TẬP ĐOÀN CÔNG NGHIỆP-VIỄN THÔNG QUÂN ĐỘI

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 5548/QĐ-CNVTQĐ

Hà Nội , ngày 26 tháng 11 năm 2021

QUYẾT ĐỊNH
Về việc ban hành Quy chế chứng thực dịch vụ chứng thực chữ ký số công cộng Viettel-CA

TỔNG GIÁM ĐỐC
TẬP ĐOÀN CÔNG NGHIỆP – VIỄN THÔNG QUÂN ĐỘI

Căn cứ ủy quyền của Tổng Giám đốc Tập đoàn Công nghiệp - Viễn thông Quân đội cho đồng chí Cao Anh Sơn - Tổng Giám đốc Tổng Công ty Viễn thông Viettel;

Căn cứ nhu cầu triển khai kinh doanh dịch vụ chứng thực chữ ký số công cộng Viettel-CA.

QUYẾT ĐỊNH:

Điều 1. Ban hành Quy chế chứng thực dịch vụ chứng thực chữ ký số công cộng với phương thức lưu khóa bí mật của thuê bao trong SIM PKI đáp ứng tiêu chuẩn FIPS PUB 140-2 tối thiểu mức 2 hoặc đáp ứng tiêu chuẩn TCVN 8709 (ISO/IEC 15408) tối thiểu EAL mức 4.

Điều 2. Quyết định có hiệu lực thi hành kể từ ngày ký. Các quy định trước đây trái với Quyết định này đều bãi bỏ.

Điều 3. Các cơ quan, đơn vị chức năng của Tổng Công ty Viễn thông Viettel, kênh bán và 63 Viettel Tỉnh/Thành phố có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Lưu: VT, VTT. Lài 01.

TUQ.TỔNG GIÁM ĐỐC
TỔNG GIÁM ĐỐC
TỔNG CÔNG TY VIỄN THÔNG VIETTEL

M.S.D.N: 0100109106-C.T.T.N.H.H * TẬP ĐOÀN CÔNG NGHIỆP VIỄN THÔNG QUÂN ĐỘI * QUẬN CẦU GIẤY-TP HÀ NỘI

Thượng tá Cao Anh Sơn

QUY CHẾ CHỨNG THỰC

DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG MOBILE-CA

MỤC LỤC

1. THÔNG TIN CHUNG

1.1. Khái quát

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

1.2. Nhận dạng tài liệu

Văn bản này là một bộ quy chế chứng thực (Certificate Practices Statement - CPS) tuyên bố về mặt nguyên tắc các chính sách quản trị của Mobile-CA trong quá trình cung cấp dịch vụ chứng thực chữ ký số công cộng.

CPS này là một chính sách quan trọng trong quá trình cung cấp dịch vụ chứng thực chữ ký số, đưa ra các yêu cầu về kinh doanh, pháp lý và kỹ thuật cho quá trình chấp thuận, cấp phát, quản lý, sử dụng, thu hồi và cấp lại chứng thư số trong hệ thống Mobile-CA. Các yêu cầu của CPS có nhiệm vụ đảm bảo tính bảo mật và toàn vẹn cho dịch vụ Mobile-CA, được áp dụng và bắt buộc tuân thủ đối với mọi thành phần tham gia dịch vụ chứng thực chữ ký số Mobile-CA.

CPS này không phải là thỏa thuận về mặt pháp lý giữa Mobile-CA với thuê bao cũng như các thành phần khác tham gia dịch vụ Mobile-CA.

Mục tiêu của văn bản này là:

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

CPS này tuân theo luật pháp Việt Nam cũng như các chính sách, quy chế liên quan đến dịch vụ chứng thực chữ ký số công cộng được ban hành bởi Bộ Thông tin và Truyền thông cũng như các cơ quan nhà nước có thẩm quyền liên quan.

CPS này được xây dựng tuân theo tiêu chuẩn RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework).

1.3. Các thành phần tham gia dịch vụ Mobile-CA

1.3.1. Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng (CA)

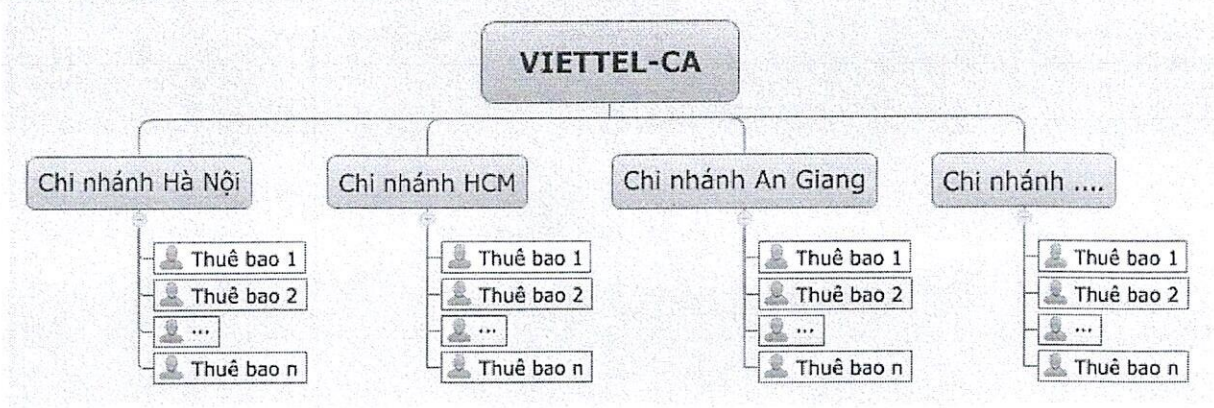
Tổ chức cung cấp dịch vụ - CA là thành phần quan trọng nhất trong hệ thống PKI. CA xác thực thông tin thuê bao cũng như đảm bảo tính bảo mật và toàn vẹn nội dung thông tin mà các thành phần tham gia dịch vụ chứng thực chữ ký số công cộng trao đổi thông qua hệ thống của CA. Mỗi CA là tổng thể hệ thống thiết bị (phần cứng, phần mềm) và những người quản trị hệ thống đó nhằm thực hiện các chức năng chính sau:

- Tạo cặp khóa bao gồm khóa công khai và khóa bí mật cho thuê bao;
- Cấp, gia hạn, tạm dừng, phục hồi và thu hồi chứng thư số của thuê bao theo quy định của pháp luật và CPS;
- Duy trì trực tuyến cơ sở dữ liệu về chứng thư số (còn hiệu lực, hết hạn, gia hạn, cấp mới, thu hồi);
- Cung cấp các dịch vụ khác có liên quan cho người sử dụng.

CA có thể thực hiện các chứng năng trên một cách trực tiếp hoặc ủy quyền cho đối tượng khác tiến hành theo quy định của pháp luật, các đối tượng này được gọi là RA (Registration Authority).

Hệ thống Mobile-CA được tổ chức theo quy định của pháp luật Việt Nam, trực thuộc RootCA (Trung tâm Chứng thực điện tử Quốc gia) do Bộ Thông tin và Truyền thông quản lý.

Mobile-CA được Bộ Thông tin và Truyền thông cấp phép cung cấp dịch vụ chứng thực chữ ký số công cộng, do đó có quyền cấp chứng thư số cho các cơ quan, tổ chức, doanh nghiệp, cá nhân (đủ điều kiện theo quy định của pháp luật và CPS này), có yêu cầu cấp chứng thư số.



Hình 1 – Sơ đồ tổ chức hệ thống Viettel – CA

1.3.2. Tiếp nhận yêu cầu cung cấp dịch vụ và xác thực thông tin thuê bao

RA (registration authority) là tổ chức được CA tin cậy, uỷ quyền tiếp nhận yêu cầu cung cấp dịch vụ và xác thực thông tin của thuê bao nhằm đảm bảo tính chính xác các thông tin trong chứng thư số của thuê bao trên toàn hệ thống.

Nhiệm vụ của RA là gồm:

- Tiếp nhận yêu cầu cấp chứng thư số và báo cho CA thông qua hệ thống thiết bị (phần cứng, phần mềm) và người vận hành hệ thống đó;
- Xác thực thông tin thuê bao theo yêu cầu của CA nhằm đảm bảo tính chính xác các thông tin trong chứng thư số trên toàn hệ thống.

Trong hệ thống Mobile-CA, RA được gọi là Viettel-RA là toàn bộ các chi nhánh của Viettel trên toàn quốc có khả năng kiểm tra, xác thực định danh các thuê bao.

1.3.3. Thuê bao

Thuê bao là tổ chức, cá nhân (đủ điều kiện theo quy định của pháp luật và CPS này) được Mobile-CA cấp chứng nhận chứng thư số.

1.3.4. Người nhận

Người nhận là các tổ chức, cá nhân sử dụng các chức năng của hệ thống Mobile-CA để giải mã/xác thực thông tin nhận được từ thuê bao của Mobile-CA.

1.3.5. Thành phần khác

Không có quy định.

1.4. Sử dụng chứng thư số

1.4.1. Chứng thư số hợp pháp

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

1.4.2. Các trường hợp không được sử dụng chứng thư số Mobile-CA

Các chứng thư số Mobile-CA không được thiết kế, dự định hoặc cho phép sử dụng như công cụ điều khiển trong tình huống nguy hiểm hay cho các sử dụng có độ yêu cầu an toàn rất cao như: hoạt động của các phương tiện hạt nhân, các hệ

thống định vị và thông tin liên lạc máy bay, hệ thống điều khiển giao thông đường không, hay hệ thống điều khiển vũ khí có ảnh hưởng trực tiếp tới sinh mạng hay phá hủy môi trường.

1.5. Chính sách quản trị

1.5.1. Tổ chức quản lý văn bản

Tổng Công ty Viễn thông Viettel – Chi nhánh Tập đoàn Công nghiệp-Viễn thông Quân đội. Địa chỉ: Số 01, phố Giang Văn Minh - Phường Kim Mã - Quận Ba Đình - Hà Nội.

1.5.2. Địa chỉ liên hệ

Tổng Công ty Viễn thông Viettel – Chi nhánh Tập đoàn Công nghiệp-Viễn thông Quân đội. Địa chỉ: Số 01, phố Giang Văn Minh - Phường Kim Mã - Quận Ba Đình - Hà Nội.

1.5.3. Đơn vị quyết định tính hợp pháp của CPS

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

1.5.4. Thủ tục phê chuẩn CPS

Viettel là đơn vị có thẩm quyền phê duyệt CPS này và những thay đổi liên quan trong quá trình hoạt động của Mobile-CA. Các thay đổi phải được thể hiện bằng văn bản dưới dạng một tài liệu chứa các sửa đổi mẫu của CPS hay các thông tin về quá trình cập nhật. Tất cả những phiên bản đã sửa đổi hoặc cập nhật thông tin được công bố tại đại chỉ **http://Viettel-CA.vn/download**.

1.6. Các định nghĩa và tên viết tắt

Chi tiết trong Phụ lục

2. CÔNG BỐ, LƯU TRỮ VÀ SỬ DỤNG THÔNG TIN THUÊ BAO

2.1. Lưu trữ

Nhằm đảm bảo tính công khai, CPS và các tài liệu khác được Mobile-CA duy trì lưu trữ trực tuyến tại địa chỉ **http://Viettel-CA.vn/download**.

2.2. Công bố thông tin chứng thư số

Khi bàn giao chứng thư số cho khách hàng, Mobile-CA yêu cầu khách hàng ký biên bản bàn giao chứng thư số, xác nhận thông tin trên chứng thư số là chính xác. Sau đó chứng thư số của khách hàng sẽ được công bố rộng rãi trên mạng internet.

Mobile-CA duy trì và đảm bảo hoạt động của kho lưu trữ cho phép thuê bao và các thành phần tham gia dịch vụ Mobile-CA khác truy xuất nhằm xác định trạng thái chứng thư số cũng như danh sách các chứng thư số bị tam ngừng, thu hồi.

Các thông tin thường xuyên được Mobile-CA cập nhật và công bố gồm có:

- Các chứng thư số do Mobile-CA cấp;
- CRL do Mobile-CA quản lý;
- Mẫu Hợp đồng dịch vụ giữa Mobile-CA với thuê bao.

2.3. Thời gian và tần suất công bố

Các cập nhật của CPS được tuân theo trong phần 9.12.

2.4. Quản lý truy cập tại các kho lưu trữ

- CRL, CPS được công bố công khai nhưng không cho phép sửa đổi hoặc thay thế tại địa chỉ **http://Viettel-CA.vn/download**.
- Cập nhật CRL được thực hiện tự động bởi hệ thống Mobile-CA;
- Mọi thay đổi của CPS chỉ được phép thực hiện bởi cấp có thẩm quyền của Viettel.

3. QUY TẮC ĐẶT TÊN TRONG CHỨNG THƯ

3.1. Kiểu tên

3.1.1. Các thuộc tính

Tên trong chứng thư số của thuê bao bao gồm các trường Issuer và Subject tuân theo chuẩn đặt tên X.509, gồm các thành phần sau:

Thuộc tính	Giá trị
Country (C)	2 ký tự chỉ định tên quốc gia theo chuẩn ISO
Organization (O)	Thuộc tính này được chỉ định như sau: - Tên của tổ chức đối với chứng thư số tổ chức và chứng thư số cá nhân thuộc tổ chức; - Tên miền đối với các chứng thư số chỉ xác nhận được tên

Thuộc tính	Giá trị
	miền.
Organizational Unit (OU)	Chứng thư số của thuê bao có thể bao gồm nhiều thuộc tính OU. Các thuộc tính này có các giá trị như sau: - Tên đơn vị nằm trong tổ chức (đối với chứng thư số tổ chức hoặc chứng thư số cá nhân thuộc tổ chức); - Giá trị mô tả loại chứng thư số; - Giá trị mô tả thực thể thực hiện xác minh; - Địa chỉ của thuê bao.
State or Province (S)	Thuộc tính này chứa tên tỉnh/ thành phố nơi cư trú của thuê bao.
Locality (L)	Thuộc tính này chứa tên địa phương nơi cư trú của thuê bao.
Common Name (CN)	Thuộc tính này bao gồm các loại giá trị sau: - Tên miền (đối với chứng thư số máy chủ web) - Tên tổ chức (đối với chứng thư số của tổ chức/ doanh nghiệp) - Tên cá nhân (đối với chứng thư số cá nhân)
E-Mail Address (E)	Thuộc tính này chứa địa chỉ email của thuê bao.

Bảng 1 – Các loại tên trong chứng thư số.

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

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

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

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

Tuy nhiên, Mobile-CA không chịu trách nhiệm về mọi tranh chấp về quyền sở hữu trí tuệ phát sinh liên quan đến việc sử dụng tên của đối tượng đăng ký chứng thư số.

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

3.2. Xác thực định danh

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 Mobile-CA công nhận. Điều kiện này không áp dụng khi cặp khóa được CA sinh ra theo theo yêu cầu của thuê bao (trường hợp khóa được sinh và lưu trữ trên smartcard).

3.2.2. Xác thực định danh cho tổ chức

Khi chứng thư số cho tổ chức hoặc chứng thư số cá nhân trong tổ chức, Mobile-CA cần phải thực hiện xác thực định danh của tổ chức nhằm đảm bảo:

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

3.2.3. Xác thực định danh cho cá nhân

Định danh của cá nhân phải được xác thực bởi người có thẩm quyền trong hệ thống Mobile-CA, bao gồm: Tên cá nhân; Địa chỉ; Chứng minh nhân dân; Hộ khẩu; Hộ chiếu; Địa chỉ thư điện tử; Thông tin về website, quyền sở hữu tên miền của cá nhân (dùng cho việc cấp chứng thư số SSL).

3.2.4. Thông tin thuê bao không xác minh

Không có quy định.

3.2.5. Công nhận quyền

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

- Xác định sự tồn tại của tổ chức thông qua ít nhất một bên thứ ba;
- Xác thực các thông tin ghi trong Phiếu yêu cầu cấp chứng thư số thông qua các tài liệu cần thiết và có thể thu thập;

- Xác định danh tính và vị trí của cá nhân trong tổ chức có tương ứng với các thông tin đã đăng ký hay không.

3.2.6. Các tiêu chuẩn thực hiện liên hoạt

Không có quy định.

3.3. Xác thực định danh đối với yêu cầu thay đổi khóa

Trước khi chứng thư số hết hạn, thuê bao cần xin cấp chứng thư số mới nhằm tiếp tục sử dụng dịch vụ. Thuê bao có thể xin cấp cặp khóa mới hoặc gia hạn cặp khóa hiện tại tùy theo mục đích và tình hình của chứng thư số. Trong phạm vi CPS này, cả hai trường hợp đều được coi là gia hạn chứng thư số. Việc thực hiện gia hạn chứng thư số cần tuân theo quy trình xác thực tương tự như yêu cầu cấp chứng thư số ban đầu.

3.4. Xác thực định danh cho yêu cầu thu hồi chứng thư số

Chỉ có người đứng tên thuê bao mới được phép thực hiện yêu cầu thu hồi chứng thư số;

Để yêu cầu thu hồi chứng thư số, thuê bao cần liên hệ với Mobile-CA hoặc Viettel-RA thông qua phương tiện liên lạc thích hợp bao gồm điện thoại, thư điện tử, giao dịch trực tiếp để chỉ định rõ chứng thư số cụ thể nào cần thu hồi.

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

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

4.1. 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.

4.1.2. Quy trình cấp chứng thư số cho thuê bao

Tất cả thuê bao đều phải ký *Hợp đồng dịch vụ* với Mobile-CA được đề cập trong phần 9.6.3 sau khi thực hiện quy trình đăng ký bao gồm:

- Yêu cầu cấp chứng thư số với các thông tin chính xác;
- Sinh một cặp khóa hoặc ủy thác sinh một cặp khóa;
- Gửi khóa công khai đến Viettel-RA (đối với trường hợp tự sinh cặp khóa);

- Chứng minh quyền sở hữu khóa bí mật tương ứng với khóa công khai đã gửi đến Viettel-RA (đối với trường hợp tự sinh cặp khóa);
- Đối tượng yêu cầu cấp chứng thư số đến các điểm giao dịch của Viettel-RA để khai báo các thông tin cần thiết trên Phiếu yêu cầu cấp chứng thư số theo mẫu do Mobile-CA ban hành, sau đó nộp cho Viettel-RA và chờ thông tin phải hồi;
- Viettel-RA tiến hành xác thực thông tin đã kê khai theo phần 3.2 và gửi kết quả xác thực cho đối tượng đăng ký;
- Viettel-RA gửi cặp khóa đến Mobile-CA;

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

a. Thực hiện xác thực định danh

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

b. Chấp nhận hoặc từ chối cấp chứng thư số

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

Mobile-CA từ chối yêu cầu cấp chứng thư số trong các trường hợp sau:

- Xác thực định danh không thành công ít nhất một trong các thông tin về đối tượng yêu cầu cấp chứng thư số theo phần 3.2;
- Đối tượng yêu cầu cấp chứng thư số không cung cấp đủ tài liệu theo yêu cầu;
- Đối tượng yêu cầu cấp chứng thư số không trả lời yêu cầu liên lạc trong hạn thời gian xác định;
- Đối tượng yêu cầu cấp chứng thư số chưa thanh toán phí dịch vụ cấp chứng thư số;
- Có căn cứ cho rằng việc Mobile-CA cấp chứng thư số cho đối tượng yêu cầu có thể ảnh hưởng tới uy tín và độ tin cậy của Mobile-CA.

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

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

4.1.4 Quy trình bàn giao SIM CA và khóa bí mật cho thuê bao

Yêu cầu, hợp đồng và hồ sơ xin cấp CTS của khách hàng sau khi đã được Mobile-CA phê duyệt hợp lệ, nhân viên Mobile-CA sẽ liên hệ khách hàng để tiến hành bàn giao SIM CA và thực hiện cấp CTS cho khách hàng.

Tại điểm giao dịch, nhân viên Viettel bàn giao SIM CA cho khách hàng:

- Hướng dẫn khách hàng kiểm tra SIM CA và tự đổi, kiểm tra mật khẩu mới.
- Nhân viên Viettel thực hiện thao tác cấp CTS cho khách hàng.
- Đến bước nhập mật khẩu để thực hiện tạo khóa bí mật, Nhân viên Viettel yêu cầu khách hàng nhập mật khẩu của SIM CA.
- Hệ thống tự động kiểm tra và hoàn tất việc cấp CTS.
- Nhân viên Viettel hướng dẫn khách hàng kiểm tra thông tin CTS, hướng dẫn sử dụng và bàn giao các giấy tờ liên quan.

Quy trình này đảm bảo CTS chỉ được kích hoạt bởi chính khách hàng.

4.2. Phát hành chứng thư số

4.2.1. Hoạt động của Mobile-CA khi phát hành chứng thư số

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

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

Mobile-CA hoặc Viettel-RA thông báo cho thuê bao về việc phát hành chứng thư số đồng thời cung cấp phương thức truy cập tới chứng thư số đó để kiểm tra tính sẵn sàng của chứng thư.

Chứng thư số có hiệu lực sẽ cho phép thuê bao tải về từ website, giao diện lập trình API hoặc sẽ được Mobile-CA gửi trực tiếp tới thuê bao.

4.3. Chấp nhận chứng thư số

4.3.1. Điều kiện chứng minh việc chấp nhận chứng thư số

Khi nhận được chứng thư số, thuê bao cần thông báo cho Mobile-CA về việc chấp nhận chứng thư số đó. Nếu thuê bao không phản hồi với Mobile-CA trong khoảng thời gian 3 ngày, chứng thư số coi như được thuê bao chấp nhận.

4.3.2. Công bố chứng thư số

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

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

Mobile-CA có trách nhiệm thông báo cho Viettel-RA về việc phát hành chứng thư số do họ xác thực định danh.

4.4. Sử dụng cặp khóa và chứng thư số

4.4.1. 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.

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

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

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

Khi sử dụng chứng thư số hợp lý, người nhận cần sử dụng phương tiện phần mềm, phần cứng hợp lý nhằm tiến hành xác minh chữ ký số hoặc các thao tác mật mã cần thiết khác. Các thao tác này bao gồm cả việc xác định chuỗi chứng thư số và kiểm tra các chữ ký số trên tất cả chứng thư số trong chuỗi.

4.5. Gia hạn chứng thư số

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

4.5.1. Điều kiện gia hạn

Nếu muốn gia hạn chứng thư số, thuê bao phải yêu cầu ViettelCA gia hạn trước 30 ngày tính đến ngày hết hạn sử dụng chứng thư số đó.

4.5.2. 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.

4.5.3. 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 Mobile-CA ban hành.

Viettel-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.

4.5.4. 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

4.5.5. 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

4.5.6. Công bố chứng thư số được gia hạn

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

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

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

4.6. Thay đổi khóa chứng thư số

4.6.1. Điều kiện thay đổi khóa

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.

4.6.2. 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.

4.6.3. 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 Mobile-CA ban hành.

Mobile-CA hoặc Viettel-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.

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

Thông báo cho thuê bao về việc thay khóa chứng thư số theo phần 4.2.2

4.6.5. Điều khoản chấp nhận thay khóa chứng thư số

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

4.6.6. Công bố chứng thư số đã thay khóa

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

4.6.7. Thông báo đến các đối tượng khác về việc thay khóa chứng thư số

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

4.7. Sửa đổi chứng thư số

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

4.7.1. Điều kiện sửa đổi chứng thư số

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

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

Xem phần 4.1.1.

4.7.3. Xử lý yêu cầu sửa đổi chứng thư số

Viettel-RA tiến hành xác thực định danh thông tin của thuê bao theo phần 3.2.

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

Xem phần 4.2.2.

4.7.5. Điều khoản chấp nhận sửa đổi chứng thư số

Xem phần 4.3.1

4.7.6. Công bố chứng thư số đã sửa đổi

Xem phần 4.3.2.

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

Xem phần 4.3.3.

4.8. Tạm dừng và thu hồi chứng thư số

4.8.1. Các trường hợp thu hồi chứng thư số

Thuê bao có quyền đề nghị thu hồi chứng thư số tại bất cứ thời điểm nào theo bất cứ lý do gì. Thuê bao cần yêu cầu Mobile-CA thu hồi chứng thư số khi:

- Bất cứ thông tin nào của chứng thư số bị thay đổi hoặc không sử dụng;
- Khóa bí mật, thiết bị lưu trữ khóa bí mật tương ứng với chứng thư số bị xâm phạm;
- Chủ sở hữu máy chủ web của thuê bao thay đổi.

Thuê bao cần nêu rõ lý do yêu cầu thu hồi khi gửi yêu cầu thu hồi chứng thư số đến Mobile-CA.

Mobile-CA thực hiện việc thu hồi chứng thư số trong các trường hợp sau:

- Khi nhận được yêu cầu thu hồi của của thuê bao như đã đề cập ở trên;
- Khóa bí mật của Mobile-CA dùng để phát hành chứng thư số bị xâm phạm;
- Thuê bao vi phạm điều khoản trong Hợp đồng dịch vụ hoặc CPS này;
- Mobile-CA phát hiện chứng thư số bị sử dụng sai mục đích;
- Mobile-CA nhận thấy thông tin trong chứng thư số khác với thông tin của thuê bao đã được xác thực định danh;

Nếu Mobile-CA đơn phương thu hồi chứng thư số, Mobile-CA sẽ thông báo cho thuê bao theo địa chỉ đã đăng ký.

4.8.2. *Đối tượng được phép yêu cầu thu hồi 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 thu hồi chứng thư số.

4.8.3. *Thủ tục yêu cầu thu hồi chứng thư số*

Sau khi Viettel-RA tiếp nhận yêu cầu thu hồi, việc xác thực đề nghị thu hồi sẽ được tiến hành theo nội dung trong phần 3.4.

Trường hợp kết quả trả về chưa hợp lý, Viettel-RA sẽ hủy bỏ đề nghị và gửi kết quả tới thuê bao;

Trường hợp kết quả trả về hợp lý, Viettel-RA có trách nhiệm báo cho Mobile-CA yêu cầu thu hồi chứng thư số của thuê bao. Mobile-CA sẽ gửi thông báo thu hồi kèm theo lý do thu hồi trực tiếp đến thuê bao hoặc thông qua Mobile-CA đã tiếp nhận và xác thực đề nghị thu hồi.

4.8.4. *Thời gian tiến hành yêu cầu thu hồi*

Không có thời gian đợi có hiệu lực cho thuê bao khi thu hồi.

4.8.5. *Thời gian xử lý đề nghị thu hồi*

Mobile-CA có trách nhiệm thực hiện các nghiệp vụ cần thiết nhằm thu hồi chứng thư số trong thời gian nhanh nhất có thể.

4.8.6. *Yêu cầu kiểm tra việc thu hồi cho người nhận*

Người nhận có thể kiểm tra trạng thái chứng thư số mà họ muốn tin cậy bằng việc tham khảo những CRL mới nhất từ Mobile-CA tại địa chỉ:

- http://crl.Viettel-CA.vn/Viettel-CA.crl
- http://crl.Viettel-CA.vn/Viettel-CA-2.crl
- http://crl.Viettel-CA.vn/Viettel-CA-v3.crl
- http://crl.Viettel-CA.vn/Viettel-CA-SHA2.crl

bằng cách sử dụng kho lưu trữ trên website hoặc bằng cách sử dụng OCSP (nếu sẵn có). Mobile-CA sẽ cung cấp cho người nhận các thông tin tìm kiếm CRL thích hợp, kho lưu trữ trên website hay OCSP để kiểm tra trạng thái thu hồi chứng thư số.

4.8.7. ***Tần suất phát hành chứng thư số bị thu hồi***

Trong trường hợp có chứng thư số bị thu hồi, Mobile-CA sẽ công bố thông tin thu hồi trên CRL chậm nhất không quá 24 giờ kể từ thời điểm thu hồi.

4.8.8. ***Thời gian trễ lớn nhất của CRL***

CRL được phát hành công khai và quá trình này được tiến hành tự động.

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

CRL truy cập tại địa chỉ:

- http://crl.Viettel-CA.vn/Viettel-CA.crl
- http://crl.Viettel-CA.vn/Viettel-CA-2.crl
- http://crl.Viettel-CA.vn/Viettel-CA-v3.crl
- http://crl.Viettel-CA.vn/Viettel-CA-SHA2.crl

4.8.10.*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.

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

Không có quy định.

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

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

4.8.13.*Các trường hợp tạm dừng*

Không có quy định.

4.8.14.*Đối tượng được phép yêu cầu tạm dừng*

Không có quy định.

4.8.15.*Thủ tục yêu cầu tạm dừng*

Không có quy định.

4.8.16.*Giới hạn thời gian tạm dừng*

Không có quy định.

4.9. Dịch vụ kiểm tra trạng thái chứng thư số

4.9.1. ***Các đặc tính hoạt động***

Trạng thái chứng thư số được kiểm tra thông qua CRL tại trang web của Viettel – CA, dịch vụ LDAP hoặc thông qua dịch vụ OCSP địa chỉ http://ocsp.Viettel-CA.vn.

4.9.2. ***Tính sẵn sàng của dịch vụ***

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

4.9.3. *Các đặc tính tùy chọn*

OCSP là dịch vụ tùy chọn không cung cấp cho mọi trường hợp mà chỉ được dùng cho một số trường hợp xác định.

4.10. Kết thúc thuê bao

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

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

4.11. Ủy thác giữ và phục hồi khóa

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

5. ĐẢM BẢO AN TOÀN, AN NINH CƠ SỞ VẬT CHẤT, QUY CHẾ LÀM VIỆC VÀ NHÂN SỰ CỦA CA

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

5.1.1. *Vị trí xây dựng*

Hoạt động của Mobile-CA và các Viettel-RA được xây dựng trong môi trường vật lý, được bảo vệ nhằm ngăn ngừa và phát hiện truy nhập trái phép vào hệ thống hoặc tiết lộ các thông tin hệ thống một cách bất hợp pháp.

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

5.1.2. *Truy cập vật lý*

Việc ra vào trụ sở Mobile-CA và Viettel-RA đòi hỏi tất cả phải có thẻ nhân viên. Trong trường hợp khách đến trụ sở để giao dịch, khách cần xuất trình chứng minh thư nhân dân/thẻ căn cước công dân hoặc hộ chiếu. Các giấy tờ này sẽ được lưu lại tại quầy lễ tân và khách sẽ được cấp thẻ khách để được đi lại trong các khu vực cho phép trong phạm vi trụ sở.

Quyền ra vào nơi đặt thiết bị phục vụ việc cung cấp dịch vụ Mobile-CA được kiểm soát bởi hệ thống sinh trắc học 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 các cố gắng xâm nhập của người không có thẩm quyền. Đối tượng được phép ra vào nơi đặt thiết bị phải là người mà nhân viên bảo vệ biết trước là có quyền hạn và trách nhiệm đi vào khu vực này, đồng thời cần xác thực và có sự cho phép của hệ thống nhận dạng sinh trắc học. Mặt khác, nơi đặt thiết bị có camera theo dõi liên tục 24 x 7.

Quyền truy cập hệ thống chỉ được trao cho những người có trách nhiệm quản trị, vận hành và theo dõi hệ thống. Do đó, các đối tượng không đủ thẩm quyền,

nếu có vượt qua được hệ thống bảo vệ và kiểm soát sinh trắc học cũng không có khả năng truy cập vào hệ thống.

5.1.3. *Điều kiện nguồn điện*

Hệ thống cung cấp dịch vụ của Mobile-CA được nối với hệ thống UPS có khả năng duy trì nguồn điện trong thời gian 30 phút. Song song với hệ thống điện lưới, tòa nhà được trang bị hệ thống máy phát điện, hệ thống này sẽ được kích hoạt ngay sau khi mất điện lưới. Điều này đảm bảo nguồn điện cung cấp cho hệ thống là liên tục.

5.1.4. *Phòng chống nước*

Trụ sở lắp đặt thiết bị hệ thống Mobile-CA đảm bảo phòng ngừa để không cho phép nước xâm nhập vào hệ thống, thiết bị.

5.1.5. *Phòng cháy, chữa cháy*

Trụ sở Mobile-CA được trang bị hệ thống phòng cháy chữa cháy và cảnh báo cháy đảm bảo có thể phát hiện, ngăn chặn và dập tắt lửa hay các thảm họa khác có thể gây cháy hay khói. Hệ thống này được thiết kế để phù hợp với tiêu chuẩn phòng cháy chữa cháy quốc gia.

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 đảm bảo an ninh thông qua các triển khai an ninh vật lý và điều khiển truy cập nhằm ngăn ngừa truy cập trái phép và bảo vệ phương tiện lưu trữ không bị phá hủy (do nước, lửa, điện từ trường…)

5.1.7. *Tiêu hủy rác*

Các tài liệu và tài nguyên nhạy cảm được cắt vụn trước khi hủy. Các phương tiện thu thập hay truyền thông tin nhạy cảm được xử lý để đảm bảo các thông tin này không bị truy cập bất hợp pháp trước khi tiêu hủy. Các thiết bị dùng để mã hóa phải được phá hủy về mặt vật lý theo hướng dẫn của nhà sản xuất trước khi tiêu hủy. Các loại rác khác phải tiêu hủy đạt yêu cầu về tiêu chuẩn tiêu hủy rác thông thường của Mobile-CA.

5.1.8. *Hệ thống dự phòng*

Hệ thống dự phòng cho dịch vụ Mobile-CA được xây dựng về mặt chức năng giống như hệ thống chính thức và được đặt ở xa hệ thống chính thức tối thiểu 10 km.

5.2. Nhân sự

5.2.1. *Người tin cậy*

Nhân viên, nhân viên tư vấn đều phải được xem xét trước khi trở thành người tin cậy làm việc tại vị trí được tin cậy của Mobile-CA. Những người được chọn là người tin cậy làm việc tại vị trí tin cậy đáp ứng yêu cầu của Mobile-CA.

Người tin cậy bao gồm tất cả các nhân viên, kỹ sư, nhân viên tư vấn có truy cập hay điều khiển quá trình xác thực hoặc mã hóa có thể gây ảnh hưởng lớn tới:

- Quá trình kiểm tra thông tin trong ứng dụng chứng thư số;
- Quá trình cung cấp dịch vụ chứng thực chữ ký số;
- Ban hành, thu hồi quyền truy cập tới các phần bị hạn chế của hệ thống;
- Chuyển giao thông tin hoặc yêu cầu của thuê bao;
- Người tin cậy bao gồm, nhưng không giới hạn bởi các thành phần sau:
- Nhân viên giao dịch, nhân viên chăm sóc khách hàng;
- Nhân viên điều hành công việc mã hóa;
- Nhân viên an ninh;
- Nhân viên bảo mật hệ thống;
- Các kỹ sư thiết kế;

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

Mobile – CA thiết lập, duy trì và có các yêu cầu nghiêm ngặt về thủ tục điều khiển để đảm bảo quá trình phân công nhiệm vụ dựa trên khả năng làm việc và đảm bảo rằng nhiều người tin cậy sẽ cùng thực hiện các công việc có tính bảo mật cao.

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

Những thủ tục điều khiển ở bên trong được thiết kế để đảm bảo ít nhất hai người tin cậy cùng tham gia truy cập tới mức vật lý hoặc mức logic của thiết bị. Truy cập tới phần cứng mã hóa yêu cầu chặt chẽ phải có nhiều người tin cậy cùng tham gia toàn bộ quá trình làm việc, từ việc nhận và kiểm tra cho tới bước cuối cùng là hủy về logic và/hoặc về vật lý. Mỗi một lần modul này được kích hoạt trong các thao tác liên quan đến khóa, các truy cập xa hơn nữa sẽ bị thu hồi để duy trì việc phân cách giữa điều khiển các truy cập ở mức vật lý và mức logic tới thiết bị. Những người có truy cập vật lý tới các modul không giữ thông tin cho phép truy cập vào hệ thống và ngược lại.

5.2.3. *Xác thực định danh các vai trò*

Tất cả mọi đối tượng muốn trở thành người tin cậy, quy trình xác thực định danh được thực hiện với sự hiện diện về mặt con người (vật lý) của đối tượng này trước khi quy trình kiểm tra thông thường bắt đầu (như kiểm tra chứng minh thư nhân dân, hộ chiếu,…). Quá trình xác thực định danh được thực hiện thêm một lần nữa thông qua thủ tục kiểm tra lý lịch.

Mobile-CA đảm bảo những nhân viên đạt được vị trí được tin cậy và trao quyền cho các nhân viên này:

- Được cấp phép truy cập tới các phạm vi cần thiết;
- Được cấp tài liệu điện tử để có thể truy cập đến và thực hiện một số chức năng trên Mobile-CA, Viettel-RA hay các hệ thống IT khác.

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

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

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

5.3. Kiểm soát nhân sự

Mobile-CA có các tài liệu về kiểm soát nhân sự và chính sách bảo mật cho Mobile-CA và Viettel-RA. Việc tuân thủ những chính sách bao gồm các yêu cầu kiểm tra độc lập được mô tả ở phần 8. Những tài liệu này chứa thông tin bảo mật nhạy cảm và chỉ dành riêng cho bên tham gia dịch vụ Mobile-CA dưới sự đồng ý của Mobile-CA.

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

5.3.2. *Thủ tục kiểm tra lý lịch*

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

- Giấy xác nhận của địa phương về cá nhân, gia đình;
- Xác nhận của đơn vị công tác trước đó;
- Kiểm tra, tham khảo từ các đồng nghiệp;
- Xác nhận cấp đào tạo cao nhất đã đạt được;
- Kiểm tra các tiền án, tiền sự ở địa phương cũng như cấp quốc gia;
- Kiểm tra thông tin về tài chính;
- Xác nhận đáp ứng các điều kiện về chính trị và an ninh của cơ quan chính trị và bảo vệ an ninh của Viettel.

Khi một trong các yếu tố bắt buộc này không thể đạt được do luật pháp hoặc hoàn cảnh nào đó, Mobile-CA sẽ sử dụng kỹ thuật đánh giá thay thế khác được luật pháp cho phép.

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

- Thông tin do ứng viên hoặc người tin cậy cung cấp không trung thực;
- Mức độ không tán thành hay tin tưởng cao của người tin cậy;
- Tiền án tiền sự;
- Thiếu khả năng hoặc có dấu hiệu không minh bạch về về tài chính.

Báo cáo bao gồm các thông tin trên được bộ phận quản trị nguồn nhân lực và các nhân viên an ninh đánh giá, từ đó đưa ra các biện pháp thích hợp cho mỗi tình huống. Các biện pháp này có thể bao gồm việc kiểm tra và loại bỏ ứng viên khỏi vị trí được tin cậy hoặc chấm dứt công việc của ứng viên.

Việc sử dụng các thông tin thu thập được từ trong quá trình kiểm tra lý lịch phải phù hợp với luật pháp và chính sách của nhà nước.

5.3.3. *Yêu cầu đào tạo*

Mobile-CA đào tạo nhân viên sau tuyển dụng cũng như trong quá trình làm việc để đảm bảo nhân viên có thể hoàn thành công việc của mình. Vietel-CA sẽ lưu giữ các tư liệu của những lần đào tạo này đồng thời thường xuyên xem xét lại và nâng cấp các chương trình đào tạo khi thấy cần thiết.

Chương trình đào tạo của Mobile-CA thích hợp cho mỗi công việc riêng lẻ và thường liên quan tới:

- Các vấn đề cơ bản của hạ tầng khóa công khai;
- Yêu cầu công việc;
- Chính sách, thủ tục an ninh và các hoạt động của Mobile-CA;
- Sử dụng và điều hành các thiết bị phần cứng, phần mềm đã triển khai;
- Báo cáo, chuyển giao các thỏa ước và các vấn đề liên quan;
- Thủ tục khôi phục sau thảm họa và duy trì công việc.

Chương trình đào tạo của Mobile-CA được thiết kế tương thích với chương trình đào tạo về chữ ký số và chứng thực chữ ký số do Trung tâm Chứng thực điện tử quốc gia (NEAC) cung cấp.

5.3.4. *Yêu cầu đào tạo lại thường xuyên*

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

5.3.5. *Tần suất luân chuyển công tác*

Không có quy định

5.3.6. *Kỉ luật đối với các hành vi vi phạm*

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

5.3.7. *Các yêu cầu ký kết độc lập*

Trong một số trường hợp nhất định, các nhân viên triển khai hay tư vấn độc lập được sử dụng vào các vị trí tin cậy. Những nhân viên này có cùng chức năng và vai trò an ninh như các nhân viên Mobile-CA ở vị trí tương ứng.

Các đối tượng trên phải là người đã hoàn thành hay vượt qua thủ tục kiểm tra lý lịch và được phép truy cập tới các phương tiện được bảo mật của dịch vụ Mobile-CA trong phạm vi quyền hạn của họ.

5.3.8. *Cung cấp tài liệu cho nhân viên*

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

5.4. Thủ tục kiểm tra

5.4.1. *Các sự kiện Mobile-CA cần ghi nhận*

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

Các dạng sự kiện có thể kiểm định bao gồm:

- Các sự kiện: (1) tạo khóa CA; (2) bật tắt các hệ thống và ứng dụng; (3) thay đổi khóa CA; (4) sự kiện có liên quan đến quản lý chu kỳ mã hóa; (5) quá trình xử lý dữ liệu kích hoạt cho khóa bí mật của CA, các bản ghi truy cập vật lý; (6) bảo trì và thay đổi cấu hình hệ thống; (7) bản ghi hủy bỏ các phương tiện chứa khóa, dữ liệu kích hoạt, hoặc thông tin thuê bao.
- 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: (1) hành động truy cập hay thoát ra; (2) tạo và xóa bỏ mật khẩu hay thay đổi đặc quyền của người sử dụng; (3) thay đổi nhân sự;
- Báo cáo về việc truy nhập vào mạng và các hệ thống không được cấp quyền;
- Lỗi trong việc đọc và ghi chứng thư số và kho lưu trữ;
- Thay đổi chính sách tạo chứng thư số, thời gian hợp lệ;
- Lỗi phát sinh liên quan đến chứng thư số và dịch vụ chứng thực chữ ký số do thuê bao thông báo hoặc do Viettel 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, Mobile-CA sẽ tiến hành kiểm tra bất thường dựa theo các cảnh báo và hiện tượng của hệ thống.

5.4.3. ***Thời gian lưu trữ bản ghi kiểm tra***

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

5.4.4. ***Bảo vệ bản ghi kiểm tra***

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

5.4.5. ***Thủ tục sao lưu bản ghi kiểm tra***

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

5.4.6. ***Hệ thống kiểm tra***

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

5.5. Lưu trữ các bản ghi

5.5.1. ***Các loại bản ghi cần lưu trữ***

Mobile-CA sẽ lưu trữ các thông tin sau

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

5.5.2. ***Thời gian lưu trữ***

Các dữ liệu sẽ được lưu trong một khoảng thời gian ít nhất 5 năm kể từ ngày chứng thư số hết hạn hoặc bị hủy bỏ.

5.5.3. ***Bảo vệ dữ liệu lưu trữ***

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

5.5.4. ***Thủ tục thực hiện sao lưu***

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

5.5.5. ***Yêu cầu dán nhãn thời gian cho các bản ghi***

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

5.6. Thay đổi khóa của Mobile-CA

Chứng thư số của Mobile-CA có thể gia hạn với điều kiện tổng thời gian sử dụng của cặp khóa không được vượt qua thời hạn sử dụng tối đa do pháp luật quy định. Cặp khóa mới của Mobile-CA có thể sinh ra khi cần thiết, ví dụ như thay thế cặp khóa cũ đã ngừng sử dụng.

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

5.7. Thỏa thuận và phục hồi sau sự cố

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

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

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

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

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

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

Nếu chứng thư số của Mobile-CA bị thu hồi, các thủ tục sau cần thực hiện:

- Trạng thái thu hồi chứng thư số của Mobile-CA sẽ được công bố trên kho lưu trữ;
- Mọi biện pháp thông báo có thể có đều được sử dụng nhằm cung cấp thông tin về sự kiện thu hồi chứng thư số CA cho các đơn vị thuộc hệ thống của Mobile-CA;
- Mobile-CA sinh cặp khóa mới theo quy định ở phần 4.6, ngoại trừ trường hợp Mobile-CA bị ngừng hoạt động theo điều khoản trong phần 4.8.

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

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

Khi có sự cố do yếu tố tự nhiên hay con người gây ra làm ngừng hoạt động hệ thống tạm thời hoặc kéo dài, đơn vị giải quyết tình trạng khẩn cấp của Mobile-CA (Mobile-CA Emergency Response Team) có nhiệm vụ thực hiện quy trình phục hồi sau sự cố.

Mobile-CA có khả năng phục hồi các hoạt động cơ bản sau 24 (hai mươi bốn) giờ sau sự cố với mức tối thiểu sau:

- Phát hành chứng thư số;
- Thu hồi chứng thư số;
- Công bố thông tin thu hồi.

Cơ sở dữ liệu dùng cho phục hồi sau sự cố được đồng bộ với hệ thống đang vận hành trong khoảng thời gian cho phép. Các thiết bị sử dụng cho kế hoạch phục hồi được bảo vệ theo quy định ở phần 5.1.1.

Mobile-CA bảo quản các thiết bị phần cứng và sao lưu dự phòng tại khu vực quản lý trang thiết bị phục hồi sau sự cố. Khóa bí mật của Mobile-CA được sao lưu vào bảo quản cho nhiệm vụ phục hồi sau thảm họa theo quy định ở phần 6.2.4.

5.8. Kết thúc hoạt động của Mobile-CA hoặc Viettel-RA

Mobile-CA sẽ thông báo khi Mobile-CA hoặc một Viettel-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, Mobile-CA sẽ thực hiện quy trình chấm dứt nhằm giảm thiểu các thiệt hại tới thuê bao, người nhận. Quy trình này có thể bao gồm các bước sau:

- Cung cấp thông tin về tình trạng chấm dứt hoạt động của Mobile-CA cho thuê bao và người nhận;
- Chịu chi phí cho các thông báo này;
- Thực hiện các thủ tục cần thiết nhằm thu hồi chứng thư số của Mobile-CA.
- Tiếp tục duy trì hệ thống lưu trữ các thông tin của Mobile-CA theo quy định của CPS này;
- Tiếp tục duy trì hệ thống hỗ trợ dịch vụ cho thuê bao;
- Tiếp tục duy trì hệ thống dịch vụ thu hồi, như CRL, OCSP.
- Tiến hành thu hồi các chứng thư số chưa bị thu hồi nếu thấy cần thiết.
- Hoàn phí cho thuê bao nếu chưa kết thúc hợp đồng;
- Hủy khóa bí mật của Mobile-CA và các thiết bị chứa khóa bí mật.
- Chuyển giao dịch vụ Mobile-CA cho đơn vị khác nếu có.

6. CÁC VẤN ĐỀ AN TOÀN KỸ THUẬT

6.1. Sinh cặp khóa và vấn đề cài đặt

6.1.1. *Sinh cặp khóa*

Quá trình sinh cặp khóa cho Mobile-CA được thực hiện bởi những người tin cậy, tiến hành trên các hệ thống an toàn và đảm bảo tính mật mã bền vững cho cặp khóa sinh ra. Thủ tục sinh khóa sẽ được ghi lại, lưu thời gian thực hiện và ký xác nhận của tất cả những người tham gia. Các dữ liệu này được lưu trữ, kiểm tra và theo dõi trong khoảng thời gian thích hợp do Mobile-CA quyết định.

Yêu cầu tối thiểu cho thiết bị mật mã sinh và lưu trữ khóa phải đạt tiêu chuẩn FIPS 140-2 level 3 theo Quyết định 06/2015/TT-BTTTT ngày 23/03/2015. Các khóa của Mobile-CA được sinh và lưu trữ trong các thiết bị mật mã phần cứng này và phải sao lưu dự phòng. Khóa gốc của Mobile-CA có thể dùng cho ký chứng thư số, CRL và ký ngoại tuyến danh sách chứng thư số bị thu hồi.

Cặp khóa của Mobile-CA được đặt tại môi trường bảo vệ an toàn có phương án sao lưu và phục hồi khóa.

6.1.2. *Chuyển giao khóa bí mật tới thuê bao*

Khi thuê bao tự thực hiện sinh cặp khóa và gửi khóa công khai tới Mobile – CA trong đăng ký chứng thư số, việc phân phối khóa bí mật tới thuê bao là không cần thiết.

Khi cặp khóa của thuê bao do Mobile-CA sinh ra bằng các thiết bị phần cứng hay smartcard, các thiết bị này cần phân phối tới thuê bao thông qua dịch vụ chuyển phát thương mại có dán nhãn đảm bảo. Dữ liệu dùng để kích hoạt các thiết bị này cần gửi qua kênh truyền độc lập khác. Các hoạt động phân phối này được Mobile-CA theo dõi và lưu lại.

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

Thuê bao gửi khóa công khai tới Mobile-CA thông qua phương tiện điện tử được quy định theo chuẩn yêu cầu chứng thư số PKCS#10 CSR hoặc phải bảo vệ đường truyền gói dữ liệu đã ký gửi đi theo chuẩn SSL. Khi cặp khóa được Mobile-CA tạo, điều kiện này là không cần thiết.

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

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

6.1.5. *Kích thước khóa*

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

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

Không có quy định.

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

Xem trong phần 7.1.2.1.

6.2. Bảo vệ khóa bí mật

Mobile-CA triển khai giải pháp tích hợp về vật lý, logic và thủ tục nhằm đảm bảo tính an toàn cho khóa bí mật của Mobile-CA.

Thuê bao được yêu cầu ký cam kết thực hiện các biện pháp cần thiết nhằm chống lại nguy cơ mất, để lộ, sửa đổi hoặc sử dụng trái phép khóa bí mật của thuê bao.

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

Mobile-CA sử dụng thiết bị mật mã phần cứng để sinh khóa và lưu trữ khóa bí mật gốc của CA. Theo yêu cầu tối thiểu, thiết bị này phải đạt tiêu chuẩn FIPS 140-2 level 3.

6.2.2. *Đa kiểm soát khóa bí mật*

Cơ chế kiểm soát khóa bí mật của Mobile-CA là cơ chế chia sẻ mã theo chuẩn quốc tế, cơ chế này tách dữ liệu kích hoạt khóa bí mật thành các phần khác nhau (n), các phần được giữ bởi các đối tượng khác nhau.

Để kích hoạt khóa cần ít nhất một số lơn hơn 1 (m) mảnh khóa (m =< n).

Tại Mobile – CA, m >= 2.

6.2.3. *Ủy thác giữ khóa bí mật*

Khóa bí mật của Mobile-CA không được ủy thác.

Khóa bí mật của thuê bao được ủy thác theo điều khoản phần 4.11.

6.2.4. *Sao lưu khóa bí mật*

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

6.2.5. *Lưu trữ khóa bí mật*

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

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

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

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

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

6.2.8. *Phương pháp kích hoạt sử dụng khóa bí mật*

Tất cả các thành phần tham gia Mobile-CA cần phải bảo vệ dữ liệu dùng cho kích hoạt khóa bí mật khỏi bị mất, đánh cắp, sửa đổi, để lộ hoặc sử dụng trái phép.

Mobile-CA sẽ thống nhất với thuê bao phương pháp kích hoạt sử dụng khóa bí mật cho từng loại chứng thư số cụ thể trong Hợp đồng dịch vụ.

6.2.9. *Phương pháp hủy khóa bí mật*

Trong trường hợp cặp khóa của Mobile-CA cần phải được hủy, Mobile-CA sẽ thực hiện việc hủy bỏ một cách triệt để, đảm bảo cặp khóa sau khi bị hủy không thể được khôi phục hoặc sử dụng bằng bất cứ hình thức nào.

Thiết bị mật mã an toàn được hủy vật lý theo hướng dẫn của nhà sản xuất, theo chuẩn do Bộ Thông tin và Truyền thông ban hành trước khi ngừng lưu trữ.

6.2.10. *Đánh giá thiết bị mật mã*

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

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

6.3.1. *Lưu trữ khóa công khai*

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

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

Thời gian hoạt động của chứng thư số được bắt đầu từ thời điểm phát hành được ghi trong thuộc tính của chứng thư số và kết thúc tại thời điểm hết hạn có đề cập trong chứng thư số ngoại trừ trường hợp chứng thư số bị thu hồi trước thời hạn. Thời gian hoạt động của cặp khóa bằng thời gian hoạt động của chứng thư số tương ứng, ngoại trừ trường hợp chúng được dùng để giải mã và kiểm tra chữ ký.

Thời gian hoạt động của cặp khóa trong chứng thư số Mobile-CA tuân theo quy định của Bộ Thông tin và Truyền thông.

6.4. Dữ liệu kích hoạt

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

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

- Được một cá nhân tạo ra;
- Có ít nhất tám ký tự;
- Có ít nhất một ký tự là chữ cái và một ký tự là chữ số;
- Có ít nhất một ký tự chữ thường;
- Một ký tự bất kỳ không lặp lại từ 3 lần trở lên;

- Không trùng tên với tên của người vận hành;
- Không chứa một phần tên trong tên của người vận hành;

6.4.2. Bảo vệ dữ liệu kích hoạt

Mobile-CA khuyến cáo thuê bao tuân theo các yêu cầu trên. Ngoài ra để tăng cường an toàn, Mobile-CA khuyến khích sử dụng các cơ chế đa xác thực (thiết bị và passphrase, sinh trắc và thiết bị, 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, Mobile – CA sử dụng các phương pháp đảm bảo không để bị mất mát, đánh cắp, sửa đổi, để lộ hoặc sử dụng trái phép khóa bí mật.

6.4.3.2. Hủy dữ liệu kích hoạt

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

6.5. An toàn hệ thống máy tính

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

Hệ thống mạng của Mobile-CA được tách biệt khỏi các hệ thống khác, được ngắt offline và cần truy cập vật lý để vận hành và sử dụng. Các thành phần trong hệ thống mạng của Mobile-CA được phân chia theo khu vực, có các thiết bị kiểm soát, phát hiện và ngăn chặn truy cập trái phép như firewall, IDS, IPS.

Mobile-CA yêu cầu mật khẩu cần được thay đổi định kỳ và tuân theo tiêu chuẩn an toàn về mật khẩu, bao gồm độ dài tối thiểu, kết hợp giữa chữ cái, chữ số và ký tự đặc biệt.

Mọi truy cập vật lý trực tiếp vào hệ thống mạng của Mobile-CA do người tin cậy thực hiện. Các thao tác truy cập được kiểm soát giới hạn theo nhiệm vụ, chức năng của từng vị trí.

6.5.2. *Đánh giá an toàn*

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

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

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

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

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

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

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

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

6.7. Quản lý an toàn mạng

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

6.8. Dán nhãn thời gian

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

7. ĐẶC TẢ CHỨNG THƯ SỐ, CRL VÀ OCSP

7.1. Thành phần của chứng thư số

Chứng thư số có định dạng X.509 phiên bản 3 (1997) và RFC 5280 - 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:

Trường	*Giá trị hoặc yêu cầu*
Serial Number	Giá trị duy nhất được gán cho mỗi tên phân biệt (DN). Giá trị này được điều khiển bởi hệ thống máy chủ của Mobile-CA và được kiểm soát theo quy tắc đặt giá trị serial number do Mobile-CA quy định.
Signature Algorithm	Số hiệu của thuật toán dùng để ký chứng thư số (Xem phần 7.1.3)
Issuer DN	Xem phần 7.1.4
Valid From	Thời gian được tính theo chuẩn thời gian quốc tế UTC. Giá trị thời gian được ghi theo định dạng trong RFC 5280.
Valid To	Thời gian được tính theo chuẩn thời gian quốc tế UTC. Giá trị thời gian được ghi theo định dạng trong RFC 5280.
Subject DN	Xem phần 7.1.4
Subject Public Key	Lưu trữ theo định dạng ghi trong RFC 5280.

Signature	Chữ ký số được tạo và lưu theo định dạng trong RFC 5280.

Bảng 2 – Thành phần chứng thư số

7.1.1. Số hiệu phiên bản

Chứng thư số của Mobile-CA có thể là X.509 phiên bản 1 hoặc phiên bản 3. Chứng thư số của thuê bao phải là X.509 phiên bản 3.

7.1.2. *Các thành phần mở rộng*

7.1.2.1. Cách sử dụng khóa (Key Usage)

Các giá trị của trường "Key Usage" trong chứng thư số X.509 phiên bản 3 phải tuân theo quy định trong RFC 5280.

7.1.2.2. *Phần mở rộng của chính sách chứng thư (Certificate Policies Extension)*

Phần mở rộng của chính sách chứng thư không được sử dụng trong chứng thư số của thuê bao.

7.1.2.3. Tên thay thế của thuê bao (Subject Alternative Names)

Trường subjectAltName trong chứng thư số X.509 phiên bản 3 khi sử dụng phải tuân theo quy định trong RFC 5280.

7.1.2.4. Các ràng buộc cơ bản (Basic Constraints)

Không có quy định

7.1.2.5. Cách sử dụng khóa mở rộng (Extended Key Usage)

Chứng thư số của Mobile-CA không sử dụng trường này.

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

7.1.2.6. 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.

7.1.2.7. Định danh khóa cho Mobile-CA

Sẽ xác định sau, theo quy định của RootCA.

7.1.2.8. Định danh khóa cho thuê bao

Sẽ xác định sau, theo quy định của RootCA.

7.1.3. *Số hiệu thuật toán*

Chứng thư số của Mobile – CA sử dụng các thuật toán:

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 Mobile-CA chính thức đi vào hoạt động.

7.1.7. *Sử dụng các ràng buộc quy chế mở rộng*

Không có quy định.

7.1.8. *Cú pháp và ngữ nghĩa quy chế*

Không có quy định.

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

Không có quy định.

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

CRL cần chứa các giá trị sau đây

Trường	*Giá trị hoặc yêu cầu*
Version	Xem phần 7.2.1
Signature Algorithm	Thuật toán dùng để ký danh sách chứng thư số bị thu hồi. Mobile-CA sử dụng thuật toán sau theo chuẩn RFC 3279. sha256withRSAEncryption (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.

Bảng 3 – Thành phần của CRL

7.2.1. *Số hiệu phiên bản của CRL*

Mobile-CA hỗ trợ định dạng CRL theo phiên bản 1 hoặc phiên bản 2 của RFC 5280.

7.2.2. *CRL và các mở rộng*

Không có quy định.

7.3. Thành phần OCSP

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

7.3.1. *Số hiệu phiên bản của OCSP*

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

7.3.2. *Các mở rộng OCSP*

Không có quy định.

8. KIỂM ĐỊNH TÍNH TUÂN THỦ VÀ CÁC ĐÁNH GIÁ

8.1. Tần suất đánh giá

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

8.2. Đơn vị thực hiện đánh giá chất lượng

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

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

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

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

8.4. Các nôi dung cần đánh giá

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

8.5. Xử lý các thiếu sót

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

8.6. Kết quả

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

9. CÁC VẤN ĐỀ KINH DOANH VÀ LUẬT PHÁP

9.1. Lệ phí

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

Thuê bao phải trả chi phí khi xin cấp, gia hạn, khôi phục chứng thư số cho Mobile-CA.

9.1.2. *Lệ phí sử dụng chứng thư số*

Thuê bao của Mobile-CA không phải trả chi phí khi truy cập kho chứng thư số hay dịch vụ cung cấp thông tin chứng thư số trực tuyến cho người nhận.

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*

Mobile-CA 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 Mobile-CA.

9.1.5. *Quy chế hoàn trả phí*

Mobile-CA sẽ đưa ra phạm vi cho việc áp dụng chính sách hoàn trả phí. Chính sách này sẽ được đưa lên website (bao gồm một danh sách các kho dữ liệu), hoặc thỏa thuận trong Hợp đồng dịch vụ.

9.2. Trách nhiệm tài chính

9.2.1. *Phạm vi bảo hiểm*

Mobile-CA sẽ bảo hiểm với các mức độ khác nhau đối với các lỗi sai hay thiếu sót thông qua các chương trình bảo hiểm của các công ty bảo hiểm hoặc tự cam kết bảo hiểm.

9.2.1.1. Các trường hợp Mobile-CA đền bù bảo hiểm và mức đền bù bảo hiểm

Mobile-CA đền bù bảo hiểm cho các trường hợp sau:

- Lỗi do Mobile-CA gây ra, bao gồm lỗi kỹ thuật khi phát hành chứng thư số theo trách nhiệm của Mobile-CA.
- Các mức đền bù bảo hiểm và trách nhiệm thực hiện bảo hiểm của Mobile-CA được thực hiện theo *Hợp đồng dịch vụ* tùy từng loại chứng thư số.

9.2.1.2. Các trường hợp không được hưởng đền bù bảo hiểm

Mobile-CA sẽ không chịu trách nhiệm trong các trường hợp:

- Sử dụng chứng thư số không được đề cập trong CPS này;
- Giả mạo chứng thư số;
- Sử dụng, cấu hình thiết bị không đúng, không nằm trong trách nhiệm của Mobile-CA được sử dụng trong quá trình xử lý chứng thư số;
- Khóa bí mật bị mất, bị phá hủy do khách hàng;

- Thuê bao đánh mất hoặc để lộ code PIN bảo vệ khóa bí mật;

9.2.2. ***Các tài sản khác***

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

9.3. Bảo mật các thông tin kinh doanh

9.3.1. ***Phạm vi của bảo mật thông tin***

Những dữ liệu sau của thuê bao, theo phần 9.3.2 sẽ được đảm bảo tính mật và riêng tư ("thông tin mật/riêng tư"):

- Các dữ liệu ứng dụng CA, được phê chuẩn hoặc không phê chuẩn;
- Các dữ liệu ứng dụng chứng thư số;
- Các dữ liệu chuyển đổi (dữ liệu đầy đủ và các dữ liệu kiểm toán của quá trình chuyển đổi);
- Các dữ liệu kiểm định được tạo hoặc lưu giữ bởi Mobile-CA hoặc một thuê bao;
- Các báo cáo kiểm định tạo bởi Mobile-CA hay thuê bao (cho việc đánh giá những báo cáo này), hoặc những kiểm định viên (nội bộ hoặc bên ngoài)
- Các dự án khôi phục do tai nạn hay khôi phục sau sự cố;
- Quản lý mức độ an ninh trong hoạt động của phần cứng, phần mềm, các quản trị viên của dịch vụ chứng thư số 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 Mobile-CA cùng các thông tin chứa bên trong chúng không được coi là các thông tin mật/riêng tư. Các thông tin mật/riêng tư trong phần 9.3.1 sẽ không được coi là riêng tư hoặc không được coi là bí mật nếu pháp luật có quy định khác.

9.3.3. ***Trách nhiệm bảo vệ thông tin mật***

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

9.4. Tính riêng tư của thông tin cá nhân

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

Mobile-CA sẽ tiến hành triển khai chính sách đảm bảo tính riêng tư của thông tin cá nhân theo quy định của pháp luật. Mobile-CA sẽ không tiết lộ tên hay bất cứ một thông tin nào về các ứng dụng chứng thư số của thuê bao cho bên thứ 3.

9.4.2. ***Những thông tin coi là riêng tư***

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

9.4.3. ***Thông tin không được coi là riêng tư***

Tất cả các thông tin được công khai trong chứng thư số được coi như không phải là thông tin riêng tư.

9.4.4. *Trách nhiệm bảo vệ thông tin riêng tư*

Những người tham gia vào dịch vụ Mobile-CA nhận các thông tin mật phải đảm bảo tính mật cho những thông tin này không bị tiết lộ với bên thứ 3 và phải tuân theo quy định của pháp luật trong phạm vi quyền hạn của mình.

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

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

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

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

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

9.4.7. *Các trường hợp làm lộ thông tin khác*

9.5. Quyền sở hữu trí tuệ

Cần xác định rõ quyền sở hữu trí tuệ giữa các thành phần tham gia dịch vụ Mobile-CA

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

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

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

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

9.5.2. *Quyền sở hữu trong CPS*

Các thành phần tham gia dịch vụ Mobile-CA chấp nhận rằng Mobile-CA có quyền sở hữu trí tuệ đối với CPS và các điều khoản ghi trong CPS này.

9.5.3. *Quyền sở hữu tên*

Người đăng ký chứng thư số có quyền sở hữu đối với thương hiệu, tên dịch vụ trong các ứng dụng chứng thư số, và với tên phân biệt (distinguished name) trong chứng thư số cấp.

9.5.4. *Quyền sở hữu khóa và các tài liệu của khóa*

Cặp khóa tương ứng với chứng thư số của Mobile-CA và thuê bao là tài sản của Mobile-CA và thuê bao, được lưu trữ và bảo vệ theo quy định của pháp luật về quyền sở hữu trí tuệ.

9.6. Vấn đề đại diện và bảo lãnh

9.6.1. *Đại diện của Mobile-CA và vấn đề bảo lãnh*

Các dịch vụ Mobile-CA bảo đảm:

- Không có những thông tin sai lệch với thực tế trong chứng thư số;
- Không có sai sót ở các thông tin trong chứng thư số;
- Chứng thư số của Mobile-CA phù hợp với yêu cầu trong CPS;
- Dịch vụ thu hồi chứng thư số và sử dụng kho lưu trữ phù hợp với tiêu chuẩn trong CPS.

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

9.6.2. *Đại diện của Viettel-RA và vấn đề bảo lãnh*

Các Mobile-CA bảo đảm:

- Không có những thông tin sai lệch với thực tế trong chứng thư số;
- Không có sai sót ở các thông tin trong chứng thư số;
- Những chứng thư số của Viettel-RA tuân theo các yêu cầu trong CPS này;
- Dịch vụ thu hồi chứng thư số và sử dụng kho lưu trữ phù hợp với tiêu chuẩn trong CPS này.

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

9.6.3. *Đại diện cho thuê bao và vấn đề bảo lãnh*

Thuê bao cam kết rằng:

- Mỗi chữ ký số được tạo sử dụng khóa bí mật tương ứng với khóa công khai liệt kê trong chứng thư số là chữ ký số của thuê bao. Chứng thư số 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 bí mật được bảo vệ và người không có thẩm quyền không thể truy cập vào khóa này.
- Tất cả các cam kết được đưa ra bởi thuê bao trong ứng dụng chứng thư số là đúng sự thật.
- Tất cả những thông tin cung cấp bởi thuê bao và chứa bên trong chứng thư số là đúng sự thật.
- Chứng thư số được sử dụng cho các mục đích hợp pháp và tuân theo những yêu cầu trong CPS này.
- Thuê bao là người dùng cuối và không phải là một CA, không được phép sử dụng khóa bí mật kết hợp với bất kì khóa công khai nào được liệt kê trong chứng thư số cho các mục đích ký số, hay đưa ra CRL, như là một CA.

Hợp đồng dịch vụ giữa Mobile-CA với thuê bao có thể có thêm các thỏa thuận 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 Mobile-CA và người nhận có thể bao gồm thêm các tuyên bố và cam kết khác.

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

Không có qui định.

9.7. Từ chối bảo lãnh

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

9.8. Giới hạn trách nhiệm pháp lý

Trong giới hạn của luật pháp, hợp đồng thuê bao và người nhận có thể giới hạn khả năng trách nhiệm pháp lý của Mobile-CA. Việc giới hạn trách nhiệm pháp lý bao gồm cả việc loại bỏ các thiệt hại ngẫu nhiên, gián tiếp, hay những thiệt hại nghiêm trọng.

Trách nhiệm pháp lý của thuê bao và Mobile-CA sẽ được thiết lập trong *Hợp đồng dịch vụ*.

9.9. Bồi thường

9.9.1. *Vấn đề bồi thường của thuê bao*

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

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

Hợp đồng dịch vụ có thể có thêm các thỏa thuận khác.

9.9.2. *Vấn đề bồi thường của người nhận*

Khi được pháp luật cho phép, Mobile-CA có quyền yêu cầu người nhận bồi thường thiệt hại trong các trường hợp:

- Lỗi của người nhận trong việc thực thi nghĩa vụ với một bên đối tác;

- Sự tin cậy của người nhận về một chứng thư số không được đáp ứng trong một số trường hợp;
- Lỗi của người nhận trong việc kiểm tra trạng thái của chứng thư số để xác định chứng thư số đã hết hạn hay bị thu hồi.

Hợp đồng với người nhận sẽ bao gồm thêm một số nghĩa vụ khác.

9.10. Thời hạn và kết thúc

9.10.1. *Thời hạn*

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

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

9.10.2. *Kết thúc*

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

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

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

9.11. Thông báo cho các bên liên quan

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

9.12. Những điều sửa đổi

9.12.1. *Thủ tục sửa đổi*

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

9.12.2. *Cơ chế và thời gian thông báo*

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

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

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

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

9.12.2.1. Thời điểm có hiệu lực

Thời điểm có hiệu lực của việc sửa đổi là 15 ngày kể từ ngày được công bố trên kho lưu trữ của dịch vụ Mobile-CA. Bất kỳ ai tham gia vào dịch vụ Mobile-CA cũng có quyền đề xuất ý kiến tới Mobile-CA cho đến lúc hết thời gian sửa đổi.

9.12.2.2. Cơ chế xử lý đề xuất

Mobile-CA sẽ xem xét tất cả các đề xuất liên quan đến vấn đề sửa đổi bổ sung và có thể:

- Cho phép các đề xuất có hiệu lực mà không cần sửa đổi;
- Sửa đổi các đề xuất và tái bản nếu cần;
- Hủy bỏ những đề xuất sửa đổi.

Mobile-CA có quyền hủy bỏ các đề xuất sửa đổi, và đưa ra ghi chú trong tài liệu của Mobile-CA. Những sửa đổi có hiệu lực sau khi hết hạn sửa đổi.

9.12.3.*Các trường hợp OID thay đổi*

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

9.13. Các điều khoản tranh chấp

9.13.1.*Tranh chấp giữa Viettel, đối tác và thuê bao*

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

9.13.2.*Tranh chấp với thuê bao hay người nhận*

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

9.14. Áp dụng luật

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

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

9.15. Chấp hành theo hệ thống luật phù hợp

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

9.16. Các điều khoản khác

9.16.1.*Điều khoản thỏa thuận chung*

Không có quy định.

9.16.2.*Trách nhiệm*

Trách nhiệm của các bên được quy định và giới hạn theo hợp đồng đã ký kết.

9.16.3.*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 quy định của pháp luật hoặc quyết định của cơ quan nhà nước có thẩm quyền thì phần còn lại của Quy chế vẫn có hiệu lực.

9.16.4.*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.

9.16.5.*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 Mobile- CA.

9.17. Yêu cầu kỹ thuật tối thiểu để sử dụng dịch vụ Viettel-CA

Điều kiện sử dụng dịch vụ trên môi trường tối thiểu như sau:

Dịch vụ	Yêu cầu kỹ thuật	
	Tối thiểu	Khuyến nghị
USB Token	Windows 8 macOS Sierra 10.12 Ubuntu 10	Windows 10 trở lên macOS Catalina 10.15 trở lên Ubuntu 12 trở lên
SIM CA	iOS 12 Android 7	iOS 14 trở lên Android 11 trở lên

*Trường hợp Khách hàng sử dụng môi trường không đáp ứng yêu cầu kỹ thuật tối thiểu, Viettel sẽ không chịu trách nhiệm về các rủi ro, hỏng hóc liên quan tới bảo mật, hiệu năng và chức năng của dịch vụ.

Chú ý: Thuê bao di động sử dụng giải pháp SIM CA cần sử dụng các gói dịch vụ di động và thiết bị di động hỗ trợ gửi, nhận tin nhắn SMS.

9.18. Thông báo thay đổi và sự cố đến NEAC

Trường hợp xảy ra sự cố, Viettel có trách nhiệm thông báo đến NEAC chậm nhất 01 ngày.

Trường hợp có thay đổi về nhân sự, mô hình, công nghệ, Viettel có trách nhiệm thông báo đến NEAC trong vòng 1 tuần.

Định kỳ báo cáo tình hình triển khai dịch vụ là 06 tháng.

9.19. Các điều khoản khác

Không có quy định.

PHỤ LỤC

Danh mục định nghĩa và thuật ngữ viết tắt

Thuật ngữ	*Giải thích*
24 x 7	24 giờ/ngày và 7 ngày/tuần
Bộ TTTT	Bộ Thông tin và Truyền thông nước Cộng hòa xã hội chủ nghĩa Việt Nam
CA	Certificate Authority – Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.
Chữ ký số	là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng theo đó người có được thông điệp dữ liệu ban đầu và khoá công khai của người ký có thể xác định được chính xác: *a) Việc biến đổi nêu trên được tạo ra bằng đúng khoá bí mật tương ứng với khoá công khai trong cùng một cặp khóa;* *b) Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.*
Chứng thư số	là một dạng chứng thư số điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp cho thuê bao.
Chứng thư số có hiệu lực	là chứng thư số chưa hết hạn, không bị tạm dừng hoặc bị thu hồi.
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.
Dịch vụ chứng thực chữ ký số	là một loại hình dịch vụ chứng thực chữ ký điện tử, do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp. Dịch vụ chứng thực chữ ký số bao gồm: *a) Tạo cặp khóa bao gồm khóa công khai và khóa bí mật cho thuê bao;* *b) Cấp, gia hạn, tạm dừng, phục hồi và thu hồi chứng thư số của thuê bao;* *c) Duy trì trực tuyến cơ sở dữ liệu về chứng thư số;*

	d) Những dịch vụ khác có liên quan theo quy định.
Hệ thống mật mã không đối xứng	là hệ thống mật mã có khả năng tạo được cặp khóa bao gồm khoá bí mật và khoá công khai.
Hợp đồng dịch vụ	Hợp đồng cung cấp và sử dụng dịch vụ chứng thực chữ ký số công cộng giữa Viettel – CA và người sử dụng dịch vụ.
Khoá	là một chuỗi các số nhị phân (0 và 1) dùng trong các hệ thống mật mã.
Khóa bí mật	là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được dùng để tạo chữ ký số.
Khóa công khai	là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được sử dụng để kiểm tra chữ ký số được tạo bởi khoá bí mật tương ứng trong cặp khoá.
Ký số	là việc đưa khóa bí mật vào một chương trình phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu.
Người ký	là thuê bao dùng đúng khoá bí mật của mình để ký số vào một thông điệp dữ liệu dưới tên của mình.
Người nhận	là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng chứng thư số của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.
OCSP	Online Certificate Status Protocol - là giao thức cho phép kiểm tra trạng thái chứng thư số trực tuyến.
PKI	Public Key Infrastructure – Hạ tầng khóa công khai.
RA	Registration Authority – Tổ chức tiếp nhận đăng ký và xác thực thông tin của người sử dụng dịch vụ.
Tạm dừng chứng thư số	là làm mất hiệu lực của chứng thư số một cách tạm thời từ một thời điểm xác định.
Thu hồi chứng thư số	là làm mất hiệu lực của chứng thư số một cách vĩnh viễn từ một thời điểm xác định.
Thuê bao	là tổ chức, cá nhân được cấp chứng thư số, chấp nhận chứng thư số và giữ khoá bí mật tương ứng với khoá công khai ghi trên chứng thư số được cấp đó.
Tổ chức cung cấp dịch vụ chứng	là tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử thực hiện hoạt động cung cấp dịch vụ chứng thực chữ ký số.

thực chữ ký số	
Viettel	Tập đoàn Công nghiệp - Viễn thông Quân đội
Mobile-CA	Dịch vụ chứng thực chữ ký số công cộng do Tập đoàn Công nghiệp - Viễn thông Quân đội (Viettel) hoặc/và Tổng Công ty Viễn thông Viettel cung cấp với tư cách là nhà cung cấp dịch vụ chứng thực chữ ký số công cộng.
Viettel-RA	Tổ chức tiếp nhận yêu cầu cung cấp dịch vụ và xác thực thông tin thuê bao Mobile-CA ủy quyền.
Xác thực định danh	là hoạt động nhằm chứng minh thông tin định danh của thuê bao, người yêu cầu cấp chứng thư số.