

**TẬP ĐOÀN BƯU CHÍNH VIỄN THÔNG VIỆT NAM**

=====\*\*\*=====

**QUY CHẾ CHỨNG THỰC**  
**DỊCH VỤ CHỮ KÝ SỐ VÀ CHỨNG THỰC CHỮ KÝ SỐ**  
**THEO MÔ HÌNH KÝ SỐ TỪ XA**

**(VNPT SMARTCA)**

**Hà Nội, năm 2021**

**DỊCH VỤ CHỮ KÝ SỐ VÀ CHỨNG THỰC CHỮ KÝ SỐ THEO  
MÔ HÌNH KÝ SỐ TỪ XA – VNPT SMARTCA**

***TÀI LIỆU QUY CHẾ CHỨNG THỰC***

---

<b>Ngày hiệu lực:</b>	04/08/2021		
<b>Lần ban hành:</b>	01		
<b>Phiên bản:</b>	1.0		
	<b>Họ và Tên</b>	<b>Chức danh</b>	<b>Đơn vị</b>
<b>Soạn thảo:</b>	Nguyễn Đăng Huy	Tổ trưởng	Trung tâm eGOV – Công ty VNPT-IT
<b>Kiểm tra:</b>	Nguyễn Thanh Phong	PDM	Trung tâm eGOV– Công ty VNPT-IT
<b>Thẩm định:</b>	Nguyễn Thị Thành Chung	Chuyên quản SPDV	Ban Tiếp thị - Bán hàng – Công ty VNPT-IT

**BẢNG THEO DÕI THAY ĐỔI TÀI LIỆU**

<b>Ngày sửa đổi</b>	<b>Nội dung thay đổi</b>	<b>Ngày hiệu lực</b>	<b>Phê duyệt</b>
01/06/2021	Tạo mới	04/08/2021	04/08/2021

# MỤC LỤC

MỤC LỤC .....	3
Lời giới thiệu .....	11
1. GIỚI THIỆU .....	12
1.1. Tổng quan .....	12
1.2. Tên và dấu hiệu nhận biết .....	12
1.3. Thành phần tham gia dịch vụ VNPT SmartCA .....	12
1.3.1. Thành phần Certification Authorities (CA) .....	12
1.3.2. Thành phần Registration Authorities (RA) .....	14
1.3.3. Thành phần Account Manager (AM) .....	14
1.3.4. Thuê bao .....	14
1.3.5. Thành phần người nhận .....	15
1.3.6. Thành phần khác .....	16
1.4. Mục đích sử dụng chứng thư số .....	16
1.4.1. Chứng thư số hợp pháp .....	16
1.4.2. Chứng thư số không hợp pháp .....	16
1.5. Quản lý cơ chế chứng thực .....	16
1.5.1. Tổ chức quản lý .....	16
1.5.2. Liên hệ .....	16
1.5.3. Đơn vị quyết định tính hợp pháp của CPS .....	17
1.5.4. Thủ tục phê duyệt CPS .....	17
1.6. Các định nghĩa và từ viết tắt .....	17
2. TRÁCH NHIỆM LƯU TRỮ VÀ CÔNG BỐ THÔNG TIN .....	17
2.1. Lưu trữ .....	17
2.2. Công bố thông tin .....	18
2.3. Thời gian, tần suất công bố thông tin .....	18
2.4. Kiểm soát việc truy cập thông tin .....	19
3. NHẬN DẠNG VÀ XÁC THỰC YÊU CẦU XIN CẤP CHỨNG THƯ SỐ .....	19
3.1. Đặt tên trong chứng thư số .....	19
3.1.1. Các thuộc tính .....	19
3.1.2. Tính rõ ràng và ý nghĩa của tên trong chứng thư .....	20
3.1.3. Trường hợp thuê bao sử dụng tên ẩn danh hay bút danh .....	20
3.1.4. Quy tắc diễn giải các mẫu tên .....	20
3.1.5. Tính duy nhất của tên thuê bao .....	20

3.1.6. Nhận dạng, xác thực và vai trò của thương hiệu.....	20
3.2. Xác minh đề nghị cấp chứng thư số.....	21
3.2.1. Phương pháp chứng minh sở hữu khóa bí mật.....	21
3.2.2. Xác minh định danh tổ chức .....	21
3.2.3. Xác minh định danh cá nhân .....	21
3.2.4. Thông tin thuê bao không xác minh.....	21
3.2.5. Xác thực thẩm quyền.....	21
3.2.6. Các tiêu chuẩn thực hiện liên hoạt .....	22
3.3. Xác minh đề nghị thay đổi cặp khóa.....	22
3.4. Xác minh đề nghị thu hồi chung thư số .....	22
4. CÁC QUY ĐỊNH VỀ VIỆC QUẢN LÝ VÒNG ĐỜI CỦA CHỨNG THƯ SỐ.....	23
4.1. Yêu cầu cấp chứng thư số .....	23
4.1.1. Đối tượng được phép yêu cầu cấp chứng thư số .....	23
4.1.2. Quy trình xử lý đơn xin cấp chứng thư số.....	23
4.2. Xử lý yêu cầu cấp chứng thư số.....	24
4.2.1. Xác thực định danh .....	24
4.2.2. Chấp nhận hoặc từ chối cấp chứng thư số.....	24
4.2.3. Thời gian xử lý yêu cầu.....	24
4.3. Phát hành chứng thư số.....	25
4.3.1. Hoạt động CA trong phát hành chứng thư số.....	25
4.3.2. Thông báo tới thuê bao.....	25
4.4. Chứng nhận chứng thư số .....	25
4.4.1. Điều kiện chứng minh việc chấp nhận chứng thư số .....	25
4.4.2. Công bố chứng thư số .....	25
4.4.3. Thông báo đến các đối tượng khác về việc phát hành chứng thư số.....	25
4.5. Sử dụng cặp khóa và chứng thư số .....	25
4.5.1 Cách sử dụng chứng thư số và khóa bí mật của thuê bao .....	25
4.5.2. Cách sử dụng chứng thư số và khóa công khai của người nhận .....	27
4.6. Gia hạn chứng thư số .....	27
4.6.1. Điều kiện gia hạn.....	27
4.6.2. Đối tượng được phép yêu cầu gia hạn.....	27
4.6.3. Xử lý yêu cầu gia hạn chứng thư số .....	28
4.6.4. Thông báo cho thuê bao về việc phát hành chứng thư số mới.....	28
4.6.5. Điều khoản chấp nhận gia hạn chứng thư số.....	28

4.6.6. Công bố chứng thư số được gia hạn.....	28
4.6.7. Thông báo đến các đối tượng khác về việc gia hạn chứng thư số.....	28
4.7. Thay đổi cặp khóa.....	28
4.7.1. Điều kiện thay đổi .....	28
4.7.2. Đối tượng được phép yêu cầu thay đổi khóa.....	28
4.7.3. Xử lý yêu cầu thay đổi khóa.....	28
4.7.4. Thông báo cho thuê bao về việc thay khóa chứng thư số .....	29
4.7.5. Điều khoản chấp nhận thay khóa chứng thư số.....	29
4.7.6. Công bố chứng thư số đã thay khóa .....	29
4.7.7. Thông báo đến các đối tượng khác về việc thay khóa chứng thư số.....	29
4.8. Hủy cặp khóa .....	29
4.9. Thay đổi chứng thư số .....	30
4.9.1. Điều kiện thay đổi .....	30
4.9.2. Đối tượng được phép yêu cầu chứng thư số.....	30
4.9.3. Xử lý yêu cầu thay đổi chứng thư số.....	30
4.9.4. Thông báo cho thuê bao về việc thay khóa chứng thư số .....	30
4.9.5. Điều khoản chấp nhận thay khóa chứng thư số.....	30
4.9.6. Công bố chứng thư số đã thay đổi.....	31
4.9.7. Thông báo đến các đối tượng khác về việc thay khóa chứng thư số.....	31
4.10. Tạm dừng và Thu hồi chứng thư số.....	31
4.10.1. Các trường hợp thu hồi chứng thư số.....	31
4.10.2. Đối tượng yêu cầu thu hồi.....	32
4.10.3. Thủ tục yêu cầu thu hồi.....	32
4.10.4. Thời gian xử lý yêu cầu thu hồi .....	32
4.10.5. Thời gian xử lý đề nghị thu hồi.....	32
4.10.6. Yêu cầu kiểm tra thu hồi cho người nhận .....	32
4.10.7. Tần suất phát hành chứng thư số bị thu hồi .....	33
4.10.8. Thời gian trễ lớn nhất của CRL.....	33
4.10.9. Hỗ trợ kiểm tra trực tuyến trạng thái chứng thư số bị thu hồi.....	33
4.10.10. Điều kiện kiểm tra trực tuyến chứng thư số bị thu hồi.....	33
4.10.11. Mẫu quảng bá chứng thư số bị thu hồi khác .....	33
4.10.12. Các điều kiện đặc biệt khi khóa bị xâm phạm.....	33
4.10.13. Các trường hợp tạm dừng.....	33
4.10.14. Đối tượng được phép yêu cầu tạm dừng .....	33

4.10.15. Thủ tục yêu cầu tạm dừng .....	33
4.10.16. Giới hạn thời gian tạm dừng .....	33
4.11. Dịch vụ kiểm tra trạng thái chứng thư số.....	33
4.11.1. Đặc tính hoạt động .....	33
4.11.2. Tính sẵn sàng của dịch vụ .....	34
4.11.3. Các đặc tính tùy chọn .....	34
4.12. Chấm dứt dịch vụ của thuê bao.....	34
4.13. Lưu trữ và phục hồi khóa bí mật của thuê bao.....	35
<b>5. KIỂM SOÁT, QUẢN LÝ VÀ VẬN HÀNH.....</b>	<b>35</b>
5.1. Thiết bị, máy móc, nguồn điện, trụ sở và các yếu tố cần thiết khác .....	35
5.1.1 Ví trí xây dựng .....	35
5.1.2. Kiểm soát an toàn, an ninh vật lý .....	35
5.1.3. Điều kiện nguồn điện .....	36
5.1.4. Phòng chống nước .....	36
5.1.5. Phòng cháy chữa cháy.....	36
5.1.6. Phương tiện lưu trữ .....	36
5.1.7. Tiêu hủy rác.....	36
5.1.8. Hệ thống dự phòng .....	36
5.2. Quy trình kiểm soát.....	37
5.2.1. Vai trò tin cậy .....	37
5.2.2. Số lượng người tin cậy yêu cầu cho mỗi công việc .....	37
5.2.3. Xác thực định danh các vai trò.....	37
5.2.4. Phân chia trách nhiệm giữa các vị trí .....	38
5.3. Kiểm soát nhân sự.....	38
5.3.1. Yêu cầu phẩm chất, kinh nghiệm và tin tưởng.....	38
5.3.2. Thủ tục kiểm tra lý lịch .....	38
5.3.3. Yêu cầu đào tạo .....	39
5.3.4. Yêu cầu đào tạo lại thường xuyên.....	39
5.3.5. Tần suất luân chuyển công tác .....	39
5.3.6. Kỉ luật đối với các hành vi vi phạm .....	40
5.3.7. Các yêu cầu ký kết độc lập.....	40
5.3.8. Cung cấp tài liệu cho nhân viên .....	40
5.4. Các quy trình ghi nhật ký hệ thống.....	40
5.4.1. Các sự kiện VNPT SmartCA cần ghi nhận .....	40

5.4.2. Tần suất xử lý bản ghi kiểm tra.....	41
5.4.3. Thời gian lưu trữ bản ghi kiểm tra .....	41
5.4.4. Bảo vệ bản ghi kiểm tra.....	41
5.4.5. Thủ tục sao lưu bản ghi kiểm tra.....	41
5.4.6. Hệ thống kiểm tra.....	41
5.5. Lưu trữ các bản ghi .....	41
5.5.1. Các loại hồ sơ cần lưu trữ.....	41
5.5.2. Thời gian lưu trữ .....	41
5.5.3. Bảo vệ dữ liệu lưu trữ.....	42
5.5.4. Thủ tục thực hiện sao lưu .....	42
5.5.5. Yêu cầu dán nhãn thời gian cho các hồ sơ .....	42
5.6. Thay đổi khóa .....	42
5.7. Xử lý sự cố, thảm họa và phục hồi .....	42
5.7.1. Thủ tục xử lý vấn đề lộ khóa và sự cố.....	42
5.7.2. Tài nguyên máy tính, phần mềm và dữ liệu .....	42
5.7.3. Thủ tục xử lý sự cố bị lộ khóa bí mật.....	43
5.7.4. Khả năng khôi phục hoạt động kinh doanh sau sự cố .....	43
5.8. Dừng hoạt động.....	44
<b>6. ĐẢM BẢO AN TOÀN AN NINH VỀ KỸ THUẬT .....</b>	<b>44</b>
6.1. Tạo và phân phối cặp khóa .....	44
6.1.1. Sinh cặp khóa .....	44
6.1.3. Chuyển giao khóa công khai tới đơn vị phát hành.....	45
6.1.4. Chuyển giao khóa công khai của CA tới thuê bao .....	45
6.1.5. Kích thước khóa .....	45
6.1.6. Sinh các tham số khóa và kiểm tra chất lượng.....	45
6.1.7. Các mục đích sử dụng khóa (quy định trong bản ghi X.509 v3 key usage) .....	45
6.2. Kiểm soát và bảo vệ khóa bí mật.....	45
6.2.1. Các chuẩn thiết bị mật mã an toàn .....	45
6.2.2. Đa kiểm soát khóa bí mật.....	45
6.2.3. Ủy thác giữ khóa bí mật .....	45
6.2.4. Sao lưu khóa bí mật.....	46
6.2.5. Lưu trữ khóa bí mật.....	46
6.2.6. Chuyển khóa bí mật vào/ra thiết bị mật mã an toàn.....	46
6.2.7. Lưu trữ khóa bí mật trên thiết bị mật mã an toàn.....	46

6.2.8. Phương pháp kích hoạt sử dụng khóa bí mật .....	46
6.2.9. Phương pháp hủy khóa bí mật.....	46
6.2.10. Đánh giá thiết bị mật mã .....	46
6.3. Các vấn đề liên quan đến việc quản lý cặp khóa .....	47
6.3.1. Lưu trữ khóa công khai .....	47
6.3.2. Thời gian chứng thư số và cặp khóa hoạt động.....	47
6.4. Kích hoạt dữ liệu.....	47
6.4.1. Sinh và triển khai dữ liệu kích hoạt.....	47
6.4.2. Bảo vệ dữ liệu kích hoạt.....	47
6.4.3. Các vấn đề khác của dữ liệu kích hoạt .....	48
6.4.3.1. Gửi dữ liệu kích hoạt.....	48
6.4.3.2. Hủy dữ liệu kích hoạt .....	48
6.5. Kiểm soát an ninh quy trình sử dụng .....	48
6.5.1. Yêu cầu kỹ thuật về an toàn hệ thống máy tính .....	48
6.5.2. Đánh giá an toàn.....	48
6.6. Kiểm soát an ninh quy trình sử dụng .....	49
6.6.1. Điều khiển quy trình phát triển hệ thống.....	49
6.6.2. Điều kiện về môi trường sử dụng dịch vụ.....	49
6.6.3. Cơ chế ủy quyền xác thực người dùng.....	49
6.6.4. Kiểm soát việc quản lý an toàn, an ninh .....	49
6.7. Giám sát an ninh hệ thống mạng.....	49
6.8. Dấu thời gian (Time-Stamping).....	50
<b>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) .....</b>	<b>50</b>
7.1. Định dạng chứng thư số .....	50
7.1.1. Số hiệu phiên bản .....	50
7.1.2. Các thành phần mở rộng.....	50
7.1.3. Số hiệu thuật toán .....	51
7.1.4. Định dạng tên .....	51
7.1.5. Các ràng buộc về tên .....	51
7.1.6. Số hiệu của quy chế chứng thực.....	51
7.1.7. Sử dụng các ràng buộc quy chế mở rộng .....	51
7.1.8. Cú pháp và ngữ nghĩa quy chế .....	51
7.1.9. Xử lý ngữ nghĩa các quy chế chứng thư số mở rộng.....	51



7.2. Định dạng danh sách thu hồi chứng thư số (CRL) .....	51
7.2.1. Số hiệu phiên bản của CRL.....	52
7.2.2. CRL và các mở rộng .....	52
7.3. Định dạng giao thức kiểm tra trạng thái chứng thư số trực tuyến (OCSP).....	52
7.3.1. Số hiệu phiên bản của OCSP.....	53
7.3.2. Các mở rộng OCSP .....	53
8. KIỂM ĐỊNH TÍNH TUÂN THỦ VÀ CÁC ĐÁNH GIÁ KHÁC .....	53
8.1. Tần suất và các tình huống kiểm tra kỹ thuật .....	53
8.2. Đơn vị, người thực hiện kiểm tra kỹ thuật.....	53
8.3. Các nội dung kiểm tra kỹ thuật .....	53
8.4. Xử lý khi phát hiện sai sót .....	53
8.5. Công bố kết quả kiểm tra kỹ thuật .....	53
<b>8.6. Tần suất và các trường hợp đánh giá.....</b>	<b>54</b>
<b>8.7. Danh tính và khả năng của đơn vị, người kiểm tra .....</b>	<b>54</b>
9. CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC .....	54
9.1. Phí/Giá .....	54
9.1.1. Lệ phí cấp hoặc gia hạn chứng thư số số .....	54
9.1.2. Lệ phí sử dụng chứng thư số .....	54
9.1.3. Lệ phí thu hồi hoặc kiểm tra trạng thái chứng thư số.....	54
9.1.4. Lệ phí sử dụng cho các dịch vụ khác .....	54
9.1.5. Quy chế hoàn trả phí .....	54
9.2. Trách nhiệm tài chính .....	54
9.2.1. Phạm vi bảo hiểm.....	54
<b>9.2.2. Các tài sản khác.....</b>	<b>55</b>
9.3. Bảo mật các thông tin nghiệp vụ.....	55
9.3.1. Phạm vi của bảo mật thông tin .....	55
9.3.2. Thông tin không thuộc phạm vi của quá trình đảm bảo tính mật.....	56
9.3.3. Trách nhiệm bảo vệ thông tin mật.....	56
9.4. Bảo mật thông tin cá nhân .....	56
9.4.1. Chính sách đảm bảo tính riêng tư.....	56
9.4.2. Những thông tin coi là riêng tư .....	56
9.4.3. Thông tin không được coi là riêng tư .....	56
9.4.4. Trách nhiệm bảo vệ thông tin riêng tư .....	56
9.4.5. Thông báo và cho phép sử dụng thông tin riêng tư.....	57
9.4.6. Cung cấp thông tin riêng tư theo yêu cầu của luật pháp hay cho quá trình quản trị .....	57

9.4.7. Các trường hợp làm lộ thông tin khác .....	57
9.5. Quyền sở hữu trí tuệ.....	57
9.6. Tuyên bố và cam kết .....	58
9.6.1. Cam kết và đảm bảo của CA .....	58
9.6.2. Cam kết và đảm bảo của RA .....	58
9.6.3. Cam kết vào đảm bảo của Thuê bao .....	58
9.6.4. Đại diện cho người nhận và vấn đề bảo lãnh .....	59
9.6.5. Đại diện cho các bên liên quan khác và vấn đề bảo lãnh .....	59
9.7. Từ chối trách nhiệm .....	59
9.8. Giới hạn trách nhiệm.....	59
9.9. Bồi thường thiệt hại .....	59
9.10. Hiệu lực của Quy chế chứng thực.....	60
9.10.1. Thời hạn .....	60
9.10.2. Kết thúc .....	60
9.10.3 Kết quả của kết thúc hiệu lực và các tồn tại .....	60
9.11. Thông báo cho các bên liên quan .....	61
9.12. Bổ sung và sửa đổi .....	61
9.12.1. Thủ tục sửa đổi .....	61
9.12.2. Cơ chế và thời gian thông báo.....	61
9.12.3. Các trường hợp OID thay đổi.....	61
9.13. Thủ tục giải quyết tranh chấp.....	61
9.14. Hệ thống pháp lý điều chỉnh .....	61
9.15. Phù hợp với pháp luật hiện hành.....	62
9.16. Các điều khoản chung .....	62
9.16.1. Điều khoản thỏa thuận chung.....	62
9.16.2. Tính độc lập của các điều khoản .....	62
9.16.3. Sự thực thi (quyền ủy nhiệm và quyền khước từ).....	62
9.16.4. Chính sách bắt buộc thực thi .....	62
9.17. Các điều khoản khác .....	62

## 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 SmartCA trong quá trình cung cấp dịch vụ chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa. 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 SmartCA. Các yêu cầu của CPS đảm bảo tính bảo mật và toàn vẹn cho dịch vụ VNPT SmartCA, được áp dụng cho tất cả các thành phần tham gia dịch vụ chứng thực chữ ký số VNPT SmartCA. Bản CPS này không phải thỏa thuận về mặt luật pháp giữa VNPT SmartCA và các thực thể sử dụng dịch vụ chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa.

Mục tiêu của văn bản này là:

- Nhà cung cấp dịch vụ VNPT SmartCA hoạt động với quy chế chứng thực chữ ký số theo mô hình ký số từ xa và tuân thủ theo các yêu cầu trong bản CPS này.
- Cung cấp cho khách hàng sử dụng dịch vụ VNPT SmartCA 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 SmartCA cung 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. GIỚI THIỆU

## 1.1. Tổng quan

VNPT SmartCA là tên gọi của dịch vụ chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa do Tập đoàn Bưu chính Viễn thông Việt Nam cung cấp. Các quy định về chính sách chứng thư số của dịch vụ VNPT SmartCA 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, quy định sử dụng dịch vụ chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa.

## 1.2. Tên và dấu hiệu 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 SmartCA trong quá trình cung cấp dịch vụ chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa. 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 SmartCA. Các yêu cầu của CPS đảm bảo tính bảo mật và toàn vẹn cho dịch vụ VNPT SmartCA, được áp dụng cho tất cả các thành phần tham gia dịch vụ chứng thực chữ ký số VNPT SmartCA. Bản CPS này không phải thỏa thuận về mặt luật pháp giữa VNPT SmartCA và các thực thể sử dụng dịch vụ chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa.

Mục tiêu của văn bản này là:

- Nhà cung cấp dịch vụ VNPT SmartCA hoạt động với quy chế chứng thực số và tuân thủ theo các yêu cầu trong bản CPS này.
- Cung cấp cho khách hàng sử dụng dịch vụ VNPT SmartCA 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 SmartCA cung 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 SmartCA.

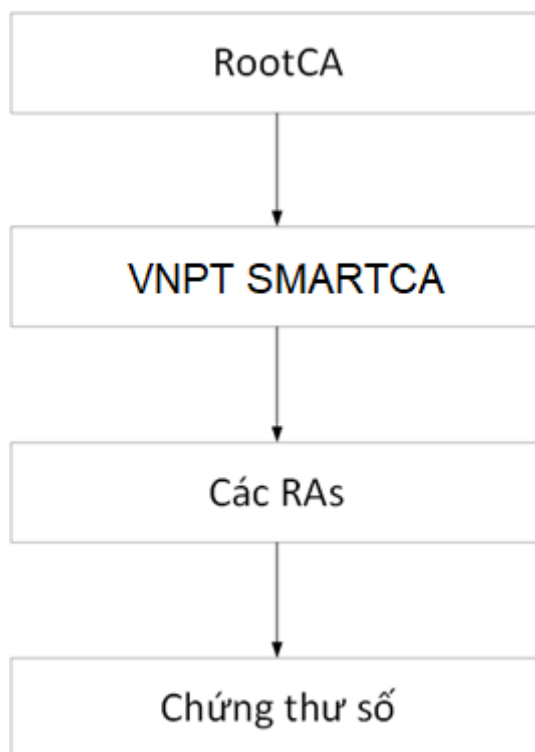
### 1.3.1. Thành phần Certification Authorities (CA)

Cấu trúc tổng quan dịch vụ VNPT SmartCA được trình bày ở sơ đồ dưới. Tại đỉnh của sự phân cấp chính là RootCA, đơn vị cấp phép cho VNPT SmartCA trở thành nhà cung cấp dịch

vụ chứng thực chữ ký số theo mô hình ký số từ xa. 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 SmartCA 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 SmartCA. Các RA của dịch vụ VNPT SmartCA 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 SmartCA hoặc qua các đơn vị RA quản lý.



#### **Quyền của VNPT SmartCA:**

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

#### **CA có nghĩa vụ sau:**

- Không được cấp chứng thư số với thông tin sai lệch so với thực tế.
- Đảm bảo cho chứng thư số của người sử dụng đầu cuối đạt tiêu chuẩn theo CPS.
- Đảm bảo nơi lưu trữ chứng thư số 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 ký dịch vụ và khởi tạo thông tin thuê bao VNPT SmartCA.

#### ***Nghĩa vụ của RA:***

- Cung cấp các thông tin chính xác về dịch vụ VNPT SmartCA cho khách hàng.
- Nhận các đơn yêu cầu cung cấp chứng thư số của khách hàng theo quy chế CPS của VNPT SmartCA.
- Gửi các đơn yêu cầu cung cấp chứng thư số thư số lên VNPT SmartCA.
- Ký các giấy tờ và biên bản bàn giao giữa hai bên.
- Tiếp nhận các thông tin yêu cầu đã được xác thực từ AM tiến hành Tạo thông tin thuê bao

### **1.3.3. Thành phần Account Manager (AM)**

#### ***Quyền của AM:***

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

#### ***Nghĩa vụ của AM:***

- Nhận các đơn yêu cầu cung cấp chứng thư số thư số của khách hàng theo quy chế CPS của VNPT SmartCA.
- Kiểm tra các thông tin Hợp đồng, Phụ lục phiếu đề nghị cung cấp dịch vụ và hồ sơ thuê bao đối chiếu với giấy tờ gốc của thuê bao
- Ký các giấy tờ và biên bản bàn giao giữa hai bên.

### **1.3.4. Thuê bao**

#### **Quyền của thuê bao:**

- Chứng thư số được cấp 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;
- Thuê bao được sử dụng dịch vụ chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa theo hiệu lực của gói cước quy định trong hợp đồng cung cấp dịch vụ.
- Thuê bao có quyền yêu cầu gia hạn, thu hồi chứng thư số của mình.
- Thuê bao có quyền xác nhận thông qua thiết bị đã được đăng ký đối với tất cả các hành động liên quan tới khóa bí mật của mình.

- Thuê bao có quyền gia hạn, tạm dừng hoặc hủy bỏ dịch vụ chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa.

#### **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.
- Không được giả mạo chứng thư số của VNPT.
- Nếu có bất kỳ sự thay đổi thông tin nào, đều phải thông báo tới đầu mối tiếp nhận của dịch vụ VNPT SmartCA.
- 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.

#### **1.3.5. 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 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 căn cứ 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 SmartCA về các điều kiện hợp tác đối với bên thứ 3.
- Chỉ tin tưởng chứng thư số do VNPT SmartCA 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.
- Chỉ tin tưởng ứng dụng VNPT SmartCA trên thiết bị di động do VNPT SmartCA cung cấp, được thông báo trên trang web chính thức của dịch vụ VNPT SmartCA
- Phải thông báo ngay cho RA nếu nghi ngờ rằng khóa bí mật bị lộ, mất cắp hay sửa đổi, phá hủy;

- Phải thông báo ngay cho RA nếu nghi ngờ ứng dụng VNPT SmartCA trên điện thoại có dấu hiệu bị sai lệch, sao chép hoặc mã PIN bị lộ.

### **1.3.6. Thành phần khác**

Ứng dụng VNPT SmartCA trên thiết bị di động.

Ứng dụng VNPT SmartCA là ứng dụng di động giúp người dùng kiểm soát tất cả các hành động liên quan tới khóa bí mật.

Ứng dụng VNPT SmartCA hỗ trợ hai nền tảng di động:

- iOS, version: 10.0 trở lên;

- Android, version: 5.0.0 trở lên.

Yêu cầu thiết bị: không hỗ trợ các thiết bị di động đã bị can thiệp, chỉnh sửa nhằm loại bỏ các hạn chế mà nhà sản xuất đã cài đặt (các hành vi này còn được gọi là root/jaibreak).

Đối với các thiết bị di động sử dụng hệ điều hành Android: bắt buộc phải có chứng chỉ Google Play Protect.

## **1.4. Mục đích 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 tài liệu CPS này

### **1.4.2. Chứng thư số không hợp pháp**

Không có

## **1.5. Quản lý cơ chế chứng thực**

### **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 (VNPT IT).

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

Và

Vinaphone

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



### 1.5.3. Đơn vị quyết định tính hợp pháp của CPS

Tài liệu 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 SmartCA chịu trách nhiệm trước pháp luật về tính hợp pháp của tài liệu CPS này.

### 1.5.4. Thủ tục phê duyệt CPS

VNPT IT là đơn vị có thẩm quyền phê duyệt CPS này và những thay đổi liên quan trong quá trình hoạt động của VNPT SmartCA. 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. Các định nghĩa và từ 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.
AM	Account Manager – Nhân sự làm đầu mối trong vấn đề liên quan đến hợp đồng với thuê bao.
PIN	Mã bí mật được sử dụng trên ứng dụng di động để xác nhận tất cả các hành động liên quan đến khóa bí mật, mã bí mật này do thuê bao đặt và chỉ thuê bao biết.

## 2. TRÁCH NHIỆM LƯU TRỮ VÀ CÔNG BỐ THÔNG TIN

### 2.1. Lưu trữ

VNPT SmartCA 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 SmartCA thực hiện bởi các server chức năng: CRL, LDAP, OCSP. Các máy chủ này được VNPT SmartCA xây dựng nằm trong phân vùng mạng công cộng có băng thông rộng, nằm trong Data Center của VNPT với đường truyền internet ổn định, tốc độ cao, điều kiện môi trường, nguồn điện ổn định và 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.

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 tạm ngưng. Hệ thống cung cấp dịch vụ VNPT SmartCA lưu trữ và tự động cập nhật định kỳ liên tục các thông tin về danh sách 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.

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**

Hệ thống VNPT SmartCA 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 SmartCA có thể truy cập lấy thông tin chứng thư số và kiểm tra trạng thái của chứng thư số.

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, tần suất công bố thông tin**

Quy chế chứng thực và chứng thư số của nhà cung cấp dịch vụ VNPT SmartCA được công bố và cập nhật khi có sự thay đổi tại địa chỉ <https://vnpt-ca.vn/download-page>.

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 (validity) 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. Kiểm soát việc truy cập thông tin

Mọi thay đổi của CPS và chứng thư số của nhà cung cấp dịch vụ VNPT SmartCA chỉ được phép thực hiện bởi cấp có thẩm quyền của VNPT.

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

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. NHẬN DẠNG VÀ XÁC THỰC YÊU CẦU XIN CẤP CHỨNG THƯ SỐ

### 3.1. Đặt tên trong chứng thư số

#### 3.1.1. Các thuộc tính

Các chứng thư của VNPT SmartCA tuân theo chuẩn ITU-T X.509 và các quy định trong RFC5280: Internet X.509 Public Key Infrastructure 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: SHA256, 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 thư 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 SmartCA sẽ là duy nhất gắn với một cặp chứng thư số xác định trong miền của dịch vụ VNPT SmartCA. 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 SmartCA 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 SmartCA 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 SmartCA có quyền chấm dứt hoặc tạm dừng bất cứ chứng thư số nào liên quan đến các tranh chấp đã nêu.

## **3.2. Xác minh đề nghị cấp chứng thư số**

### **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 SmartCA 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 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.

### **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 minh đề nghị thay đổi cặp khóa

Thuê bao muốn thay đổi cặp khóa phải đưa ra hợp đồng đăng ký sử dụng chứng thư số đã ký nhằm chứng 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 người sử dụng chứng thư.

#### **Đối với cá nhân**

- Địa chỉ.
- Bản sao hợp lệ CMND/CCCD hoặc hộ chiếu.

### 3.4. Xác minh đề nghị thu hồi chứng thư số

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

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

- VNPT SmartCA 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 SmartCA hoặc RA có lý do 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 SmartCA 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 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 SmartCA.

Khi xem xét việc sử dụng chứng thư số có gây nguy hại cho VNPT SmartCA hay không, VNPT SmartCA 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 SmartCA có thể thu hồi chứng thư số quản trị nếu thẩm quyền của người quản trị kết thúc.

Thỏa thuận giữa VNPT SmartCA và thuê bao yêu cầu thuê bao này phải thông báo kịp thời cho VNPT SmartCA về nguy cơ bị lộ khóa bí mật của chứng thư số của thuê bao, lộ mã PIN, ứng dụng VNPT SmartCA trên thiết bị di động có dấu hiệu bị làm sai lệch thông tin hoặc bị sao chép.

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

### **4.1. Yêu cầu 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 cấp phát theo sự chấp thuận đơn xin chứng thư số của VNPT SmartCA hoặc nhận được yêu cầu của RA để ban hành giấy chứng thư số. VNPT SmartCA cấp phát 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 điểm giao dịch của VNPT SmartCA, 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 SmartCA ban hành. Sau đó chuyển lại cho RA và chờ thông tin xác thực phản hồi.

Các RA tiến 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 yêu cầu cấp chứng thư số**

### **4.2.1. Xác thực định danh**

VNPT SmartCA 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**

VNPT SmartCA 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 và dịch vụ chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa cho VNPT SmartCA.

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

### **4.2.3. Thời gian xử lý yêu cầu**

VNPT SmartCA 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 SmartCA từ chối.



### **4.3. Phát hành chứng thư số**

#### **4.3.1. Hoạt động CA trong 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. VNPT SmartCA 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 SmartCA sẽ trực tiếp 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 số**

Khi thuê bao hoàn thành việc kích hoạt dịch vụ trên ứng dụng di động và được cấp chứng thư số, thuê bao cần ký xác nhận các thủ tục hoàn thành cấp chứng thư số và khởi tạo dịch vụ chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa.

#### **4.4.2. Công bố chứng thư số**

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

Khi thuê bao kích hoạt dịch vụ thành công trên ứng dụng di động, 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 SmartCA sẽ trực tiếp 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 hoặc hết hạn gói cước dịch vụ chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa được quy định trong hợp đồng cung cấp dịch vụ.

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 Signing
Criticality		TRUE	FALSE	FALSE	FALSE
0	digitalSignature	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

Thuê bao kiểm soát mọi hành động liên quan tới khóa bí mật, bao gồm: sinh khóa bí mật, sinh yêu cầu cấp chứng thư số, ký số.

Thuê bao sử dụng ứng dụng VNPT SmartCA trên thiết bị di động để xác thực việc sử dụng khóa bí mật

Thuê bao tiến hành ký số bằng việc xác nhận mã PIN trên thiết bị di động đã đăng ký.

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

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

- VNPT SmartCA 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 SmartCA 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 số**

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 SmartCA 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 SmartCA 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 SmartCA ban hành. VNPT SmartCA 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 SmartCA có trách nhiệm thông báo cho thuê bao về việc gia hạn chứng thư số.

#### **4.7.5. Điều khoản chấp nhận thay khóa chứng thư số**

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 SmartCA 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 số**

VNPT SmartCA có trách nhiệm thông báo cho AM về việc thay đổi khóa của thuê bao do họ xác thực định danh.

### **4.8. Hủy cặp khóa**

*Các trường hợp khóa của thuê bao bị hủy:*

- Thuê bao gửi yêu cầu hủy khóa.
- 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.

#### ***Thủ tục hủy khóa***

Dịch vụ VNPT SmartCA sẽ tiến hành chuyển trạng thái của thuê bao trên hệ thống sang trạng thái không hoạt động và tiến hành hủy khóa và gửi thông báo tới thuê bao một cách tự động trong trường hợp:

- 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.

Trường hợp thuê bao gửi yêu cầu hủy khóa, VNPT SmartCA sẽ thực hiện thủ tục sau:

#### **Thuê bao:**

- Gửi đơn yêu cầu hủy khóa tới nhà cung cấp dịch vụ với chữ ký hoặc con dấu hợp pháp của chủ thể.

#### **AM:**

- Tiến hành xác minh và xác thực chính xác thông tin yêu cầu hủy khóa từ phía đối tượng gửi đơn hủy khóa.

- Trường hợp thông tin không đủ hợp lệ, AM 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, AM gửi báo cáo thông tin xác thực kèm theo đề nghị thu hủy khóa tới RA làm cơ sở thực hiện yêu cầu.

#### **RA:**

- Thực hiện gửi yêu cầu hủy khóa của thuê bao tới VNPT SmartCA.

#### **VNPT SmartCA:**

- VNPT SmartCA xác thực RA và các thông tin RA gửi, nếu hợp lệ, VNPT SmartCA sẽ tiến hành hủy khóa của thuê bao.

- VNPT SmartCA trách nhiệm cập nhật thông tin trên cơ sở dữ liệu về việc hủy khóa của thuê bao.

- VNPT SmartCA gửi thông báo về việc hủy khóa trực tiếp cho thuê bao hoặc thông qua RA quản lý trực tiếp.

### **4.9. Thay đổi chứng thư số**

#### **4.9.1. 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 thông tin đã đăng ký sử dụng chứng thư số gốc theo quy định trong phần 3.2.

#### **4.9.2. Đối tượng được phép yêu cầu chứng thư số**

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 chứng thư số.

#### **4.9.3. Xử lý yêu cầu thay đổi chứng thư số**

AM tiến hành xác thực thông tin của thuê bao trong yêu cầu thay đổi chứng thư số theo phần 3.2. Nếu thông tin xác thực, AM chuyển thông tin lên hệ thống để RA thực hiện việc Khởi tạo yêu cầu thay đổi chứng thư số. Nếu thông tin sai lệch, yêu cầu bị từ chối.

#### **4.9.4. Thông báo cho thuê bao về việc thay khóa chứng thư số**

VNPT SmartCA có trách nhiệm thông báo cho AM về việc thay đổi chứng thư số do họ xác thực định danh.

#### **4.9.5. Điều khoản chấp nhận thay khóa chứng thư số**

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

#### **4.9.6. Công bố chứng thư số đã thay đổi**

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

#### **4.9.7. Thông báo đến các đối tượng khác về việc thay khóa chứng thư số**

VNPT SmartCA có trách nhiệm thông báo cho AM về việc thay đổi chứng thư số do họ xác thực định danh.

#### **4.10. Tạm dừng và Thu hồi chứng thư số**

##### **4.10.1. 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 SmartCA thu hồi và được công bố trên CRL.

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

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

- VNPT SmartCA hoặc RA hoặc AM có lý do 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 SmartCA hoặc AM 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 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 SmartCA.

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

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

- Xác nhận người khiếu nại.

- Cường chế theo luật.

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

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

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

#### **4.10.2. 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.

#### **4.10.3. Thủ tục yêu cầu thu hồi**

##### **Thuê bao:**

- 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.

##### **AM:**

- 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, AM 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, AM gửi báo cáo thông tin xác thực kèm theo đề nghị thu hồi chứng thư tới RA làm có cơ sở thực hiện yêu cầu.

##### **RA:**

- Thực hiện gửi yêu cầu Ngừng chứng thư số tới VNPT SmartCA

##### **VNPT SmartCA:**

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

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

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

#### **4.10.4. 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.

#### **4.10.5. 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.

#### **4.10.6. Yêu cầu kiểm tra thu hồi cho người nhận**

Kiểm tra trạng thái chứng thư số tại các địa chỉ: với đường dẫn OCSP là <http://ocsp-sha256.vnpt-ca.vn/responder> và CRL là <http://crl-sha256.vnpt-ca.vn/vnptca-sha256.crl>.



#### **4.10.7. 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.

#### **4.10.8. Thời gian trễ lớn nhất của CRL**

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

#### **4.10.9. 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: với đường dẫn OCSP là <http://ocsp-sha256.vnpt-ca.vn/responder> và CRL là <http://crl-sha256.vnpt-ca.vn/vnptca-sha256.crl>.

#### **4.10.10. 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.

#### **4.10.11. Mẫu quảng bá chứng thư số bị thu hồi khác**

Không có

#### **4.10.12. Các điều kiện đặc biệt khi khóa bị xâm phạm**

VNPT SmartCA 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 SmartCA bị xâm phạm.

#### **4.10.13. Các trường hợp tạm dừng**

Không có quy định

#### **4.10.14. Đối tượng được phép yêu cầu tạm dừng**

Không có quy định.

#### **4.10.15. Thủ tục yêu cầu tạm dừng**

Không có quy định.

#### **4.10.16. Giới hạn thời gian tạm dừng**

Không có quy định.

### **4.11. Dịch vụ kiểm tra trạng thái chứng thư số**

#### **4.11.1. Đặc tính hoạt động**

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

#### **4.11.2. Tính sẵn sàng của dịch vụ**

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

#### **4.11.3. Các đặc tính tùy chọn**

Không có quy định

#### **4.12. Chấm dứt dịch vụ của thuê bao**

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

- Thuê bao gửi yêu cầu chấm dứt dịch vụ.
- 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.

#### ***Thủ tục chấm dứt dịch vụ***

Dịch vụ VNPT SmartCA sẽ tiến hành chuyển trạng thái của thuê bao trên hệ thống sang trạng thái không hoạt động và gửi thông báo tới thuê bao một cách tự động trong trường hợp:

- 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.

Trường hợp thuê bao gửi yêu cầu chấm dứt dịch vụ, VNPT SmartCA sẽ thực hiện thủ tục sau:

#### **Thuê bao:**

- Gửi đơn yêu cầu chấm dứt dịch vụ tới nhà cung cấp dịch vụ với chữ ký hoặc con dấu hợp pháp của chủ thể.

#### **AM:**

- Tiến hành xác minh và xác thực chính xác thông tin yêu cầu chấm dứt dịch vụ từ phía đối tượng gửi đơn.

- Trường hợp thông tin không đủ hợp lệ, AM 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, AM gửi báo cáo thông tin xác thực kèm theo đề nghị chấm dứt dịch vụ của thuê bao tới RA làm cơ sở thực hiện yêu cầu.

#### **RA:**

- Thực hiện gửi yêu cầu chấm dứt dịch vụ của thuê bao tới VNPT SmartCA.

#### **VNPT SmartCA:**

- VNPT SmartCA xác thực RA và các thông tin RA gửi, nếu hợp lệ, VNPT SmartCA sẽ tiến hành chấm dứt dịch vụ của thuê bao.

- VNPT SmartCA trách nhiệm cập nhật thông tin trên cơ sở dữ liệu về việc chấm dứt hoạt động của thuê bao.

- VNPT SmartCA gửi thông báo về việc chấm dứt dịch vụ trực tiếp cho thuê bao hoặc thông qua RA quản lý trực tiếp.

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

Không cung cấp.

### **5. KIỂM SOÁT, QUẢN LÝ VÀ VẬN HÀNH**

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

##### **5.1.1 Vị trí xây dựng**

Hoạt động của VNPT SmartCA và 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 giấu.

VNPT SmartCA cũng 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. Kiểm soát an toàn, an ninh vật lý**

Đơn vị chủ quản dịch vụ chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa VNPT SmartCA 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, căn cước công 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 chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa được kiểm soát bởi hệ thống 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 SmartCA 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 SmartCA 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 SmartCA 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 SmartCA 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 SmartCA 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 khi 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 SmartCA được đặt tại IDC Nam Thăng Long, Hà Nội.

Hệ thống dự phòng (back up) cho dịch vụ VNPT SmartCA cũng được xây dựng về mặt chức năng giống 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. Quy trình kiểm soát**

### **5.2.1. Vai trò tin cậy**

Nhân viên đều phải được xem xét trước khi trở thành người tin cậy làm việc tại vị trí được tin cậy của VNPT SmartCA. Những người được chọn là người tin cậy làm việc tại vị trí tin cậy đáp ứng yêu cầu của VNPT SmartCA. 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 chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa.
- Ban hành, thu hồi quyền truy cập tới các phân 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 SmartCA đã 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 SmartCA đảm 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 CNTT khác.

#### **5.2.4. Phân chia trách nhiệm giữa các vị trí**

Những vai trò yêu cầu phân chia trách nhiệm bao gồm nhưng không 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 SmartCA 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 SmartCA 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 SmartCA 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 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 SmartCA 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 SmartCA 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 SmartCA 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 SmartCA.
- 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 SmartCA 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 SmartCA 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 SmartCA. 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 SmartCA 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 SmartCA trong phạm vi quyền hạn của họ.

### **5.3.8. Cung cấp tài liệu cho nhân viên**

VNPT SmartCA 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. Các quy trình ghi nhật ký hệ thống**

### **5.4.1. Các sự kiện VNPT SmartCA cần ghi nhận**

Các sự kiện có thể kiểm định phải được ghi lại bởi VNPT SmartCA 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 SmartCA 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 chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa do thuê bao thông báo hoặc do VNPT phát 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 SmartCA 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 bản 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 SmartCA sẽ thực hiện thao tác kiểm tra thủ công.

### **5.5. Lưu trữ các bản ghi**

#### **5.5.1. Các loại hồ sơ cần lưu trữ**

VNPT SmartCA 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 SmartCA 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 SmartCA 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**

Chứng thư số của VNPT SmartCA 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 SmartCA 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 SmartCA hết hạn, VNPT SmartCA sẽ tiến hành quy trình gia hạn nhằm đảm bảo hệ thống hoạt động thông suốt. VNPT SmartCA sẽ xin gia hạn chứng thư số từ NEAC không chậm hơn 90 ngày trước thời điểm hết hạn.

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

### **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.

Trường hợp thuê bao đang thực hiện giao dịch có xảy ra sự cố liên quan đến thiết bị như hỏng, cháy nổ, thiên tai, ... khiến giao dịch không thể thực hiện thì giao dịch đó gọi là lỗi và thuê bao phải thực hiện lại giao dịch khi hệ thống hoạt động bình thường.

Trường hợp thuê bao đang thực hiện giao dịch có xảy ra sự cố phần mềm, dữ liệu thì trách nhiệm giữa VNPT và Thuê bao được áp dụng thực thi căn cứ trong các điều khoản quy định trong hợp đồng giữa VNPT và thuê bao.

### **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 SmartCA, đơn vị xử lý sự cố của VNPT SmartCA (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 SmartCA chấp thuận. Nếu chứng thư số của VNPT SmartCA bị thu hồi, các thủ tục sau cần thực hiện:

- Trạng thái thu hồi chứng thư số của VNPT SmartCA 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 SmartCA xây dựng hệ thống dự phòng cách vị trí hệ thống chính thức tối thiểu 10 km. VNPT SmartCA 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 SmartCA (VNPT SmartCA Emergency Response Team) có nhiệm vụ thực hiện quy trình phục hồi sau sự cố. VNPT SmartCA 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 SmartCA 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 SmartCA được sao lưu vào bảo quản cho nhiệm vụ phục hồi sau thảm họa theo quy định ở phần 6.2.4.

## **5.8. Dừng hoạt động**

VNPT SmartCA sẽ thông báo khi VNPT SmartCA 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 SmartCA 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 SmartCA 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 SmartCA.
- Tiếp tục duy trì hệ thống lưu trữ các thông tin của VNPT SmartCA 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 SmartCA và các thiết bị token chứa khóa bí mật
- Chuyển giao dịch vụ VNPT SmartCA cho đơn vị khác nếu có

## **6. ĐẢM BẢO AN TOÀN AN NINH VỀ KỸ THUẬT**

### **6.1. Tạo và phân phối cặp khóa**

#### **6.1.1. Sinh cặp khóa**

Việc sinh cặp khóa của nhà cung cấp dịch vụ chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa 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 ngẫu 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 SmartCA tuân theo chuẩn PKCS #1 phiên bản 2.1, đáp ứng theo tiêu chuẩn trong Thông tư số 16/2019/TT-BTTTT của Bộ Thông tin và Truyền thông ban hành ngày 05 tháng 12 năm 2019.

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

Cặp khóa của thuê bao sẽ được sinh phía VNPT SmartCA và được lưu trữ trên thiết bị HSM.

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

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

Thuê bao gửi khóa công khai tới VNPT SmartCA 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 SmartCA yêu cầu thuê bao phải tải và cài đặt khóa công khai của VNPT SmartCA. Khóa công khai của VNPT SmartCA 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 SmartCA 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.

## **6.2. Kiểm soát và bảo vệ khóa bí mật**

### **6.2.1. Các chuẩn thiết bị mật mã an toàn**

VNPT SmartCA 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 EN 419221-5:2018.

### **6.2.2. Đa kiểm soát khóa bí mật**

Cơ chế kiểm soát khóa bí mật của VNPT SmartCA 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 lon hơn 1 (m) mảnh khóa ( $m \leq n$ ). Tại VNPT SmartCA, áp dụng  $m \geq 2$ .

### **6.2.3. Ủy thác giữ khóa bí mật**

Khóa bí mật của VNPT SmartCA 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 SmartCA được sao lưu dự phòng trên thiết bị phân 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 SmartCA 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 SmartCA 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 SmartCA 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 SmartCA 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 SmartCA cần phải được hủy, VNPT SmartCA 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 SmartCA, 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 SmartCA 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. Kích hoạt dữ liệu**

#### **6.4.1. Sinh và triển khai dữ liệu kích hoạt**

VNPT SmartCA 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 SmartCA khuyến cáo thuê bao tuân theo các yêu cầu trên. Ngoài ra để tăng cường an toàn, VNPT SmartCA khuyến khích sử dụng các cơ chế đa xác thực (token và passphrase, sinh trắc và token, sinh trắc và passphrase) 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– KYSO 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 SmartCA 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. Kiểm soát an ninh quy trình sử dụng**

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

Hệ thống mạng của VNPT SmartCA 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 SmartCA 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 SmartCA 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 SmartCA 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 SmartCA 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.

Module ký số của VNPT SmartCA đạt chứng chỉ đáp ứng tiêu chuẩn EN 419 241-2:2019 và ISO 15408.

VNPT SmartCA tuân theo các tiêu chuẩn eIDAS về “Tiêu chuẩn hệ thống thiết bị quản lý khóa bí mật, chứng thư số và tạo chữ ký số của khách hàng” được quy định tại phục lục “DANH MỤC TIÊU CHUẨN BẮT BUỘC ÁP DỤNG VỀ CHỮ KÝ SỐ VÀ DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ THEO MÔ HÌNH KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG VÀ KÝ SỐ TỪ XA” trong thông tư 16/2019/TT-BTTTT.



## **6.6. Kiểm soát an ninh quy trình sử dụng**

### **6.6.1. Điều khiển quy trình phát triển hệ thống**

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

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

### **6.6.2. Điều kiện về môi trường sử dụng dịch vụ**

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

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

VNPT SmartCA cung cấp API tích hợp đối với ứng dụng của bên thứ 3, không phụ thuộc vào các nền tảng ứng dụng.

VNPT SmartCA cung cấp ứng dụng di động cho thuê bao kiểm soát hoạt động của khóa bí mật.

Thiết bị di động của thuê bao cài đặt ứng dụng VNPT SmartCA, sẽ được VNPT SmartCA định danh và gắn với thuê bao;

VNPT SmartCA chỉ hỗ trợ thuê bao cài đặt ứng dụng VNPT SmartCA trên một thiết bị di động duy nhất cho một chứng thư số trong vòng đời chứng thư số.

Thuê bao có nhu cầu thay đổi thiết bị sẽ cần thực hiện yêu cầu thay đổi cặp khóa tại mục 4.7.

### **6.6.3. Cơ chế ủy quyền xác thực người dùng**

Dịch vụ không hỗ trợ cơ chế ủy quyền xác thực giữa thuê bao này và thuê bao khác khi thực hiện các giao dịch cần sự xác thực của người dùng.

### **6.6.4. Kiểm soát việc quản lý an toàn, an ninh**

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

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

## **6.7. Giám sát an ninh hệ thống mạng**

Đối với các trao đổi thông tin giữa VNPT SmartCA và RA được thực hiện qua môi trường mạng, VNPT SmartCA 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. Dấu thời gian (Time-Stamping)

Không cung cấp.

## 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 chứng thư số

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

<i>Trường</i>	<i>Giá trị hoặc yêu cầu</i>
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 SmartCA và được kiểm soát theo quy tắc đặt giá trị serial number do VNPT SmartCA 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 SmartCA 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 SmartCA 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– KYSO 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}

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

CRL cần chứa các giá trị sau đây

<i>Trường</i>	<i>Giá trị hoặc yêu cầu</i>
Version	Xem phần 7.2.1
Signature Algorithm	Thuật toán dùng để ký danh sách chứng thư số bị thu hồi. VNPT SmartCA 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 SmartCA 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. Định dạng giao thức kiểm tra trạng thái chứng thư số trực tuyến (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 SmartCA 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 KHÁC**

### **8.1. Tần suất và các tình huống kiểm tra kỹ thuật**

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 SmartCA.

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

Đơn vị kiểm định thực hiện kiểm tra VNPT SmartCA 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 kỹ thuật an toàn thông tin.
- Được chứng nhận bởi RootCA.

### **8.3. Các nội dung kiểm tra kỹ thuật**

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

### **8.4. Xử lý khi phát hiện sai 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 SmartCA. Nếu các vấn đề này ảnh hưởng nghiêm trọng tới tính an toàn và toàn vẹn của VNPT SmartCA, bộ phận quản lý VNPT SmartCA 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 SmartCA sẽ lượng giá mức độ và xác định các hành động cần thực hiện.

Đối với các sự cố nghiêm trọng, bộ phận quản lý VNPT SmartCA sẽ báo cáo đầy đủ nội dung nguyên nhân, cách khắc phục và mức độ ảnh hưởng với Trung tâm Chứng thực điện tử Quốc gia (NEAC) trong vòng 48h.

### **8.5. Công bố kết quả kiểm tra kỹ thuật**

Kết quả kiểm định hệ thống VNPT SmartCA được công bố trên website của

VNPT SmartCA.

## **8.6. Tần suất và các trường hợp đánh giá**

Đánh giá kiểm tra được thực hiện ít nhất định kỳ hàng năm hoặc theo thời hạn chứng chỉ của các thành phần hệ thống bởi đơn vị kiểm định đáp ứng yêu cầu theo quy định của pháp luật và yêu cầu của VNPT SmartCA.

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

Đơn vị kiểm tra VNPT SmartCA 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 kỹ thuật an toàn thông tin.

- Được chứng nhận bởi RootCA.

# **9. CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC**

## **9.1. Phí/Giá**

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

Các thuê bao sử dụng dịch vụ VNPT SmartCA 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 SmartCA 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**

VNPT SmartCA không thu phí truy cập CPS này. Việc xem văn bản với các mục đích như sao chép, phân bổ lại sẽ phải được sự chấp thuận bằng văn bản của VNPT SmartCA.

### **9.1.5. Quy chế hoàn trả phí**

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

- Lỗi do VNPT SmartCA gây ra, bao gồm lỗi kỹ thuật khi phát hành chứng thư theo trách nhiệm của CA.

- VNPT SmartCA đưa 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 SmartCA sẽ 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 thiết bị HSM, khi có lỗi xảy ra, hãng cung cấp thiết bị HSM sẽ chịu trách nhiệm đền bù cho khách hàng. Việc đền bù được thực hiện theo hợp đồng với thuê bao.

- 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 SmartCA 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 nghiệp vụ**

### **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 VNPT SmartCA, 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 SmartCA hoặc một thuê bao.
- Các báo cáo kiểm toán tạo bởi VNPT SmartCA 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 SmartCA cùng các thông tin chứa bên trong chứng 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 SmartCA đảm bảo các thông tin riêng tư không bị tiết lộ với bên thứ 3.

## **9.4. Bảo mật thông tin cá nhân**

### **9.4.1. Chính sách đảm bảo tính riêng tư**

VNPT SmartCA sẽ tiến hành triển khai chính sách đảm bảo tính riêng, tuân theo luật riêng tư. VNPT SmartCA 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 SmartCA, 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 trong 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 SmartCA 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 SmartCA chứ không phải giữa các thuê bao và các bên đối tác được không 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 SmartCA 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 SmartCA ban hành.

VNPT SmartCA 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 SmartCA 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 SmartCA chấp nhận rằng VNPT SmartCA 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. Tuyên bố và cam kết**

### **9.6.1. Cam kết và đảm bảo của CA**

VNPT SmartCA đảm bảo rằng:

- Không có những thông tin sai lệch 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 SmartCA đảm bảo:

- Không có những thông tin sai lệch 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.

- Mã PIN do thuê bao đặt là số có độ dài 6 ký tự là các chữ số. Mã PIN không thể thay đổi được.
- Thuê bao phải có trách nhiệm bảo vệ và không chia sẻ mã PIN.
- Không thể thay đổi mã PIN của thuê bao. Nếu trong trường hợp có nguy cơ người khác biết được mã PIN của thuê bao, thuê bao phải thông báo với nhà cung cấp dịch vụ yêu cầu kích hoạt lại và tạo mã PIN khác.

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 SmartCA 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 trách nhiệm**

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

#### **9.8. Giới hạn trách nhiệm**

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 thiệt hại**

##### **Vấn đề bồi thường của thuê bao sử dụng**

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

- Những thông tin sai lệch 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 sót hay làm sai lệch do sự cầu 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 bồi thường cho VNPT SmartCA 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. Hiệu lực của Quy chế chứng thực**

### **9.10.1. Thời hạn**

CPS này bắt đầu có hiệu lực khi hệ thống VNPT SmartCA 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 SmartCA.

### **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 SmartCA 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 SmartCA 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. Bổ sung và sửa đổi**

### **9.12.1. Thủ tục sửa đổi**

Những sửa đổi của CPS này sẽ được thực hiện bởi VNPT SmartCA. 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 SmartCA tại địa chỉ <https://www.vnpt-ca.vn/>

### **9.12.2. Cơ chế và thời gian thông báo**

VNPT SmartCA 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 SmartCA tại địa chỉ: <http://www.vnpt-ca.vn/>

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

Ngoài ra, nếu VNPT SmartCA cho rằng thay đổi CPS là cần thiết để ngăn chặn xâm phạm đến an toàn của dịch vụ VNPT SmartCA, 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 SmartCA 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. Thủ tục giải quyết tranh chấp**

### **Tranh chấp giữa VNPT, đối tác và thuê bao**

Việc giải quyết tranh chấp giữa VNPT SmartCA, 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. Hệ thống pháp lý điều chỉnh**

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 SmartCA cũng như giải quyết các tranh chấp phát sinh các thành phần tham gia dịch vụ VNPT SmartCA cũng như các bên liên quan sẽ áp dụng pháp luật của nước Cộng hòa xã hội chủ nghĩa Việt Nam.

#### **9.15. Phù hợp với pháp luật hiện hành**

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 điều khoản chung**

##### **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 SmartCA.

#### **9.17. Các điều khoản khác**

Không có quy định.