TỔNG CÔNG TY VIỄN THÔNG MOBIFONE

QUY CHẾ CHỨNG THỰC
MOBIFONECA

Phiên bản:

OID:

MOBIFONECA

MỤC LỤC

I. Giới thiệu.

1.1 Tổng quan

Tài liệu này là quy chế chứng thực chữ ký số của MobiFoneCA. Tài liệu nêu rõ những Quy chế của cơ quan chứng thực MobiFoneCA sử dụng trong quá trình cung cấp dịch vụ chứng thực chữ ký số công cộng bao gồm phát hành, quản lý, thu hồi và cấp lại chứng thư số.

Tài liệu này phù hợp với chuẩn RFC 3647 (IETF Certificate Policy and Certification Practice Statement)

1.2 Tên tài liệu và nhận dạng

Tài liệu này được xác định bởi bộ định dạng đối tượng (OID).

OID của Quy chế chứng thực này là 1.3.6.1.4.1.30339.1.x.3, được xác định theo quy định của Trung tâm Chứng thực chữ ký số quốc gia có sử dụng dạng đánh số chuẩn của IANA như sau:

1.3.6.1.4.1.30339.[codeTypeCA].[codeCA].[codeCPS]

Trong đó, codeTypeCA được đặt là 1 (công cộng) và codeCA được xác định khi MobiFoneCA đăng ký với Bộ Thông tin và Truyền thông, codeCPS được gán là 3.

Tên tài liệu: Khung quy chế chứng thực và chính sách chứng thư của MobiFoneCA

1.3 Các bên tham gia

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng là các tổ chức cung cấp dịch vụ chứng thực chữ ký số cho cơ quan, tổ chức, cá nhân sử dụng trong các hoạt động công cộng. Hoạt động của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng là hoạt động nhằm mục đích kinh doanh.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng là tổ chức cung cấp dịch vụ chứng thực chữ ký số cho các cơ quan, tổ chức, cá nhân có cùng tính chất hoạt động hoặc mục đích công việc và được liên kết với nhau thông qua điều lệ hoạt động hoặc văn bản quy phạm pháp luật quy định cơ cấu tổ chức chung hoặc hình thức liên kết, hoạt động chung. Hoạt động của tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng là hoạt động nhằm phục vụ nhu cầu giao dịch nội bộ và không nhằm mục đích kinh doanh.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia (Root Certification Authority) là tổ chức cung cấp dịch vụ chứng thực chữ ký số cho các tổ chức cung cấp dịch vụ chữ ký số công cộng. Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia là duy nhất.

Trung tâm Chứng thực chữ ký số quốc gia là đơn vị có chức năng giúp thực hiện công tác quản lý nhà nước về lĩnh vực chứng thực chữ ký số; quản lý các tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng và chuyên dùng; cấp phát chứng thư số cho các tổ chức đăng ký cung cấp dịch vụ chứng thư số công cộng; tổ chức các hoạt động thúc đẩy việc sử dụng chữ ký số trong các ứng dụng công nghệ thông tin phục vụ phát triển kinh tế - xã hội trong phạm vi cả nước. Trung tâm Chứng thực chữ ký số quốc gia vận hành hệ thống tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia.

Tổ chức đăng ký chứng thư số (Registration Authorities hay RA) liên hệ trực tiếp với các thuê bao. Họ thực hiện việc nhận dạng và xác thực dữ liệu của người xin cấp chứng thư số dựa trên các giấy tờ hợp pháp (như chứng minh nhân dân, hộ chiếu...), họ có thể khởi tạo, chấp nhận hoặc huỷ bỏ các yêu cầu thay mặt cho Tổ chức cung cấp dịch vụ chứng thực chữ ký số.

Tổ chức đăng ký chứng thư số thực hiện việc đăng ký các thông tin của thuê bao xin cấp chứng thư số:

- Xác thực cá nhân chủ thể đăng ký chứng thư số.
- Kiểm tra tính hợp lệ của thông tin do chủ thể cung cấp.
- Xác nhận quyền của chủ thể đối với những thuộc tính chứng thư số yêu cầu.
- Kiểm tra xem chủ thể có thực sự sở hữu khoá bí mật đang được đăng ký hay không.
- Tạo cặp khoá bí mật/khoá công khai.
- Thay mặt chủ thể thực thể cuối khởi tạo quá trình đăng ký với CA.
- Khởi sinh quá trình khôi phục khoá.
- Phân phối thẻ thông minh chứa khoá bí mật.

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

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

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

1.4 Sử dụng chứng thư số

Trong chứng thư số, trường KeyUsage chứa thông tin về mục đích sử dụng chứng thư số. Thuê bao sử dụng chứng thư số vào các mục đích được quy định bởi trường "Mục đích sử dụng" (KeyUsage) trong chứng thư số.

Mục đích sử dụng không bị cấm bởi phát luật, chính sách chứng thư số của RootCA, chính sách chứng thư số và quy chế chứng thực của MobiFoneCA và thỏa thuận của thuê bao với MobiFoneCA. Chứng thư số MobiFoneCA cấp được phân ra các loại sau đây:

- Chứng thư số cho cá nhân: Là chứng thư số cấp cho cá nhân Thuê bao sử dụng chứng thư số này trong việc ký các ứng dụng, ký email, ký các giao dịch điện tử.

Chứng thư số cho cá nhân có thời hạn không quá 2 năm và không được vượt quá thời hạn của chứng thư số MobiFoneCA.

- Chứng thư số cho cá nhân thuộc tổ chức doanh nghiệp: Là chứng thư số cấp cho cá nhân, trong chứng thư số có thông tin về tổ chức doanh nghiệp mà thuê bao trực thuộc. Thuê bao sử dụng chứng thư số này trong việc ký các ứng dụng, ký email, ký các giao dịch điện tử.

Chứng thư số cho cá nhân thuộc tổ chức doanh nghiệp có thời hạn không quá 2 năm và không được vượt quá thời hạn của chứng thư số MobiFoneCA.

- Chứng thư số cho các tổ chức doanh nghiệp: Thuê bao là tổ chức doanh nghiệp. Thuê bao sử dụng chứng thư số này trong việc ký các ứng dụng, ký email, kê khai thuế điện tử, hải quan điện tử và ký các giao dịch điện tử khác.

Chứng thư số cho tổ chức doanh nghiệp có thời hạn không quá 3 năm và không được vượt quá thời hạn của chứng thư số MobiFoneCA.

Khi thuê bao là cá nhân đăng ký xin cấp chứng thư số thì bản thân thuê bao đứng ra thực hiện đăng ký.

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

- Chứng thư số dùng cho cá nhân.
- Chứng thư số dùng cho tổ chức.
- Chứng thư số dùng cho các dịch vụ.

Chứng thư của MobiFoneCA được phân loại dựa trên mức độ bảo mật và mức độ bảo hiểm đối với từng chứng thư của người dùng đăng ký gồm:

Chứng thư cấp 1: Dịch vụ có chất lượng cao nhất về tính an toàn và cam kết trách nhiệm của nhà cung cấp. Một hợp đồng bảo hiểm sẽ cần thiết cho cam kết trách nhiệm của nhà cung cấp. Chứng thực các chứng thư số cấp 1 dựa trên sự có mặt của người/ đại diện doanh nghiệp xin cấp chứng thư trước khi CA hay RA kiểm định tính hợp pháp. Việc kiểm tra danh tính của người/doanh nghiệp xin cấp chứng thư số dựa trên thủ tục để nhận dạng của cơ quan nhà nước quản lý như giấy chứng minh thư nhân dân, hộ chiếu hay giấy chứng nhận đăng ký kinh doanh (đối với doanh nghiệp). Các khách hàng này thường có giao dịch liên quan trực tiếp đến kinh doanh (thương mại điện tử), giao dịch tiền như các công ty chứng khoán, ngân hàng, thanh toán trực tuyến…

Chứng thư cấp 2: Dịch vụ có chất lượng về tính an toàn và cam kết trách nhiệm của nhà cung cấp. Các khách hàng này sử dụng sản phẩm trong giao dịch hành chính là chủ yếu, ví dụ như kê khai thuế, khai báo hải quan, dùng cho cá nhân, bảo mật thư điện tử…

Chứng thư cấp 3: Dịch vụ không yêu cầu cao về tính an toàn. Đây là các đối tượng khách hàng sử dụng sản phẩm cho các mục dích nghiên cứu thăm dò, giao dịch hành chính nội bộ.

1.5 Quản lý chính sách

1.5.1 Tổ chức quản lý tài liệu

Tên cơ quan: TỔNG CÔNG TY VIỄN THÔNG MOBIFONE

Địa chỉ: Tòa nhà MobiFone, lô VP1, phường Yên Hòa, quận Cầu Giấy, Hà Nội.

Điện thoại: 0936.110.116

E-mail: contact-itc@mobifone.vn

Website: mobifone.vn, mobica.vn

1.5.2 Người liên hệ

Người quản lý tài liệu

Họ và tên: Trần Quốc Việt

Điện thoại: 0903.994.789

Hỗ trợ kỹ thuật:

Họ và tên: Phùng Xuân Chiến

Điện thoại: 0904.669.355

1.5.3 Công nhận sự phù hợp của quy chế chứng thực

Bộ Thông tin và Truyền thông và Tổng công ty Viễn thông MobiFone xác nhận sự phù hợp của quy chế chứng thực này.

1.5.4 Thủ tục phê chuẩn quy chế chứng thực

Tổng công ty Viễn thông MobiFone sẽ phê chuẩn CPS. Mỗi phiên bản của CPS có một bộ định danh đối tượng duy nhất (OID). Các thay đổi, cập nhật của CPS được ghi trong một tài liệu chứa các sửa đổi của CPS hay các thông tin về quá trình cập nhật và được công bố tại https://mobica.vn/cps

Các quá trình xem xét và phê duyệt phải đảm bảo rằng việc này CP-CPS tuân thủ RFC 3647 và các quy định có liên quan.

Khi có sự thay đổi thông tin trong quy chế chứng thực, tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng phải có thông báo bằng văn bản đến Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia và phải được sự đồng ý văn bản của tổ chức cung cấp dịch vụ chứng thực chứ ký số quốc gia đối với các nội dung thay đổi.

Tất cả các phiên bản Quy chế chứng thực dựa trên đó các chứng thư số hợp lệ đang hoặc đã được cấp phát phải được lưu trữ để cung cấp cho các bên tin tưởng khi có yêu cầu. Các phiên bản của Quy chế chứng thực được công bố tại: https://mobica.vn/cps/version/

1.6 Công nhận sự phù hợp của CPS

Bộ Thông tin và Truyền Thông và Tổng công ty Viễn thông MobiFone xác nhận sự phù hợp của quy chế chứng thực này.

1.6.1 Thủ tục phê chuẩn CPS

Tổng công ty Viễn thông MobiFone sẽ phê chuẩn CPS. Mỗi phiên bản của CPS có một bộ định danh đối tượng duy nhất (OID). Các thay đổi, cập nhật của CPS được ghi trong một tài liệu chứa các sửa đổi của CPS hay các thông tin về quá trình cập nhật và được công bố tại https://mobica.vn

Các quá trình xem xét và phê duyệt phải đảm bảo rằng việc này CP-CPS tuân thủ RFC 3647 và các quy định có liên quan.

Khi có sự thay đổi thông tin trong quy chế chứng thực, tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng phải có thông báo bằng văn bản đến Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia và phải được sự đồng ý bằng văn bản của tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia đối với các nội dung thay đổi.

Tất cả các phiên bản Quy chế chứng thực dựa trên đó các chứng thư số hợp lệ đang hoặc đã được cấp phát phải được lưu trữ để cung cấp cho các bên tin tưởng khi có yêu cầu. Các phiên bản của Quy chế chứng thực được công bố tại: https://mobica.vn

1.7 Các Định nghĩa và viết tắt

1.7.1 Các định nghĩa

Thuật ngữ	Giải thích
Chứng thư số MobiFoneCA	Là một dạng chứng thư điện tử do MobiFoneCA số cấp.
Chứng thư số có hiệu lực	Là chứng thư số chưa hết hạn, không bị tạm dừng hoặc bị thu hồi.
Chữ ký số	Là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng theo đó người có được thông diệp dữ liệu ban đầu và khoá công khai của người ký có thể xác định được chính xác: • Việc biến đổi nêu trên được tạo ra bằng đúng khoá bí mật tương ứng với khoá công khai trong cùng một cặp khóa; • Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.
Dịch vụ chứng thực chữ ký số	Là một loại hình dịch vụ chứng thực chữ ký điện tử, do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp. Dịch vụ chứng thực chữ ký số bao gồm: • Tạo cặp khóa bao gồm khóa công khai và khóa bí mật cho thuê bao; • Cấp, gia hạn, tạm dừng, phục hồi và thu hồi chứng thư số của thuê bao; • Duy trì trực tuyến cơ sở dữ liệu về chứng thư số; • Những dịch vụ khác có liên quan theo quy định.
Hệ thống mật mã không đối xứng	Là hệ thống mật mã có khả năng tạo được cặp khóa bao gồm khoá bí mật và khóa công khai.

Thuật ngữ	Giải thích
Khoá	Là một chuỗi các số nhị phân (0 và 1) dùng trong các hệ thống mật mã.
Khóa bí mật	Là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được dùng để tạo chữ ký số.
Khóa công khai	Là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được sử dụng để kiểm tra chữ ký số được tạo bởi khoá bí mật tương ứng trong cặp khoá.
Ký số	Là việc đưa khóa bí mật vào một chương trình phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu.
Người ký	Là thuê bao dùng đúng khoá bí mật của mình để ký số vào một thông điệp dữ liệu dưới tên của mình.
Người nhận	Là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng chứng thư số của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.
Thuê bao	Là tổ chức, cá nhân được cấp chứng thư số, chấp nhận chứng thư số và giữ khoá bí mật tương ứng với khoá công khai ghi trên chứng thư số được cấp đó.
Tạm dừng chứng thư số	Là làm mất hiệu lực của chứng thư số một cách tạm thời từ một thời điểm xác định.
Thu hồi chứng thư số	Là làm mất hiệu lực của chứng thư số một cách vĩnh viễn từ một thời điểm xác định.

1.7.2 Từ viết tắt

ARLs	Authority Revocation Lists
CA	Certificate Authority
CMS	Cryptographic Message Syntax
CP	Certificate Policy

CPS	Certification Practice Statement
CRLs	Certificate Revocation Lists
CRR	Certificate Revocation Request
CSP	Certification Service Provider
DAP	Directory Access Protocol
DES	Data Encryption Standard
DNS	Domain Name System
HTTPS	Secure Hypertext Transaction Standard
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5 Hash Algorithm
OCSP	Online Certificate Status Protocol
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Extended Public Key Infrastructure
RA	Registration Authorities
RFC	Request For Comments
RSA	Rivest Shamir Adleman
S/MIME	Secure Multipurpose Internet Mail Extensions
SHA-1	Secure Hash Standard
SSL	Secure Socket Layer
TLS	Transport Layer Security
X.500	X.500 The ITU-T (International Telecommunication Union-T) standard that establishes a distributed, hierarchical directory protocol organized by country, region, Organization, etc.
X.501	The ITU-T (International TelecommuniCAtion Union-T) standard for use of Distinguished Names in an X.500 directory.
X.509	ITU-T standard for Certificates format

II. Trách nhiệm công bố và lưu trữ

2.1 Lưu trữ

Trung tâm chứng thực MobiFoneCA có trách nhiệm duy trì việc phát hành trực tuyến chứng thư số. Việc lưu trữ được tiến hành trên cả hai nền tảng LDAP và nền tảng web để cung cấp dữ liệu cần thiết cho người dùng như chứng thư số cấp bởi MobiFoneCA hay danh sách thu hồi chứng thư số (CRLs). Các tài liệu lên quan đến dịch vụ của MobiFoneCA (CPS) cũng được cung cấp thông qua giao diện web.

MOBIFONECA lưu trữ và sử dụng thông tin của thuê bao bí mật, an toàn tại ứng dụng quản lý khách hàng CRM sử dụng khai thác nội bộ và chỉ sử dụng thông tin này vào mục đích liên quan đến chứng thư số.

Các thông tin thuê bao được MOBIFONECA lưu trữ đầy đủ, chính xác và cập nhật thông tin của thuê bao phục vụ việc cấp chứng thư số trong suốt thời gian chứng thư số có hiệu lực và trong ít nhất là 05 năm kể từ khi chứng thư số hết hiệu lực.

Danh sách các chứng thư số có hiệu lực, tạm dừng và đã hết hiệu lực được lưu trữ đầy đủ, chính xác và cập nhật cho phép, hướng dẫn người sử dụng Internet truy nhập trực tuyến 24 giờ trong ngày và 7 ngày trong tuần qua các đường dẫn được công bố tại mục 2.2. Công bố thông tin.

Toàn bộ các 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 được MobiFoneCA lưu trữ 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 chứng thư

Trung tâm chứng thực MobiFoneCA thực hiện lưu trữ trực tuyến an toàn gồm:

- Chứng thư số của MobiFoneCA.
- Danh sách thu hồi chứng thư số.
- Chứng thư số do MobiFoneCA đã phát hành.
- Bản sao CP/CPS của MobiFoneCA và các phiên bản trước của các tài liệu này.
- Các thông tin liên quan khác.

Các kho lưu trữ trực tuyến được công bố tại địa chỉ URL sau:

http://crl.mobica.vn/mobifoneca.crl

Địa chỉ công bố truy cập trả lời OCSP: http://ocsp.mobica.vn

2.3 Thời gian, tần số công bố thông tin

Chứng thư số MobiFoneCA sẽ được công bố ngay sau khi có sự chấp nhận của thuê bao phù hợp với các thủ tục mà MobiFoneCA yêu cầu.

Tần số công bố các dữ liệu thu hồi là: hàng ngày.

Tần số công bố CP/CPS: Một phiên bản mới của CP/CPS sẽ được công bố ngay sau khi được phê chuẩn và phiên bản cũ sẽ được lưu trữ trong kho lưu trữ một cách an toàn.

MobiFoneCA công bố và duy trì thông tin 24 giờ trong ngày và 7 ngày trong tuần các thông tin quy định tại Mục 2.2 và cập nhật các thông tin này trong vòng 24 giờ khi có thay đổi.

2.4 Kiểm soát truy cập thông tin

MobiFoneCA không yêu cầu bất kỳ một xác thực để truy cập đối với bên thứ 3 khi truy cập vào các thông tin thu hồi (CRL), chứng thư số của MobiFoneCA, và các tài liệu (CP/CPS) của MobiFoneCA thông qua địa chỉ công bố truy cập trực tuyến.

MobiFoneCA sử dụng biện pháp kỹ thuật để hạn chế những hành động thêm, xóa hay sửa kho lưu trữ. Các hành động truy cập trái phép sẽ bị xử lý theo quy định của công ty và pháp luật.

III. Nhận dạng và Xác thực yêu cầu cấp chứng thư số

3.1 Đặt tên trong chứng thư số

Chứng thư số chứa một tên để phan biệt với các chứng thư số khác (Distinguished Names – DN) theo chuẩn X.501 trong trường Issuer và Subject. Trường "subject" của chứng thư số tuân theo chuẩn X.509 v3. Nội dung của trường "subject" của chứng thư số chứa tên các thành phần sau đây:

- EmailAddress (E): Định dạng của thành phần EmailAddress tuân theo chuẩn IETF RFC 2822.
- CommonName (CN): Phân biệt cho mỗi cá nhân, mỗi host, mỗi dịch vụ. Tên đối tượng sở hữu chứng thư số, tên miền nếu là chứng thư số SLL.
- LocalityName (L): Tên khu vực mà đối tượng sở hữu chứng thư số thuộc. Danh sách LocalityName được định nghĩa trước dựa trên các quy định quản trị của MobiFoneCA.
- OrganizationalUnitName (OU): Bộ phận thuộc tổ chức (O) mà đối tượng sở hưu chứng thư số thuộc. Tên của tổ chức.
- OrganizationName (O): Tên tổ chức mà đối tượng sở hữu chứng thư số thuộc. Giá trị của thành phần OrganizationName được định nghĩa trước (MobiFoneCA) và nó cũng là thành phần gốc của LDAP.
- CountryName (C): Hai chữ cái chỉ tên quốc gia theo ISO, Việt Nam được ký hiệu là "VN". Giá trị của thành phần CountryName được định nghĩa trước (VN) và nó cũng là thành phần gốc của LDAP.

✓ Trong trường hợp chứng thư số cấp cho cá nhân nội dung trường "subject" phải bao gồm Họ và tên của thuê bao.

✓ Trong trường hợp chứng thư số cấp cho host/server nội dung trường "subject" phải bao gồm FQDN (Fully Qualified Domain Name) của host/server.

Minh hoạ đầy đủ nội dung của trường "subject" của một chứng thư số cấp cho cá nhân:

E=anvannguyen@mobifoneca.vn, CN=Nguyễn Văn An, L=Hanoi, OU=Administrator Dept, O=MobiFoneCA, C=VN.

3.1.1 Cần thiết cho tên trở nên có ý nghĩa

Nội dung của chứng thư số và các trường tên phải có một sự kết hợp với tên được xác thực của thuê bao. Trong trường hợp là các cá nhân, tên thường dùng được xác thực sẽ kết hợp với họ, tên đệm và các chữ cái đầu tùy chọn khác. Đối với các cá nhân đại diện cho một tổ chức, doanh nghiệp có thể bao gồm vị trí và vai trò của tổ chức đó. Trong trường hợp thuê bao là một tổ chức, doanh nghiệp sẽ phản ánh tên đăng ký theo luật pháp của thuê bao đó. Khi mà chứng thư số chỉ tới một vai trò hay một vị trí, nó cũng phải bao gồm nhận dạng của người có vai trò hay vị trí đó. Một chứng thư số được cấp phát cho một thiết bị điện tử phải bao gồm cả việc tên được xác thực của thiết bị điện tử và/hoặc tên của cá nhân hay tổ chức chịu trách nhiệm.

- Các thuộc tính trong DN của chứng thư số do MobiFoneCA cấp cho thuê bao là doanh nghiệp được mô tả như sau:

Thuộc tính	Giá trị
Tổ chức (O)	Tên tổ chức mà thuê bao sở hữu chứng thư số
Bộ phận tổ chức (OU)	Bộ phận thuộc tổ chức (O) mà thuê bao sở hữu chứng thư số trực thuộc.
Quận, huyện (L)	Địa chỉ quận/huyện của thuê bao
Tỉnh, thành phố (ST)	Địa chỉ tỉnh, thành phố của thuê bao
Quốc gia (C)	Tên quốc gia của thuê bao
Mã định danh của thuê bao – UID	Mã số Thuế: Đối với khách hàng là tổ chức, doanh nghiệp
Tên thường gọi (CN)	Tên tổ chức, doanh nghiệp (Theo như quyết định thành lập hay giấy đăng ký dinh doanh, và một số giấy giờ khác)
Địa chỉ email (E)	Địa chỉ email giao dịch của thuê bao sở hữu chứng thư số

- Các thuộc tính trong DN của chứng thư số do MobiFoneCA cấp cho thuê bao là cá nhân thuộc doanh nghiệp được mô tả như sau:

Thuộc tính	Giá trị
Tổ chức (O)	Tên tổ chức mà thuê bao sở hữu chứng thư số
Bộ phận tổ chức (OU)	Bộ phận thuộc tổ chức (O) mà thuê bao sở hữu chứng thư số trực thuộc.
Quận, huyện (L)	Địa chỉ quận/huyện của thuê bao
Tỉnh, thành phố (ST)	Địa chỉ tỉnh, thành phố của thuê bao
Quốc gia (C)	Tên quốc gia của thuê bao

Mã định danh của thuê bao – UID	CMND: Đối với khách hàng cá nhân thuộc tổ chức, doanh nghiệp
Tên thường gọi (CN)	Tên thuê bao sở hữu chứng thư số (Theo như giấy giới thiệu của tổ chức doanh nghiệp, hợp đồng lao động và một số giấy tờ khác)
Địa chỉ email (E)	Địa chỉ email giao dịch của thuê bao sở hữu chứng thư số

- Các thuộc tính trong DN của chứng thư số do MobiFoneCA cấp cho thuê bao cá nhân được mô tả như sau:

Thuộc tính	Giá trị
Quận, huyện (L)	Địa chỉ quận/huyện của thuê bao
Tỉnh, thành phố (ST)	Địa chỉ tỉnh, thành phố của thuê bao
Quốc gia (C)	Tên quốc gia của thuê bao
Mã định danh của thuê bao – UID	CMND: Đối với khách hàng cá nhân
Tên thường gọi (CN)	Tên thuê bao sở hữu chứng thư số (Theo như giấy CMND và một số giấy tờ khác)
Địa chỉ email (E)	Địa chỉ email giao dịch của thuê bao sở hữu chứng thư số

DN trong chứng thư số có thành phần là CN (viết tắt của Common Name – tên thường gọi) và đặt trong trường 'Subject name' của thuê bao. CN trong chứng thư số của thuê bao là tên cá nhân, tổ chức, doanh nghiệp hoặc tên miền, tên thiết bị, … CN được kiểm tra, xác thực trong quá trình cấp chứng thư số.

3.1.2 Tính duy nhất của tên

Tên thuê bao được nêu ra trong chứng thư số phải rõ ràng và duy nhất với toàn bộ các chứng thư số do CA phát hành cấp phát, và tuân theo tiêu chuẩn X.500 về tính duy nhất của tên. Khi cần thiết, có thể thêm số hoặc các ký tự vào tên gốc để đảm bảo tính duy nhất của tên trong toàn bộ danh mục chứng thư số do CA phát hành. Ở đây không cho phép bất kỳ sự tạo thành tên một cách lộn xộn nào. Mỗi tên sẽ phải là duy nhất đối với thuê bao duy nhất.

3.2 Xác minh đề nghị cấp chứng thư số

3.2.1 Phương thức chứng minh sở hữu khóa bí mật

Người đăng ký cấp chứng thư số được yêu cầu phải chứng minh tính sở hữu khóa bí mật của họ thích hợp với khóa công khai trong một yêu cầu chứng thư số thông qua việc ký yêu cầu với khóa bí mật. MobiFoneCA sẽ xác minh rằng người nộp đơn có phải

là người sở hữu khóa bí mật tương ứng với khóa công khai đã được đưa ra cùng với các ứng dụng phù hợp với một giao thức an toàn hay không.

Trong trường hợp khóa bí mật được tạo ra trực tiếp trên một Token, hoặc khóa được tạo ra bằng cách chuyển tiếp từ khóa vào Token, sau đó tới thuê bao, được coi là sở hữu khóa bí mật tại thời điểm tạo ra hoặc chuyển tiếp. Nếu thuê bao không sở hữu Token khi khóa được tạo ra thì Token sẽ chuyển ngay lập tức đến thuê bao qua một phương pháp tin cậy và có trách nhiệm. Việc chứng minh sự sở hữu khóa bí mật không phải thực hiện khi cặp khóa được MOBIFONECA sinh ra trên USB token.

Các phương pháp chứng minh thuê bao thực sự sở hữu khóa riêng:

Tệp tin đề nghị cấp chứng thư số mã hóa theo chuẩn PKCS#10 sinh từ PKI Smartcard, PKI Token, PKI Virtual Token đạt chuẩn FIPS 140-2 Level 2 trở lên, hoặc tương đương do thuê bao thực hiện;

Hoặc thuê bao ủy quyền cho MOBIFONECA, MOBIFONECA sinh khóa theo ủy quyền của thuê bao sử dụng PKI Smartcard, PKI Token, PKI Virtual Token đạt chuẩn FIPS 140-2 Level 2 trở lên. Theo quy trình, MOBIFONECA đảm bảo quyền sở hữu khóa riêng của thuê bao và bàn giao an toàn tránh các rủi ro trong quá trình giao nhận.

3.2.2 Nhận dạng và xác thực đối với chủ thể cá nhân

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

a) Tài liệu nhận dạng danh tính

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

- Chứng minh thư nhân dân.
- Chứng minh thư quân đội.
- Hộ khẩu hoặc giấy khai sinh.
- Hộ chiếu.
- Bằng lái xe hoặc các giấy tờ nhận dạng khác do cơ quan chính phủ cấp.
- Giấy xác nhận hộ khẩu do Cơ quan Công an xác nhận có đăng ký hộ khẩu thường trú.

b) Thực hiện nhận dạng cá nhân

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

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

Tổ chức đăng ký chứng thư số hoặc một đại lý tin cậy của RA thực hiện việc nhận dạng cá nhân này. RA tiến hành sẽ so sánh thông tin đăng ký với thông tin thực tế của cá nhân thông qua các tài liệu nhận dạng danh tính.

MOBIFONECA không xác minh những thông tin của thuê bao mà không liên quan đến quy trình quản lý vòng đời chứng thư số. MOBIFONECA không chịu trách nhiệm về những thông tin này.

Hồ sơ xin cấp gồm có:

- Đơn xin cấp chứng thư (theo mẫu của MOBIFONECA)

- Giấy tờ xác thực nhận dạng cá nhân

- Giấy tờ liên quan khác (nếu có)

Quy trình xác thực nhận dạng của cá nhân đăng ký chứng thư số như sau:

- Người đăng ký nộp hồ sơ cho MOBIFONECA/RA hoặc một đại lý tin cậy.

- MOBIFONECA/RA xác minh thông tin trên hồ sơ với các thông tin trên Giấy tờ xác thực nhận dạng cá nhân.

Nếu thông tin trên hồ sơ không thỏa mãn với các thông tin trên giấy tờ xác thực nhận dạng cá nhân thì đơn xin cấp chứng thư số sẽ không được chấp nhận.

3.2.3 Nhận dạng và xác thực đối với tổ chức

Yêu cầu cấp chứng thư số của một tổ chức có thể được thực hiện qua phương thức điện tử phải bao gồm tên theo pháp luật và địa chỉ của tổ chức. Những yêu cầu tối thiểu Nhận dạng và xác thực về tổ chức đó theo CP đòi hỏi xác nhận rằng:

- Tổ chức tồn tại hợp pháp và có địa chỉ kinh doanh theo địa chỉ được nêu ra trong đơn xin cấp chứng thư số.
- Thông tin nêu ra trong đơn cấp chứng thư số là chính xác.

Nhận dạng và xác thực được thực hiện bởi RA, được tiến hành trên cơ sở quy định "Thông tin về khách hàng" của tổ chức và các thủ tục tương tự khác, chúng có thể bao gồm một báo cáo của cơ quan chính phủ, và/hoặc sự tham gia của bên thứ ba có uy tín

về thông tin kinh doanh để cung cấp thông tin có hiệu lực về tổ chức đề nghị cấp chứng thư số như:

- Tên hợp pháp của công ty;
- Loại hình hoạt động;
- Năm thành lập;
- Tên của giám đốc và cán bộ;
- Địa chỉ;
- Số điện thoại;
- Bằng chứng chắc chắn đơn vị nộp đơn đang trong thời gian sát nhập hoặc tổ chức.

Thông tin của tổ chức có thể được xác nhận qua sự kiểm tra chéo với thông tin trong cơ sở dữ liệu thông tin của MobiFoneCA, từ một bên thứ ba, hoặc từ một tổ chức tài chính liên quan, và bằng cách gọi điện đến số điện thoại của tổ chức đó. Trong trường hợp điện thoại không liên lạc được, các thông tin về tổ chức đó là sai, không có hiệu lực hoặc bị nghi ngờ thì cần có sự kiểm tra thêm để bảo đảm thông tin. Nếu thông tin tiếp theo không thỏa mãn, hoặc nếu tổ chức nộp đơn từ chối trả lời những thông tin yêu cầu này thì đơn xin cấp chứng thư số sẽ không được chấp nhận. RA có thể tin cậy vào thông tin có được trước đó đối với tổ chức này và sẽ lưu trữ chi tiết thông tin để sử dụng cho xác minh nhận dạng. Quá trình này sẽ không mâu thuẫn với các quy định khác trong CP.

MOBIFONECA không xác minh những thông tin của thuê bao mà không liên quan đến quy trình quản lý vòng đời chứng thư số. MOBIFONECA không chịu trách nhiệm về những thông tin này.

Khi chứng thư số của tổ chức có chứa tên cá nhân làm đại diện, cần thực hiện các thủ tục xác thực sự ủy quyên, các thủ tục xác thực này bao gồm:

o Xác thực sự tồn tại của tổ chức như 3.2.3.

o Xác thực cá nhân như 3.2.2 và xác thực sự ủy quyền của tổ chức đối với cá nhân đó bằng giấy ủy quyền. Trong một số trường hợp cần làm rõ, MOBIFONECA sẽ xác thực bổ sung bằng cách gọi điện hoặc xác thực trực tiếp tại tổ chức về cá nhân đó.

3.3 Nhận dạng và xác thực trong yêu cầu cấp lại khoá (RE-KEY)

3.3.1 Nhận dạng và xác thực trong thủ tục cấp lại khoá

Trong thời hạn hiệu lực của chứng thư số thuê bao của MobiFoneCA có thể yêu cầu phát hành một chứng thư số với một cặp khoá mới. Cấp lại khoá trước khi chứng thư số hết hạn được thực hiện bằng cách gửi yêu cầu cấp lại khoá dựa trên khoá công khai mới trong một e-mail được ký với khoá bí mật cũ tới RA của MobiFoneCA. RA đảm bảo rằng cá nhân hay một tổ chức muốn cấp lại khoá cho chứng thư số phải là chủ thuê bao của chứng thư số đó.

Để chấp thuận yêu cầu cấp lại khoá của thuê bao, RA phải nhận dạng và xác nhận các thông tin thuê bao đưa ra là chính xác và không thay đổi. Sau khi cấp lại khoá CA hoặc RA của MobiFoneCA sẽ xác nhận lại việc nhận dạng và xác thực thuê bao sao cho phù hợp với các yêu cầu của đơn xin cấp chứng thư ban đầu.

MOBIFONECA hoặc RA có trách nhiệm xác thực yêu cầu cấp lại khóa của thuê bao sau khi nhận đơn đề nghị thay đổi cặp khóa. MOBIFONECA sử dụng một trong hai phương pháp xác thực làm căn cứ để chấp nhận một yêu cầu xin cấp lại khóa.

- Chứng minh quyền sở hữu khóa bí mật: thuê bao sử dụng chứng thư số của mình để gửi yêu cầu đề nghị thay đổi cặp khóa lên MOBIFONECA, khi thuê bao yêu cầu thay đổi cặp khóa chứng thư số yêu cầu này ngay lập tức được MOBIFONECA chấp nhận.
- Sử dụng phương pháp xác thực: Thuê bao phải trả lời đúng toàn bộ các câu hỏi xác thực để được MOBIFONECA chấp nhận yêu cầu đề nghị thay đổi cặp khóa.
- Sau khi xác thực, MOBIFONECA ban hành ngay chứng thư số mới cho thuê bao.
- Sau khi ban hành chứng thư số mới cho thuê bao, MOBIFONECA hoặc RA xác minh lại nhận dạng của đối tượng yêu cầu cấp lại khóa và các thông tin liên quan:
- MOBIFONECA hoặc RA liên lạc với thuê bao hoặc đại diện được ủy quyền nếu là tổ chức thông qua điện thoại, email, thư tín hay các phương tiện khác để khẳng định lại chính thuê bao đã yêu cầu làm mới chứng thư số. MOBIFONECA cũng xác minh lại đối tượng yêu cầu làm mới có phải là thành viên của tổ chức như trong thông tin đăng ký ban đầu hay không.

Các đặc trưng (DN) trong chứng thư số tên miền, hoặc sự tồn tại thực sự của tổ chức có thể được kiểm tra bổ sung dựa vào nhà cung cấp tên miền hoặc các đơn vị hữu quan như Cơ quan thuế Sở kế hoạch Đầu tư.

3.3.2 Nhận dạng và xác thực việc cấp lại khoá sau khi đã bị thu hồi

Chứng thư số đã bị thu hồi và hết hạn sử dụng có thể không được cấp lại khóa, làm mới hoặc cập nhật. Việc xin cấp lại khóa sau khi thu hồi và hết hạn sẽ được tuân theo các thủ tục giống như lần đăng ký đầu tiên.

3.4 Nhận dạng và xác thực đối với yêu cầu thu hồi chứng thư số

Thuê bao có thể yêu cầu thu hồi chứng thư số của mình tại bất kỳ thời điểm nào với bất kỳ lý do nào. MobiFoneCA khi gặp phải những yêu cầu như vậy, cần phải có cơ chế xác thực để ngăn chặn các yêu cầu trái phép khi đề nghị thu hồi chứng thư số một cách nhanh chóng. Bởi vậy, trong trường hợp các yêu cầu được gửi điện tử, thuê bao đưa yêu cầu này có thể được xác thực dựa trên cơ sở chữ ký số được sử dụng khi gửi thông điệp. Nếu yêu cầu được ký bởi khóa bí mật tương ứng với khóa công khai của người gửi yêu cầu, yêu cầu này sẽ được chấp nhận xem là có hiệu lực.

Tất cả những yêu cầu thu hồi chứng thư số phải được gửi đến MobiFoneCA hoặc RA thay mặt cho MobiFoneCA, thông qua một quá trình xử lý trực tuyến được chấp nhận hoặc thông qua văn bản. Yêu cầu thu hồi được xác thực hoặc bất kỳ các hành động tương ứng nào của CA sẽ được ghi và giữ lại theo quy định. Trong trường hợp khi một chứng thư số bị thu hồi, sự đánh giá về việc thu hồi này cũng sẽ được lưu giữ bằng văn bản. Khi chứng thư số của thuê bao bị thu hồi, việc thu hồi sẽ được công bố tại CRL thích hợp của MobiFoneCA.

Trong trường hợp thuê bao bị mất thiết bị lưu trữ khoá bí mật (Token/smartcard) thuê bao phải báo ngay cho RA mà thuê bao đã đăng ký trước kia theo một trong các cách sau: điện thoại, fax, thư điện tử, thư tín hay các dịch vụ đưa tin khác. Để yêu cầu thu hồi chứng thư số của mình, thuê bao phải đến trực tiếp RA trước kia xác thực lại các thông tin sở hữu chứng thư số. Khi đó yêu cầu thu hồi chứng thư mới được xem là hợp lệ.

Quy trình xác minh đề nghị thu hồi chứng thư số

Khi có một yêu cầu thu hồi chứng thư số từ thuê bao, MOBIFONECA hoặc RA sẽ tiến hành xác thực thuê bao gửi yêu cầu thu hồi. Thủ tục xác thực yêu cầu có thể sử dụng một trong hai phương pháp sau:

- Sử dụng chữ ký số: MOBIFONECA nhận một thông điệp từ thuê bao yêu cầu thu hồi chứng thư số, yêu cầu thu hồi này được ký bằng chứng thư số đã được cấp. Nếu chữ ký đúng, chứng thư số sẽ bị thu hồi tự động.

- MOBIFONECA sẽ xác nhận lại yêu cầu thu hồi chứng thư số của khách hàng, qua thông tin liên hệ khách hàng đã cung cấp, khi đăng ký cấp chứng thư số.
- Sau khi xác thực, MOBIFONECA sẽ tiến hành xác thực bổ sung bằng cách liên lạc với đối tượng yêu cầu thu hồi để đảm bảo chắc chắn rằng chính thuê bao đã yêu cầu thu hồi chứng thư số. Tùy từng hoàn cảnh, việc liên lạc này có thể thông qua điện thoại, email, thư tín hay thông qua các phương tiện truyền thông.
- RA sử dụng hệ thống quản lý chứng thư số có thể đệ trình nhiều yêu cầu thu hồi tới MOBIFONECA một lúc. Mỗi yêu cầu sẽ được xác thực thông qua chữ ký số của RA.

IV. Các yêu cầu đối với vòng đời hoạt động của chứng thư số thuê bao

4.1 Đơn xin cấp chứng thư số

4.1.1 Ai có thể đệ trình đơn xin cấp chứng thư số

Cá nhân hay tổ chức có thể nộp đơn xin cấp chứng thư số.

Hồ sơ đề nghị cấp chứng thư số bao gồm:

Đơn xin cấp chứng thư theo mẫu;

Đối với Khách hàng là cá nhân: Bản sao hợp lệ giấy CMND/Hộ chiếu/Căn cước công dân.

Đối với Khách hàng là cá nhân thuộc tổ chức đoanh nghiệp: Bản sao hợp lệ Giấy ĐKKD của tô chức, bản sao hợp lệ giấy CMND/Thẻ căn cước công dân/Hộ chiếu của cá nhân. Xác nhận của tổ chức về chức danh đăng ký trên chứng thư; hoặc giấy giới thiệu của tổ chức đoanh nghiệp, hợp đồng lao động.

Đối với khách hàng là tổ chức doanh nghiệp: Bản sao hợp lệ Giấy ĐKKD/Quyết định thành lập/Giấy phép đầu tư của tổ chức; bản sao giấy CMND/Hộ chiếu của người đại diện theo pháp luật, giấy tờ ủy quyền (nếu người ký trên văn bản đăng ký không phải là người đại diện theo pháp luật).

Cá nhân hoặc tô chức có quyền lựa chọn bản sao công chứng còn thời hạn hoặc bản sao đi kèm bản gốc để đối chiếu đối với các giấy tờ văn bản sau: Chứng minh thư nhân dân, Thẻ căn cước công dân, Hộ chiếu, Giấp phép đăng ký kinh doanh, Giấy phép đầu tư, Quyết định thành lập.

4.2 Quá trình xử lý cấp chứng thư

1. Thuê bao đến RA để đăng ký chứng thư số. Thuê bao sẽ kê khai vào các phần có liên quan bao gồm cả phần đại diện và phần đảm bảo và chịu trách nhiệm về quá trình xử lý bao gồm:

- Hoàn thành bản kê khai và cung cấp các thông tin đúng, chính xác
- Tự tạo khoá hoặc yêu cầu tạo cặp khoá
- Cung cấp khoá công khai đến RA
- Chứng minh sự tương thích giữa khoá bí mật và khoá công khai cho RA
- Hồ sơ xin cấp chứng thư số bao gồm:
  - ✓ Đơn xin cấp chứng thư theo mẫu;
  - ✓ Đối với Khách hàng là cá nhân: Bản sao hợp lệ giấy CMND/Hộ chiếu/Căn cước công dân.
  - ✓ Đối với Khách hàng là cá nhân thuộc tổ chức doanh nghiệp: Bản sao hợp lệ Giấy ĐKKD của tổ chức, bản sao hợp lệ giấy CMND/Thẻ căn cước công dân/Hộ chiếu của cá nhân. Xác nhận của tổ chức về chức danh đăng ký trên chứng thư; hoặc giấy giới thiệu của tổ chức doanh nghiệp, hợp đồng lao động.
  - ✓ Đối với khách hàng là tổ chức doanh nghiệp: Bản sao hợp lệ Giấy ĐKKD/Quyết định thành lập/Giấy phép đầu tư của tổ chức; bản sao giấy CMND/Hộ chiếu của người đại diện theo pháp luật, giấy tờ ủy quyền (nếu người ký trên văn bản đăng ký không phải là người đại diện theo pháp luật).
  - ✓ Đối với khách hàng đăng ký chứng thư số cho máy chủ: Tương tự như hồ sơ cấp chứng thư số cho cá nhân hoặc tổ chức, doanh nghiệp.
  - ✓ Cá nhân hoặc tổ chức có quyền lựa chọn bản sao công chứng còn thời hạn hoặc bản sao đi kèm bản gốc để đối chiếu đối với các giấy tờ văn bản sau: Chứng minh thư nhân dân, Thẻ căn cước công dân, Hộ chiếu, Giấp phép đăng ký kinh doanh, Giấy phép đầu tư, Quyết định thành lập.

2. RA xác thực thông tin đăng ký và nhận dạng thuê bao và trả lời chấp nhận hay từ chối cấp chứng thư số.

- Từ chối duyệt yêu cầu: Kiểm tra thông tin yêu cầu cung cấp dịch vụ không đúng, không hợp lệ thì thực hiện Từ chối phê duyệt yêu cầu và ghi rõ lý do không hợp lệ.

- Phê duyệt yêu cầu: MOBIFONECA kiểm tra thông tin yêu cầu cung cấp dịch vụ hợp lệ thì thực hiện Phê duyệt yêu cầu.

3. Trong trường hợp chấp nhận, RA gắn kết định danh thuê bao với khoá công khai bằng form điện tử sau đó ký và gửi lên CA.

4.2.1 Thời gian xử lý yêu cầu cấp chứng thư

MobiFoneCA có trách nhiệm xử lý các đơn xin cấp chứng thư trong khoảng thời gian phù hợp. Không có quy định thời gian hoàn thành quá trình xử lý một đơn xin cấp chứng thư trừ khi được đưa ra trong hợp đồng với thuê bao, trong CPS hoặc thoả thuận giữa các bên của dịch vụ MobiFoneCA. Thông thường, nếu không có vướng mắc, hệ thống cung cấp dịch vụ MobiFoneCA có thể khởi tạo một chứng thư mới tối đa trong 03 ngày.

4.3 Cấp phát chứng thư

4.3.1 Hoạt động trong suốt quá trình phát hành chứng thư

Khi một đơn xin cấp chứng thư được cấp bởi MobiFoneCA sẽ phải được phê duyệt của đơn xin cấp chứng thư đó.

Chứng thư số được cấp phát sau khi MobiFoneCA chấp nhận hồ sơ xin cấp chứng thư số.

MobiFoneCA tạo cho thuê bao một chứng thư số dựa vào những thông tin trong hồ sơ xin cấp chứng thư số và yêu cầu cấp chứng thư số.

4.3.2 Thông báo của MobiFoneCA đến người dùng về việc cấp chứng thư

MobiFoneCA cấp phát các chứng thư trực tiếp tới người dùng hoặc thông qua RA. MobiFoneCA thông báo cho người dùng rằng chứng thư của họ đã được tạo đồng thời cung cấp cho người dùng quyền truy cập tới chứng thư đó để kiểm tra tính sẵn sàng của chứng thư. Chứng thư có hiệu lực sẽ cho phép người dùng tải về từ website hoặc thông qua LDAP server.

MobiFoneCA gửi email, tin nhắn SMS hoặc điện thoại, fax thông báo cho thuê bao về việc yêu cầu cấp chứng thư số của thuê bao đã được phê duyệt.

- MOBIFONECA tạo chứng thư số và gửi chứng thư số cho Token Manager để cập nhật vào thiết bị token.
- Thuê bao xác nhận các thông tin trong chứng thư số sẽ được cấp là chính xác.
- Quá trình truyền nhận giữa token và server được mã hóa, sử dụng phương thức SSL nhằm đảm bảo tính toàn vẹn và bí mật.

Khi bàn giao chứng thư số, thuê bao có trách nhiệm ký vào bản xác nhận đã nhận đầy đủ chứng thư số của mình và gửi lại cho MobiFoneCA.

Nếu thông tin trong chứng thư số không phù hợp, người dùng thông báo lại cho đại lý hoặc RA của MobiFoneCA để được xử lý.

Thông tin tiếp nhận: Tổng Công ty Viễn thông MobiFone

Địa chỉ: Tòa nhà MobiFone, lô VP1, phường Yên Hòa, quận Cầu Giấy, Hà Nội

Điện thoại: 09036110116

E-mail: support.cntt@mobifone.vn

Thời gian thông báo cho thuê bao sau khi tạo xong chứng thư số tối đa 24h.

4.4 Chấp nhận chứng thư

4.4.1 Điều kiện chứng minh việc chấp nhận chứng thư

Khi thuê bao nhận chứng thư số và khoá bí mật lưu trong thiết bị lưu trữ (Token) từ thông báo của MobiFoneCA, điều này chứng minh việc chấp thuận của thuê bao đối với thông báo đó.

Trong trường hợp từ chối, thuê bao phải thông báo cho MobiFoneCA từ chối chứng chỉ và giải thích lý do từ chối. Trong vòng một tuần thuê bao không trả lời thông báo của MobiFoneCA, chứng thư số đó coi như được khách hàng chấp nhận.

4.4.2 Việc công khai chứng thư của MobiFoneCA

Sau khi nhận được chấp nhận chứng chỉ MobiFoneCA công bố chứng thư số đã phát hành, MobiFoneCA công bố tất cả các chứng thư hợp lệ trong kho lưu trữ trực tuyến trên cả web lẫn kho lưu trữ LDAP. (Xem mục 2.2 Công bố thông tin chứng thư).

Chứng thư số được coi là chính thức chấp nhận khi được MobiFoneCA công bố trên website, kho dữ liệu chứng thư số. MobiFoneCA công bố chứng thư số của thuê bao tại trang web: http://www.mobica.vn trong vòng 24h ngay khi nhận được xác nhận của thuê bao về tính chính xác của thông tin.

4.4.3 Thông báo sự phát hành chứng thư đến các đối tượng khác

MobiFoneCA sẽ gửi thông báo về việc phát hành chứng thư đến các RA xử lý yêu cầu của thuê bao.

4.5 Sử dụng cặp khoá của chứng thư

4.5.1 Sử dụng chứng thư và khoá bí mật của thuê bao

Chứng thư số phát hành bởi MobiFoneCA và khoá bí mật tương ứng với khoá công khai trong chứng thư được sử dụng hợp pháp theo bản thoả thuận của thuê bao với các điều khoản có trong CP/CPS của nhà cung cấp chứng thư. Chứng thư sử dụng phải khớp với đuôi mở rộng trong trường KeyUsage có trong chứng thư (Trường KeyUsage được định nghĩa trước trong chứng thư và xác định một số chức năng và hoạt động của giao thức như SSL, TLS).

Mục đích sử dụng chứng thư số phải nhất quán với phạm vi sử dụng được phép của chứng thư số đó (quy định trong trường KeyUsage trong chứng thư số). Ví dụ, nếu không có chức năng "Digital Signature" thì chứng thư số đó không được sử dụng để ký điện tử.

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

4.5.2 Sử dụng chứng thư và khoá công khai của đối tác tin cậy

Các đối tác tin cậy phải đánh giá một cách độc lập các chứng thư số phát hành bởi MobiFoneCA, phải kiểm tra chứng thư số hợp lệ bằng cách:

- Kiểm tra có đúng chứng thư số do MobiFoneCA phát hành;
- Kiểm tra chứng thư số chưa bị thu hồi;
- Chứng thư số được sử dụng theo đúng phần mở rộng của trường KeyUsage và extKeyUsage trong chứng thư;
- Việc sử dụng chứng thư cho các mục đích phù hợp và xác định rằng chứng thư sẽ được sử dụng đúng mục đích không bị ngăn cấm hoặc bị giới hạn bởi CP/CPS của MobiFoneCA.

4.6 Gia hạn chứng thư

4.6.1 Các trường hợp cần gia hạn chứng thư

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

4.6.2 Đối tượng cần gia hạn chứng thư

Chủ sở hữu của chứng thư có thể yêu cầu gia hạn chứng thư trước khi nó hết hạn bằng cách gửi cho RA tương ứng một e-mail ký với khóa bí mật của chứng thư yêu cầu gia hạn hoặc gửi yêu cầu bằng văn bản theo mẫu MOBIFONECA công bố trên website có ký xác nhận của chủ thuê bao.

4.6.3 Xử lý các yêu cầu gia hạn chứng thư

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

Nếu thông tin thuê bao không thay đổi, chứng thư số mới của thuê bao sẽ được ban hành ngay sau khi MOBIFONECA nhận được yêu cầu mà không cần có sự hiện diện vật lý của thuê bao tại MOBIFONECA hoặc RA.

4.6.4 Điều kiện chấp nhận gia hạn chứng thư

Tuân theo mục 4.4.1

4.6.5 Công bố các chứng thư được gia hạn

Tuân theo mục 4.4.2

4.6.6 Thông báo việc cấp chứng thư của MobiFoneCA đến các đối tượng khác

Tuân theo mục 4.4.3

4.7 Thay đổi cặp khóa của thuê bao

Quá trình cấp lại khoá cho chứng thư là việc cấp lại một chứng thư mới với cặp khoá mới.

4.7.1 Đối tượng yêu cầu thay đổi khóa

Chỉ có thuê bao của chứng thư mới có thể yêu cầu thay đổi khóa. Nếu chứng thư đã hết hạn thì thủ tục yêu cầu chứng thư tuân theo như yêu cầu cấp chứng thư đầu tiên.

4.7.2 Trường hợp được thay đổi cặp khóa của thuê bao

Vì lý do an toàn, cấp lại khoá chứng thư được ưu tiên phát hành một chứng thư mới cho một thuê bao có chứng thư sắp hết hạn hoặc những người muốn thay đổi các tham số của chứng thư.

4.7.3 Xử lý các yêu cầu cấp khoá mới cho chứng thư

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

4.7.4 Thông báo phát hành chứng thư mới tới thuê bao

Tuân theo mục 4.3.2

4.7.5 Thông báo chấp nhận cấp mới khoá chứng thư

Tuân theo mục 4.4.1

4.7.6 Phát hành chứng thư đã được cấp mới khoá của MobiFoneCA

Tuân theo mục 4.4.2

4.7.7 Thông báo cấp chứng thư của MobiFoneCA tới các đối tượng khác

Tuân theo mục 4.4.3

4.8 Thay đổi thông tin chứng thư

Việc sửa đổi giấy chứng nhận có thể được thực hiện bằng cách thu hồi chứng thư và phát hành lại chúng với các khoá được tạo (re-key).

4.8.1 Các trường hợp sửa đổi chứng thư

Chứng thư số không được sửa đổi. Chứng thư cũ phải được thu hồi, và một cặp khoá mới phải được tạo ra và yêu cầu sửa đổi các nội dung chứng thư được chấp nhận với cặp khoá mới. Việc thu hồi trên điều kiện phát hành và chấp nhận một chứng thư mới và do đó chứng thư cũ chỉ được thu hồi sau khi một chứng thư mới được chấp nhận.

4.8.2 Đối tượng yêu cầu sửa đổi chứng thư

Không áp dụng

4.8.3 Quá trình xử lý yêu cầu sửa đổi chứng thư

Không áp dụng

4.8.4 Thông báo phát hành chứng thư mới tới thuê bao

Không áp dụng

4.8.5 Điều kiện chấp nhận sửa đổi thuê bao

Không áp dụng

4.8.6 Phát hành chứng thư đã được sửa đổi từ MobiFoneCA

Không áp dụng

4.8.7 Thông báo phát hành chứng thư của MobiFoneCA tới các đối tượng khác

Không áp dụng

4.9 Tạm dừng và thu hồi chứng thư

MobiFoneCA không cung cấp dịch vụ tạm dừng chứng thư.

4.9.1 Các trường hợp thu hồi

Yêu cầu thu hồi chứng thư số sẽ được xử lý khi thuê bao đề nghị, do MobiFoneCA quyết định hoặc theo yêu cầu của pháp luật.

Nếu chứng thư số đã bị thu hồi, thông tin chứng thư số bị thu hồi sẽ được công bố lên danh sách chứng thư số bị thu hồi (CRL) và cập nhật vào cơ sở dữ liệu chứng thư số.

Cụ thể chứng thư số bị thu hồi trong các trường hợp sau:

- Thông tin trong chứng thư số được phát hiện sai khác so với thực tế
- Khóa bí mật của thuê bao có chứng thư số bị lộ
- Thuê bao đề nghị thu hồi
- Chứng thư số có tên mạo danh hoặc vi phạm quyền sở hữu trí tuệ
- Chứng thư số sử dụng sai mục đích
- Chứng thư số đã được tạo ra không tuân theo những thủ tục được yêu cầu bởi quy chế chứng thực này
- Có lệnh dừng sử dụng chứng thư số hoặc dừng toàn bộ hệ thống
- Theo quy định của pháp luật hay theo yêu cầu của các cơ quan có thẩm quyền

Khi khóa bí mật của thuê bao bị mất/lộ hoặc nghi ngờ bị mất/lộ, thuê bao phải báo ngay lập tức cho MobiFoneCA.

4.9.2 Đối tượng có thể yêu cầu thu hồi

Yêu cầu thu hồi chứng thư được thực hiện bởi:

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

4.9.3 Thủ tục yêu cầu thu hồi chứng thư

Trong trường hợp khẩn cấp, nếu không gửi được e-mail việc thu hồi chứng thư có thể thông báo trực tiếp với RA hoặc CA của MobiFoneCA. Trước khi thu hồi chứng thư MobiFoneCA phải xác nhận nguồn gốc của yêu cầu theo thủ tục được sử dụng cho việc đăng ký ban đầu.

Thu hồi theo yêu cầu: Khi nhận yêu cầu thu hồi từ một thuê bao cho chứng thư số của mình, MOBIFONECA sẽ tạm dừng chứng thư số, và kiểm tra để đảm bảo yêu cầu đó là chính xác. Trong trường hợp thuê bao thông báo khẩn cấp bằng phương tiện liên lạc như điện thoại, thư điện tử,... chỉ khi thuê bao có đơn yêu cầu thu hồi chứng thư số có xác nhận của tổ chức, doanh nghiệp đối với tổ chức doanh nghiệp hoặc chính cá nhân và nêu rõ lý do, MOBIFONECA mới chính thức thu hồi và công bố thông tin thu hồi chứng thư số.

- Xác minh quyết định yêu cầu thu hồi chứng thư số của đơn vị có thẩm quyền.

- Nếu MOBIFONECA có đủ cơ sở để xác minh khách hàng bị lộ khoá bí mật gây mất an toàn, MOBIFONECA có quyền tạm dừng dịch vụ và thông báo cho thuê bao biết để xác nhận thông tin và bảo vệ an toàn thông tin cho thuê bao.

4.9.4 Thời gian cho một yêu cầu thu hồi chứng thư

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

4.9.5 Thời gian MobiFoneCA xử lý yêu cầu thu hồi chứng thư

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

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

Trước khi sử dụng một chứng thư số, bên nhận phải xác nhận CRL gần dây nhất. MobiFoneCA sẽ cung cấp các thông tin tìm kiếm CRL thích hợp, kho lưu trữ trên website hay OCSP để kiểm tra trạng thái thu hồi.

4.9.7 Tần số cấp phát CRL

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

4.9.8 Thời gian trễ tối đã cho các CRL

Các CRL được sao chép vào một thiết bị di động ngay khi được tạo ra bởi hệ thống CA (Các CA hoạt động offline) và chuyển ngay lập tức đến kho lưu trữ trực tuyến.

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

Thông tin trạng thái chứng thư và thông tin thu hồi chứng thư được lưu trữ trực tuyến trên kho của MobiFoneCA truy cập qua nền tảng LDAP và web và có thể truy cập qua OCSP. MobiFoneCA sẽ cho phép đối tác tin cậy truy vấn trực tuyến các thông tin thu hồi và trạng thái chứng thư.

4.9.10 Những yêu cầu kiểm tra trạng thái chứng thư trực tuyến

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

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

4.10 Dịch vụ trạng thái chứng thư số

4.10.1 Các đặc tính hoạt động

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

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

4.10.2 Tính sẵn sàng của dịch vụ

Dịch vụ cung cấp trạng thái hoạt động của chứng thư luôn sẵn sàng 24/7, ngoại trừ các hoạt động bảo trì không thể tránh khỏi và do đặc tính tự nhiên của internet (Phụ thuộc vào dịch vụ của các ISP) khi dịch vụ này không thể truy cập được.

4.10.3 Các tính năng khác

OCSP là dịch vụ tùy chọn, có thể sẽ thu phí.

4.11 Kết thúc hợp đồng

Yêu cầu kết thúc thuê bao chứng thư số có hiệu lực trong các trường hợp sau:

- Có yêu cầu dừng sử dụng chứng thư số hoặc đừng toàn bộ hệ thống MobiFoneCA hoặc MobiFoneCA hết thời hạn hoạt động
- Thuê bao đã hết hạn mà không gia hạn
- Thu hồi chứng thư số xảy ra mà không xin cấp một chứng thư số mới

Thời hạn sử dụng của chứng thư số được chỉ rõ trong chứng thư số.

- Thủ tục chấm dứt dịch vụ:

Thuê bao có thể đơn phương chấm dứt dịch vụ bằng các cách:

- Hủy hợp đồng thuê bao
- Chứng thư số hết hạn mà không gia hạn
- Yêu cầu thu hồi trước thời hạn.

4.12 Cam kết và khôi phục khoá

4.12.1 Chính sách và thực hiện cam kết khôi phục khoá

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

Tuy nhiên, cơ chế này hoàn toàn có thể thay đổi, phụ thuộc vào yêu cầu của pháp luật.

4.12.2 Chính sách và thực hiện phục hồi và đóng gói khoá phiên

Xem mục 4.12.1.

V. Kiểm soát, quản lý và vận hành

5.1 Kiểm soát an toán, an ninh vật lý

MOBIFONECA thực hiện các biện pháp kiểm soát và các thủ tục kiểm soát nhằm đảm bảo an ninh vật lý cho toàn bộ hệ thống. Được thể hiện theo các nội dung dưới đây.

5.1.1 Vị trí đặt và xây dựng hệ thống

CA MobiFoneCA được đặt tại địa chỉ của tổ chức được quản lý trong tài liệu này (xem mục 1.5.1).

Hệ thống thiết bị MOBIFONECA được đặt tại hai trung tâm dữ liệu là trung tâm chính tại tòa nhà MobiFone, lô VP1, Phường Yên Hòa, Quận Cầu Giấy, Hà Nội và trung tâm dự phòng tại trung tâm dữ liệu của MobiFone, Node 3 , Quận 9, Thành Phố Hồ Chí Minh.

Mỗi địa điểm đặt thiết bị được trang bị nhiều lớp bảo vệ khác nhau: bảo vệ vật lý vòng ngoài của tòa nhà, bảo vệ khu đặt thiết bị, bảo vệ tủ đặt thiết bị, bảo vệ chống cháy nổ.

5.1.2 Truy cập vật lý

Các Server của RA và CA được đặt trong một môi trường được kiểm soát, truy cập bị hạn chế bởi quyền truy cập cá nhân. Máy tính đóng vai trò ký của CA và khoá bí mật lưu giữ bằng khoá an toàn khi không sử dụng.

Hệ thống MOBIFONECA được bảo vệ nhất bởi các lớp an ninh vật lý, phải vượt qua được lớp bảo vệ thấp trước khi có thể tiếp cận được lớp bảo vệ cao hơn. Hệ thống camera giám sát hoạt động 24/7 cho phép ghi lại toàn bộ các hoạt động.

- Lớp bảo vệ vòng ngoài - bảo vệ tòa nhà
- Lớp bảo vệ khu đặt thiết bị
- Việc truy nhập qua các lớp được được kiểm soát chặt chẽ, chỉ những người có quyền truy cập mới được truy nhập vào các lớp tương ứng. Càng truy nhập vào các lớp quản lý yêu cầu an ninh cao, sự hạn chế càng tăng.
- Tất cả mọi truy nhập đều được ghi nhận.

5.1.3 Điều hoà và nguồn điện

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

Các Server của hệ thống MobiFoneCA được bảo vệ bằng hệ thống UPS và máy phát điện dự phòng trong trường hợp mất điện lưới.

5.1.4 Tiếp xúc với nước

Địa điểm đặt thiết bị hệ thống của MobiFoneCA được lựa chọn thích hợp, và xây dựng phương án phòng ngừa để ngăn chặn nước, lụt xâm nhập vào hệ thống.

5.1.5 Phòng cháy chữa cháy

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

5.1.6 Phương tiện lưu trữ

Có phương tiện lưu trữ dữ liệu (máy chủ, hệ thống SAN) được bảo vệ khỏi nước, lửa hay môi trường huỷ hoại và được bảo vệ tránh sử dụng truy cập trái phép hay phá huỷ.

5.1.7 Quá trình xử lý rác, tiêu hủy thông tin nhạy cảm

Các thiết bị và tài liệu nhạy cảm phải được xử lý trước khi bỏ đi.

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

Các phương pháp phá hủy đảm bảo theo tiêu chuẩn nhà sản xuất trước khi vứt rác và đảm bảo thông tin trên rác thải không thể đọc bằng mọi phương pháp.

Quy trình xử lý rác được thực hiện qua các công đoạn như sau:

Tài liệu có dữ liệu nhạy cảm được MOBIFONECA xử lý theo cách an toàn. Các tài liệu và vật liệu nhạy cảm được cắt nhỏ trước khi xử lý. Phương tiện được sử dụng để thu thập hoặc truyền thông tin nhạy cảm không thể đọc được trước khi thải bỏ.

Các chất thải khác được xử lý theo các yêu cầu xử lý chất thải thông thường của MOBIFONECA. Các thiết bị mật mã, thẻ thông minh và các thiết bị khác có thể chứa khóa cá nhân hoặc tài liệu quan trọng sẽ bị phá hủy vật lý hoặc nghiền vụn nếu thấy cần thiết, MOBIFONECA thực hiện hủy theo hướng dẫn của nhà sản xuất trước khi xử lý. Việc phá hủy này cần có sự cho phép để xử lý tất cả các thiết bị lưu trữ có chứa các dữ liệu quan trọng. Việc phá hủy khóa riêng của CA sẽ được lãnh đạo -MOBIFONECA phê duyệt và phải có sự chứng kiến của ít nhất 2 cá nhân trong vai trò quản lý khóa CA của MOBIFONECA và việc phá hủy được lưu giữ hồ sơ biên bản của tất cả các bước.

5.1.8 Hệ thống dự phòng

MobiFoneCA đảm bảo rằng các thiết bị được sử dụng để sao lưu bên ngoài sẽ phải có mức độ an ninh giống như khu vực CA. Hệ thống sao lưu, có khả năng khôi phục khi hệ thống bị hỏng, sẽ được định kỳ thực hiện. Ít nhất một bản sao sẽ được lưu trữ tại một địa điểm bên ngoài (tách biệt với khu vực có thiết bị của CA). Chỉ cần lưu trữ lại lần sao lưu gần nhất. Sao lưu sẽ được lưu trữ tại một địa điểm với các cơ chế và quy trình

kiểm soát tương tự như cơ chế và quy trình kiểm soát khi hệ thống hoạt động của hệ thống CA.

5.2 Quy trình kiểm soát

5.2.1 Những thành viên được tin cậy

Tất cả các nhân viên có quyền truy cập hoặc điều khiển các hoạt động được mã hóa có thể ảnh hưởng chủ yếu tới việc cấp phát, sử dụng, thu hồi, hủy bỏ chứng thư số, bao gồm cả việc truy cập tới khu vực điều khiển hạn chế của CA.

Những nhân viên này bao gồm nhưng không giới hạn là nhân viên quản trị hệ thống, điều hành, nhân viên kỹ thuật, nhân viên hỗ trợ kỹ thuật, kiểm toán viên, quản trị viên được chỉ định để quản lý hoạt động của CA

5.2.2 Số lượng người yêu cầu cho mỗi công việc

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

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

Những thủ tục điều khiển ở bên trong được thiết kế để đảm bảo ít nhất 03 cá nhân được tin tưởng cùng tham gia truy cập tới mức vật lý hoặc mức logic của thiết bị truy cập tới phần cứng mã hoá yêu cầu chặt chẽ phải có nhiều người được tin tưởng cùng tham gia toàn bộ quá trình làm việc từ việc nhận và kiểm tra cho tới bước cuối cùng là huỷ về logic hoặc về vật lý.

5.2.3 Nhận dạng và xác thực cho từng thành viên

Tất cả các nhân viên CA phải được xác minh nhận dạng và xác thực trước khi họ:

(i) Có trong danh sách truy cập tới các vị trí CA;
(ii) Có trong danh sách truy cập đến hệ thống CA;
(iii) Được cung cấp một chứng thư số để thực hiện nhiệm vụ CA;
(iv) Được cung cấp một tài khoản trên hệ thống PKI.

Mọi cá nhân trước khi trở thành người được tin tưởng trong hệ thống MOBIFONECA đều phải được xác minh nhân thân, nhận dạng và trình độ.

MOBIFONECA đảm bảo rằng các cá nhân hoàn toàn được tin tưởng trước khi thực hiện các công việc nhạy cảm.

5.2.4 Vai trò yêu cầu phân chia trách nhiệm

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

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

5.3 Kiểm soát nhân sự

5.3.1 Năng lực, kinh nghiệm và các yêu cầu khác

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

- MOBIFONECA yêu cầu cán bộ thể hiện được sự tin tưởng, trình độ chuyên môn và kinh nghiệm phù hợp với vai trò và nhiệm vụ đảm trách.
- Nhân sự quản lý và vận hành hệ thống có bằng đại học trở lên, chuyên ngành an toàn thông tin hoặc công nghệ thông tin hoặc điện tử viễn thông.

5.3.2 Thủ tục kiểm tra lai lịch

Trước khi nhân viên bắt đầu việc làm trong một vai trò được tin cậy, MobiFoneCA tiến hành kiểm tra nền tảng đó bao gồm:

- Xác nhận việc làm trước đó;
- Kiểm tra các nguồn thông tin tham khảo;
- Xác nhận trình độ chuyên môn, bằng cấp liên quan;
- Bản xác minh sơ yếu lí lịch;
- Kiểm tra về thông tin tài chính, tín dụng;

Các yếu tố trong thủ tục kiểm tra lai lịch được xem là căn cứ để từ chối các ứng cử viên cho vị trí được tin tưởng hoặc là căn cứ để chống lại những người đã được tin tưởng thường bao gồm:

- Các ứng cử viên hoặc người tin tưởng cung cấp sai thông tin;
- Nguồn tham khảo bất lợi hoặc không đáng tin cậy;
- Có tiền án tiền sự;
- Có vấn đề liên quan đến tài chính.

5.3.3 Yêu cầu về đào tạo

MobiFoneCA tổ chức các chương trình đào tạo cần thiết cho nhân viên để thực hiện nhiệm vụ và công việc của mình một cách phù hợp và chuyên nghiệp. Việc định kỳ đánh giá và tăng cường các chương trình đào tạo này là cần thiết.

Chương trình đào tạo được thiết kế riêng cho nhiệm vụ công việc của nhân viên bao gồm:

- Khái niệm căn bản về PKI;
- Trách nhiệm công việc;
- Các chính sách, quy chế an ninh của nhà nước và của MobiFoneCA;
- Các phiên bản phần cứng phần mềm được sử dụng và các thức vận hành hệ thống CA;
- Báo cáo, chuyển giao các thoả hiệp và các vấn đề liên quan;
- Thủ tục khôi phục sau thảm hoạ và duy trì công việc.

5.3.4 Chu kỳ tái đào tạo

MobiFoneCA thường xuyên đào tạo lại và cập nhật thông tin cho nhân viên của mình với mức độ và tần suất phù hợp để nhân viên duy trì mức độ tin tưởng và thực hiện tốt công việc của mình.

Việc tổ chức đào tạo lại bắt buộc khi hệ thống sử dụng phần mềm hoặc các tính năng mới cũng như các thủ tục của tổ chức được triển khai.

5.3.5 Kỷ luật đối với các hoạt động không hợp pháp

MobiFoneCA cơ quyền truy tố các hành động trái phép theo các quy định của Việt Nam. Các biện pháp kỷ luật hoặc chấm dứt hợp đồng tuỳ thuộc vào mức độ nghiêm trọng của hành động bất hợp pháp.

5.3.6 Yêu cầu đối với các nhà thầu độc lập

Các nhà thầu độc lập hoặc tư vấn có thể được coi là đối tượng tin cậy. Bất cứ nhà thầu hoặc tư vấn được coi cùng chức năng và tiêu chuẩn bảo mật tương tự áp dụng cho một nhân viên của MobiFoneCA ở vị trí tương đương.

5.3.7 Cung cấp tài liệu cho nhân viên

MobiFoneCA cung cấp tất cả các 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 loại bản ghi sự kiện

MOBIFONECA ghi nhật ký (log) các sự kiện sau, việc ghi log được thực hiện tự động hay và thủ công tùy vào từng trường hợp:

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

Mỗi bản ghi nhật ký gồm các thông tin sau:

- Thời gian của bản ghi
- Thứ tự của bản ghi (đối với bản ghi được tạo tự động).
- Đối tượng tạo ra bản ghi
- Loại bản ghi.

5.4.2 Tần suất xử lý bản ghi sự kiện

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

5.4.3 Thời gian duy trì cho kiểm định bản ghi

Khoảng thời gian lưu giữ tối thiểu đối với các bản ghi kiểm toán là 05 năm.

5.4.4 Bảo vệ các bản ghi kiểm định

Bản ghi kiểm định sẽ được bảo vệ bằng hệ thống bản ghi kiểm định điện tử bao gồm các cơ chế bảo vệ bản ghi log khỏi các truy cập, sửa đổi, xoá bỏ hoặc can thiệp bất hợp pháp. Bản ghi kiểm định chỉ được truy cập bởi các điều hành và quản lý CA.

5.4.5 Thủ tục sao lưu dự phòng cho các bản ghi kiểm định

Nhật ký được backup theo chế độ backup chung của MOBIFONECA.

5.5 Lưu trữ các bản ghi

5.5.1 Những kiểu bản ghi được lưu trữ

Xem 5.4.1.

5.5.2 Thời gian duy trì tài liệu lưu trữ

Khoảng thời gian lưu giữ tối thiểu là 05 năm.

5.5.3 Bảo mật tài liệu lưu trữ

Hệ thống lưu dữ liệu lưu trữ được bảo vệ để chỉ những người được phép mới có thể truy nhập. Dữ liệu lưu trữ được bảo vệ theo các phương pháp cần thiết, chống lại việc xem, thay đổi, xóa hay các thao tác khác không được cho phép. Hệ thống chứa dữ liệu lưu trữ và ứng dụng xử lý dữ liệu lưu trữ được duy trì để đảm bảo dữ liệu lưu trữ có thể được truy nhập trong khoảng thời gian được quy định trong quy chế chứng thực này.

5.5.4 Thủ tục sao lưu và dự phòng dữ liệu

Dữ liệu lưu trữ được backup theo chế độ backup chung của MOBIFONECA

5.5.5 Yêu cầu nhãn thời gian cho dữ liệu

Tất cả các bản ghi sự kiện phải được đóng dấu thời gian.

5.5.6 Hệ thống thu thập dữ liệu lưu trữ (nội bộ và bên ngoài)

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

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

Tất cả chứng thư số được cấp bởi MobiFoneCA được công bố công khai. Dữ liệu được sử dụng cho việc đăng ký và thẩm định thuê bao chỉ dùng cho nội bộ của MobiFoneCA.

Tính toàn vẹn lưu trữ thông tin của MobiFoneCA được xác minh:

- Vào thời gian chuẩn bị lưu trữ;
- Vào thời điểm kiểm toán an ninh;
- Bất cứ lúc nào khác khi một kiểm toán an toàn là bắt buộc.

5.6 Thay đổi khoá

Không có quy định.

5.7 Lộ khóa và khôi phục sau thảm hoạ

5.7.1 Các thủ tục xử lý vấn đề lộ khoá và sự cố

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

Nếu khóa bí mật của MobiFoneCA bị tổn hại, quản lý CA phải:

- Cố gắng hết sức để thông báo cho các thuê bao và các RA;
- Chấm dứt việc phát hành và phân phối các chứng chỉ và CRLs;
- Yêu cầu thu hồi giấy chứng nhận thỏa hiệp;
- Khởi tạo một cặp khoá và chứng thư của MobiFoneCA mới và công bố trong kho lưu trữ;
- Thu hồi tất cả các chứng chỉ hợp lệ ký bởi khoá bị xâm hại;
- Xuất bản danh sách CRL mới trong kho của MobiFoneCA;
- Thông báo tới cơ quan an ninh liên quan và Trung tâm Chứng thực chữ ký số Quốc gia;
- Thông báo tới các bên tin tưởng, các CA có liên quan.

MOBIFONECA có trách nhiệm vận hành một kế hoạch khôi phục sự cố và đảm bảo việc giữ duy trì hoạt động kinh doanh. Kế hoạch chi tiết là tài liệu nội bộ không công bố, tuy nhiên sẽ được cung cấp tới những người có trách nhiệm, và được ủy quyền tiến hành kiêm tra an ninh.

Một hệ thống sao lưu dâm bảo phục hồi nguyên trạng MOBIFONECA được đặt tại trung tâm dự phòng.

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

MobiFoneCA sẽ có những nỗ lực phòng ngừa tốt nhất để giúp phục hồi.

Để có thể tiếp tục phục hồi các hoạt động một cách nhanh nhất sau khi máy tính của MobiFoneCA bị lỗi, các bước sau đây sẽ được thực hiện:

- Tất cả các phần mềm trên MobiFoneCA sẽ được sao lưu trên phương tiên lưu trữ di động, sau khi cài đặt một phiên bản mới của bất kỳ một thành phần nào của MobiFoneCA.
- Tất cả các file dữ liệu của các CA hoạt động offline sẽ được sao lưu trên phương tiện lưu trữ di động sau mỗi lần thay đổi.

Nếu phần cứng hoặc phần mềm của Server ký bị lỗi, trạng thái này sẽ được chẩn đoán và phục hồi kịp thời. Nếu có bất kỳ một nghi ngờ nào về mức độ thiệt hại chưa được khắc phục Server này được cài đặt lại từ đầu bằng cách sử dụng các thiết bị gốc và các phần mềm kèm theo.

Nếu dữ liệu bị lỗi, sẽ được chẩn đoán và phục hồi lại dữ liệu sao lưu gần nhất.

Hệ thống sẽ được khởi động lại dựa trên phần cứng dự phòng bằng cách sử dụng phần mềm sao lưu dữ liệu được sao lưu tại DRDC của MobiFoneCA, sau đó sẽ được kiểm tra và đưa vào hoạt động trong một điều kiện đảm bảo an toàn.

Hệ thống máy tính bị lỗi sau đó sẽ được phân tích tìm sự cố.

Nếu cần thiết, thêm các biện pháp bảo vệ cũng sẽ đưa ra để ngăn chặn sự xuất hiện của sự cố tương tự trong tương lai.

MobiFoneCA có các hợp đồng với các chuyên gia về PKI để phân tích các sự cố này.

MobiFoneCA thông báo với Trung tâm Chứng thực điện tử quốc gia về sự cố này không muộn quá 01 ngày làm việc kể từ khi sự cố xảy ra, theo các quy định của Thông tư 06/2015/TT-BTTTT về Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số do Bộ Thông tin truyền thông ban hành.

5.7.3 Khả năng phục hồi hoạt động sau thảm họa.

MobiFoneCA cần có kế hoạch dự phòng, đảm bảo hoạt động liên tục kể cả có thảm họa hay sự cố lớn. Các kế hoạch này cần được kiểm tra, thử nghiệm và xem xét định kỳ.

MobiFoneCA có khả năng phục hồi những hoạt động quan trọng sau đây trong 01 ngày làm việc sau khi một thảm học xảy ra.

a. Công bố thông tin thu hồi chứng thư số

b. Ban hành chứng thư số

c. Thu hồi chứng thư số

MobiFoneCA dự phòng các thiết bị phần cứng và phần mềm cung cấp dịch vụ. Khóa bí mật của MobiFoneCA cũng được dự phòng và duy trì phục vụ cho mục đích phục hồi hệ thống như phần VI.2.4.

Cơ sở dữ liệu của MOBIFONECA phục hồi thảm họa sẽ được đồng bộ với cơ sở dữ liệu chính trong thời gian phù hợp, ít nhất là một ngày một lần đồng bộ.

Kế hoạch phục hồi của MOBIFONECA được thiết kế có khả năng phục hồi hoạt động toàn bộ hệ thống trong vòng một tuần.

5.8 Dừng hoạt động

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

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

Thông báo tạm dừng dịch vụ không ít hơn 60 ngày trong trường hợp chấm dứt bình thường. Các CA quản lý tại thời điểm chấm dứt có trách nhiệm lưu trữ tất cả các hồ sơ theo yêu cầu trong phần 5.5.2. Thực hiện chuyển giao cần thiết của dịch vụ CA tới các CA đang hoạt động theo thỏa thuận.

VI. Đảm bảo an toàn an ninh về kỹ thuật

6.1 Tạo và phân phối cặp khoá

6.1.1 Cách thức tạo cặp khóa, kích thước cặp khoá

Cặp khoá cho MobiFoneCA được tạo ra bởi các nhân viên thẩm quyền chứng thực trên máy tính không kết nối vào mạng. Cặp khoá này được sinh trực tiếp bên trong thiết bị HSM của hãng Utimaco đạt chuẩn FIPS 140-2 Level 3 trở lên với thuật toán RSA. Quản lý và bảo mật khóa CA sử dụng mô-đun phần cứng bảo mật (HSM) này bảo mật quá trình khởi tạo khóa; phần cứng chuyên nghiệp bảo vệ và quản lý vòng đời khóa bảo mật; gắn kết chính sách bảo mật vào HSM; nâng cao hiệu suất và đảm bảo tính ổn định, sẵn sàng và yêu cầu cao về an toàn bảo mật hệ thống.

Đối với cặp khoá của thuê bao sinh tại nhà cung cấp dịch vụ. Cơ quan cung cấp dịch vụ chứng thực sử dụng thiết bị chuyên dụng HSM của máy chủ thực hiện khởi tạo và quản lý cặp khoá với thuật toán mã hoá phi đối xứng RSA hoặc cặp khoá được sinh ngay trong phần cứng của thiết bị đầu cuối của thuê bao (eToken) đạt chuẩn FIPS 140-2 Level 2 trở lên. Mỗi cặp khoá đảm bảo được tính duy nhất và không bị suy ra khoá bí mật từ khoá công khai tương ứng. Việc phân phối khoá đến thuê bao được thực hiện bằng thiết bị lưu trữ thông minh, đảm bảo an toàn bảo mật tuyệt đối trong việc phân phối khoá.

Đối với cặp khoá thuê bao tự sinh: MobiFoneCA cung cấp phần mềm để thuê bao sinh cặp khoá theo thuật toán phi đối xứng RSA hoặc thuê bao tự sử dụng chương trình sinh cặp khoá của mình theo thuật toán RSA.

6.1.2 Chuyển giao khoá bí mật cho thuê bao

Thiết bị phần cứng Token sẽ sinh cặp khóa (bao gồm private key và public key). Chứng thư số của thuê bao được tạo ra dựa trên thông tin về public key và các thông tin khác liên quan đến việc xác định của chủ thể (tên doanh nghiệp, mã số thuế, địa chỉ, ...). Hệ thống CA sẽ tạo chứng thư số dựa trên các thông tin đó, sau đó ký vào chứng thư đã được tạo và chuyển chứng thư cho Hệ thống RA. Hệ thống RA sẽ trả về chứng thư cho thiết bị Token. Sau đó Thiết bị được bàn giao tới khách khàng (Bao gồm Thiết bị Token, và giấy chứng nhận).

6.1.3 Chuyển giao khoá công khai tới tổ chức ban hành chứng thư

Các RA chứng thực các yêu cầu truyền các yêu cầu xác nhận có chứa khóa công khai trong một e-mail được ký bởi một trong các đại lý của nó.

MobiFoneCA có thể xử lý yêu cầu cấp phát chứng thư dựa trên tải yêu cầu theo định dạng PKCS#10.

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

Chứng thư số của CA (có chứa khoá công khai) được chuyển giao cho thuê bao bằng giao dịch trực tuyến từ Server website trực tuyến. Chứng thư của CA cũng có thể tải về từ kho lưu trữ (xem mục 2.1)

6.1.5 Kích thước khoá

Chuẩn hiện tại của dịch vụ MobiFoneCA yêu cầu chiều dài tối thiểu của cặp khoá để đảm bảo mức độ mã hoá đủ mạnh là 2048 bits RSA.

Khoá của MobiFoneCA có chiều dài là 2048 bits.

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

Không có quy định.

6.1.7 Mục đích sử dụng khoá (như trong X.509 v3 lĩnh vực sử dụng khoá)

Khoá được sử dụng theo mỗi loại chứng thư:

- Với thuê bao:
  - ✓ Chứng thực;
  - ✓ Chống chối bỏ;

- ✓ Mã hoá dữ liệu;
- ✓ Thiết lập phiên giao dịch;
- ✓ Kiểm tra tính toàn vẹn của dữ liệu.

- Với chứng thư tự ký của CA
  - ✓ Ký chứng thư;
  - ✓ Ký CRL;
  - ✓ Thu hồi chứng thư.

6.2 Kiểm soát và bảo vệ khóa bí mật

6.2.1 Tiêu chuẩn kỹ thuật đối với thiết bị mật mã

Các khoá bí mật được lưu giữ trong môi trường phần cứng an toàn (các khoá ký) và được lưu trữ trong cơ sở dữ liệu của máy chủ (các khoá mã).

Hệ thống CA của MobiFoneCA sử dụng thiết bị HSM của hãng Utimaco. Các thiết bị này quản lý khoá trên thiết bị phần cứng từ khi sinh khoá quản lý khoá CA, ký chứng thư số, xác nhận, lưu trữ và sao lưu khoá.

Các thao tác với khoá chỉ được thực hiện bên trong thiết bị phần cứng nhằm ngăn chặn những người không có quyền truy cập được phép sử dụng.

Các thiết bị HSM này tuân theo chuẩn FIPS PUB 140-2 level 3.

Đối với thuê bao PKI Token sử dụng chuẩn FIPS 140-2 Level 2.

6.2.2 Cơ chế kiểm soát, bảo vệ khóa bí mật

Kiểu điều khiển này chưa được cài đặt.

Cơ chế kiểm soát khóa bí mật được MOBIFONECA sử dụng là cơ chế chia sẻ mã. Cơ chế này tách dữ liệu kích hoạt khóa bí mật thành N phần khác nhau, các phần này được giữ bởi các đối tượng khác nhau.

- Với mỗi chức năng nhất định, cần có M phần (M nhỏ hơn hoặc bằng N) mã chia sẻ để kích hoạt chứng năng đó.
- Tại MOBIFONECA,N = 5;M=3 Theo nguyên tắc này, khóa MBK sẽ được chia thành 5 mảnh và ghi vào trong 5 smartcard và được phân phối cho 5 nhân sự (n=5) của MOBIFONECA. Để có thể sử dụng được khóa này, cần ít nhất tối thiểu 3 nhân sự (m=3) sử dụng thẻ để xác thực.

6.2.3 Sao lưu dự phòng khóa bí mật

MOBIFONECA không lưu khóa bí mật của thuê bao.

MOBIFONECA sao lưu các khóa bí mật của CA cho mục đích sử dụng cho hệ thống dự phòng, khôi phục và khắc phục sau thảm hoạ.

6.2.4 Lưu trữ khoá bí mật

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

6.2.5 Cách thức sao lưu khoá bí mật

Hiện nay MobiFoneCA sao lưu khóa từ HSM vào Smartcard chuyên dụng của HSM đó, trong quá trình sao lưu thì HSM đã mã hóa dữ liệu. Khóa từ Smartcard được đưa vào HSM và chỉ có HSM đó mới giải mã được. Thực hiện như vậy sẽ ngăn chặn mất mát, ăn trộm, sửa đổi, tiết lộ và sử dụng trái phép khoá bí mật. Việc chuyển giao này sẽ bị giới hạn để tạo ra các bản sao dự phòng khoá bí mật trên mô đun phần cứng phù hợp với tiêu chuẩn quy định trong chính sách bảo mật của MobiFoneCA. Công việc này để đề phòng khi HSM chính bị hư hỏng vật lý, hoặc do thiên tai thảm họa xảy ra thì còn có HSM dự phòng đã được sao lưu khóa bí mật.

6.2.6 Phương thức kích hoạt khoá bí mật

Khoá bí mật của CA được sử dụng HSM để lưu trữ khóa bí mật, việc kích hoạt khóa bí mật yêu cầu các mã chia sẻ theo cơ chế chia sẻ mã trong 6.2.2.

Việc kích hoạt khóa riêng thuê bao PKI Token được thực hiện bởi mã số PIN, khóa bí mật của thuê bao được quản lý bảo mật theo tiêu chuẩn FIPS 140-2 Level 2.

6.2.7 Phương thức dừng hiệu lực của một khoá bí mật

Bản rõ của khoá bí mật của CA được lưu trữ trong RAM và xoá hoàn toàn khi hoạt động của cần thiết của nó kết thúc.

Khoá bí mật của thuê bao dừng hiệu lực sau khi hoàn thành hoạt động cần thiết của nó như mỗi khi đăng xuất khỏi hệ thống, hoặc gỡ bỏ thẻ lưu trữ ra khỏi đầu đọc thẻ (phụ thuộc vào loại thiết bị lưu trữ đầu cuối mà thuê bao sử dụng).

6.2.8 Phương thức huỷ khoá bí mật

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

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

6.2.9 *Phương pháp ngừng kích hoạt khóa bí mật*

Khóa bí mật của MOBIFONECA /RA bị ngừng kích hoạt khi không chứa trong Token Reader (HSM). RA của MOBIFONECA được yêu cầu phải đăng xuất khỏi hệ thống khi rời chỗ làm việc.

Khóa bí mật của quản trị hệ thống, của RA và của thuê bao có thể bị ngừng kích hoạt sau mỗi nhiệm vụ, sau khi đăng xuất hệ thống hoặc sau khi loại bỏ USB Token khỏi máy tính. Trong mọi trường hợp, thuê bao phải có nghĩa vụ thực hiện các biện pháp bảo vệ khóa bí mật của mình.

6.3 Các khía cạnh khác của việc quản lý cặp khoá

6.3.1 Lưu trữ khoá công khai

MOBIFONECA phải lưu trữ tất cả các chứng thư đã phát hành trên máy chủ LDAP Slaver và sao lưu định kỳ theo quy trình sao lưu tập trung của MOBIFONECA.

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

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

Không có quy định về tính hợp lệ của cặp khoá tạo ra. Chỉ có hiệu lực của chứng thư do MobiFoneCA được xác định bởi tài liệu CP/CPS này.

Mặc định thời gian hoạt động chứng thư của thuê bao là 395 ngày (xấp xỉ 01 năm, 01 tháng), thời gian hoạt động chứng thư RA là 03 năm.

Thời gian hoạt động của chứng thư số MobiFoneCA là 05 năm.

Thêm vào đó dịch vụ MobiFoneCA ngưng cấp phát các chứng thư mới trước ngày chứng thư của CA hết hạn nhằm đảm bảo rằng không có một chứng thư nào được cấp phát bởi một CA cấp dưới sẽ bị hết hạn sau khi các chứng thư của các CA cấp trên đó hết hạn sử dụng.

6.4 Kích hoạt dữ liệu

6.4.1 Quá trình khởi tạo và cài đặt dữ liệu kích hoạt khóa bí mật.

Dữ liệu kích hoạt khóa bí mật của MOBIFONECA được chia thành các mã chia sẻ, các mã chia sẻ này được tạo theo các yêu cầu trong phần 6.2.2 và tuân theo các thủ tục của nghi lễ sinh khóa. Quá trình tạo và phân phối mã chia sẻ được ghi nhật ký.

MobiFoneCA khuyến cáo đối với thuê bao sử dụng mật khẩu đủ mạnh để bảo vệ các khóa bí mật của họ (bao gồm ít nhất 12 ký tự). MobiFoneCA cũng khuyến nghị sử dụng cơ chế xác thực 2 nhân tố (ví dụ: thẻ và mã nhận dạng cá nhân (PIN), thẻ và sinh trắc học, hay sinh trắc học và mã bảo vệ cá nhân) để kích hoạt khóa bí mật.

6.4.2 Bảo vệ dữ liệu kích hoạt

MobiFoneCA khuyến cáo thuê bao của mình lưu trữ các khóa bí mật của họ ở dạng mã hoá và bảo vệ khóa bí mật của mình thông qua sử dụng thiết bị phần cứng đầu cuối/ hoặc mật khẩu đủ mạnh. MobiFoneCA khuyến khích sử dụng cơ chế xác thực hai nhân tố.

Trường hợp chứng thư số được lưu trên token và bảo vệ bằng mật khẩu MobiFoneCA khuyến cáo thuê bao định kỳ thay đổi mật khẩu.

Bất kỳ dự phòng của mật khẩu bảo vệ khóa bí mật (trên máy hoặc trên giấy) phải được lưu trữ ở nơi an toàn.

6.4.3 Những khía cạnh khác của dữ liệu kích hoạt.

Không có quy định.

6.4.4 Quy trình kích hoạt dữ liệu khóa bí mật

Đối với khóa thuê bao: khóa bí mật của thuê bao được tạo trực tiếp PKI Token tiêu chuẩn FIPS 140-2 Level 2. Mã PIN kích hoạt được sinh ngẫu nhiên, và bàn giao tách riêng đến thuê bao. PKI Token được bàn giao cho thuê bao trước khi MOBIFONECA bàn giao mã PIN kích hoạt PKI Token. Sau khi MOBIFONECA xác nhận việc bàn giao hợp lệ PKI Token tới thuê bao, và sau khi thuê bao đã xác nhận nội dung của chứng thư số do MOBIFONECA cấp mã PIN kích hoạt Token sẽ được MOBIFONECA gửi riêng tới thuê bao.

Đối với khóa bí mật của MOBIFONECA:

Bước 1: Đăng nhập HSM

Thực hiện nhập mật khẩu đăng nhập HSM

Bước 2: Đăng nhập vùng chứa khóa bí mật

Thực hiện nhập mật khẩu xác thực việc đăng nhập vào vùng chứa khóa bí mật.

Bước 3: Kích hoạt khóa bí mật

Hệ thống MOBIFONECA được quản lý bảo mật bên trong HSM chuẩn bảo mật 140-2 Level 3 và được kiểm soát bằng bộ thẻ thông minh chuyên dụng theo cơ chế 3 x5. Thực hiện sử dụng tối thiểu 3 thẻ mật mã để kích hoạt khóa bí mật.

6.5 Kiểm soát an ninh máy tính

6.5.1 Các yêu cầu an ninh đối với hệ thống máy tính

MobiFoneCA đảm bảo chắc chắn rằng các hệ thống chứa phần mềm CA và các tệp dữ liệu phải là hệ thống đáng tin cậy chống lại được các truy cập trái phép. Thêm vào đó, MobiFoneCA cũng giới hạn tối đa các truy cập đến máy chủ chính với những lý do quyền hạn để truy cập.

Lớp mạng máy tính được phân tách logic thành các phần khác nhau. Phân tách này ngăn chặn truy cập mạng, ngoài trừ thông qua các xử lý ứng dụng đã được xác định. Tất cả các phiên làm việc đều được xác thực bằng mật khẩu hoặc chứng thư proxy để đăng nhập.

6.5.2 Định kỳ đánh giá an ninh hệ thống máy tính

Hệ thống máy chủ cung cấp dịch vụ của MOBIFONECA được đánh giá định kỳ 6 tháng một lần.

6.6 Kiểm soát an ninh quy trình sử dụng

6.6.1 Kiểm soát về phát triển hệ thống

MOBIFONECA sử dụng các hệ thống có chứng chỉ tiêu chuẩn công nghệ thông tin.

6.6.2 Kiểm soát vấn đề quản lý bảo mật

MOBIFONECA áp dụng cơ chế kiểm soát và giám sát theo quy định của nhà sản xuất.

6.6.3 Kiểm soát về mặt bảo mật đối với một chu kỳ sống

Không có quy định.

6.6.4 Quy trình, thủ tục giám sát, quản lý giám sát việc triển khai hoạt động của hệ thống

Bước 1: MOBIFONECA phân vai trò, quyền sử dụng phân công trách nhiệm cho từng đối tượng tham gia sử dụng hệ thống

Bước 2: MOBIFONECA sử dụng các phần mềm ứng dụng lưu lại toàn bộ nhật ký trong quá trình sử dụng hệ thống. Đặc biệt đối với những thay đổi liên quan đến dữ liệu hoặc cấu hình gây ảnh hưởng đến an ninh của hoạt động của hệ thống.

Bước 3: MOBIFONECA có hệ thống cảnh báo trong các trường hợp thay đôi dẫn đến ảnh hưởng của hệ thống.

Bước 4: Đối với việc nâng cấp, thay đổi các chức năng phần mềm, phần cứng thiết bị nằm trên hệ thống MOBIFONECA ghi nhận hiện trạng, nhật ký thời gian bắt đầu, kết thúc, nội dung thực hiện, kết quả thực hiện, các lỗi xây ra trong quá trình thực hiện. Toàn bộ nội dung nhật ký chi tiết được MOBIFONECA lưu lại để có thể truy vết hoặc đánh giá nguyên nhân dựa trên nội dung nhật ký.

6.7 Giám sát an ninh hệ thống

Những chức năng CA và RA được thực hiện dùng mạng được bảo mật đáp ứng phù hợp với những tài liệu chuẩn trong chính sách bảo mật nhằm ngăn chặn sự truy cập trái phép, sự xáo trộn, và tấn công dịch vụ. Sự truyền thông và các thông tin quan trọng sẽ được bảo vệ bằng cách dụng mã hoá điểm-điểm để đảm bảo tính tin cậy và chữ ký số để xác nhận và xác thực.

MOBIFONECA phân đoạn hệ thống cấp chứng thư số thành các vùng mạng dựa trên mối quan hệ chức năng và logic của chúng. Các vùng mạng được thiết lập trong hệ thống CA của MOBIFONECA khi lắp đặt được bảo vệ khỏi người dùng trái phép thông qua một loạt tường lửa dựa trên mạng và máy chủ lưu trữ cũng như các hệ thống giám sát và phát hiện khác. Tường lửa được định cấu hình với các quy tắc hỗ trợ các dịch vụ, giao thức, công và thông tin liên lạc mà MOBIFONECA đã xác định là cần thiết cho hoạt động của hệ thống.

Đánh giá rủi ro định kỳ và phân tích mối đe dọa được thực hiện bởi nhóm Đánh giá Bảo mật để xác định các mối đe dọa và lỗ hổng trong hệ thống CA của MOBIFONECA. Quyền truy cập hợp lý vào hệ thống CA bị hạn chế đối với các cá nhân được ủy quyền trong các vai trò đáng tin cậy. Hệ thông CA được định cấu hình bằng cách xóa / vô hiệu hóa các tài khoản, ứng dụng, dịch vụ, giao thức và công không được sử dụng trong hoạt động của CA. Phần mềm chống vi-rút và phát hiện phần mềm độc hại được cài đặt trên hệ thống CA của MOBIFONECA.

Những chức năng CA và RA được thực hiện dùng mạng được bảo mật đáp ứng phù hợp với những tài liệu chuẩn trong chính sách bảo mật nhằm ngăn chặn sự truy cập trái phép, sự xáo trộn, và tấn công dịch vụ. Sự truyền thông và các thông tin quan

trọng sẽ được bảo vệ bằng cách dụng mã hoá điểm - điểm để đảm bảo tính tin cậy và chữ ký số để xác nhận và xác thực. Máy chủ ký của MOBIFONECA được hoạt động trong vùng mạng không có kết nối trực tiếp với Internet.

Tất cả các máy tính CA khác được bảo vệ bằng firewall và Hệ thống phát hiện xâm nhập và phòng chống truy cập trái phép (IDS/IPS) hoặc bằng cách loại bỏ các dịch vụ không cần thiết.

6.8 Nhãn thời gian

Các chứng chỉ, thông tin thu hồi (CLS, OCSP) có chứa thông tin về thời gian và ngày.

Các thông tin thời gian cần thiết như trên không được mã hoá.

VII. Định dạng chứng thư số, danh sách thu hồi chứng thu số (CRL), giao thức kiểm tra chứng thư số trực tuyến (OCSP)

7.1 Định dạng của chứng thư số

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

Tên trường		Giá trị
Phiên bản (Version)		MobiFoneCA phát hành chứng thư X.509 phiên bản 3
Số hiệu chứng thư/ Serial Number		Do MobiFoneCA gán, là định dạng duy nhất của chứng thư số, số nguyên dương xác định duy nhất một số chứng thư số do CA cấp thuê bao, độ dài không quá 20 octet (byte)
Thuật toán ký chứng thư số của CA (Signature)		Sha256RSA
Issuer	Tên của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng	MOBIFONECA

	(commonName)	
	Tên của tổ chức/doanh nghiệp CA (organizationName)	MOBIFONECA
	Tên (countryName)	VN
Validity	Thời điểm chứng thư bắt đầu có hiệu lực (notBefore)	Thời điểm chứng thư bắt đầu có hiệu lực. Được đồng bộ với NTP Server.
	Thời điểm chứng thư hết hiệu lực/ Not After	Thời điểm chứng thư hết hiệu lực. Được đồng bộ với NTP Server.
Subject	Định danh thuê bao (userID)	MST: [mã số thuế] hoặc MNS: [mã quan hệ ngân sách] hoặc BHXH: [mã số bảo hiểm xã hội] hoặc CMND:[số chứng minh nhân dân] hoặc HC: [số hộ chiếu] hoặc CCCD: [số thẻ căn cước công dân]
	Tên của thuê bao	Tên của thuê bao được cấp chứng thư số

	(commonName)	
	Tên của tổ chức/đơn vị quản lý thuê bao (organizationName)	Tên của tổ chức quản lý thuê bao (nếu có)
	Tên tỉnh/TP nơi sống/làm việc của thuê bao (stateOrProvinceName)	Tên của tỉnh/TP nơi sống/làm việc của thuê bao bằng tiếng Việt, có dấu, các chữ cái đầu viết hoa
	Tên nước (countryName)	VN
Subject Public Key Info	Thuật toán sinh khóa (algorithm)	RSA (2048 bits)
	Khóa công khai của thuê bao (subjectPulic Key)	Khóa công khai của thuê bao. Được mã hóa theo tiêu chuẩn RFC 3280; Xác định thuật toán RSA được sử dụng cùng với khoá
Thuật toán chữ ký số áp dụng/ Signature Algorithm		Sha256RSA
Chữ ký số của trung tâm chứng thư số / Signature		Chữ ký số của trung tâm chứng thư số MobiFoneCA

Các thông tin khác cho mục đích quản lý, sử dụng, an toàn, bảo mật do tổ chức cung cấp dịch vụ chữ ký số quy định.	

7.1.1 Phiên bản

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

7.1.2 Phần mở rộng của chứng thư

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

Chứng thư số dùng cho cá nhân

Basic Constraints	critical, ca: false
Subject Key Identifier	hash
Authority Key Identifier	keyid
Key Usage	digitalSignature nonRepudiation keyEncipherment dataEncipherment keyAgreement
Extended Key Usage	clientAuth codeSigning emailProtection timeStamping
Certificate Policies	OID của CP/CPS có hiệu lực tại thời điểm phát hành chứng thư

Subject alternative name	Chứng thư được cấp cho cá nhân địa chỉ e-mail có liên quan để liên lạc với thuê bao được quy định trong CP/CPS này.
Issuer Alternative Name	Liên kết (URL) đến chứng thư của MobiFoneCA
CRL Distribution Points	URL của CRL

Chứng thư số dùng cho dịch vụ / Máy chủ

Basic Constraints	critical, ca: false
Subject Key Identifier	hash
Authority Key Identifier	keyid
Key Usage	digitalSignature nonRepudiation keyEncipherment dataEncipherment keyAgreement
Extended Key Usage	clientAuth serverAuth
Certificate Policies	OID của CP/CPS có hiệu lực tại thời điểm phát hành chứng thư
Subject alternative name	Tên miền đầy đủ của máy chủ lưu trữ (DNS:FQDN)
Issuer Alternative Name	Liên kết (URL) đến chứng thư của MobiFoneCA

CRL Distribution Points	URL của CRL

7.1.3 Thuật toán nhận biết đối tượng

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

- sha256withRSAEncryption OBJECT IDENTIFIER := ({iso(1) memberbody(2) us(840) rsadsi(113549) pkes(1) pkes-1(1) 11}

- Thủ tục ký chứng thư số áp dụng lược đồ RSASSA-PSS được quy định trong PKCS#1 phiên bản 2.1

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

7.1.4 Cấu trúc tên

Mỗi chứng thư có một tên duy nhất và rõ ràng. Tên phân biệt trong tất cả các chứng thư phát hành bởi MobiFoneCA và tuân theo cấu trúc được định nghĩa trong tiêu chuẩn ITU-T Standards Recommendation X.501 (Xem mục 3.1.1).

7.1.5 Ràng buộc tên

Không có những ràng buộc khác hơn so với quy định tại mục 4.1.4, và 3.1.1, 3.1.2.

7.1.6 Chính sách nhận biết đối tượng

OID của Quy chế chứng thực này là 1.3.6.1.4.1.30339.1.x.3

Trong đó, x được xác định khi MobiFoneCA đăng ký với Bộ Thông tin và Truyền thông.

7.1.7 Cách dùng của sự mở rộng chính sách ràng buộc

Không có ràng buộc nào

7.1.8 Chính sách hạn định cấu trúc và ngữ nghĩa

Không có quy định

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

Không có quy định

7.1.10 Khuôn dạng của danh sách thu hồi chứng thư CRL

Version	V2

Signature	SHA256 WithRSAEncryption
Issuer	MobiFoneCA
This Update	Chỉ ra ngày và thời gian CRL được công bố
Next Update	Chỉ ra ngày và thời gian danh sách thu hồi kế tiếp được cấp.
Revoked Certificates	serialNumbers của chứng thư bị thu hồi

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

7.1.11 Phiên bản

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

7.1.12 CRL và phần mở rộng đầu vào CRL

Không có quy định

7.2 Profile của OCSP

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

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

7.2.1 Phiên bản

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

7.2.2 Phần mở rộng của OCSP

Chưa được xác định

VIII. Kiểm định tính tuân thủ và các đánh giá khác

8.1 Tần suất và các trường hợp đánh giá

Các cuộc kiểm tra sự tuân thủ điều khoản CP/CPS được tiến hành ít nhất mỗi năm một lần.

MobiFoneCA tiến hành kiểm tra sự tuân thủ các thủ tục của mỗi RA với CP/CPS có hiệu lực ít nhất mỗi năm một lần.

8.2 Đơn vị, người thực hiện kiểm tra kỹ thuật

Người thực hiện kiểm tra kỹ thuật được chỉ định bởi RootCA để thực hiện các cuộc kiểm tra kỹ thuật MOBIFONECA.

8.3 Các nội dung kiểm tra kỹ thuật

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

- Hạ tầng hệ thống.
- Các quy trình quản lý khóa.
- Quy trình vận hành hệ thống
- Các nội dung khác theo yêu cầu của đơn vị kiểm tra kỹ thuật.

8.4 Xử lý khi phát hiện sai sót

Sau khi có báo cáo kiểm toán kỹ thuật, MOBIFONECA sẽ làm việc với RootCA về những nội dung chưa phù hợp.

- MOBIFONECA sẽ nghiên cứu và đề ra và thực hiện phương án xử lý những nội dung chưa phù hợp trong thời gian thống nhất với RootCA.
- MOBIFONECA hành động ngay lập tức nếu đánh giá cho thấy một sự vi phạm các quy định trong CP/CPS. Nếu phát hiện vi phạm trực tiếp tới sự tin cậy của chứng thư, Chứng thư được phát hành vi phạm sẽ bị thu hồi ngay lập tức.

Dịch vụ của MOBIFONECA sẽ bị ngừng trong các tình huống sau:

- Báo cáo kiểm tra kỹ thuật cho thấy có lỗi nghiêm trọng có thể ảnh hưởng ngay lập tức tới an ninh của hệ thông MOBIFONECA.
- MOBIFONECA thực hiện kế hoạch xử lý nhưng không có kết quả.

8.5 Công bố kết quả kiểm tra kỹ thuật.

Báo cáo kết quả kiểm toán kỹ thuật được MOBIFONECA công bố tại http:/mobica.vn.

Quản lý CA sẽ công bố kết quả trên trang web của MOBIFONECA với thông tin chi tiết về sự vi phạm CP/CPS.

8.6 Tần suất và các trường hợp đánh giá

Không quy định

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

Người thực hiện kiểm định phải là đơn vị độc lập có năng lực thành thạo về công nghệ hạ tầng khóa công khai, công cụ và kĩ thuật an toàn thông tin và được chứng nhận bởi RootCA.

IX. Các nội dung nghiệp vụ và pháp lý khác

9.1 Phí/Giá

9.1.1 Lệ phí cấp Chứng thư hoặc gia hạn chứng thư

Khách hàng của dịch vụ MobiFoneCA phải trả phí khi xin cấp chứng thư cho nhà cung cấp dịch vụ.

9.1.2 Lệ phí sử dụng chứng thư

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

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

Các thành phần tham gia dịch vụ MobiFoneCA không phải trả phí cho việc phát hành các CRL. Tuy nhiên MobiFoneCA sẽ thu phí khi cung cấp dịch vụ OCSP hoặc các dịch vụ cung cấp thông tin trạng thái khác.

9.1.4 Lệ phí sử dụng cho các dịch vụ khác

- Phí cho những dịch vụ khác như là thông tin về chính sách: MobiFoneCA, RA và đại lý có thể thiết lập và tính một mức phí hợp lý cho dịch vụ khác.
- Phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số: Dựa trên cơ sở pháp lý Thông tư 305/2016/TT-BTC ngày 15/11/2016 quy định mức thu, chế độ thu, nộp, quản lý và sử dụng phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số. Tức thu phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số: 3000đồng/chữ ký số/tháng. Chứng thư số phát sinh hiệu lực hoạt động tại bất cứ thời điểm nào của tháng được tính là 01(một) tháng sử dụng.

9.1.5 Chính sách hoàn trả phí

Bất kỳ các khoản phí nào cho việc xin cấp chứng thư số mà không được phê chuẩn sẽ được hoàn trả.

9.2 Trách nhiệm tài chính

9.2.1 Đăng thông tin bảo hiểm

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

9.2.2 Các trường hợp MobiFoneCA tiến hành đền bù bảo hiểm

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

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

9.2.3 Các trường hợp không được đền bù bảo hiểm

MobiFoneCA không chịu trách nhiệm trong các trường hợp:

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

9.2.4 Các tài sản khác

Không được đề cập.

9.2.5 Trường hợp bị thu hồi giấy phép

MOBIFONECA đã thực hiện bảo lãnh thanh toán của một ngân hàng thương mại hoạt động tại Việt Nam không dưới 5 (năm) tỷ đồng, để giải quyết các rủi ro và các khoản đền bù có thể xảy ra trong quá trình cung cấp dịch vụ và thanh toán chi phí tiếp nhận và duy trì cơ sở dữ liệu của MOBIFONECA trong trường hợp bị thu hồi giấy phép.

9.3 Bảo mật các thông tin nghiệp vụ

9.3.1 Phạm vi thông tin nghiệp vụ cần được bảo vệ

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

- Các dữ liệu CA, được phê chuẩn hoặc không phê chuẩn;
- Các dữ liệu về đơn xin cấp chứng thư;
- Các khoá bí mật của thuê bao;
- Các dữ liệu kiểm toán.

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

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

9.4 Bí mật thông tin cá nhân

9.4.1 Kế hoạch đảm bảo tính riêng tư

Mọi thông tin thuê bao không được công bố qua nội dung của chứng thư số, dịch vụ Directory và CRL được coi là bí mật.

9.4.2 Những thông tin được coi là riêng tư

Thông tin có trong chứng thư và các CRL do MOBIFONECA phát hành không được coi là riêng tư. Khi yêu câu một chứng thư từ MOBIEFONECA các thuê bao đã đồng ý bao gồm các thông tin này như một phần của chứng thư được công bố.

9.4.3 Trách nhiệm mật thông tin cá nhân

MOBIFONECA và các RA được công nhận của nó có trách nhiệm bảo vệ thông tin riêng tư của các thuê bao và phải tuân theo những luật riêng tư trong phạm vi quyền hạn của mình.

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

Trong trường hợp MOBIFONECA hoặc bất kỳ một RA của nó muốn sử dụng thông tin riêng tư của thuê bao phải được các thuê bao đồng ý bằng văn bản.

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

MobiFoneCA có trách nhiệm cung cấp thông tin riêng tư nếu:

- Khi có yêu cầu của cơ quan pháp luật có thẩm quyền hoặc các quá trình liên quan đến luật pháp đã được quy định.
- Khi có yêu cầu truy cập thông tin để phục vụ cho quản trị (yêu cầu xác nhận, yêu cầu cho quá trình tạo tài liệu).

9.4.6 Những trường hợp làm lộ thông tin khác

Không có quy định.

9.5 Quyền sở hữu trí tuệ

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

Các tên phân biệt (DN) của các CA của MobiFoneCA vẫn là tài sản của MobiFoneCA và tuân theo những quyền sở hữu này.

9.6 Vấn đề đại diện và bảo lãnh

9.6.1 Đại diện của CA và vấn đề bảo lãnh

Các thông tin được công bố trong chứng thư, CRLs và OCSP đáp ứng một cách chính xác khả năng cung cấp tốt nhất của MobiFoneCA. Không bảo lãnh khác được đưa ra.

MOBIFONECA đảm bảo rằng:

- Không thay đổi thông tin đăng ký chứng thư số được cung cấp bởi đối tượng đăng ký.
- Không có lỗi trong quá trình duyệt và ban hành chứng thư số
- Chứng thư số do MOBIFONECA ban hành đáp ứng các yêu cầu trong quy chế này.
- Cung cấp dịch vụ thu hồi và cho phép sử dụng địa chỉ lưu trữ phù hợp với quy chế chứng thực này.
- Chịu trách nhiệm về việc quản lý và xác minh các điều kiện hoạt động của RA theo quy định của pháp luật.

9.6.2 Tuyên bố và cam kết của RA

Tất cả các RA thực hiện nhiệm vụ của họ về nhận dạng và xác thực của các bên yêu cầu như được mô tả trong 3.2.3 và 3.2.2 với trách nhiệm và khả năng tốt nhất. Không có bảo lãnh khác được đưa ra.

RA đảm bảo rằng:

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

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

- Loại chứng thư số mà RA được phép tham gia cung cấp
- Các bước trong quy trình cấp phát chứng thư số RA được thực hiện.
- Chứng thư số chỉ được cấp sau khi BkavCA đã nhận đầy đủ hồ sơ của thuê bao, và thông tin thuê bao được thẩm định.
- Cam kết của RA với MOBIFONECA đúng như trong hợp đồng đã ký và theo quy định của pháp luật.

- Nhân viên RA trực tiếp tham gia vào quy trình cung cấp chứng thư số phải có hiểu biết pháp luật về chữ ký số và dịch vụ chứng thực chữ ký số.

9.6.3 Tuyên bố và cam kết của thuê bao

Thuê bao đảm bảo rằng:

- Khi ký: sử dụng khóa bí mật tương ứng với khóa công khai trong chứng thư số; tại thời điểm ký, thuê bao chấp nhận chứng thư số và chứng thư số đang có hiệu lực (không hết hạn hoặc bị thu hồi).
- Khóa bí mật của mình được bảo vệ và không cho người khác sử dụng.
- Mọi thông tin cung cấp bởi thuê bao là đúng.
- Sử dụng chứng thư số đúng mục đích của chứng thư số, phù hợp với quy định của pháp luật và quy chế chứng thực này
- Không sử dụng chứng thư số được cấp thực hiện các chức năng của một CA. Thỏa thuận thuê bao có thể bao gồm thêm những điều khoản khác. Nội dung thỏa thuận thuê bao được trình bày trong phần phụ lục.

9.6.4 Tuyên bố và cam kết của người nhận

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

- Người nhận phải chịu trách nhiệm cho những hành động của mình do không thực hiện theo các nội dung liên quan được quy định trong thỏa thuận người nhận hoặc quy chê chứng thực này.
- Thỏa thuận thuê bao có thể bao gồm thêm những điều khoản khác. Nội dung thỏa thuận thuê bao được trình bày trong phần phụ lục.

9.7 Từ chối trách nhiệm

MOBIFONECA không quy định cụ thể về việc từ chối trách nhiệm.

9.8 Giới hạn trách nhiệm

CPS này tùy thuộc vào hệ thống các điều luật, quy tắc, các điều chỉnh, quy định, các sắc lệnh và mệnh lệnh thuộc phạm vi địa phương, bang, quốc gia, nhưng không giới hạn hay hạn chế cho lĩnh vực xuất khẩu phần mềm, phần cứng và các thông tin kỹ thuật.

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

- Các điều khoản có tính độc lập: Trong trường hợp một điều khoản hay sự sửa đổi bổ sung của 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.

9.9 Bồi thường thiệt hại

9.9.1 Vấn đề bồi thường của khách hàng

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

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

9.9.2 Vấn đề bồi thường của đại lý

Khi được pháp luật cho phép, bản thỏa thuận với đại lý sẽ yêu cầu đại lý bồi thường cho MobiFoneCA:

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

9.10 Hiệu lực của Quy chế chứng thực

9.10.1 Thời hạn bắt đầu có hiệu lực

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

9.10.2 Thời hạn hết hiệu lực

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

9.10.3 Ảnh hưởng của sự quy chế chứng thực hết hiệu lực

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

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

Tất cả các e-mail liên lạc giữa CA và các RA phải được ký bằng khoá của chứng thư.

Tất cả các e-mail liên lạc giữa CA hoặc RA và thuê bao phải được ký điện tử để làm bằng chứng. Mọi yêu cầu bất kỳ đều phải ký điện tử.

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

9.12 Bổ sung và sửa đổi

9.12.1 Các thủ tục sửa đổi

Những sửa đổi của CP/CPS sẽ được thực hiện bởi Cấp quản lý chính sách có thẩm quyền (xem mục 1.5.4). Nội dung sửa đổi lưu tại http://mobica.vn Nội dung sửa đổi sẽ thay thế các nội dung trong các điều khoản tương đương trong phiên bản quy chế chứng thực tương ứng và mọi tài liệu liên quan khác. Đối với các thay đổi không quan trong như thay đổi URL, thông tin liên hệ, lỗi in ấn... MOBIFONECA PMA có quyền thay đổi quy chế mà không cần thông báo về sự thay đôi. Đối với các thay đổi theo đề xuất từ các thành viên, MOBIFONECA sẽ xem xét yêu cầu thay đôi. Nếu quy chế cần thay đổi, MOBIFONECA sẽ đưa ra thông báo về sự thay đỗi này. Trong một số trường hợp đặc biệt, liên quan tới an ninh của hệ thống, MOBIFONECA sẽ thực hiện sự thay đổi quy chế này lập tức, sau đó sẽ thông báo cho các thành viên. Các thành viên của MOBIFONECA được quyền góp ý cho quy chế chứng thư số trong vòng 15 ngày từ ngày quy chế được công bố. MOBIFONECA sẽ xem xét mọi góp ý sửa đổi. MOBIFONECA sẽ thực hiện một trong các tình huống sau:

- Không thay đổi gì góp ý ban đầu; hoặc
- Sửa đổi những góp ý sửa đổi và công bố lại chúng; hoặc
- Hủy bỏ góp ý sửa đổi.

9.12.2 Các trường hợp cần sửa đổi nhận diện đối tượng (OID)

Thay đổi đáng kể điều mục trong CP/CPS sẽ làm OID thay đổi. Quyết định này được thực hiện bởi quản lý CP/CPS của MobiFoneCA.

9.13 Thủ tục giải quyết tranh chấp

Tranh chấp phát sinh từ CP/CPS sẽ được giải quyết bởi quản lý CP/CPS của MobiFoneCA.

- Việc giải quyết tranh chấp giữa MobiFoneCA, cộng tác và thuê bao phải tuân thủ theo các điều khoản được ghi trong hợp đồng.
- Việc giải quyết tranh chấp giữa MobiFoneCA và đại lý phải tuân thủ theo các điều khoản được ghi trong hợp đồng Đại Lý. Thời gian đàm phán là 60 ngày, sau đó có thể được đưa lên toàn án có đủ quyền xử lý.

9.14 Hệ thống pháp lý điều chỉnh

Hoạt động của MobiFoneCA phải tuân theo luật của nước CHXHCN Việt Nam và luật Thương mại điện tử của Việt Nam. Tất cả các tranh chấp phát sinh từ điều khoản của CP/CPS này, các hoạt động của CA, RA, việc sử dụng các dịch vụ của họ, việc sử dụng và chấp nhận bất kỳ chứng thư được phát hành bởi MobiFoneCA được xử lý theo luật của nước CHXHCN Việt Nam.

Tài liệu Quy chế chứng thực của các tổ chức cung cấp dịch vụ chứng thực chữ ký số được điều chỉnh bởi các văn bản quy phạm pháp luật, bao gồm:

- Luật giao dịch điện tử năm 2005;
- Nghị định số 130/2018/NĐ-CP ngày 27/9/2020 của Chính phủ quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số;
- Thông tư 06/2015/TT-BTTTT về Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký sô và dịch vụ chứng thực chữ ký số.
- Thông tư 31/2020/TT-BTTTT ban hành quy chế chức thực của tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia.

9.15 Phù hợp với pháp luật hiện hành

Mọi hoạt động liên quan đến yêu cầu, phát hành, sử dụng hoặc chấp nhận của một chứng thư MobiFoneCA phải tuân thủ luật pháp nước CHXHCN Việt Nam.

Nếu có quy định trong quy chế này xung đột với quy định của các văn bản pháp luật, lúc này quy định của văn bản pháp luật sẽ có hiệu lực.

9.16 Các điều khoản chung

9.16.1. Thỏa thuận bao trùm mọi thành viên

Quy chế chứng thực này là thỏa thuận mà mọi thành viên của MOBIFONECA

phải tuân thủ.

9.16.2. Sự chuyển nhượng

Không có quy định nào cho phép chuyển nhượng quyền sử dụng chứng thư số.

MOBIFONECA không quy định các trường hợp chuyên nhượng khác.

9.16.3. _ Tính độc lập của các điều khoản

Nếu như một số điều khoản trong quy chế chứng thực này không hợp pháp các điều khoản đó sẽ không có giá trị, nhưng không ảnh hưởng đến hiệu lực của các điều khoản khác.

9.16.4. Sự ép buộc

Không có sự ép buộc nào đưa đến việc ban hành chứng thư của MOBIFONECA

9.16.5. Trường hợp bất khả kháng

Thỏa thuận thuê bao và thỏa thuận người nhận sẽ có điều khoản về trường hợp bất khả kháng để bảo vệ cho MOBIFONECA.

9.17 Các điều khoản khác

Không áp dụng.

TÀI LIỆU THAM CHIẾU

1) Luật giao dịch điện tử số 51/2005/QH11 ngày 29/11/2005.

2) Nghị định 130/2018/NĐ-CP ngày ngày 27 tháng 9 năm 2018 của Chính phủ Quy định chi tiết thi hành luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số.

3) Thông tư 06/2015/TT-BTTTT về Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số.

4) RFC 3647 (https://www.ietf.org/rfc/rfc3647.txt).