-CA sẽ lưu trữ các thông tin sau:

- Các dữ liệu kiểm tra trong phần 5.4.
- Thông tin đăng ký chứng thư số.
- Các tài liệu, văn bản kèm theo Phiếu yêu cầu cấp chứng thư số.
- Thông tin về vòng đời chứng thư số.
- Và các thông tin khác theo quy định của RootCA.

5.5.2. Thời gian lưu trữ

Các dữ liệu sẽ được lưu trong một khoảng thời gian ít nhất 10 năm kể từ ngày chứng thư số hết hạn hoặc bị hủy bỏ.

5.5.3. Bảo vệ dữ liệu lưu trữ

VNPT-CA cam kết chỉ các đối tượng được cấp phép mới có khả năng truy cập và sử dụng dữ liệu lưu trữ. Phương tiện lưu trữ dữ liệu thường xuyên được bảo trì và quản lý, luôn sẵn sàng phục vụ truy cập.

5.5.4. Thủ tục thực hiện sao lưu

VNPT-CA sao lưu tăng cường các thông tin chứng thư số hàng ngày và sao lưu toàn bộ hàng tuần. Các bản sao tài liệu văn bản giấy được lưu tại địa điểm an toàn.

5.5.5. Yêu cầu dán nhãn thời gian cho các hồ sơ

Các bản ghi thông tin về chứng thư số, CRL và các sự kiện thu hồi cần ghi lại thời gian xảy ra sự kiện.

5.6. Thay đổi khóa của VNPT-CA

Chứng thư số của VNPT-CA có thể gia hạn với điều kiện tổng thời gian sử dụng của cặp khóa không được vượt qua thời hạn sử dụng tối đa do pháp luật quy định. Cặp khóa mới của VNPT-CA có thể sinh ra khi cần thiết, ví dụ như thay thế cặp khóa cũ đã ngừng sử dụng. Trước khi chứng thư số của VNPT-CA hết hạn, VNPT-CA sẽ tiến hành quy trình gia hạn nhằm đảm bảo hệ thống hoạt động thông suốt. VNPT-CA sẽ xin gia hạn chứng thư số từ NEAC không chậm hơn 90 ngày trước thời điểm hết hạn.

5.7. Thỏa thuận và khắc phục thảm họa

5.7.1. Thủ tục xử lý vấn đề lộ khóa và sự cố

Việc dự phòng và sao lưu cần tiến hành tại địa điểm, thiết bị khác nhằm phòng ngừa khả năng lộ khóa và sự cố. Các dữ liệu cần sao lưu gồm: dữ liệu đăng ký chứng thư số, dữ liệu kiểm tra, cơ sở dữ liệu của các chứng thư số đã phát hành. Sao lưu dự phòng khóa bí mật của CA tuân theo quy định trong phần 6.2.4.

5.7.2. Tài nguyên máy tính, phần mềm và dữ liệu

Khi xảy ra sự cố đối với tài nguyên máy tính, gồm phần cứng, phần mềm, dữ liệu, các thông tin cần gửi ngay tới đơn vị chuyên trách xử lý sự cố nhằm thực hiện quy trình xử lý đã dự tính. Trong trường hợp cần thiết, chức năng phục hồi sau sự cố sẽ được kích hoạt sử dụng.

5.7.3. Thủ tục xử lý sự cố bị lộ khóa bí mật

Khi nghi ngờ, phát hiện sự cố bị lộ khóa bí mật của VNPT-CA, đơn vị xử lý sự cố của VNPT-CA (Incident Response Team) sẽ chuyên trách xử lý bằng các thủ tục, quy trình đã dự tính. Nhân sự của đơn vị xử lý sự cố bao gồm chuyên gia về mật mã, an ninh, kinh doanh, vận hành hệ thống và các chức năng khác sẽ khảo sát hiện trạng, đề ra phương án giải quyết và triển khai kế hoạch hành động sau khi được đơn vị quản lý điều hành của VNPT-CA chấp thuận. Nếu chứng thư số của VNPT-CA bị thu hồi, các thủ tục sau cần thực hiện:

- Trạng thái thu hồi chứng thư số của VNPT-CA sẽ được công bố trên kho lưu trữ.

- Mọi biện pháp thông báo có thể có đều được sử dụng nhằm cung cấp thông tin về sự kiện thu hồi chứng thư số CA cho các đơn vị thuộc hệ thống của VNPTCA.

5.7.4. Khả năng khôi phục hoạt động kinh doanh sau sự cố

VNPT-CA xây dựng hệ thống dự phòng cách vị trí hệ thống chính thức tối thiểu 10 km. VNPT-CA sẽ lập kế hoạch, triển khai và thử nghiệm phương án phục hồi sau sự cố nhằm giảm tối đa các hậu quả gây ra do yếu tố tự nhiên hay con người. Kế hoạch này thường xuyên được kiểm tra, xem xét và cập nhật cho phù hợp với tình hình thực tế. Khi có sự cố do yếu tố

tự nhiên hay con người gây ra làm ngừng hoạt động hệ thống tạm thời hoặc kéo dài, đơn vị giải quyết tình trạng khẩn cấp của VNPT-CA (VNPT-CA Emergency Response Team) có nhiệm vụ thực hiện quy trình phục hồi sau sự cố. VNPT-CA có khả năng phục hồi các hoạt động cơ bản sau 24 (hai mươi bốn) giờ sau sự cố với mức tối thiểu sau:

- Phát hành chứng thư số.

- Thu hồi chứng thư số.

- Công bố thông tin thu hồi. Cơ sở dữ liệu dùng cho phục hồi sau sự cố được đồng bộ với hệ thống đang vận hành trong khoảng thời gian cho phép. Các thiết bị sử dụng cho kế hoạch phục hồi được bảo vệ theo quy định ở phần 5.1.1. VNPT-CA bảo quản các thiết bị phần cứng và sao lưu dự phòng tại khu vực quản lý trang thiết bị phục hồi sau sự cố. Khóa bí mật của VNPT-CA được sao lưu vào bảo quản cho nhiệm vụ phục hồi sau thảm họa theo quy định ở phần 6.2.4.

5.8. Kết thúc hoạt động của VNPT-CA hoặc RA

VNPT-CA sẽ thông báo khi VNPT-CA hoặc một RA chấm dứt hoạt động cho các đối tác, thuê bao bằng các phương tiện truyền thông hợp lý có thể sử dụng. Khi chấm dứt hoạt động, VNPT-CA sẽ thực hiện quy trình chấm dứt nhằm giảm thiểu các thiệt hại tới thuê bao, người nhận. Quy trình này có thể bao gồm các bước sau:

- Cung cấp thông tin về tình trạng chấm dứt hoạt động của VNPT-CA cho thuê bao và người nhận.

- Chịu chi phí cho các thông báo này.

- Thực hiện các thủ tục cần thiết nhằm thu hồi chứng thư số của VNPT-CA.

- Tiếp tục duy trì hệ thống lưu trữ các thông tin của VNPT-CA theo quy định của CPS này.

- Tiếp tục duy trì hệ thống hỗ trợ dịch vụ cho thuê bao.

- Tiếp tục duy trì hệ thống dịch vụ thu hồi, như CRL, OCSP.

- Tiến hành thu hồi các chứng thư số chưa bị thu hồi nếu thấy cần thiết.

- Hoàn phí cho thuê bao nếu chưa kết thúc hợp đồng.

- Hủy khóa bí mật của VNPT-CA và các thiết bị token chứa khóa bí mật

- Chuyển giao dịch vụ VNPT-CA cho đơn vị khác nếu có

6. CÁC VẤN ĐỀ AN TOÀN KỸ THUẬT

6.1. Sinh cặp khóa và vấn đề cài đặy

6.1.1. Sinh cặp khóa

Việc sinh cặp khóa của nhà cung cấp dịch vụ chứng thực chữ ký số công cộng bao gồm việc sinh cặp khóa của chính nhà cung cấp (được ký bởi Root CA quốc gia) và tạo cặp khóa bao gồm khóa công khai và khóa bí mật cho thuê bao (theo điều 3, Nghị định 130/2018/NĐ-CP).

Để hệ thống cung cấp dịch vụ có thể đảm bảo tạo cặp khóa ngẫn nhiên và duy nhất, có khả năng đảm bảo khóa bí mật không bị phát hiện khi có khóa công khai tương ứng, quá trình sinh khóa của hệ thống VNPT-CA tuân theo chuẩn PKCS #1 phiên bản 2.1, đáp ứng theo tiêu chuẩn trong Thông tư số 06/2015/TT-BTTTT của Bộ Thông Tin và Truyền Thông ban hành ngày 23 tháng 3 năm 2015.

Phương án sinh cặp khóa của VNPT-CA trong từng trường hợp như sau:

Đối với cặp khóa của nhà cung cấp dịch vụ: sẽ được sinh trực tiếp ở bên trong thiết bị HSM tuân theo tiêu chuẩn PKCS #1 phiên bản 2.1 trong Thông tư 06/2015/TT-BTTTT. Thiết bị HSM mà VNPT-CAsử dụng là của hãng SafeNet với các dòng thiết bị Luna SA 5. Thiết bị đạt chuẩn FIPS 140-2 level 3, có thể xem thêm tại Phụ lục 3 và Phụ lục 26 đặc tả kỹ thuật của thiết bị HSM SafeNet.

Đối với cặp khóa của thuê bao, có hai phương án:

- Cặp khóa được sinh ở phía thuê bao: tại phía thuê bao khóa sẽ được sinh bên trong thiết bị phần cứng đạt chuẩn tối thiểu FIPS 140-2 level 2, theo đúng tiêu chuẩn PKCS #1 phiên bản 2.1 trong Thông tư 06/2015/TT-BTTTT. VNPT-CA không cung cấp USB Token/Smart Card để sinh khóa phía thuê bao, thuê bao tự chuẩn bị thiết bị phần cứng đạt chuẩn tối thiểu FIPS 140-2 level 2 để sinh khóa.

- Trường hợp sinh khóa phía VNPT-CA (trong trường hợp thuê bao có thỏa thuận cho phép tạo khóa phía VNPT-CA): cặp khóa sẽ được sinh ra bên trong thiết bị phần cứng đạt chuẩn tối thiểu FIPS 140-2 level 2, theo đúng tiêu chuẩn PKCS #1 phiên bản 2.1 trong Thông tư 06/2015/TT-BTTTT. Thiết bị Usb Token sau đó được chuyển tận tay cho khách hàng (VNPT-CA cung cấp cho khách hàng thiết bị Usb token là ST3 ACE Token của Secure Metric. Xem thêm thông tin tại phụ lục 19).

Sau khi cặp khóa được sinh ra, tiếp theo sẽ tạo Certificate signing request (CSR) và dùng CSR này để tạo chứng thư số. Trong quá trình tạo chứng thư số hệ thống CoreCA sẽ kiểm tra tính trùng lặp của cặp khóa bằng cách kiểm tra trong cơ sở dữ liệu có tồn tại khóa công khai,

nếu trùng thông báo trùng cặp khóa và thực hiện tạo cặp khóa khác; nếu không trùng kết thúc quá trình sinh chứng thư số.

VNPT-CA cấp chứng thư số cho thuê bao có độ dài khóa tối thiểu là RSA 2048 bits nên đảm báo khóa bí mật không bị phát hiện khi có khóa công khai tương ứng.

VNPT-CA sử dụng USB Token loại ST3 ACE Token của Secure Metric để tạo cặp khóa trực tiếp trong thiết bị. Mặc khác thiết bị đạt tiêu chuẩn FIPS 186-4, có tiêu chuẩn về tạo cặp khóa RSA trong mục "5.1 RSA Key Pair Generation" đã mô tả cách tạo cặp khóa đảm bảo tạo cặp khóa chỉ cho phép mỗi cặp khóa được tạo ra ngẫu nhiên. Các tham số tạo khóa như p, q, e được tạo ngẫu nhiên bởi thuật toán Random Bit Generator (Tài liệu tham chiếu: https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2302 và https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf)

6.1.2. Chuyển giao khóa bí mật tới thuê bao

Theo quy định của Nghị định 130/2018/NĐ-CP thì nhà cung cấp dịch vụ chứng thực chữ ký số công cộng có thể tạo cặp khóa bao gồm khóa công khai và khóa bí mật cho thuê bao; cấp, gia hạn, tạm dừng, phục hồi và thu hồi chứng thư số của thuê bao; duy trì trực tuyến cơ sở dữ liệu về chứng thư số của thuê bao.

Như vậy hệ thống cung cấp dịch vụ của VNPT-CA yêu cầu phải có kênh phân phối khóa an toàn cho thuê bao, bảo sự toàn vẹn và bảo mật của cặp khóa. Các phương thức phân phối khóa như sau:

- Phương thức phân phối khóa tận tay: Hệ thống cung cấp dịch vụ VNPT-CA có thể sử dụng phân phối khóa tận tay (theo phương thức chìa khóa trao tay), bằng cách VNPT-CA tạo cặp khóa bên trong thiết bị phần cứng đạt chuẩn FIPS 140-2 level 3 (USB Token, Smartcard,…) tại trụ sở của nhà cung cấp theo tiêu chuẩn PKCS #1 phiên bản 2.1 được quy định trong Thông tư 06/2015/TT-BTTTT của Bộ Thông Tin và Truyền Thông, ký tạo và cấp chứng thư số cho thuê bao sau đó bàn giao thiết bị tới tận tay cho người đăng ký.

- Phương thức người dùng tự sinh cặp khóa: Hệ thống dịch vụ VNPT-CA có thể cho phép thuê bao lựa chọn phương thức đăng ký chứng thư số bằng cách tự sinh cặp khóa phía thuê bao và gửi request theo tiêu chuẩn PKCS #10 đến RA để xin cấp chứng thư số tại hệ thống CA server của nhà cung cấp dịch vụ.

- Hệ thống VNPT-CA không phân phối khóa bí mật trên mạng Internet, chỉ tiếp nhận Certificate signing request qua mạng Internet (có SSL) để sinh chứng thư số.

6.1.3. Chuyển giao khóa công khai tới đơn vị phát hành

Thuê bao gửi khóa công khai tới VNPT-CA thông qua phương tiện điện tử được quy định theo chuẩn yêu cầu chứng thư số PKCS#10 CSR hoặc phải bảo vệ đường truyền gói dữ liệu đã ký gửi đi theo chuẩn SSL.

6.1.4. Chuyển giao khóa công khai của CA tới thuê bao

VNPT-CA yêu cầu thuê bao phải tải và cài đặt khóa công khai của VNPT-CA. Khóa công khai của VNPT-CA có thể truy xuất theo điều khoản trong phần 2.1.

6.1.5. Kích thước khóa

Kích thước khóa cần phải đủ dài để đảm bảo tính an toàn của khóa bí mật. Chuẩn độ dài cặp khóa của VNPT-CA quy định tối thiểu phải tương đương với độ an toàn của cặp khóa RSA 2048 bits đối với thuê bao.

6.1.6. Sinh các tham số khóa và kiểm tra chất lượng

6.1.7. Các mục đích sử dụng khóa (quy định trong bản ghi X.509 v3 key usage)

Xem trong phần 7.1.2.1.

6.2.Bảo vệ khóa bí mật

6.2.1. Các chuẩn thiết bị mật mã an toàn

VNPT-CA sử dụng thiết bị mật mã phần cứng để sinh khóa và lưu trữ khóa bí mật gốc của CA. Theo yêu cầu tối thiểu, thiết bị này phải đạt tiêu chuẩn FIPS 140- 2 level 2.

6.2.2. Đa kiểm soát khóa bí mật

Cơ chế kiểm soát khóa bí mật của VNPT-CA là cơ chế chia sẻ mã theo chuẩn quốc tế, cơ chế này tách dữ liệu kích hoạt khóa bí mật thành các phần khác nhau (n), các phần được giữ bởi các đối tượng khác nhau. Để kích hoạt khóa cần ít nhất một số lơn hơn 1 (m) mảnh khóa (m =< n). Tại VNPT– CA, m >= 2.

6.2.3. Ủy thác giữ khóa bí mật

Khóa bí mật của VNPT-CA không được ủy thác. Khóa bí mật của thuê bao được ủy thác theo điều khoản phần 4.11.

6.2.4. Sao lưu khóa bí mật

Cặp khóa bí mật của VNPT-CA được sao lưu dự phòng trên thiết bị phần cứng an toàn và được đặt cách xa vị trí lưu trữ bản chính tối thiểu 10 km.

6.2.5. Lưu trữ khóa bí mật

Khi chứng thư số hết hạn, cặp khóa của VNPT-CA được lưu trữ an toàn trong vòng ít nhất 5 năm tiếp theo trên thiết bị mật mã phần cứng theo tiêu chuẩn do Bộ Thông tin và Truyền thông ban hành. Cặp khóa này không được sử dụng vào bất cứ hoạt động ký xác nhận nào sau thời gian hết hạn, trừ khi chứng thư số của VNPT-CA được gia hạn.

6.2.6. Chuyển khóa bí mật vào/ra thiết bị mật mã an toàn

Quy trình chuyển khóa bí mật vào thiết bị mật mã an toàn được tiến hành theo hướng dẫn của nhà cung cấp thiết bị, theo chuẩn do Bộ Thông tin và Truyền thông ban hành.

6.2.7. Lưu trữ khóa bí mật trên thiết bị mật mã an toàn

Quy trình lưu trữ khóa bí mật vào thiết bị mật mã an toàn được tiến hành theo hướng dẫn của nhà cung cấp thiết bị, theo chuẩn do Bộ Thông tin và Truyền thông ban hành.

6.2.8. Phương pháp kích hoạt sử dụng khóa bí mật

Tất cả các thành phần tham gia VNPT-CA cần phải bảo vệ dữ liệu dùng cho kích hoạt khóa bí mật khỏi bị mất, đánh cắp, sửa đổi, để lộ hoặc sử dụng trái phép. VNPT-CA sẽ thống nhất với thuê bao phương pháp kích hoạt sử dụng khóa bí mật cho từng loại chứng thư số cụ thể trong Hợp đồng dịch vụ.

6.2.9. Phương pháp hủy khóa bí mật

Trong trường hợp cặp khóa của VNPT-CA cần phải được hủy, VNPT-CA sẽ thực hiện việc hủy bỏ một cách triệt để, đảm bảo cặp khóa sau khi bị hủy không thể được khôi phục hoặc sử dụng bằng bất cứ hình thức nào. Thiết bị mật mã an toàn được hủy vật lý theo hướng dẫn của nhà sản xuất, theo chuẩn do Bộ Thông tin và Truyền thông ban hành trước khi ngừng lưu trữ.

6.2.10. Đánh giá thiết bị mật mã

Áp dụng chuẩn đánh giá thiết bị mật mã quy định tại phần 6.2.1.

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

6.3.1. Lưu trữ khóa công khai

Khóa công khai và chứng thư số được lưu trữ tại kho lưu trữ của VNPT-CA, theo phần 2.1.

6.3.2. Thời gian chứng thư số và cặp khóa hoạt động

Thời gian hoạt động của chứng thư số được bắt đầu từ thời điểm phát hành được ghi trong thuộc tính của chứng thư số và kết thúc tại thời điểm hết hạn có đề cập trong chứng thư số ngoại trừ trường hợp chứng thư số bị thu hồi trước thời hạn. Thời gian hoạt động của cặp khóa bằng thời gian hoạt động của chứng thư số tương ứng, ngoại trừ trường hợp chúng được dùng để giải mã và kiểm tra chữ ký. Thời gian hoạt động của cặp khóa trong chứng thư số VNPT-CA tuân theo quy định của Bộ Thông tin và Truyền thông. Thời gian hoạt động của cặp khóa trong chứng thư số thuê bao không được quá 5 năm.

6.4. Dữ liệu kích hoạt

6.4.1. Sinh và triển khai dữ liệu kích hoạt

VNPT-CA chọn mật khẩu đủ mạnh để bảo vệ khóa bí mật. Yêu cầu của mật khẩu đăng nhập hệ thống cần phải:

- Được một cá nhân tạo ra.
- Có ít nhất tám ký tự.
- Có ít nhất một ký tự là chữ cái và một ký tự là chữ số.
- Có ít nhất một ký tự chữ thường.
- Một ký tự bất kỳ không lặp lại từ 3 lần trở lên.
- Không trùng tên với tên của người vận hành.
- Không chứa một phần tên trong tên của người vận hành.

6.4.2. Bảo vệ dữ liệu kích hoạt

VNPT-CA khuyến cáo thuê bao tuân theo các yêu cầu trên. Ngoài ra để tăng cường an toàn, VNPT-CA khuyến khích sử dụng các cơ chế đa xác thực (token và passphRAe, sinh trắc và token, sinh trắc và passphRAe) cho quá trình kích hoạt khóa bí mật.

6.4.3. Các vấn đề khác của dữ liệu kích hoạt

6.4.3.1. Gửi dữ liệu kích hoạt

Khi tiến hành gửi dữ liệu kích hoạt khóa bí mật cho thuê bao, VNPT– CA sử dụng các phương pháp đảm bảo không để bị mất mát, đánh cắp, sửa đổi, để lộ hoặc sử dụng trái phép khóa bí mật.

6.4.3.2. Hủy dữ liệu kích hoạt

Khi cần thiết, dữ liệu kích hoạt khóa bí mật sẽ được VNPT-CA hủy bỏ bằng các phương pháp thích hợp, đảm bảo dữ liệu không bị mất mát, đánh cắp, sửa đổi, để lộ hoặc sử dụng trái phép khóa bí mật được bảo vệ bởi dữ liệu kích hoạt đó.

6.5. An toàn hệ thống máy tính

6.5.1. Yêu cầu kỹ thuật về an toàn hệ thống máy tính

Hệ thống mạng của VNPT-CA được tách biệt khỏi các hệ thống khác, được ngắt offline và cần truy cập vật lý để vận hành và sử dụng. Các thành phần trong hệ thống mạng của VNPT-CA được phân chia theo khu vực, có các thiết bị kiểm soát, phát hiện và ngăn chặn truy cập trái phép như firewall, IDS, IPS. VNPT-CA yêu cầu mật khẩu cần được thay đổi định kỳ và tuân theo tiêu chuẩn an toàn về mật khẩu, bao gồm độ dài tối thiểu, kết hợp giữa

chữ cái, chữ số và ký tự đặc biệt. Mọi truy cập vật lý trực tiếp vào hệ thống mạng của VNPT-CA do người tin cậy thực hiện. Các thao tác truy cập được kiểm soát giới hạn theo nhiệm vụ, chức năng của từng vị trí.

6.5.2. Đánh giá an toàn

VNPT-CA tuân theo chuẩn an toàn hệ thống máy tính ISO 27001. Công việc đánh giá và kiểm tra được tiến hành theo định kỳ và đột xuất căn cứ theo tình hình thực tế. Đơn vị quản lý hệ thống chịu trách nhiệm xử lý các báo cáo kiểm tra khảo sát và đưa ra biện pháp, kế hoạch và triển khai giải quyết các vấn đề trong báo cáo kiểm tra.

6.6. Các vấn đề quản lý kỹ thuật theo chu kỳ

6.6.1. Điều khiển quy trình phát triển hệ thống

VNPT-CA có trách nhiệm xây dựng và phát triển các phần mềm quản lý cho VNPT-CA và RA.

VNPT-CA cũng cung cấp cả phần mềm cho thuê bao và người nhận để thực hiện các chức năng tương tác với VNPT-CA.

6.6.2. Kiểm soát việc quản lý an toàn, an ninh

VNPT-CA có các cơ chế, chính sách để điều khiển và giám sát cấu hình hệ thống VNPT-CA.

Với các phần mềm ứng dụng, VNPT-CA tạo các giá trị mã hóa để đảm bảo tính toàn vẹn khi chuyển đến người dùng.

6.7. Quản lý an toàn mạng

Đối với các trao đổi thông tin giữa VNPT-CA và RA được thực hiện qua môi trường mạng, VNPT-CA đều có các biện pháp bảo mật tương ứng với các tiêu chuẩn quy định trong chính sách về bảo mật nhằm ngăn chặn các truy cập trái phép và các hoạt động tấn công khác.

6.8. Dán nhãn thời gian

Các chứng thư số, các CRL đều được dán nhãn thời gian phù hợp.

7. ĐẶC TẢ CHỨNG THƯ SỐ, CRL VÀ OCSP

7.1. Thành phần của chứng thư số

Chứng thư số có định dạng X.509 phiên bản 3 (1997) và RFC 3280 – Internet X.509 Public Key InfRAtructure Certificate, theo Thông tư 06/2015/TT-BTTTT. Tối thiểu thành phần chứng thư số phải có như sau:

Trường	*Giá trị hoặc yêu cầu*

Serial Number	Giá trị duy nhất được gán cho mỗi tên phân biệt (DN). Giá trị này được điều khiển bởi hệ thống máy chủ của VNPT-CA và được kiểm soát theo quy tắc đặt giá trị serial number do VNPT-CA quy định.
Signature Algorithm	Số hiệu của thuật toán dùng để ký chứng thư số (Xem phần 7.1.3)
Issuer DN	Bộ TTTT quy định
Valid From	Thời gian được tính theo chuẩn thời gian quốc tế UTC. Giá trị thời gian được ghi theo định dạng trong RFC 3280.
Valid To	Thời gian được tính theo chuẩn thời gian quốc tế UTC. Giá trị thời gian được ghi theo định dạng trong RFC 3280.
Subject DN	Bộ TTTT quy định
Subject Public Key	Lưu trữ theo định dạng ghi trong RFC 3280.
Signature	Chữ ký số được tạo và lưu theo định dạng trong RFC 3280.

7.1.1. Số hiệu phiên bản

Chứng thư số của VNPT-CA có thể là X.509 phiên bản 3.

Chứng thư số của thuê bao phải là X.509 phiên bản 3.

7.1.2. Các thành phần mở rộng

Cách sử dụng khóa (Key Usage) trong chứng thư số X.509 phiên bản 3 phải tuân theo quy định trong RFC 3280.

Phần mở rộng của chính sách chứng thư (Certificate Policies Extension) không được sử dụng trong chứng thư số của thuê bao.

Tên thay thế của thuê bao (Subject Alternative Names) trong chứng thư số X.509 phiên bản 3 khi sử dụng phải tuân theo quy định trong RFC 3280.

Các ràng buộc cơ bản (Basic Constraints): Không có quy định

Cách sử dụng khóa mở rộng (Extended Key Usage): Chứng thư số của VNPT-CA không sử dụng trường này.

Đối với chứng thư số của thuê bao các giá trị của trường này được sử dụng theo thỏa thuận trong Hợp đồng dịch vụ.

Điểm công bố danh sách chứng thư số bị thu hồi: Trường cRLDistributionPoints của chứng thư số X.509 phiên bản 3 có chứa địa chỉ URL để người dùng truy cập tới CRL nhằm kiểm tra trạng thái chứng thư số.

7.1.3. Số hiệu thuật toán

Chứng thư số của VNPT– CA sử dụng các thuật toán sau đây:

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

- sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member- body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

7.1.4. Định dạng tên

Định dạng tên của chứng thư số tuân theo quy định trong phần 3.1.1

7.1.5. Các ràng buộc về tên

Không có quy định.

7.1.6. Số hiệu của quy chế chứng thực

Số hiệu (OID) của CPS này sẽ được đăng ký khi hệ thống của VNPT-CA chính thức đi vào hoạt động.

7.1.7. Sử dụng các ràng buộc quy chế mở rộng

Không có quy định.

7.1.8. Cú pháp và ngữ nghĩa quy chế

Không có quy định.

7.1.9. Xử lý ngữ nghĩa các quy chế chứng thư số mở rộng

Không có quy định.

7.2. Thành phần danh sách chứng thư số bị thu hồi

CRL cần chứa các giá trị sau đây

Trường	*Giá trị hoặc yêu cầu*
Version	Xem phần 7.2.1
Signature Algorithm	Thuật toán dùng để ký danh sách chứng thư số bị thu hồi. VNPT-CA sử dụng thuật toán sau theo chuẩn RFC 3279. sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
Issuer	Thực thể thi hành ký và phát hành danh sách chứng thư số bị thu hồi.
Effective Date	Ngày có hiệu lực của danh sách chứng thư số bị thu hồi. Các CRL có hiệu lực ngay khi phát hành.
Next Update	Ngày cập nhật phiên bản tiếp theo của danh sách chứng thư số bị thu hồi.
Revoked Certificates	Danh các các chứng thư số bị thu hồi, bao gồm số hiệu (Serial Number) của chứng thư số bị thu hồi và ngày thu hồi.

7.2.1. Số hiệu phiên bản của CRL

VNPT-CA hỗ trợ định dạng CRL theo phiên bản 1 hoặc phiên bản 2 của RFC 3280.

7.2.2. CRL và các mở rộng

Không có quy định.

7.3. Thành phần OCSP

OCSP (Online Certificate Status Protocol) là giao thức cho phép kiểm tra trạng thái chứng thư số trực tuyến.

7.3.1. Số hiệu phiên bản của OCSP

VNPT-CA hỗ trợ giao thức OCSP phiên bản 1 được tuân theo chuẩn RFC 2560.

7.3.2. Các mở rộng OCSP

Không có quy định.

8. KIỂM ĐỊNH TÍNH TUÂN THỦ VÀ CÁC ĐÁNH GIÁ

8.1. Tần suất đánh giá

Đánh giá kiểm tra được thực hiện ít nhất định kỳ hàng năm bởi đơn vị kiểm định đáp ứng yêu cầu theo quy định của pháp luật và yêu cầu của VNPT-CA.

8.2. Đơn vị thực hiện đánh giá chất lượng

Đơn vị kiểm định thực hiện kiểm tra VNPT-CA phải là đơn vị độc lập có khả năng sau:

- Có năng lực thành thạo về công nghệ hạ tầng khóa công khai, công cụ và kĩ thuật an toàn thông tin.
- Được chứng nhận bởi RootCA.

8.3. Mối quan hệ của đơn vị thực hiện đánh giá

Quá trình thực hiện đánh giá phải do đơn vị kiểm định độc lập với VNPT– CA tiến hành.

8.4. Các nôi dung cần đánh giá

Phạm vi đánh giá bao gồm môi trường hoạt động của VNPT-CA, các hoạt động quản lý khóa, các quy trình kiểm soát điều khiển và quản trị VNPT-CA, quản lý thời gian sống của các chứng thư số và quá trình thực tế hoạt động kinh doanh.

8.5. Xử lý các thiếu sót

Căn cứ theo kết quả đánh giá và kiểm định, các vấn đề sự cố và thiếu sót phải được chỉ ra và xử lý bởi bộ phận quản lý của VNPT-CA. Nếu các vấn đề này ảnh hưởng nghiêm trọng tới tính an toàn và toàn vẹn của VNPT-CA, bộ phận quản lý VNPT-CA phải xây dựng kế hoạch hành động và triển khai ngay lập tức trong khoảng thời gian thương mại hợp lý. Đối với các sự cố kém nghiêm trọng hơn, bộ phận quản lý VNPT-CA sẽ lượng giá mức độ và xác định các hành động cần thực hiện.

8.6. Kết quả

Kết quả kiểm định hệ thống VNPT-CA được công bố trên website của VNPT-CA.

9. KINH DOANH VÀ LUẬT PHÁP

9.1. Lệ phí

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

Các thuê bao sử dụng dịch vụ VNPT-CA phải trả phí khi xin cấp chứng thư, quản lí và tạo mới chứng thư cho nhà cung cấp.

9.1.2. Lệ phí sử dụng chứng thư số

Các thuê bao sử dụng dịch vụ VNPT-CA và RA không phải trả phí để tạo ra kho Chứng thư hay dịch vụ cung cấp trực tuyến thông tin của chứng thư cho các đối tác tin cậy.

9.1.3. Lệ phí thu hồi hoặc kiểm tra trạng thái chứng thư số

Theo quy định của nhà nước.

9.1.4. Lệ phí sử dụng cho các dịch vụ khác

Các CA không được trả phí khi truy cập các CPS này. Việc xem văn bản với các mục đích như sao chép, phân bổ lại, sửa chữa hoặc tạo mới các công việc phát sinh sẽ phải chấp thuận bản thỏa thuận hợp pháp với người đang nắm giữ phiên bản copy của văn bản này.

9.1.5. Quy chế hoàn trả phí

VNPT-CA sẽ đưa ra phạm vi cho việc áp dụng chính sách hoàn trả phí. Chính sách này sẽ được đưa vào văn bản thỏa thuận với thuê bao sử dụng dịch vụ hay hợp đồng.

9.2. Trách nhiệm tài chính

9.2.1. Phạm vi bảo hiểm

VNPT-CA sẽ duy trì ở mức độ thương mại đáng kể cho các thông tin bảo hiểm đối với những lỗi sai hay thiếu sót, hoặc thông qua các chương trình bảo hiểm lỗi sai 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.

VNPT-CAtiến 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.

- VNPT-CAđưa ra các mức đền bù bảo hiểm và có trách nhiệm thực hiện theo các mức bảo hiểm chứng thư khác nhau đó.

- Việc đền bù bảo hiểm thực hiện theo đúng hợp đồng với thuê bao.

VNPT-CAsẽ không chịu trách nhiệm trong các trường hợp:

- Các trường hợp sử dụng chứng thư không được đề cập đến trong CP, CPS

- Các trường hợp giả mạo xử lý chứng thư.

- 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.

- Khóa riêng bị mất, bị phá hủy do khách hàng.

- Khách hàng đánh mất hoặc để lộ code PIN bảo vệ khóa bí mật.

- Lỗi của RA, bao gồm lỗi xác thực, việc nhận biết dữ liệu, số chứng thư, giá trị khóa công cộng, RA không gửi yêu cầu chính xác… Khi có lỗi này xảy ra, RA sẽ chịu hoàn toàn trách nhiệm với khách hàng. Việc đền bù được thực hiện theo hợp đồng với thuê bao.

9.2.2. Các tài sản khác

VNPT-CA có quyền tự chủ tài chính để duy trì hoạt động và thực hiện các nhiệm vụ của mình, đồng thời có trách nhiệm pháp lý đối với các rủi ro cho thuê bao và người nhận.

9.3. Bảo mật các thông tin kinh doanh

9.3.1. Phạm vi của bảo mật thông tin

Những dữ liệu sau của thuê bao, sẽ được đảm bảo tính mật và riêng tư (“thông tin mật/riêng tư”)

- Các dữ liệu ứng dụng CA, phê chuẩn hoặc không phê chuẩn.

- Các khóa riêng được giữ bởi thuê bao doanh nghiệp sử dụng hệ thống quản lý khóa công cộng và các thông tin cần thiết để khôi phục các khóa này.

- Các dữ liệu chuyển đổi (đầy đủ và các dữ liệu kiểm toán của quá trình chuyển đổi).

- Các dữ liệu kiểm toán tạo hoặc lưu giữ bởi VNPT-CA hoặc một thuê bao .

- Các báo cáo kiểm toán tạo bởi VNPT-CA hay thuê bao, hoặc những kiểm toán viên bên ngoài.

- Các dự án khôi phục do tai nạn hay khôi phục sau thảm họa.

- Quản lý mức độ an ninh trong hoạt động của phần cứng, phần mềm, các quản trị viên của dịch vụ chứng thư và của các dịch vụ khác.

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

Chứng thư số, thu hồi chứng thư số và các thông tin về trạng thái của chứng thư số, nơi lưu giữ của VNPT-CA cùng các thông tin chứa bên trong chúng không được coi là các thông tin mật/riêng tư. Các thông tin mật/riêng tư trong phần 9.3.1 sẽ không được coi là riêng tư hoặc không được coi là bí mật nếu pháp luật có quy định khác.

9.3.3. Trách nhiệm bảo vệ thông tin mật

VNPT-CA đảm bảo các thông tin riêng tư không bị tiết lộ với bên thứ 3.

9.4. Tính riêng tư của thông tin cá nhân

9.4.1. Chính sách đảm bảo tính riêng tư

VNPT-CA sẽ tiến hành triển khai chính sách đảm bảo tính riêng, tuân theo luật riêng tư. VNPT-CA sẽ không tiết lộ tên hay bất cứ một thông tin nào về các ứng dụng chứng chỉ của thuê bao ra bên ngoài.

9.4.2. Những thông tin coi là riêng tư

Tất cả những thông tin về thuê bao là không được công bố, bao gồm chứng thư ban hành, thư mục chứng thư và các CRL trực tuyến được coi như thông tin riêng tư.

9.4.3. Thông tin không được coi là riêng tư

Theo luật địa phương, tất cả các thông tin được công khai trong một chứng thư được coi như không phải giữ riêng tư.

9.4.4. Trách nhiệm bảo vệ thông tin riêng tư

Những người tham gia trong dịch vụ VNPT-CA, nhận các thông tin mật sẽ phải đảm bảo tính mật cho những thông tin này không bị phơi bày với bên thứ ba và phải tuân theo những luật lệ địa phương trọng phạm vi quyền hạn của mình.

9.4.5. Thông báo và cho phép sử dụng thông tin riêng tư

Theo quy định của pháp luật hoặc theo thỏa thuận giữa các bên, các thông tin riêng tư sẽ không được sử dụng mà không có sự cho phép của người sở hữu chúng.

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

VNPT-CA sẽ được phép công bố những thông tin mật/riêng tư nếu:

- Quá trình công bố là cần thiết để đáp ứng yêu cầu của cơ quan nhà nước có thẩm quyền, quá trình quản trị hay các quá trình liên quan đến luật pháp, các hoạt động quản lý.
- Quá trình công bố nhằm tuân thủ quy định của pháp luật.

9.4.7. Các trường hợp làm lộ thông tin khác

9.5. **Quyền sở hữu trí tuệ**

Việc xác định rõ quyền sở hữu trí tuệ giữa các miền con tham gia của VNPT-CA chứ không phải giữa các thuê bao và các bên đối tác được khống chế bởi các thỏa thuận hợp lý giữa các bên miền con liên quan. Những phần sau sẽ sử dụng tới quyền sở hữu trí tuệ liên quan tới thuê bao và các bên đối tác.

Quyền sở hữu trong chứng thư số và thông tin thu hồi chứng thư số

VNPT-CA có tất cả quyền sở hữu trí tuệ liên quan đến chứng thư số và các thông tin thu hồi chứng thư số do VNPT-CA ban hành.

VNPT-CA được phép sao chép và phân phối chứng thư số mà không cần trả phí với điều kiện phải đảm bảo tính nguyên vẹn của chứng thư số.

VNPT-CA và thuê bao cho phép người nhận sử dụng các thông tin về tình trạng thu hồi của chứng thư số để thực hiện chức năng của mình tuân theo thỏa thuận sử dụng CRL, thỏa thuận với người nhận hay các thỏa thuận thích hợp khác.

Quyền sở hữu trong CPS

Các bên liên quan tới dịch vụ VNPT-CA chấp nhận rằng VNPT-CA lưu trữ quyền sở hữu tương ứng với CPS này.

Quyền sở hữu tên

Một người dùng chứng thư nắm giữ tất cả các quyền về thương hiệu như tên dịch vụ, thương mại thuộc ứng dụng chứng thư của họ và được phân biệt tên với các chứng thư đã được ban hành.

Quyền sở hữu khóa và các tài liệu của khóa

Cặp khóa tương ứng với chứng thư số của CA và thuê bao đầu cuối được sở hữu bởi CA và thuê bao đầu cuối.

9.6. Vấn đề đại diện và bảo lãnh

9.6.1. Cam kết và đảm bảo của CA

VNPT-CA đảm bảo rằng:

- Không có những thông tin sai lạc với thực tế trong chứng thư.
- Những chứng thư của VNPT đạt tiêu chuẩn yêu cầu trong CPS này.
- Dịch vụ thu hồi và sử dụng chứng thư, lưu trữ chứng thư thích hợp với tiêu chuẩn trong CPS này.
- Thỏa thuận thuê bao có thể chứa thêm các tuyên bố và cam kết khác

9.6.2. Cam kết và đảm bảo của RA

Các RA của VNPT-CA đảm bảo:

- Không có những thông tin sai lạc với thực tế trong chứng thư.
- Những chứng thư của RA đạt tiêu chuẩn trong yêu cầu trong CPS này.
- Dịch vụ thu hồi và sử dụng chứng thư của nơi lưu trữ thích hợp với tiêu chuẩn trong CPS.

Thỏa thuận thuê bao có thể chứa thêm các tuyên bố và cam kết khác.

9.6.3. Cam kết vào đảm bảo của Thuê bao

Người thuê bao sử dụng cam kết rằng:

- Mỗi chữ ký điện tử sử dụng khóa bí mật tương ứng với khóa công khai liệt kê trong chứng thư số là chữ ký điện tử của thuê bao và chứng thư được chấp nhận và hoạt động (khi chưa hết hạn hay bị thu hồi) trong thời gian chữ ký điện tử này được tạo
- Khóa riêng bí mật của họ được bảo vệ và những người không có thẩm quyền không thể truy cập vào khóa này.
- Tất cả những thông tin cung cấp bởi thuê bao và chứa bên trong chứng thư là đúng sự thật
- Chứng thư được sử dụng cho các mục đích hợp pháp và tuân theo những yêu cầu trong CPS.
- Thuê bao là người sử dụng cuối và không phải là một CA, và không sử dụng khóa riêng tương ứng với bất cứ khóa công khai nào được liệt kê trong chứng thư cho các mục đích chữ ký điện tử cho bất cứ chứng thư nào(hoặc các dạng khóa công khai được chứng nhận khác) hay CRL, như là một CA.

Thỏa thuận thuê bao có thể chứa thêm các tuyên bố và cam kết khác.

9.6.4. Đại diện cho người nhận và vấn đề bảo lãnh

Thỏa thuận với người nhận yêu cầu người nhận phải có đủ thông tin để đưa ra một quyết định dựa vào các thông tin trong chứng thư số. Họ có trách nhiệm quyết định tin tưởng hay không vào các thông tin trong chứng thư số. Người nhận phải chịu trách nhiệm pháp lý nếu vi phạm các điều khoản về nghĩa vụ của người nhận quy định trong CPS này.

Thỏa thuận giữa VNPT-CA và người nhận có thể bao gồm thêm các tuyên bố và cam kết khác.

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

Không có qui định.

9.7. Từ chối bảo lãnh

Trong giới hạn cho phép của luật pháp, hợp đồng thuê bao và người nhận có thể bị VNPT-CA từ chối bảo lãnh.

9.8. Giới hạn trách nhiệm pháp lý

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

9.9. Bồi thường

Vấn đề bồi thường của thuê bao sử dụng

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

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

Hợp đồng với thuê bao tương ứng có thể có một số nghĩa vụ khác.

Vấn đề bồi thường của các đối tác tin cậy

Khi được pháp luật cho phép, bản thỏa thuận của đối tác tin cậy sẽ yêu cầu các đối tác tin cậy bồithường cho VNPT-CA khi:

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

Thỏa thuận tương ứng bên đối tác có thể có thêm một số nghĩa vụ khác.

9.10. Thời hạn và kết thúc

9.10.1. Thời hạn

CPS này bắt đầu có hiệu lực khi hệ thống VNPT-CA chính thức đi vào hoạt động.

Các điều sửa đổi bổ sung cho CPS này có hiệu lực khi có sự công bố từ kho lưu trữ của dịch vụ VNPT-CA.

9.10.2. Kết thúc

CPS này này khi được bổ sung, sửa đổi sẽ vẫn giữ hiệu lực cho đến khi được thay thế bởi một văn bản mới.

9.10.3. Kết quả của kết thúc hiệu lực và các tồn tại

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

9.11. Thông báo cho các bên liên quan

VNPT-CA sẽ sử dụng các biện pháp thích hợp để thông báo cho các bên liên quan về nội dung sửa đổi, bổ sung CPS này.

9.12. Những điều sửa đổi

9.12.1. Thủ tục sửa đổi

Những sửa đổi của CPS này sẽ được thực hiện bởi VNPT-CA. Những điều sửa đổi có thể ở dạng tài liệu chứa tất cả những điều sửa đổi cho CPS hoặc ở dạng cập nhật. Phiên bản sửa đổi hay cập nhật được liên kết đến phần thông báo và cập nhật trong kho lưu trữ của dịch vụ VNPT-CA tại địa chỉ https://www.vnpt-ca.vn/

9.12.2. Cơ chế và thời gian thông báo

VNPT-CA có quyền quyết định việc thay đổi là cần thiết hay không cần thiết.

Những đề xuất thay đổi CPS sẽ được nêu ra trong tài liệu của VNPT-CA tại địa chỉ: http://www.vnpt-ca.vn/

VNPT-CA tập hợp những đề nghị thay đổi CPS từ các thành phần tham gia dịch vụ VNPT-CA. Nếu VNPT-CA cho rằng một sự thay đổi nào đó là cần thiết thì việc thay đổi sẽ được thực hiện.

Ngoài ra, nếu VNPT-CA cho rằng thay đổi CPS là cần thiết để ngăn chặn xâm phạm đến an toàn của dịch vụ VNPT-CA, thì việc thay đổi sẽ ngay lập tức được thực hiện và có hiệu lực.

9.12.3. Các trường hợp OID thay đổi

Nếu cần thiết, VNPT-CA có thể thay đổi OID cho các chính sách chứng thư số tương ứng với từng cấp chứng thư số. Nếu không, việc sửa đổi sẽ không bao gồm việc sửa đổi OID.

9.13. Các điều khoản tranh chấp

Tranh chấp giữa VNPT, đối tác và thuê bao

Việc giải quyết tranh chấp giữa VNPT-CA, người nhận và thuê bao phải tuân thủ theo các điều khoản được ghi trong hợp đồng và trên cơ sở quy định của pháp luật.

Tranh chấp với thuê bao hay người nhận

Trường hợp này được thực hiện theo quy định của pháp luật.

9.14. Áp dụng luật

CPS này được xây dựng theo quy định của pháp luật của nước Cộng hòa xã hội chủ nghĩa Việt Nam.

Trong quá trình cung cấp, sử dụng dịch vụ VNPT-CA cũng như giải quyết các tranh chấp phát sinh các thành phần tham gia dịch vụ VNPT-CA cũng như các bên liên quan sẽ áp dụng pháp luật của nước Cộng hòa xã hội chủ nghĩa Việt Nam.

9.15. Chấp hành theo hệ thống luật phù hợp

Trong trường hợp điều ước quốc tế mà Việt Nam tham gia hoặc phê chuẩn có quy định khác pháp luật trong nước thì áp điều ước đó.

9.16. Các quy định khác

9.16.1. Điều khoản thỏa thuận chung

Không có quy định.

9.16.2. Tính độc lập của các điều khoản

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 toàn hay một cuộc xét xử có thẩm quyền, phần còn lại của CPS vẫn có hiệu lực.

9.16.3. Sự thực thi (quyền ủy nhiệm và quyền khước từ)

Bất kỳ một bên nào chiếm ưu thế trong những tranh cãi nảy sinh ngoài hợp đồng đều được quyền ủy nhiệm hoặc quyền khước từ do sự vi phạm một trong các điều khoản trong hợp đồng.

9.16.4. Chính sách bắt buộc thực thi

Trong phạm vi luật pháp cho phép, thỏa thuận của thuê bao và thỏa thuận bên liên quan bắt buộc phải tuân theo các điều khoản bảo vệ dịch vụ VNPT- CA.

9.17. Các điều khoản khác

Không có quy định.