TẬP ĐOÀN BƯU CHÍNH VIỄN THÔNG VIỆT NAM
CÔNG TY CÔNG NGHỆ THÔNG TIN VNPT

QUY CHẾ CHỨNG THỰC

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

Hà Nội, năm 2025

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

Ngày hiệu lực:	04/08/2021
Lần ban hành:	01
Phiên bản:	2.0

	Họ và Tên	**Chức danh**	**Đơn vị**
Soạn thảo:	Nguyễn Đăng Huy	Tổ trưởng	Trung tâm eGOV – Công ty VNPT-IT
Kiểm tra:	Nguyễn Thanh Phong	PDM	Trung tâm eGOV– Công ty VNPT-IT
Thẩm định:	Nguyễn Thị Thành Chung	Chuyên quản SPDV	Ban Tiếp thị - Bán hàng – Công ty VNPT-IT

BẢNG THEO DÕI THAY ĐỔI TÀI LIỆU

Ngày sửa đổi	**Nội dung thay đổi**	**Ngày hiệu lực**	**Phê duyệt**
01/06/2021	Tạo mới	04/08/2021	04/08/2021
08/06/2022	Cập nhật nội dung	28/07/2022	28/07/2022

MỤC LỤC

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 18

2.1. Lưu trữ 18
2.2. Công bố thông tin 18
2.3. Thời gian, tần suất công bố thông tin 19
2.4. Kiểm soát việc truy cập thông tin 19

3. NHẬN DẠNG VÀ XÁC THỰC YÊU CẦU XIN CẤP CHỨNG THƯ SỐ 20

3.1. Đặt tên trong chứng thư số 20
3.1.1. Các thuộc tính 20
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 21
3.1.4. Quy tắc diễn giải các mẫu tên 21
3.1.5. Tính duy nhất của tên thuê bao 21
3.1.6. Nhận dạng, xác thực và vai trò của thương hiệu 21

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 22
3.2.4. Thông tin thuê bao không xác minh 22
3.2.5. Xác thực thẩm quyền 22
3.2.6. Các tiêu chuẩn thực hiện liên hoạt 22
3.3. Xác minh đề nghị thay đổi cặp khóa 23
3.4. Xác minh đề nghị thu hồi chưng thư số 23
4. CÁC QUY ĐỊNH VỀ VIỆC QUẢN LÝ VÒNG ĐỜI CỦA CHỨNG THƯ SỐ 24
4.1. Yêu cầu cấp chứng thư số 24
4.1.1. Đối tượng được phép yêu cầu cấp chứng thư số 24
4.1.2. Quy trình xử lý đơn xin cấp chứng thư số 24
4.2. Xử lý yêu cầu cấp chứng thư số 25
4.2.1. Xác thực định danh 25
4.2.2. Chấp nhận hoặc từ chối cấp chứng thư số 25
4.2.3. Thời gian xử lý yêu cầu 26
4.3. Phát hành chứng thư số 26
4.3.1. Hoạt động CA trong phát hành chứng thứ số 26
4.3.2. Thông báo tới thuê bao 26
4.4. Chứng nhận chứng thư số 26
4.4.1. Điều kiện chứng minh việc chấp nhận chứng thư số 26
4.4.2. Công bố chứng thư số 26
4.4.3. Thông báo đến các đối tượng khác về việc phát hành chứng thư số 26
4.5. Sử dụng cặp khóa và chứng thư số 27
4.5.1 Cách sử dụng chứng thư số và khóa bí mật của thuê bao 27
4.5.2. Cách sử dụng chứng thư số và khóa công khai của người nhận 28
4.6. Gia hạn chứng thư số 29
4.6.1. Điều kiện gia hạn 29
4.6.2. Đối tượng được phép yêu cầu gia hạn 29
4.6.3. Xử lý yêu cầu gia hạn chứng thư số 29
4.6.4. Thông báo cho thuê bao về việc phát hành chứng thư số mới 29
4.6.5. Điều khoản chấp nhận gia hạn chứng thư số 29
4.6.6. Công bố chứng thư số được gia hạn 29

4.6.7. Thông báo đến các đối tượng khác về việc gia hạn chứng thư số 30
4.7. Thay đổi cặp khóa 30
4.7.1. Điều kiện thay đổi 30
4.7.2. Đối tượng được phép yêu cầu thay đổi khóa 30
4.7.3. Xử lý yêu cầu thay đổi khóa 30
4.7.4. Thông báo cho thuê bao về việc thay khóa chứng thư số 30
4.7.5. Điều khoản chấp nhận thay khóa chứng thư số 30
4.7.6. Công bố chứng thư số đã thay khóa 30
4.7.7. Thông báo đến các đối tượng khác về việc thay khóa chứng thư số 30
4.8. Hủy cặp khóa 30
4.9. Thay đổi chứng thư số 32
4.9.1. Điều kiện thay đổi 32
4.9.2. Đối tượng được phép yêu cầu chứng thư số 32
4.9.3. Xử lý yêu cầu thay đổi chứng thư số 32
4.9.4. Thông báo cho thuê bao về việc thay khóa chứng thư số 32
4.9.5. Điều khoản chấp nhận thay khóa chứng thư số 32
4.9.6. Công bố chứng thư số đã thay đổi 32
4.9.7. Thông báo đến các đối tượng khác về việc thay khóa chứng thư số 32
4.10. Tạm dừng và Thu hồi chứng thư số 32
4.10.1. Các trường hợp thu hồi chứng thư số 32
4.10.2. Đối tượng yêu cầu thu hồi 33
4.10.3. Thủ tục yêu cầu thu hồi 33
4.10.4. Thời gian xử lý yêu cầu thu hồi 34
4.10.5. Thời gian xử lý đề nghị thu hồi 34
4.10.6. Yêu cầu kiểm tra thu hồi cho người nhận 34
4.10.7. Tần suất phát hành chứng thư số bị thu hồi 34
4.10.8. Thời gian trễ lớn nhất của CRL 34
4.10.9. Hỗ trợ kiểm tra trực tuyến trạng thái chứng thư số bị thu hồi 34
4.10.10. Điều kiện kiểm tra trực tuyến chứng thư số bị thu hồi 34
4.10.11. Mẫu quảng bá chứng thư số bị thu hồi khác 34
4.10.12. Các điều kiện đặc biệt khi khóa bị xâm phạm 35
4.10.13. Các trường hợp tạm dừng 35
4.10.14. Đối tượng được phép yêu cầu tạm dừng 35
4.10.15. Thủ tục yêu cầu tạm dừng 35

4.10.16. Giới hạn thời gian tạm dừng 37
4.11. Dịch vụ kiểm tra trạng thái chứng thư số 37
4.11.1. Đặc tính hoạt động 37
4.11.2. Tính sẵn sàng của dịch vụ 37
4.11.3. Các đặc tính tùy chọn 37
4.12. Chấm dứt dịch vụ của thuê bao 37
4.13. Lưu trữ và phục hồi khóa bí mật của thuê bao 38
5. KIỂM SOÁT, QUẢN LÝ VÀ VẬN HÀNH 38
5.1. Thiết bị, máy móc, nguồn điện, trụ sở và các yếu tố cần thiết khác 38
5.1.1 Ví trí xây dựng 38
5.1.2. Kiểm soát an toàn, anh ninh vật lý 38
5.1.3. Điều kiện nguồn điện 39
5.1.4. Phòng chống nước 39
5.1.5. Phòng cháy chữa cháy 39
5.1.6. Phương tiện lưu trữ 39
5.1.7. Tiêu hủy rác 39
5.1.8. Hệ thống dự phòng 39
5.2. Quy trình kiểm soát 40
5.2.1. Vai trò tin cây 40
5.2.2. Số lượng người tin cậy yêu cầu cho mỗi công việc 40
5.2.3. Xác thực định danh các vai trò 40
5.2.4. Phân chia trách nhiệm giữa các vị trí 41
5.3. Kiểm soát nhân sự 41
5.3.1. Yêu cầu phẩm chất, kinh nghiệm và tin tưởng 41
5.3.2. Thủ tục kiểm tra lý lịch 41
5.3.3. Yêu cầu đào tạo 42
5.3.4. Yêu cầu đào tạo lại thường xuyên 42
5.3.5. Tần suất luân chuyển công tác 43
5.3.6. Kỉ luật đối với các hành vi vi phạm 43
5.3.7. Các yêu cầu ký kết độc lập 43
5.3.8. Cung cấp tài liệu cho nhân viên 43
5.4. Các quy trình ghi nhật ký hệ thống 43
5.4.1. Các sự kiện VNPT SmartCA cần ghi nhận 43
5.4.2. Tần suất xử lý bản ghi kiểm tra 44

5.4.3. Thời gian lưu trữ bản ghi kiểm tra 44
5.4.4. Bảo vệ bản ghi kiểm tra 44
5.4.5. Thủ tục sao lưu bản ghi kiểm tra 44
5.4.6. Hệ thống kiểm tra 44
5.5. Lưu trữ các bản ghi 44
5.5.1. Các loại hồ sơ cần lưu trữ 44
5.5.2. Thời gian lưu trữ 45
5.5.3. Bảo vệ dữ liệu lưu trữ 45
5.5.4. Thủ tục thực hiện sao lưu 45
5.5.5. Yêu cầu dán nhãn thời gian cho các hồ sơ 45
5.6. Thay đổi khóa 45
5.7. Xử lý sự cố, thảm họa và phục hồi 45
5.7.1. Thủ tục xử lý vấn đề lộ khóa và sự cố 45
5.7.2. Tài nguyên máy tính, phần mềm và dữ liệu 46
5.7.3. Thủ tục xử lý sự cố bị lộ khóa bí mật 46
5.7.4. Khả năng khôi phục hoạt động kinh doanh sau sự cố 46
5.8. Dừng hoạt động 47
6. ĐẢM BẢO AN TOÀN AN NINH VỀ KỸ THUẬT 47
6.1. Tạo và phân phối cặp khóa 47
6.1.1. Sinh cặp khóa 47
6.1.2. Chuyển giao khóa công khai tới đơn vị phát hành 48
6.1.3. Chuyển giao khóa công khai của CA tới thuê bao 48
6.1.4. Kích thước khóa 48
6.1.5. Sinh các tham số khóa và kiểm tra chất lượng 48
6.1.6. Các mục đích sử dụng khóa (quy định trong bản ghi X.509 v3 key usage) 48
6.2. Kiểm soát và bảo vệ khóa bí mật 48
6.2.1. Các chuẩn thiết bị mật mã an toàn 48
6.2.2. Đa kiểm soát khóa bí mật 48
6.2.3. Ủy thác giữ khóa bí mật 49
6.2.4. Sao lưu khóa bí mật 49
6.2.5. Lưu trữ khóa bí mật 49
6.2.6. Chuyển khóa bí mật vào/ra thiết bị mật mã an toàn 49
6.2.7. Lưu trữ khóa bí mật trên thiết bị mật mã an toàn 49
6.2.8. Phương pháp kích hoạt sử dụng khóa bí mật 49

6.2.9. Phương pháp hủy khóa bí mật 49
6.2.10. Đánh giá thiết bị mật mã 50
6.3. Các vấn đề liên quan đến việc quản lý cặp khóa 50
6.3.1. Lưu trữ khóa công khai 50
6.3.2. Thời gian chứng thư số và cặp khóa hoạt động 50
6.4. Kích hoạt dữ liệu 50
6.4.1. Sinh và triển khai dữ liệu kích hoạt 50
6.4.2. Bảo vệ dữ liệu kích hoạt 50
6.4.3. Các vấn đề khác của dữ liệu kích hoạt 51
6.4.3.1. Gửi dữ liệu kích hoạt 51
6.4.3.2. Hủy dữ liệu kích hoạt 51
6.5. Kiểm soát an ninh quy trình sử dụng 51
6.5.1. Yêu cầu kỹ thuật về an toàn hệ thống máy tính 51
6.5.2. Đánh giá an toàn 51
6.6. Kiểm soát anh ninh quy trình sử dụng 52
6.6.1. Điều khiển quy trình phát triển hệ thống 52
6.6.2. Điều kiện về môi trường sử dụng dịch vụ 52
6.6.3. Cơ chế ủy quyền xác thực người dùng 52
6.6.4. Kiểm soát việc quản lý an toàn, an ninh 52
6.7. Giám sát an ninh hệ thống mạng 52
6.8. Dấu thời gian (Time-Stamping) 53
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) 53
7.1. Định dạng chứng thư số 53
7.1.1. Số hiệu phiên bản 59
7.1.2. Các thành phần mở rộng 59
7.1.3. Số hiệu thuật toán 59
7.1.4. Định dạng tên 59
7.1.5. Các ràng buộc về tên 59
7.1.6. Số hiệu của quy chế chứng thực 60
7.1.7. Sử dụng các ràng buộc quy chế mở rộng 60
7.1.8. Cú pháp và ngữ nghĩa quy chế 60
7.1.9. Xử lý ngữ nghĩa các quy chế chứng thư số mở rộng 60
7.2. Định dạng danh sách thu hồi chứng thư số (CRL) 60

7.2.1. Số hiệu phiên bản của CRL 60
7.2.2. CRL và các mở rộng 60
7.3. Định dạng giao thức kiểm tra trạng thái chứng thư số trực tuyến (OCSP) 60
7.3.1. Số hiệu phiên bản của OCSP 61
7.3.2. Các mở rộng OCSP 61
8. KIỂM ĐỊNH TÍNH TUÂN THỦ VÀ CÁC ĐÁNH GIÁ KHÁC 61
8.1. Tần suất và các tình huống kiểm tra kỹ thuật 61
8.2. Đơn vị, người thực hiện kiểm tra kỹ thuật 61
8.3. Các nội dung kiểm tra kỹ thuật 61
8.4. Xử lý khi phát hiện sai sót 61
8.5. Công bố kết quả kiểm tra kỹ thuật 61
9. CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC 62
9.1. Phí/Giá 62
9.1.1. Lệ phí cấp hoặc gia hạn chứng thư số số 62
9.1.2. Lệ phí sử dụng chứng thư số 62
9.1.3. Lệ phí thu hồi hoặc kiểm tra trạng thái chứng thư số 62
9.1.4. Lệ phí sử dụng cho các dịch vụ khác 62
9.1.5. Quy chế hoàn trả phí 62
9.2. Trách nhiệm tài chính 62
9.2.1. Phạm vi bảo hiểm 62
9.3. Bảo mật các thông tin nghiệp vụ 63
9.3.1. Phạm vi của bảo mật thông tin 63
9.3.2. Thông tin không thuộc phạm vi của quá trình đảm bảo tính mật 64
9.3.3. Trách nhiệm bảo vệ thông tin mật 64
9.4. Bảo mật thông tin cá nhân 64
9.4.1. Chính sách đảm bảo tính riêng tư 64
9.4.2. Những thông tin coi là riêng tư 64
9.4.3. Thông tin không được coi là riêng tư 64
9.4.4. Trách nhiệm bảo vệ thông tin riêng tư 64
9.4.5. Thông báo và cho phép sử dụng thông tin riêng tư 65
9.4.6. Cung cấp thông tin riêng tư theo yêu cầu của luật pháp hay cho quá trình quản trị 65
9.4.7. Các trường hợp làm lộ thông tin khác 65
9.5. Quyền sở hữu trí tuệ 65
9.6. Tuyên bố và cam kết 66
9.6.1. Cam kết và đảm bảo của CA 66

9.6.2. Cam kết và đảm bảo của RA 66
9.6.3. Cam kết vào đảm bảo của Thuê bao 66
9.6.4. Đại diện cho người nhận và vấn đề bảo lãnh 67
9.6.5. Đại diện cho các bên liên quan khác và vấn đề bảo lãnh 67
9.7. Từ chối trách nhiệm 67
9.8. Giới hạn trách nhiệm 67
9.9. Bồi thường thiệt hại 67
9.10. Hiệu lực của Quy chế chứng thực 68
9.10.1. Thời hạn 68
9.10.2. Kết thúc 68
9.10.3 Kết quả của kết thúc hiệu lực và các tồn tại 68
9.11. Thông báo cho các bên liên quan 68
9.12. Bổ sung và sửa đổi 69
9.12.1. Thủ tục sửa đổi 69
9.12.2. Cơ chế và thời gian thông báo 69
9.12.3. Các trường hợp OID thay đổi 69
9.13. Thủ tục giải quyết tranh chấp 69
9.14. Hệ thống pháp lý điều chỉnh 69
9.15. Phù hợp với pháp luật hiện hành 69
9.16. Các điều khoản chung 70
9.16.1. Điều khoản thỏa thuận chung 70
9.16.2. Tính độc lập của các điều khoản 70
9.16.3. Sự thực thi (quyền ủy nhiệm và quyền khước từ) 70
9.16.4. Chính sách bắt buộc thực thi 70
9.17. Các điều khoản khác 70

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.

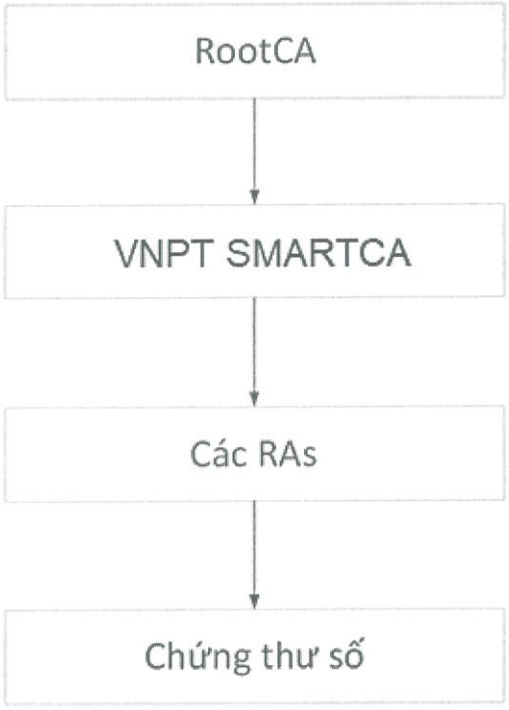
1.3.1. Thành phần Certification Authorities (CA)

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.



Nếu thuê bao đăng ký mua dịch vụ VNPT SmartCA sẽ được xác thực danh tính bằng công nghệ eKYC trên app VNPT SmartCA. Sau khi xác thực thành công, việc khởi tạo thuê bao sẽ được nhân sự CA duyệt cấp chứng thư số. Để sử dụng dịch vụ, thuê bao tiến hành kích hoạt khóa và nhận chứng thư số vừa được cấp.

Thời gian thuê bao chờ CA phê duyệt để được cấp chứng thư số:

- Đối với ngày thường: tối đa 4 giờ.
- Đối với ngày nghỉ: tối đa 8 giờ.

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 mới tiếp nhập 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 (vadility) của các chứng thư thông qua hai dịch vụ OCSP và CRL được đảm bảo liên tục và trực tuyến qua mạng Internet 24h trong một ngày và 7 ngày trong tuần.

2.4. Kiểm soát việc truy cập thông tin

Các thay đổi của CPS được thực hiện trên 2 yếu tố: (1) Theo các văn bản quy phạm pháp luật mới của Chính phủ, Bộ Thông tin và Truyền thông, Trung tâm Chứng thực điện tử quốc gia ban hành. (2) Theo các thực tế yêu cầu của quá trình cung cấp dịch vụ cho khách hàng nhưng vẫn phải đảm bảo các quy định của cơ quan quản lý nhà nước.

Thay đổi CPS được Công ty VNPT-IT dự thảo và thực hiện ban hành như sau:

- Báo cáo Tập đoàn – đơn vị chủ sở hữu giấy phép.
- Cung cấp cho VNPT – VinaPhone – đơn vị được Tập đoàn giao nhiệm vụ ký hợp đồng dịch vụ với khách hàng.
- Lập báo cáo đột xuất theo thông tư 17 /2014/TT-BTTTT của Bộ thông tin truyền thông ban hành ngày 26 tháng 11 năm 2014 quy định chế độ báo cáo về hoạt động chứng thực chữ ký số gửi Trung tâm Chứng thực điện tử quốc gia

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 Infastructure Certificate and CRL Profile ("RFC5280").

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

Tên trường	**Giá trị hoặc những ràng buộc**
Serial Number	Duy nhất cho một Issuer
Signature Algorithm	Thuật toán Hash: 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 thưu số. Được đồng bộ với U.S.Naval Observatory.
Subject	Thông tin về người nhận chứng thư số
Public Key	Được mã hóa theo tiêu chuẩn RFC5280 Mã hóa RSA 2048 bit

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

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

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

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

3.1.4. Quy tắc diễn giải các mẫu tên

Không có quy định.

3.1.5. Tính duy nhất của tên thuê bao

Tên thuê bao của dịch vụ VNPT SmartCA sẽ là duy nhất gắn với một cấp 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:

- Mã số thuế
- 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 trường hợp xác minh thông tin thuê bao sử dụng công cụ xác minh danh tính điện tử, nội dung xác thực bao gồm:

- Xác minh giấy tờ tùy thân (CMT/CCCD/ HC) bản gốc, thời hạn hiệu lực giấy tờ.
- Xác minh giấy chứng nhận đăng ký doanh nghiệp.
- So khớp khuôn mặt và giấy tờ tùy thân của người đại diện pháp luật và so khớp thông tin giấy chứng nhận đăng ký doanh nghiệp.

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.

Đối với trường hợp xác minh thông tin thuê bao sử dụng công cụ xác minh danh tính điện tử, nội dung xác thực bao gồm:

- Xác minh giấy tờ tùy thân (CMT/CCCD/HC) bản gốc, thời hạn hiệu lực giấy tờ

- So khớp khuôn mặt và giấy tờ tùy thân.

Đối với trường hợp thông tin người dân được chia sẻ từ Cơ sở dữ liệu Quốc gia về dân cư thông qua ứng dụng VneID, nội dung xác thực bao gồm:

- Xác thực chữ ký trên bản tin sử dụng Chứng thư số mà Bộ Công An cung cấp.

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

4.1.2.1. Hình thức truyền thống

Thuê bao muốn đăng ký sử dụng chứng thư số cần đến các điểm đăng ký bao gồm các 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.

4.1.2.2. Áp dụng xác minh danh tính qua công cụ điện tử

Thuê bao khai báo thông tin cần thiết theo mẫu của dịch vụ trên ứng dụng bán hàng, sau khi tiến hành thanh toán và ký hợp đồng điện tử, thông tin đăng ký của thuê bao được chấp nhận và chuyển qua bước xác minh danh tính.

Xác minh danh tính của thuê bao được thực hiện tự động qua công cụ điện tử; thông tin cần xác minh được mô tả tại mục 3.2.2 và 3.2.3 tài liệu này.

4.1.2.3. Quy trình cấp Chứng thư số từ dữ liệu được chia sẻ qua VNeID

Người dân xác nhận chia sẻ thông tin định danh trên ứng dụng VneID, dữ liệu định danh sẽ được đóng gói và ký số bởi cặp khóa do Bộ Công An quản lý, sau đó được truyền tới CA qua kênh truyền đã mã hóa

Xác minh danh tính thuê bao được thực hiện như mô tả tại mục 3.2.3 tài liệu này

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 thứ 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 tự động thông báo cho Thuê bao về việc yêu cầu Thuê bao kích hoạt dịch vụ qua email và SMS ngay sau khi tài khoản được khởi tạo thành công. Email và số điện thoại nhận SMS đã được đăng ký khi thuê bao lập phiếu yêu cầu cấp chứng thư số.
- VNPT SmartCA tự động thông báo cho Thuê bao việc chứng thư số của họ vừa được cấp thông qua thông báo trên ứng dụng di động (VNPT SmartCA) ngay sau khi chứng thư số 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 Signning
Criticality		TRUE	FALSE	FALSE	FALSE
0	digitalSingnature	Clear	Set	Set	Set
1	nonRepudiation	Clear	Set	Clear	Set
2	keyEnciphermentt	Clear	Set	Set	Clear
3	dataEnciphermen t	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 gồm các nội dung như sau:

+ Tuân theo quy định của Pháp luật liên quan đến chữ ký số công cộng như: Luật giao dịch điện tử, Thông tư 16, Thông tư 22, và các văn bản khác theo Quy định của Pháp luật.

+ Thực hiện các giao dịch hành chính công: Thuế, Hải Quan, Kho bạc, Bảo hiểm xã hội, Y tế, Giáo dục, Cổng dịch vụ công Quốc gia, và các hệ thống khác theo quy định của Pháp luật.

+ Thực hiện các giao dịch như: Ngân hàng, chứng khoán, Bảo hiểm (nhân thọ, phi nhân thọ), hợp đồng điện tử.

- VNPT SmartCA có trách nhiệm hướng dẫn Thuê bao sử dụng chứng thư số đảm bảo đúng mục đích theo Quy định như mô tả ở trên và trong nội dung của Hợp đồng.

- VNPT SmartCA có trách nhiệm phối hợp với cơ quan chức năng có thẩm quyền thực hiện kiểm tra, đánh giá việc sử dụng chứng thư số của Thuê bao có đúng theo Quy định của Pháp luật hay không trong trường hợp có yêu cầu của cơ quan có thẩm quyền.

- 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 huỷ 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 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 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 thư 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 so để tin rằng Thuê bao vi phạm nghĩa vụ trách nhiệm đối với hợp đồng hoặc các thỏa thuận đã cam kết của thuê bao.

- VNPT 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.

- 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.

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

VNPT SmartCA sẽ tạm dừng chứng thư số của thuê bao khi đang xử lý việc thu hồi chứng thư số của thuê bao.

VNPT SmartCA có thể trực tiếp tạm dừng chứng thư số trong trường hợp phát hiện thuê bao vi phạm điều khoản trong hợp đồng cung cấp dịch vụ hoặc vi phạm các điều khoản theo quy định pháp luật hiện hành.

Chủ sở hữu chứng thư số đề nghị yêu cầu tạm dừng chứng thư số.

Cơ quan nhà nước có thẩm quyền phát hiện thuê bao vi phạm quy định pháp luật hiện hành.

4.10.14. Đối tượng được phép yêu cầu tạm dừng

Cơ quan nhà nước có thẩm quyền (như cơ quan tố tụng, cơ quan công an hoặc Bộ Thông tin và Truyền thông).

VNPT SmartCA có thể tạm dừng chứng thư số trong trường hợp phát hiện thuê bao thực hiện không đúng các điều khoản trong hợp đồng, vi phạm quy định pháp luật hiện hành.

Đối với thuê bao cá nhân: Chỉ có duy nhất Chủ sở hữu chứng thư số cá nhân mới có quyền đề nghị yêu cầu tạm dừng chứng thư số.

Đối với thuê bao tổ chức, doanh nghiệp: chỉ có duy nhất người đại diện cho tổ chức đã được ủy quyền đứng tên trên chứng thư số mới có quyền yêu cầu tạm dừng chứng thư số.

4.10.15. Thủ tục yêu cầu tạm dừng

Trường hợp thuê bao yêu cầu tạm dừng:

Thuê bao:

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

AM:

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

- Trường hợp thông tin không đủ hợp lệ tạm dừng, AM hướng dẫn thuê bao điền thông tin trong phiếu đề nghị tạm dừng chứng thư số.

- Trường hợp thông tin là hợp lệ để tạm dừng, AM gửi báo cáo thông tin xác thực kèm theo đề nghị tạm dừng chứng thư tới RA làm có cơ sở thực hiện yêu cầu.

Nhân sự RA:

- Tiếp nhận và tạo phiếu yêu cầu tạm dừng
- Chuyển phiếu yêu cầu tạm dừng sang nhân sự CA

Nhân sự CA:

- Thực hiện kiểm tra và duyệt phiếu yêu cầu tạm dừng chứng thư số của thuê bao

VNPT SmartCA:

- VNPT SmartCA xác thực CA và các thông tin CA gửi, nếu hợp lệ, VNPT SmartCA sẽ tiến hành tạm dừng 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 tạm dừng.

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

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

AM:

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

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

Nhân sự RA:

- Tiếp nhận và tạo phiếu yêu cầu tạm dừng
- Chuyển phiếu yêu cầu tạm dừng sang nhân sự CA

Nhân sự CA:

- Thực hiện kiểm tra và duyệt phiếu yêu cầu tạm dừng chứng thư số của thuê bao

VNPT SmartCA:

- VNPT SmartCA xác thực CA và các thông tin CA gửi, nếu hợp lệ, VNPT SmartCA sẽ tiến hành tạm dừng 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 tạm dừng.

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

4.10.16. Giới hạn thời gian tạm dừng

Ngay sau khi kết thúc thẩm định yêu cầu.

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 Ví 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 dấu.

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, anh 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 thông kiểm tra dấu vân tay và nhân viên bảo vệ. Bản thân nhân viên bảo vệ không có quyền ra vào nơi đặt thiết bị. Nhân viên

này có nhiệm vụ ngăn chặn những cố gắng xâm nhập của người lạ, không có thẩm quyền. Những người có thể vào nơi đặt thiết bị phải là những người mà nhân viên bảo vệ biết trước là có quyền hạn và trách nhiệm đi vào khu vực này, đồng thời phải xác thực và cho phép của hệ thống nhận dạng vân tay. Mặt khác, nơi đặt thiết bị có camera theo dõi liên tục (24/7).

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

5.1.3. Điều kiện nguồn điện

Hệ thống cung cấp dịch vụ VNPT 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 khu tiêu hủy. Các loại rác khác được tiêu hủy đạt yêu cầu về tiêu hủy rác thông thường của VNPT.

5.1.8. Hệ thống dự phòng

Hệ thống chính của dịch vụ VNPT 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 hệt hệ thống chính thức và được đặt tại IDC Tân Thuận: Lô Va.02c-03a, đường 24, khu chế xuất Tân Thuận, phường Tân Thuận Đông, quận 7, Thành phố Hồ Chí Minh.

5.2. 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 phần bị hạn chế của hệ thống.
- Chuyển giao thông tin hoặc yêu cầu của thuê bao.
- Người tin cậy bao gồm, nhưng không giới hạn bởi các thành phần sau:
  - Nhân viên giao dịch, nhân viên chăm sóc khách hàng.
  - Nhân viên điều hành công việc mã hóa.
  - Nhân viên an ninh.
  - Nhân viên bảo mật hệ thống.
  - Các kỹ sư thiết kế.

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

VNPT 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 ko giới hạn:

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

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

- Quá trình ban hành, thu hồi các chứng thư số, bao gồm những cá nhân được truy cập tới những phần hạn chế truy cập của kho lưu trữ.

- Quá trình chuyển giao những thông tin thuê bao hay các yêu cầu từ khách hàng.

- Quá trình tạo, ban hành hay tiêu hủy một chứng thư số.

5.3. Kiểm soát nhân sự

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

Tất cả các đối tượng muốn trở thành người tin cậy và làm việc tại các vị trí tin cậy hệ thống của VNPT 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 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:

- Các sự kiện xác minh danh tính của thuê bao bằng công cụ điện tử.
- 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 bàn ghi log khỏi các truy nhập, sửa đổi, xóa bỏ hoặc can thiệp bất hợp pháp.

5.4.5. Thủ tục sao lưu bản ghi kiểm tra

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

5.4.6. Hệ thống kiểm tra

Kiểm tra hệ thống tự động được thực hiện ở mức ứng dụng, mạng và hệ điều hành. Nhân viên chuyên trách của VNPT 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.

Các dữ liệu sẽ được lưu trong một khoảng thời gian ít nhất 10 năm kể từ ngày ký hợp đồng cung cấp dịch vụ. Sau thời gian đó VNPT vẫn tiếp tục lưu trữ dữ liệu của Thuê bao nhưng không có trách nhiệm cam kết thời hạn lưu trữ trong bao lâu.

Với trường hợp bị đình chỉ hoặc thu hồi giấy phép, thực hiện lưu trữ toàn bộ thông tin và các cơ sở dữ liệu về thuê bao, chứng thư số trong thời gian tối thiểu 05 năm, kể từ khi giấy phép bị tạm đình chỉ hoặc thu hồi (theo điều 33, Nghị định 130/2018)

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 sảy 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 sảy 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 ngẫn nhiên và duy nhất, có khả năng đảm bảo khóa bí mật không bị phát hiện khi có khóa công khai tương ứng, quá trình sinh khóa của hệ thống VNPT 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 báo khóa bí mật không bị phát hiện khi có khóa công khai tương ứng.

6.1.2. 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.

6.1.3. 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.

6.1.4. 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.

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

6.1.6. 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 lơn hơn 1 (m) mảnh khóa (m =< n). Tại VNPT SmartCA, áp dụng m >= 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 phần cứng an toàn và được đặt cách xa vị trí lưu trữ bản chính tối thiểu 10 km.

6.2.5. Lưu trữ khóa bí mật

Khi chứng thư số hết hạn, cặp khóa của VNPT 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 anh 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:

VIETNAM NATIONAL ROOT CA	
Version	V3
Serial Number	009592BB8CEEAD5A24A6B8F71D7D323B5A
Signature Algorithm	SHA256withRSA
Signature Hash Algorithm	SHA256
Issuer DN	CN=Vietnam National Root CA OU=National Centre of Digital Signature Authentication O=Ministry of Information and Communications C=VN
Valid From	4/15/2014, 11:29:20 PM ICT
Valid To	4/15/2039, 11:29:20 PM ICT
Subject DN	CN=Vietnam National Root CA OU=National Centre of Digital Signature Authentication O=Ministry of Information and Communications C=VN
Public Key Size	4096 bits
Public Key Parameters	05 00
Public Key	30 82 02 0a 02 82 02 01 00 b8 ac 5a 7b 08 30 d9 70 7a 69 f5 1f e3 37 95 4e 14 03 97 f1 bd c6 3e 7a 52 84 fe f0 a6 d6 ec 17 88 8e 45 1e bf 09 54 98 ae 7f 8f 81 d0 68 8b 8d 83 b8 3d a2 24 1a 53 61 ad ed 63 3f 7d 34 7c a7 f3 e4 41 3e f2 ce e6 34 b8 bc d2 c5 43 b7 77 c2 f1 06 71 51 87 3f f9 56 79 3a 71 f5 9c b1 95 30 08 48 14 fc b1 eb 9d 5b 91 8c 86 2c 7d f7 5c dd 80 e0 50 99 1c 6e 79 f1 46 ae b3 4c 5f 41 1b 6c 47 dd fd c2 eb c0 b8 63 7c 84 45 a7 b9 30 2b a4 a4 d1 0b 5e 1e 86 72 d4 51 d8 59 12 84 57 88 4f 32 54 65 28 2e 08 42 49 02 3e 6a 61 6d eb 6a 42 6e 77 85 e3 14 55 60 32 79 7a fb bf 0f 63 1b e5 00 0f 28 15 0a d4 6c 0c b0 5a ae

	8b ce 7e b3 72 9a 3e 39 9b 96 7c 5e cd 15 51 84 70 0b 43 b8 dd 68 ca fb 2d f8 7e bc 7f a8 22 67 8f 9d 28 8e 1d 05 ca c5 91 82 7e a6 d7 fd f3 e0 de bf f2 23 ea 89 e3 38 b8 15 80 4f fa 2f 0a 6b 0c 85 58 ed 7d 2f 76 a1 86 ec d6 e1 ea 06 9e ba 00 86 e7 f9 98 b4 85 64 1e 1c 0f 2b e2 9c 4c f1 13 61 92 43 63 14 f7 ad 42 1a 85 a6 21 d5 0a 7e 2d f1 03 5d 32 48 d9 71 8a 7b 2f 65 06 49 85 81 d1 a9 65 8e b9 a7 7c 6f ad 85 be 34 77 1c 6e d3 ec 47 eb 30 72 eb 86 45 5e d4 3f f9 dd 99 15 f4 f0 68 9a 31 37 ca ae 44 7b 57 94 6f 7d ea c3 89 0f ef 7b 37 ea da 10 cf 1e 2c c5 6a ac 6d 22 64 d4 bb cc 05 bd 71 9b a3 5d 61 b2 ba 8b 09 a2 90 c5 94 e8 a2 76 29 ec 40 95 60 50 ee 7a e2 fb 13 a5 29 e1 c5 e5 7a bd 6a 2e fa 77 c3 e4 19 55 1e 2b e7 c2 0a bf 15 6b b4 76 91 89 95 2c 6c 36 b7 df 97 40 95 68 e0 68 92 3c 41 66 78 1c e1 d5 64 b4 23 ad 7f 89 92 30 cf 25 33 07 37 1b 8c 12 41 25 ac 24 85 de b5 ea 50 a6 7f 24 cb ea 29 e6 35 ea 34 03 68 7d 02 03 01 00 01
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Subject Key Identifier	7EF087EDB1B89DFB08836FA416FDF1B8AC629B01
Basic Constraints	Subject Type=CA Path Length Constraint=None
Thumbprint	8EA95975898EFEF73B5CA92BF03F712BFBC7615F

VNPT SMARTCA RS

Version	V3
Serial Number	00FC060D806FD75F4D8BF525C77697591F
Signature Algorithm	SHA256withRSA
Signature Hash Algorithm	SHA256
Issuer DN	CN=Vietnam National Root CA OU=National Centre of Digital Signature Authentication O=Ministry of Information and Communications C=VN
Valid From	11/18/2021, 10:55:57 AM ICT
Valid To	11/18/2026, 10:55:58 AM ICT
Subject DN	CN=VNPT SmartCA RS O=VIETNAM POSTS AND TELECOMMUNICATIONS GROUP C=VN
Public Key Size	2048 bits
Public Key Parameters	05 00
Public Key	30 82 01 0a 02 82 01 01 00 ec 7f 4d 64 58 9e f3 17 1e d6 50 24 eb 30 09 cc 60 fe 2c d8 af 74 8c 4a 81 50 b7 d5 3c 4f 81 55 28 c4 ee b8 94 75 b3 72 61 80 0e 62 ab f5 e7 9e 91 1e 20 dc 61 17 27 59 49 f2 96 6e 2e 42 c8 04 8c 73 2d 77 c6 0b 59 f7 78 df 85 21 13 11 01 b2 04 87 44 8c 0b 11 b2 1f 73 39 33 32 47 eb 87 58 76 75 1a f1 4d 42 a9 fe 5e ec a8 9a

	a6 7c 88 d7 fa f7 bd 8a 4e a3 d9 85 c9 25 ec 21 a2 2a 83 78 04 2d c1 cb 18 6a e6 bd 2e 05 4a 6e 8d 96 50 7f 51 23 76 d8 c5 a4 52 00 8b a0 0a 10 12 e9 4f d0 74 09 b4 c4 ce 57 ea 29 83 d3 95 a9 03 e1 40 8b 8f 95 96 7c 37 54 71 28 bf 3e cf 63 0f 91 6d 35 24 f1 09 8b 36 58 d2 62 60 8b 24 9c 70 b8 00 97 51 d1 b9 73 54 a8 95 b3 1f 48 41 1a df 2e 53 62 01 70 3c e5 8c 3a 76 a0 fc a3 8e 47 fd fa 80 ff 8f 0f 72 01 51 de 3f f5 be b6 f8 5b 32 5f 98 c1 02 03 01 00 01
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Subject Key Identifier	5FEFC4EB3AF622F772D2DA193C292559BBA0FD2F
Basic Constraints	Subject Type=CA Path Length Constraint=0
Thumbprint	7ABC082FEAADD9F35A5D17FFEAFC477D909D554B

VNPT-CA SHA-256

Version	V3
Serial Number	4FEEF2A430ABB3820ADFB69198BF12D6
Signature Algorithm	SHA256withRSA
Signature Hash Algorithm	SHA256
Issuer DN	CN=Vietnam National Root CA OU=National Centre of Digital Signature Authentication O=Ministry of Information and Communications C=VN
Valid From	7/28/2020, 6:09:47 PM ICT
Valid To	7/28/2025, 6:09:47 PM ICT
Subject DN	CN=VNPT-CA SHA-256 O=VIETNAM POSTS AND TELECOMMUNICATIONS GROUP C=VN
Public Key Size	2048 bits
Public Key Parameters	05 00
Public Key	30 82 01 0a 02 82 01 01 00 c6 97 80 f9 68 c9 4a 70 13 e3 ac 5e 75 cb 10 c0 64 18 8d d0 ab 33 32 75 a1 e1 45 e5 a7 2d 45 10 23 5c 96 c6 f8 24 bd 6f 83 f2 9b 71 f6 b2 ae f8 41 f1 ef 19 c9 b4 2b 56 85 c3 3f 88 b3 32 0c 30 9e c3 c5 8f 38 3c 0e 55 69 74 d4 6b 0b e3 63 cb 05 35 b4 11 ea d3 7a 8c 41 82 60 bc df b5 3b d2 10 a1 9b d7 f4 15 6b b9 81 d7 21 09 e9 11 fa 6e b7 0a e3 60 15 36 09 2e 33 3b 2b b3 c1 87 5e c5 52 06 4a 17 a2 6f 60 21 1a 64 c8 be f4 92 f8 9f b9 c8 8c b8 5f fb 9c 25 42 ac 12 06 a8 32 89 13 ed ea ed 9d cc ee 85 52 97 d5 7b 98 00 0f 78 8e 26 09 09 09 8f 9e 64 cb 11 5d 2b 33 d1 c5 02 73 69 29 37 29 31 17 cd 20 34 07 2c 1d ca 5e 14 d7 50 8d 6e 2a 97 b5 a5 63 eb 5c 91 29 34 77 5e 2a 3c 22 d8 f2 4f 53 9d ea 83 ec e1 41 37 26 66 d5 86 59 1e 5c fc 66 d4 0d ab 01 a0 c5 d3 e0 d4 23 02 03 01 00 01

Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Subject Key Identifier	B64D6B6BD6A69D34ED3239EC4254ACBE3263D871
Basic Constraints	Subject Type=CA Path Length Constraint=0
Thumbprint	6E8DB7A7A020659749F0F082AF7945F600D5AD56

MIC NATIONAL ROOT CA	
Version	V3
Serial Number	1BE4738A1F3EC08F479FA6CF35C59822
Signature Algorithm	SHA1withRSA
Signature Hash Algorithm	SHA1
Issuer DN	CN=MIC National Root CA OU=National CA Center O=Ministry of Information and Communications C=VN
Valid From	5/16/2008, 8:12:49 AM ICT
Valid To	5/16/2040, 8:20:32 AM ICT
Subject DN	CN=MIC National Root CA OU=National CA Center O=Ministry of Information and Communications C=VN
Public Key Size	2048 bits
Public Key Parameters	05 00
Public Key	30 82 01 0a 02 82 01 01 00 a1 3f 59 51 0e fe 30 ff 61 db 96 78 14 8b db 43 3c 36 be 61 af dc b5 3f 60 1e d3 0d 01 41 ad f8 c9 8a 42 8e c8 ed 32 86 47 c5 fe b5 f7 ea d6 44 37 10 12 c3 48 08 51 50 ba e5 57 e9 ce 35 c9 8e 1c 73 09 85 33 4c e1 bb 38 ac 8e ad b7 13 04 2e 66 81 57 2d cc fb 1a fd 2e 9c 8b fd 09 40 f0 60 17 9b 71 45 6d 7d e3 db 2a d2 bb 9a dd eb cc 5e e4 00 df d5 6c 30 85 9b bd 57 7f 2d d4 24 d3 80 fb e0 28 51 be b0 d6 61 07 cc e5 a0 47 e7 91 6d 2f 87 58 e8 b4 ad c1 b1 46 b3 dc 5a 1d 38 09 d9 fb b5 27 98 9e 5e fc f1 f4 48 ff e8 a1 3b ff 50 33 d9 26 ab b2 99 62 9d cc 7b c8 52 4d 9e 5c 42 8b 6f 74 7e fc 94 13 de 0a d2 f0 b5 6a f8 96 4c 50 9c e6 21 8e c1 e5 97 01 4e cd 9f b0 40 19 7c 1b 59 6f 5c 38 19 9a 37 da d1 81 39 16 32 ef 81 ad b0 21 6b 11 97 c2 c1 08 bd 6f 23 5c 04 0f d3 02 03 01 00 01
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Subject Key Identifier	CD6271E461BDFE3DECB24060D38175DD3AAC6BC6
Basic Constraints	Subject Type=CA Path Length Constraint=None

CA Version	V0.0
Thumbprint	42843BC401476CDA242034B945BBF409A6BDD5C7

VNPT-CA SHA-256

Version	V3
Serial Number	71DEEFBD000000000016
Signature Algorithm	SHA1withRSA
Signature Hash Algorithm	SHA1
Issuer DN	CN=Vietnam National Root CA OU=National Centre of Digital Signature Authentication O=Ministry of Information and Communications C=VN
Valid From	6/26/2019, 2:52:00 PM ICT
Valid To	6/26/2024, 3:02:00 PM ICT
Subject DN	CN=VNPT Certification Authority OU=VNPT-CA Trust Network O=VNPT Group C=VN
Public Key Size	4096 bits
Public Key Parameters	05 00
Public Key	30 82 02 0a 02 82 02 01 00 cf 5b 28 46 68 43 c8 58 84 18 7b ff 30 2a 9e be 9c 1f 0b 7b d7 a4 03 c3 53 d3 e3 0b e8 54 b7 b1 99 4f e1 38 8c 73 39 6f 3d a1 1b cc bd 74 c1 c4 b4 cb 5a eb b6 a5 56 f9 db aa 68 9a 2c d5 56 47 47 52 57 00 a1 da e6 99 03 b7 f9 3d 6c 54 f1 9a b0 dd f3 6e 6a 4e 97 8b 7e 6c 45 86 29 39 bf ee 95 94 cc df 5a 29 f8 f0 a0 8c 89 23 6c ee b5 36 63 b3 aa f0 ce 13 e7 44 ec c5 50 c2 8c 80 b5 49 b1 04 7d 11 38 0f 5c 74 2f 7f 82 29 84 67 fa 84 24 a4 c8 58 93 73 e7 69 35 d8 0f 0e 45 1b 0b 75 45 33 a3 8c 0c 4a f3 95 38 2c e3 77 da 8c 5e 55 c2 29 19 55 b1 01 36 e3 e4 81 1b e7 49 c8 79 0e 55 f7 00 ca 9d 1c bc b3 11 26 6a 8b a1 a5 44 af 53 88 85 6e 78 fa 0e 00 c1 4e 4f 74 2b 3f 65 b1 12 2c 2c d9 47 0a d1 88 51 54 72 c0 0a 19 49 80 5a 1d 4a a9 7d e3 39 43 71 2d 82 e1 a6 22 66 ad dc e0 06 4e 85 00 5a f0 6d 34 0a cf e4 8d 38 a2 8d 6c 13 23 ec 19 e3 73 c1 74 7b b7 35 2a 91 ed b1 39 d6 4f ea 23 49 6b 03 c4 7a 12 9c a7 81 67 af 7b 60 4f 4c 5a e6 14 2f 95 72 05 e5 65 35 32 bf 3a d0 b3 f7 7d f6 46 29 7c 95 48 e4 d8 03 be 0b 29 07 b3 4e c0 f5 20 d8 85 a2 a1 92 d4 7b d7 bd 02 80 d5 e4 cd a9 18 14 ec 06 9a c8 24 58 d8 ba ca 86 a7 c7 d0 f6 7d 9e e9 31 3c 1f 54 cf a0 d4 35 08 3b 9f e1 5d 2c 64 50 5d ab 9a 0e 7e 6a e8 90 14 f6 33 9d d6 f1 3d 36 53 01 be 9b 11 86 6d ab 1b 36 d9 f4 b4 4d ed 88 63 72 80 1e 2d ce 77 91 7a de 7a f2 22 e8 5a dd b7 49 ad ef 34 86 bb da c3 c6 1f 13 ff 1c 67 75 c7 50 8e ff 64 15 51 67 8a 4f 28 c5 1b b0 0a e9 8e 1e c8 44 7b 89 d9 04 eb 1d 29 b3 f8 ae 93 b1 e0 da cd 4a 09 a6 71 ed 6f 51 26 89 ca 9e 37 bd 78 f5 c7 cc 9b fb 02 03 01 00 01
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

Subject Key Identifier	0669C0D5D5028A158D467DE97CE2680A55AC6AAF
Basic Constraints	Subject Type=CA Path Length Constraint=0
Thumbprint	B1ADEC6EF075F1F98E9F51774E90B9808EDC5A60

VNPT-CA SHA-256	
Version	V3
Serial Number	71DEEFBD000000000016
Signature Algorithm	SHA1withRSA
Signature Hash Algorithm	SHA1
Issuer DN	CN=Vietnam National Root CA OU=National Centre of Digital Signature Authentication O=Ministry of Information and Communications C=VN
Valid From	6/26/2019, 2:52:00 PM ICT
Valid To	6/26/2024, 3:02:00 PM ICT
Subject DN	CN=VNPT Certification Authority OU=VNPT-CA Trust Network O=VNPT Group C=VN
Public Key Size	4096 bits
Public Key Parameters	05 00
Public Key	30 82 02 0a 02 82 02 01 00 cf 5b 28 46 68 43 c8 58 84 18 7b ff 30 2a 9e be 9c 1f 0b 7b d7 a4 03 c3 53 d3 e3 0b e8 54 b7 b1 99 4f e1 38 8c 73 39 6f 3d a1 1b cc bd 74 c1 c4 b4 cb 5a eb b6 a5 56 f9 db aa 68 9a 2c d5 56 47 47 52 57 00 a1 da e6 99 03 b7 f9 3d 6c 54 f1 9a b0 dd f3 6e 6a 4e 97 8b 7e 6c 45 86 29 39 bf ee 95 94 cc df 5a 29 f8 f0 a0 8c 89 23 6c ee b5 36 63 b3 aa f0 ce 13 e7 44 ec c5 50 c2 8c 80 b5 49 b1 04 7d 11 38 0f 5c 74 2f 7f 82 29 84 67 fa 84 24 a4 c8 58 93 73 e7 69 35 d8 0f 0e 45 1b 0b 75 45 33 a3 8c 0c 4a f3 95 38 2c e3 77 da 8c 5e 55 c2 29 19 55 b1 01 36 e3 e4 81 1b e7 49 c8 79 0e 55 f7 00 ca 9d 1c bc b3 11 26 6a 8b a1 a5 44 af 53 88 85 6e 78 fa 0e 00 c1 4e 4f 74 2b 3f 65 b1 12 2c 2c d9 47 0a d1 88 51 54 72 c0 0a 19 49 80 5a 1d 4a a9 7d e3 39 43 71 2d 82 e1 a6 22 66 ad dc e0 06 4e 85 00 5a f0 6d 34 0a cf e4 8d 38 a2 8d 6c 13 23 ec 19 e3 73 c1 74 7b b7 35 2a 91 ed b1 39 d6 4f ea 23 49 6b 03 c4 7a 12 9c a7 81 67 af 7b 60 4f 4c 5a e6 14 2f 95 72 05 e5 65 35 32 bf 3a d0 b3 f7 7d f6 46 29 7c 95 48 e4 d8 03 be 0b 29 07 b3 4e c0 f5 20 d8 85 a2 a1 92 d4 7b d7 bd 02 80 d5 e4 cd a9 18 14 ec 06 9a c8 24 58 d8 ba ca 86 a7 c7 d0 f6 7d 9e e9 31 3c 1f 54 cf a0 d4 35 08 3b 9f e1 5d 2c 64 50 5d ab 9a 0e 7e 6a e8 90 14 f6 33 9d d6 f1 3d 36 53 01 be 9b 11 86 6d ab 1b 36 d9 f4 b4 4d ed 88 63 72 80 1e 2d ce 77 91 7a de 7a f2 22 e8 5a dd b7 49 ad ef 34 86 bb da c3 c6 1f 13 ff 1c 67 75 c7 50

	8e ff 64 15 51 67 8a 4f 28 c5 1b b0 0a e9 8e 1e c8 44 7b 89 d9 04 eb 1d 29 b3 f8 ae 93 b1 e0 da cd 4a 09 a6 71 ed 6f 51 26 89 ca 9e 37 bd 78 f5 c7 cc 9b fb 02 03 01 00 01
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Subject Key Identifier	0669C0D5D5028A158D467DE97CE2680A55AC6AAF
Basic Constraints	Subject Type=CA Path Length Constraint=0
Thumbprint	B1ADEC6EF075F1F98E9F51774E90B9808EDC5A60

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

Trường	*Giá trị hoặc yêu cầu*
Version	Xem phần 7.2.1
Signature Algorithm	Thuật toán dùng để ký danh sách chứng thư số bị thu hồi. VNPT SmartCA sử dụng thuật toán sau theo chuẩn RFC 3279. Sha2WithRSAEncryption (OID: 1.2.840.113549.1.1.11)
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 kĩ 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 kĩ 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 chúng không được coi là các thông tin mật/riêng tư. Các thông tin mật/riêng tư trong phần 9.3.1 sẽ không được coi là riêng tư hoặc không được coi là bí mật nếu pháp luật có quy định khác.

9.3.3. Trách nhiệm bảo vệ thông tin mật

VNPT 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 trọng phạm vi quyền hạn của mình.

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

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

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

VNPT 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 khống chế bởi các thỏa thuận hợp lý giữa các bên miền con liên quan. Những phần sau sẽ sử dụng tới quyền sở hữu trí tuệ liên quan tới thuê bao và các bên đối tác.

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

VNPT 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 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.
- VNPT đảm bảo rằng các thiết bị mật mã sử dụng trong quá trình cung cấp dịch vụ đã được chứng nhận.

9.6.2. Cam kết và đảm bảo của RA

Các RA của VNPT SmartCA đảm bảo:

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

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

9.6.3. Cam kết vào đảm bảo của Thuê bao

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 vơi 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 lạc hoặc xuyên tạc sự thật do thuê bao cung cấp trên chứng thư số

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

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

Vấn đề bồi thường của các đối tác tin cậy

Khi được pháp luật cho phép, bản thỏa thuận của đối tác tin cậy sẽ yêu cầu các đối tác tin cậy 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

Việc thay đổi CPS theo nội dung mô tả tại mục 2.4 của tài liệu này.

Tài liệu CPS đã được thay đổi mới nhất sẽ được VNPT SmartCA cung cấp tại địa chỉ: http://www.vnpt-ca.vn/

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

VNPT SmartCA không có thẩm quyền thay đổi thông OID, việc thay đổi nội dung OID theo quy định và hướng dẫn của NEAC. Nếu VNPT SmartCA thấy cần thiết thay đổi OID, VNPT SmartCA có thể đề xuất với NEAC thông qua hình thức bằng văn bản.

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

CPS của dịch vụ VNPT SmartCA tuân thủ theo tiêu chuẩn Quy định của Việt Nam (Thông tư 16/2019/TT-BTTT, các văn bản khác có liên quan) và các Quy định trong tiêu chuẩn eIDAS.

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.