CÔNG TY CỔ PHẦN VIỄN THÔNG NEW TELECOM

DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ NEWTEL–CA

*****

QUY CHẾ CHỨNG THỰC

Hà Nội 04/2020

MỤC LỤC

I GIỚI THIỆU

CÔNG TY CỔ PHẦN VIỄN THÔNG NEW-TELECOM là công ty hoạt động trong lĩnh vực công nghệ thông tin và viễn thông. Công ty có thế mạnh về tiềm lực tài chính, độ ngũ kỹ thuật giàu kinh nghiệm, có các kênh phân phối tại cả 3 miền Bắc, Trung, Nam.

CÔNG TY CỔ PHẦN VIỄN THÔNG NEW-TELECOM là một trong số những doanh nghiệp được Bộ Thông tin và Truyền thông lựa chọn cấp phép trở thành đơn vị cung cấp dịch vụ chứng thực chữ ký số. NEWTEL-CA là tên gọi của dịch vụ chứng thực chữ ký số công cộng do CÔNG TY CỔ PHẦN VIỄN THÔNG NEW-TELECOM thành lập. NEWTEL-CA có đầy đủ thẩm quyền cấp chứng thư số cho các tổ chức, doanh nghiệp, cá nhân có yêu cầu xin cấp và sử dụng chứng thư số.

NEWTEL-CA bao gồm một CA, các tổ chức đăng ký chứng thư số và các đại lý được ủy quyền. RA và các đại lý có trách nhiệm tiếp nhận và xác thực thông tin từ phía khách hàng sử dụng dịch vụ.

NEWTEL-CA dự kiến triển khai cung cấp dịch vụ chứng thực chữ ký số công cộng phục vụ khách hàng trên toàn quốc với các đối tượng chính khách hàng cá nhân, các cá nhân thuộc tổ chức doanh nghiệp và tổ chức, doanh nghiệp.

I.1 Giới thiệu về Quy chế chứng thực

Quy chế chứng thực là một tài liệu quan trọng để NEWTEL-CA phục vụ cho các hoạt động cung cấp dịch vụ chứng thực chữ ký số công cộng. Quy chế chứng thực đề cập đến các yêu cầu về quy trình, luật pháp, kỹ thuật cho quá trình xét duyệt hồ sơ, chấp nhận, tạo lập, cấp phát, quản lý, thu hồi và cấp lại chứng thư số. Các bên tham gia cấp phát và sử dụng chứng thư số phải tuân thủ các yêu cầu được đề ra trong Quy chế chứng thực này.

Quy chế chứng thực đóng vai trò quan trọng trong quá trình cung cấp dịch vụ chứng thực chữ ký số và được áp dụng cho tất cả các thành phần tham gia dịch vụ chứng thực chữ ký số NEWTEL-CA. Các thành phần tham gia dịch vụ NEWTEL-CA phải tuân thủ các yêu cầu của Quy chế chứng thực này.

Quy chế chứng thực của NEWTEL-CA được xây dựng tuân theo khuyến nghị RFC 3647. Đồng thời Quy chế chứng thực này tuân theo luật pháp Việt Nam cũng như tuân theo các chính sách, quy chế, văn bản và thủ tục ban hành của Bộ Thông tin và Truyền thông và các đơn vị chức năng có liên quan.

I.2 Tên và định danh của tài liệu

OID của Quy chế chứng thực này là 1.3.6.1.4.1.30339.x.x.x, được xác định theo Quy định của Trung tâm Chứng thực điện tử quốc gia có sử dụng dạng đánh số chuẩn của IANA như sau:

1.3.6.1.4.1.30339.[codeTypeCA].[code-CA].[codeCPS]

Trong đó, CodeTypeCA được đặt là 1, code-C được xác định khi NEWTEL-CA được Bộ Thông tin và Truyền thông cấp giấy phép hoạt động, codeCPS được gán là 3 là mã số của Quy chế chứng thực trong các tài liệu an toàn thông tin của NEWTEL-CA.

I.3 Thành viên tham gia hệ thống PKI công cộng

- *Trung tâm Chứng thực điện tử quốc gia* là đơn vị do Bộ Thông tin và Truyền thông thành lập có chức năng giúp tham mưu 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 điện tử quốc gia vận hành Tổ chức cung cấp dịch vụ chứng thực chữ ký số Quốc gia (NEAC).
- *Tổ chức cung cấp dịch vụ chứng thực chữ ký số* (CA) 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 dịch vụ chứng thực chữ ký số công cộng là hoạt động nhằm mục đích kinh doanh. RootCA Quốc gia cấp chứng thư số cho các CA công cộng. NEWTEL-CA là CA công cộng cung cấp dịch vụ chứng thực chữ ký số công cộng cho cơ quan, tổ chức, cá nhân sử dụng trong các hoạt động công cộng.
- *Tổ chức đăng ký chứng thư số* (RA) là một tổ chức được NEWTEL-CA tin cậy ủy quyền để đảm bảo tính xác minh tính đúng đắn nội dung thông tin trong chứng thư số của thuê bao. Nhiệm vụ của RA là: Xác thực các thuê bao xin chứng thư số. Các RA phải tuân thủ các quy định được chỉ rõ trong Quy chế chứng thực này. RA và NEWTEL-CA sẽ ký thoả thuận quy định về quyền hạn và trách nhiệm của các Bên trong việc cung cấp dịch vụ chứng thực chữ ký số.
- *Thuê bao* trong hệ thống NEWTEL-CA là các cá nhân hay tổ chức sở hữu chứng thư số do NEWTEL-CA ban hành.
- *Bên tin tưởng* là đối tượng tin tưởng chứng thư số hay một chữ ký số được cung cấp bởi NEWTEL-CA phụ thuộc vào quy định sử dụng chứng thư số, bên tin tưởng có thể là thuê bao hoặc không là thuê bao của NEWTEL-CA.
- *Các đối tượng khác:* NEWTEL-CA không quản lý đối tượng nào khác ngoài thuê bao và các bên tin tưởng.

I.4 Phương thức sử dụng chứng thư số

Trong chứng thư số, trường KeyUsage chứa thông tin về mục đích sử dụng chứng thư số. Chứng thư số do NEWTEL-CA 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 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 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.

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

Chứng thư số không được sử dụng cho các mục đích ngoài mục đích đã nêu trong trường KeyUsage.

Trong mọi trường hợp, cấm sử dụng chứng thư số do NEWTEL-CA cấp phát vào những mục đích đảm bảo an ninh cho lĩnh vực hạt nhân, hệ thống điều khiển vũ khí, trong lĩnh vực an ninh, quân sự, đảm bảo an ninh quốc gia, cho các hoạt động vi phạm pháp luật hoặc làm chứng thư số gốc của CA khác.

I.5 Tổ chức quản lý chính sách

I.5.1 Tổ chức quản trị tài liệu

CÔNG TY CỔ PHẦN VIỄN THÔNG NEW-TELECOM

Địa chỉ: Tầng 3, Tòa nhà GP Invest, số 170 đường La Thành, Phường Ô Chợ Dừa, Quận Đống Đa, Thành phố Hà Nội, Việt Nam.

Điện thoại: 04 37727766 Fax: 04 37727755

Người được ủy quyền quản trị Quy chế chứng thực:

Ông Nguyễn Viết Lý, Giám đốc Công ty Cổ phần Viễn thông NEW TELECOM

I.5.2 Tổ chức phê chuẩn quy chế chứng thực

Quy chế chứng thực của NEWTEL-CA được phê chuẩn bởi Giám đốc Công ty Cổ phần Viễn thông NEW TELECOM và được thông qua bởi NEAC. Sự sửa đổi quy chế chứng thực này được thực hiện bởi Công ty Cổ phần Viễn thông NEW-TELECOM.

I.5.3 Thủ tục phê chuẩn quy chế chứng thực

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 bất cứ sự thay đổi lớn trong nội dung Quy chế chứng thực, tài liệu phải được công bố trên trang thông tin của NEWTEL-CA, và sự thay đổi phải được thông báo cho Trung tâm Chứng thực điện tử quốc gia trước khi NEWTEL-CA cấp bất cứ chứng thư số nào mới. Các thay đổi, cập nhật của Quy chế chứng thực được công bố tại http://newtel-ca.vn/download.

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: http://www.newtel-ca.vn/download.

I.6 Định nghĩa và viết tắt.

Viết tắt	Ý nghĩa
CA	Certification Authority – Tổ chức cung cấp dịch vụ chứng thực chữ ký số
Chính sách bảo mật	Văn bản quy định về thông tin được coi là bí mật và trách nhiệm giữ bí mật thông tin của các đối tượng liên quan
Chữ ký số	Là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng theo đó người có được thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định được chính xác: a, Việc biến đổi nêu trên được tạo ra bằng đúng khóa bí mật tương ứng với khóa công khai trong cùng một cặp khóa; b, Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.
Chứng thư số	Một dạng chứng thực điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp
Chứng thư số có hiệu lực	Chứng thư số chưa hết hạn, không bị tạm dừng hoặc bị thu hồi
Chuỗi chứng thư số	Danh sách có thứ tự các chứng thư số, bắt đầu từ chứng thư số của RootCA hoặc CA (nếu đứng riêng) đến chứng thư số của người dùng cuối. Chứng thư số của đối tượng đứng trước trong danh sách được dùng để ký lên chứng thư số của đối tượng đứng sau trong danh sách.
CN	Common Name – một thuộc tính trong trường DN của chứng thư số, CN biểu diễn tên thường gọi của đối tượng là chủ thể của chứng thư số.
CRL	Certificate Revocation List – Danh sách thu hồi chứng thư số
Dịch vụ chứng thực chữ ký số	Một loại hình dịch vụ chứng thực chữ ký điện tử, do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp. Dịch vụ chứng thực chữ ký số bao gồm: a, Tạo ra cặp khóa bao gồm công khai và khóa bí mật cho thuê bao;

	b, Cấp, gia hạn, tạm dừng, phục hồi và thu hồi chứng thư số của thuê bao; c, Duy trì tuyến cơ sở dữ liệu về chứng thư số; d, Những dịch vụ khác có liên quan theo quy định.
DN	Distinguished Names – một trường trong chứng thư số, DN chưa thông tin nhận dạng đối tượng là chủ thể chứng thư số
Hệ thống mật mã không đối xứng	Là hệ thống mật mã có khả năng tạo được cặp khóa bao gồm khóa bí mật và khóa công khai.
KeyUsage	Mục đích sử dụng khóa
Khóa	Một chuỗi các số nhị phân (0 và 1) dùng trong các hệ thống mật mã.
Khóa bí mật	Một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được dùng để tạo chữ ký số.
Khóa công khai	Một khóa trong cặp khóa thuộc hệ thống mật m không đối xứng, được sử dụng để kiểm tra chữ ký số được tạo bởi khóa bí mật tương ứng trong cặp khóa
Ký số	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.
LDAP	Lightweight Directory Access Protocol - Giao thức truy cập thư mục rút gọn
Người ký	Thuê bao dùng đúng khóa bí mật của mình để ký số vào một thông điệp dữ liệu dưới tên của mình.
Người nhận (Bên tin tưởng)	Tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng chứng thư số của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.
OCSP	Online Certificate Status Protocol – Giao thức cung cấp trạng thái chứng thư số trực tuyến.
PKI	Public Key Infrastucture – Hạ tầng khóa công khai
RA	Registration Authority – Tổ chức đăng ký chứng thư số: Có chức năng giúp đỡ CA duyệt đơn đăng ký chứng thư số, đơn gia hạn chứng thư số, đơn thu hồi chứng thư số và quản lý thông tin thuê bao.
Tạm dừng chứng thư số	Làm mất hiệu lực của chứng thư số một cách tạm thời từ một thời điểm xác định.
Thu hồi chứng thư số	Làm mất hiệu lực của chứng thư số một cách vĩnh viễn từ một thời điểm xác định
Thuê bao	Tổ chức, cá nhân được cấp chứng thư số, chấp nhận chứng thư số và giữ khóa bí mật tương ứng với khóa công khai ghi trên chứng thư số được cấp đó.
Tổ chức cung cấp dịch vụ chứng thực chữ	Tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử thực hiện hoạt động cung cấp dịch vụ chứng thực chữ ký số.

ký số	
Token	Thiết bị lưu khóa cứng
Reponsitory	Kho dữ liệu

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
DN	Distinguished Name
DNS	Domain Name System
DRDC	Disater Recovery Data Center
HTTPS	Secure Hypertext Transaction Standard
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5 Hash Algorithm
OCSP	Online Certificate Status Protocol
PDC	Primary Data Center
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 VỀ CÔNG BỐ VÀ LƯU TRỮ

II.1 Kho lưu trữ

NEWTEL-CA duy trì một kho dữ liệu về các chứng thư số đã được cấp, danh sách thu hồi chứng thư số mới nhất và tất cả các phiên bản Quy chế chứng thực dựa trên đó các chứng thư số hợp lệ đã được cấp.

NEWTEL-CA duy trì kho chứa chứng thư số có hiệu lực trên nền tảng LDAP và các phiên bản chứng thư số đã được cấp phát trước đó.

Các kho dữ liệu này được xây dựng với chế độ sẵn sàng 24x7.

II.2 Công bố thông tin về chứng thư số

NEWTEL-CA cung cấp cho người dùng phương thức kiểm tra trạng thái chứng thư số thông qua CRL và dịch vụ OCSP.

Thông tin về CRL của hệ thống SHA1 được công bố tại: http:// http://crl2.newca.vn/newtel-ca.crl.

Thông tin về CRL của hệ thống SH256 được công bố tại: http://crl-sha256.newtel-ca.vn/newtel-ca-sha256.crl.

Thông tin về OCSP của hệ thống SHA1 được công bố tại: http://ocsp2.newca.vn/responder.

Thông tin về OCSP của hệ thống SHA256 được công bố tại: http://ocsp-sha256.newtel-ca.vn/responder.

Ngoài chứng thư số cấp cho thuê bao, NEWTEL-CA công bố tại trang web http://www.newtel-ca.vn/download/ các thông tin sau:

- Chứng thư số gốc của NEWTEL-CA
- Biểu mẫu đăng ký cấp chứng thư số và thỏa thuận với người sử dụng
- Các thông tin về NEWTEL-CA
- Quy trình cấp phát, quản lý và sử dụng chứng thư số

II.3 Thông tin về tần suất công bố

NEWTEL-CA công bố thông tin với tần số sau đây:

Chứng thư số được công bố theo thời gian thực hiện.

CRL được công bố hàng ngày.

Quy chế chứng thực được công bố ngay khi có hiệu lực.

Các thông tin khác: theo yêu cầu

II.4 Kiểm soát truy cập vào kho lưu trữ

Truy cập đến các thông tin nêu trong Kho lưu trữ mục II.1 và công bố thông tin chứng thư số với mục đích đọc không bị giới hạn. NEWTEL-CA không sử dụng biện pháp kỹ thuật để giới hạn truy cập với mục đích lấy chứng thư số và kiểm tra thông tin trạng thái của chứng thư số.

NEWTEL-CA 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. ĐỊNH DANH VÀ XÁC THỰC

III.1 Đặt tên

Tên của chứng thư số NEWTEL-CA cấp phát được dùng để phân biệt với các chứng thư số khác theo chuẩn X.509 v3 trong trường ‘Issuer’ và ‘Subject’.

Nguyên tắc đặt tên với ý nghĩa dễ hiểu cho phép nhận dạng được cá nhân, tổ chức, doanh nghiệp sở hữu chứng thư số đó. Tên có ý nghĩa thuê bao trong chứng thư số là tên cho phép xác định được đối tượng sở hữu của chứng thư số. Khi có yêu cầu của pháp luật, tên trong một chứng thư số được cấp phát phải chỉ ra đúng thuê bao mà tên này được gán.

- Các thuộc tính trong DN của chứng thư số do NEWTEL-CA 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 NEWTEL-CA 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 NEWTEL-CA 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

- Mã định danh của thuê bao là duy nhất trên hệ thống.

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.

Biệt hiệu hay nặc danh: Chứng thư số của các thuê bao không được sử dụng biệt hiệu hoặc nặc danh cho tên. Việc sử dụng biệt hiệu hoặc nặc danh cho tên trong chứng thư số chỉ được chấp nhận khi có yêu cầu của pháp luật và cần có giải trình với NEWTEL-CA để xem xét.

Chấp nhận, xác thực và vai trò của nhãn hiệu đăng ký (TradeMarks): Thuê bao đăng ký xin cấp chứng thư số không được sử dụng những tên vi phạm quyền sở hữu trí tuệ. Nếu có sự tranh chấp say ra về sở hữu thì NEWTEL-CA có quyền thu hồi, tạm dừng chứng thư số hay loại bỏ đơn xin cấp chứng thư số mà không phải chịu trách nhiệm pháp lý.

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.

III.2 Kiểm tra định danh khởi đầu

Khi cần thiết, người có thẩm quyền của NEWTEL-CA có thể yêu cầu gặp trực tiếp người đăng ký thuê bao hay đại diện có thẩm quyền của tổ chức, doanh nghiệp đăng ký thuê bao chứng thư số khi người đại diện này đến xin cấp chứng thư số.

III.2.1 Xác thực nhận dạng thông tin của cá nhân

Nhận dạng của cá nhân và thông tin liên quan được cung cấp bởi đối tượng đăng ký chứng thư số sẽ được xác minh theo thủ tục được NEWTEL-CA quy định, bao gồm ít nhất các bước sau:

- Kiểm tra tính hợp lệ của đơn đề nghị cấp chứng thư số
- Kiểm tra thông tin đăng ký của cá nhân thuê bao với thông tin như CMND
- Đối với khách hàng đăng ký chứng thư cá nhân thuộc tổ chức doanh nghiệp thì kiểm tra giấy giới thiệu, các giấy tờ chứng minh khách hàng đang công tác tại tổ chức doanh nghiệp.

- Trong trường hợp cần thiết, xác thực thông tin cá nhân dựa vào sự hiện diện và kiểm tra các giấy tờ tùy thân như hộ chiếu, chứng minh thư của cá nhân người đăng ký.

Xác thực nhận dạng bằng cách so sánh thông tin đăng ký với thông tin chứa trong cơ sở dữ liệu của đối tác đáng tin cậy.

III.2.2 Kiểm tra nhận dạng thông tin của tổ chức doanh nghiệp

Kiểm tra nhận dạng của người đại diện theo pháp luật của tổ chức doanh nghiệp dựa trên các thủ tục thông thường để nhận dạng

Người đại điện của tổ chức, doanh nghiệp khi đến giao dịch cần xuất trình:

- Kiểm tra tính hợp lệ của đơn đề nghị cấp chứng thư số.
- Giấy giới thiệu, giấy ủy quyền của tổ chức, doanh nghiệp.
- CMTND hoặc Thẻ căn cước công dân hoặc Hộ chiếu của người đại diện.
- Các giấy tờ liên quan như quyết định thành lập, giấy phép đăng ký kinh doanh, mã số thuế.
- Các thông tin khác theo quy định của pháp luật (nếu cần).
- Các thông tin cần thiết sẽ được ghi lại bởi hệ thống của NEWTEL-CA.

III.2.3 Xác thực danh tính tên miền hoặc thiết bị

Khi có một yêu cầu đăng ký chứng thư số cho tên miền hoặc thiết bị, nhận dạng của thuê bao được kiểm tra trên các hệ thống đang hoạt động và xác minh về quyền sở hữu của tổ chức với domain và email đó.

Thông tin định danh sau đây của tên miền hoặc thiết bị bắt buộc phải được xác minh và ghi lại:

- Giấy giới thiệu, ủy quyền của tổ chức, doanh nghiệp (nếu ủy quyền)
- Chứng minh thư nhân dân của người được ủy quyền.
- Các giấy tờ liên quan như quyết định thành lập, giấy phép đăng ký kinh doanh, mã số thuế.
- Giấy tờ chứng minh quyền sở hữu tên miền, thiết bị.
- Nếu tổ chức doanh nghiệp ủy quyền cho một cá nhân đứng tên đăng ký chứng thư số cho mình hay cho thiết bị thì giấy giới thiệu, ủy quyền phải được lưu lại.

III.2.4 Phương pháp chứng minh sở hữu khóa riêng

Tệp tin đề nghị cấp chứng thu số mã hóa theo chuẩn PKCS #10. Thuê bao có thể tự tạo cặp khoá trên các thiết bị sinh và lưu khoá do thuê bao lựa chọn và được NEWTEL-CA xác nhận tính an toàn trước khi cấp chứng thư, hoặc thuê bao có thể ủy quyền cho NEWTEL-CA sinh khóa theo thoả thuận cụ thể giữa 02 bên.

III.2.5 Thông tin xác minh dành cho trường hợp cần xác minh thêm thông tin

Trong trường hợp hồ sơ chưa đầy đủ, thuê bao hoặc thuê bao được uỷ quyền được sẽ được yêu cầu và đồng ý cấp bổ sung giấy tờ trước khi NEWTEL-CA có thể cấp chứng thư. Để đảm bảo anh toàn thông tin, NEWTEL-CA có thể xác nhận thêm thông tin thông qua việc gọi điện cho chủ sở hữu chính thức doanh nghiệp.

III.3 Định danh và xác thực khi yêu cầu tạo khóa lại

Trước khi chứng thư số hết hạn, nếu có nhu cầu thuê bao cần phải đăng ký để có được một chứng thư số mới. Hệ thống cho phép gia hạn (renewal) theo nghĩa sinh một cặp khóa mới thay thế cặp khóa trong chứng thư số đã hết hạn.

III.3.1 Nhận dạng và xác thực yêu cầu gia hạn chứng thư số

NEWTEL-CA chỉ cho phép kéo dài thời gian có hiệu lực của chứng thư số, với thông tin giữ nguyên.

Ít nhất là 30 ngày trước ngày hết hạn của chứng thư số, thuê bao có quyền yêu cầu gia hạn chứng thư số.

Có đơn đề nghị gia hạn chứng thư số của thuê bao

Có giấy ủy quyền cho đại diện đến giao dịch gia hạn chứng thư số của tổ chức, doanh nghiệp là thuê bao ngoài.

Chứng minh quyền sở hữu khóa bí mật: thuê bao sử dụng chứng thư số và khóa bí mật của mình để chứng minh là có sở hữu khóa này.

NEWTEL-CA sẽ liên lạc với thuê bao thông qua điện thoại, e-mail, thư tín hay các phương tiện khác để khẳng định lại chính thuê bao đã yêu cầu làm mới chứng thư số. 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.

III.3.2 Định danh và xác thực khi yêu cầu thu hồi chứng thư số

Việc định danh và xác thực khi yêu cầu thu hồi chứng thư số phải có đơn xin thu hồi chứng thư số nêu rõ lý do.

NEWTEL-CA liên lạc với thuê bao thông qua điện thoại, email, thư tín hay các phương tiện khác (đã được lưu lại khi khách hàng đăng ký chứng thư số) để khẳng định lại chính thuê bao đã yêu cầu thu hồi chứng thư số.

III.3.3 Định danh và xác thực khi yêu cầu tạo khóa lại

NEWTEL-CA chỉ cho phép tạo khóa lại trong thời gian có hiệu lực của chứng thư số, với thông tin giữ nguyên và cặp khóa được tạo mới.

Ngay khi thuê bao nghi ngờ khóa bí mật không an toàn

Có đơn đề nghị tạo khóa lại của thuê bao

Đối với thuê bao cá nhân: Thuê bao phải xuất trình CMND

Đối với thuê bao là tổ chức, doanh nghiệp: Có giấy ủy quyền cho đại diện, giấy CMND của người được ủy quyền.

Chứng minh quyền sở hữu cặp khóa bí mật: thuê bao sử dụng chứng thư số và cặp khóa bí mật của mình để chứng minh là có sở hữu khóa này.

NEWTEL-CA sẽ là liên lạc với thuê bao thông qua điện thoại, email, thư tín hay các phương tiện khác để khẳng định lại chính thuê bao đã yêu cầu tạo khóa lại.

IV.YÊU CẦU VẬN HÀNH VỀ VÒNG ĐỜI CHỨNG THƯ SỐ

IV.1 Đăng ký chứng thư số

IV.1.1 Các đối tượng có thể xin cấp chứng thư số

Các đối tượng sau có thể gửi đăng ký cấp chứng thư số:

- Cá nhân;
- Cá nhân thuộc tổ chức, doanh nghiệp;
- Tổ chức, doanh nghiệp đang hoạt động hợp pháp.

IV.1.2 Hồ sơ xin cấp chứng thư 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/Quyết định thành lập/Giấy phép đầu tư 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, 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.

IV.1.3 Đăng ký cấp chứng thư số và trách nhiệm của các bên

Thủ tục cấp phát chứng thư số

Bước 1: Gửi hồ sơ xin cấp phát chứng thư số

Thuê bao nộp hồ sơ xin cấp phát Chứng thư số trực tiếp cho NEWTEL-CA hoặc các đại lý được ủy quyền của NEWTEL-CA.

Bước 2: Đại lý được ủy quyền tiếp nhận, xác minh sự hợp lệ của hồ sơ gửi hồ sơ tới RA để nhập thông tin vào hệ thống.

Sau khi nhận đủ hồ sơ hợp lệ, đại lý thông báo với thuê bao thời gian sẽ trả kết quả, ký kết hợp đồng và bàn giao chứng thư số.

Các đại lý có trách nhiệm tư vấn cho khách hàng hoàn thiện hồ sơ xin cấp chứng thư số đầy đủ, hợp lệ. Nhân viên được giao nhiệm vụ tại các đại lý tiếp nhận hồ sơ xin cấp chứng thư số, kiểm tra và xác minh định danh:

- Kiểm tra việc khai báo đầy đủ thông tin theo yêu cầu, thực hiện xác minh định danh theo quy định của NEWTEL-CA. Nếu thông tin không đúng và không đầy đủ thông báo cho thuê bao để cập nhật bổ sung, hoặc thông báo từ chối cấp chứng thư số. Nếu đúng thì thông báo và hẹn thời gian để thuê bao đăng nhập thông tin vào hệ thống.
- Chuyển hồ sơ khách hàng đến RA thông qua fax, email hoặc qua phần mềm chuyên dụng

Bước 3: Nhập thông tin yêu cầu xin cấp chứng thư số

RA sẽ nhận hồ sơ, xác minh lại các hồ sơ xin cấp chứng thư số. Nếu đúng và đầy đủ theo quy định, RA nhập thông tin vào hệ thống. Nếu hồ sơ không đúng và không đầy đủ theo quy định thì RA thông báo lại cho đại lý.

Bước 4: Thực hiện cấp phát chứng thư số

Bộ phận CA phê duyệt cấp phát chứng thư số (Approve) chứng thư số cho các thuê bao do RA nhập:

- Đối chiếu thông tin do RA nhập yêu cầu cấp phát chứng thư số với các thông tin trong hồ sơ của thuê bao đồng thời có thể đối chiếu với các nguồn thông tin khác (nếu cần). Khi thấy thông tin là đúng và đủ theo quy định, sẽ thực hiện phê duyệt cấp phát chứng thư số (Approve)
- Sau khi cấp phát xong, ký vào hồ sơ hoặc xác nhận bằng Email hoặc phần mềm chuyên dụng và chuyển lại cho RA để thực hiện kiểm tra việc cấp phát.
- Giữ liệu liên quan đến hồ sơ thuê bao xin cấp chứng thư số sẽ được hệ thống lưu trữ có bảo mật theo quy định.

Bước 5: Thông báo chứng thư số được phê duyệt

Cặp khóa của thuê bao được sinh trực tiếp trong các thiết bị chuyên dụng. Đồng thời chứng thư số được đưa vào trong thiết bị.

Hệ thống NEWTEL-CA sẽ gửi một thư điện tử (email) vào thư điện tử của thuê bao (đã đăng ký trong hồ sơ), tin nhắn SMS, fax hoặc thông báo qua điện thoại về việc hoàn tất cấp phát chứng thư số.

Bước 6: Xác nhận đã nhận chứng thư số

Khi thuê bao nhận thông tin chứng thư số và khoá bí mật lưu trong thiết bị lưu trữ (Token và SIM PKI) từ thông báo của NEWTEL-CA, 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 NEWTEL-CA từ chối chứng chỉ và giải thích lý do từ chối. Trong vòng một tuần thuê bao không trả lời thông báo của NEWTEL-CA, chứng thư số đó coi như được khách hàng chấp nhận.

Bước 7: Công bố trạng thái chứng thư số

Sau khi được chấp nhận chứng thư số thì hệ thống NEWTEL-CA sẽ công bố chứng thư số thông qua dịch vụ web, CRL và OCSP theo quy định.

Thuê bao và bên tin tưởng có thể tải CRL hoặc dùng dịch vụ OCSP để kiểm tra trạng thái của chứng thư số hoặc dùng cho các ứng dụng khác thông qua máy chủ web.

IV.2 Xử lý hồ sơ đăng ký chứng thư số

IV.2.1 Nhận dạng và xác thực

Các đại lý và RA thực hiện nhận dạng và xác thực mọi thông tin trong yêu cầu cấp chứng thư số

IV.2.2 Duyệt đăng ký cấp chứng thư số

NEWTEL-CA sẽ chấp nhận đơn đăng ký chứng thư số nếu các điều kiện sau đây thỏa mãn:

- Mọi thông tin cần xác thực được nhận dạng và xác thực đúng.
- Thuê bao nộp đầy đủ các khoản phí theo quy định
- Khóa công khai trên chứng thư số sẽ được cấp là duy nhất và cùng cặp với khóa bí mật của tổ chức, cá nhân xin cấp chứng thư số.

NEWTEL-CA không chấp nhận đơn đăng ký chứng thư số nếu:

- Một trong các thông tin cần xác thực là không chính xác.
- Thuê bao không cung cấp đầy đủ tài liệu xác minh thông tin đã kê khai trong đơn đăng ký.
- Đối tượng không thuộc diện được cấp chứng thư số.
- Newtel là đơn vị có thẩm quyền cao nhất trong việc phê duyệt.

IV.2.3 Thời gian xử lý đăng ký cấp chứng thư số

NEWTEL-CA 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 NEWTEL-CA. Thông thường, nếu không có vướng mắc, hệ thống cung cấp dịch vụ NEWTEL-CA có thể khởi tạo một chứng thư mới tối đa trong 03 ngày.

IV.3 Cấp chứng thư số

IV.3.1 Thuê bao đăng ký cấp chứng thư số

Thuê bao có nhu cầu sử dụng chứng thư số liên hệ với đại lý, RA để được tư vấn sau đó hoàn thiện hồ sơ theo yêu cầu rồi gửi tới đại lý hoặc RA.

IV.3.2 NEWTEL-CA tạo chứng thư số

Chứng thư số được cấp phát sau khi NEWTEL-CA chấp nhận đơn xin cấp chứng thư số.

NEWTEL-CA tạo cho thuê bao một chứng thư số dựa vào những thông tin trong đơn xin cấp chứng thư số và yêu cầu cấp chứng thư số.

IV.3.3 Thông báo cho thuê bao khi đã tạo xong chứng thư số

NEWTEL-CA 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.

Khi bàn giao chứng thư số, thuê bao có trách nhiệm kiểm tra chứng thư số của mình.

Nếu thông tin trong chứng thư số không phù hợp, người dùng thông báo lại cho đại lý hoặc RA của NEWTEL-CA trong thời gian quy định để được xử lý.

Thông tin tiếp nhận: Công ty Cổ phần Viễn thông New-Telecom

Địa chỉ: Tầng 3, Tòa nhà GP INVEST – Số 170 đường La Thành, Phường Ô Chợ Dừa, quận Đống Đa, thành phố Hà Nội.

Điện thoại: 024.37.727.766 Fax: 024.37.727.755

Email: support@newtel.vn

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

IV.4 Chấp nhận chứng thư số

IV.4.1 Công bố chứng thư số

Chứng thư số được coi là chính thức chấp nhận khi được NEWTEL-CA công bố trên website, kho dữ liệu chứng thư số.

Thông tin về OCSP của hệ thống SHA1 được công bố tại: http://ocsp2.newca.vn/responder.

Thông tin về OCSP của hệ thống SHA256 được công bố tại: http://ocsp-sha256.newtel-ca.vn/responder.

Thời gian công bố chứng thư số chậm nhất là 24 giờ sau khi phát hành nếu không có phản hồi từ chối từ phía thuê bao.

IV.4.2 Thông báo sự ban hành chứng thư số

NEWTEL-CA sẽ thông báo về việc cấp chứng thư số các thuê bao khác nếu cần thiết.

IV.4.3 Tổ chức bàn giao và xác nhận chứng thư số

NEWTEL-CA sẽ bàn giao chứng thư số cho thuê bao, thuê bao nhận được chứng thư số sẽ kiểm tra tính chính xác của chứng thư số và nếu thông tin trong chứng thư số không phù hợp, người dùng thông báo lại cho đại lý hoặc RA của NEWTEL-CA trong thời gian quy định để được xử lý.

Thông tin tiếp nhận: Mục IV.3.3

Đối với SIM PKI, khách hàng sẽ được yêu cầu đặt và xác nhận mã PIN cho thuê bao qua tin nhắn OTA. Đối với Token, khách hàng sẽ được gửi mã PIN cho thuê bao qua phiếu hướng dẫn cài đặt thiết bị.

IV.5 Sử dụng chứng thư số và cặp khóa

IV.5.1 Sử dụng khóa bí mật và chứng thư số

Thuê bao được sử dụng chứng thư số và khóa bí mật tương ứng nếu chứng thư số được coi là chấp nhận.

Chứng thư số phát hành bởi NEWTEL-CA 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.

Mục đích sử dụng chứng thư số phải nhất quán với phạm vi sử dụng được phép và có ghi tại trường KeyUsage trong chứng thư số.

IV.5.2 Sử dụng khóa công khai và chứng thư số

Người nhận cần dựa vào các thông tin sau để đánh giá sự tin cậy của chứng thư số:

- Kiểm tra có đúng chứng thư số do NEWTEL-CA phát hành.
- Trạng thái của chứng thư số.
- Mục đích sử dụng của chứng thư số thể hiện trên chứng thư số (trong trường KeyUsage). Chi tiết của các mục đích sử dụng này được thể hiện trong các tài liệu thoả thuận thuê bao, quy chế chứng thực, chính sách chứng thư số và các tài liệu liên quan đến các hoạt động nghiệp vụ có sử dụng dịch vụ chứng thực chữ ký số của NEWTEL-CA.
- 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 NEWTEL-CA.

IV.6 Gia hạn chứng thư số

Gia hạn chứng thư số là việc ban hành một chứng thư số mới và một cặp khóa mới cho thuê bao sau thời hạn sử dụng chứng thư số, mọi thông tin khác trong chứng thư số đều không thay đổi.

Bước 1: Gửi hồ sơ xin gia hạn

Thuê bao làm hồ sơ theo mẫu để xin gia hạn chứng thư.

Bước 2: Tiếp nhận, xác minh định danh của thuê bao xin gia hạn

- Nhân viên được giao nhiệm vụ tại RA tiếp nhận hồ sơ xin gia hạn chứng thư, và thực hiện:
- Thời gian gia hạn chứng thư số của thuê bao: Ít nhất là 30 ngày trước ngày hết hạn của chứng thư số. Dưới 30 ngày trước ngày hết hạn chứng thư số, yêu cầu gia hạn chứng thư số sẽ không được chấp nhận, thuê bao ngoài phải thực hiện lại các bước đăng ký mới.
- Kiểm tra hồ sơ và xác minh định danh theo quy định như trường hợp xin cấp mới. Nếu không đúng và không đầy đủ theo quy định thì thông báo cho thuê bao biết và bổ sung hoặc từ chối cấp. Nếu đúng và đầy đủ thì hẹn thời gian xử lý yêu cầu gia hạn.
- Chỉ tiếp nhận hồ sơ khi thông tin về chứng thư không thay đổi, chỉ thay đổi về thời hạn của chứng thư.
- Nếu đúng và đầy đủ theo quy định, RA nhập thông tin về thuê bao gia hạn và chuyển hồ sơ tới CA để thực hiện gia hạn.

Bước 3: Nhập thông tin gia hạn chứng thư số

RA sẽ nhận, kiểm tra các hồ sơ xin gia hạn chứng thư số, xác minh định danh. Nếu đúng và đầy đủ theo quy định, RA nhập thông tin về thuê bao gia hạn và chuyển hồ sơ tới CA để thực hiện gia hạn. Nếu hồ sơ không đúng và không đầy đủ theo quy định, RA thông báo tới các đại lý.

Bước 4: Phê duyệt gia hạn chứng thư số

Bộ phận CA thực hiện phê duyệt (Approve):

- Đối chiếu thông tin được RA nhập yêu cầu gia hạn chứng thư số với thông tin trong hồ sơ khách hàng và đồng thời có thể đối chiếu các nguồn thông tin khác (nếu cần). Khi thấy thông tin đúng và đầy đủ theo quy định, cán bộ quản trị cấp phát chứng thư số sẽ thực hiện phê duyệt gia hạn chứng thư số (Approve).
- Chứng thư số gia hạn được sinh trong thiết bị chuyên dụng
- Dữ liệu liên quan đến hồ sơ thuê bao xin gia hạn chứng thư số sẽ được hệ thống lưu trữ có bảo mật theo quy định.

Bước 5: Thông báo chứng thư số được phê duyệt

NEWTEL-CA sẽ gửi thư điện tử (email) tới thư điện tử của thuê bao (đã đăng ký trong hồ sơ), hoặc điện thoại, SMS, fax tới thuê bao với nội dung thư thông báo hoàn thành việc gia hạn và hẹn thời gian bàn giao chứng thư số

Bước 6: Xác nhận đã nhận chứng thư số

NEWTEL-CA sẽ bàn giao chứng thư số cho thuê bao, thuê bao nhận được chứng thư số sẽ kiểm tra tính chính xác của chứng thư số và nếu thông tin trong chứng thư số không phù hợp, người dùng thông báo lại cho đại lý hoặc RA của NEWTEL-CA trong thời gian quy định để được xử lý.

Thông tin tiếp nhận: Mục IV.3.3

Bước 7: Công bố trạng thái chứng thư số

Hệ thống NEWTEL-CA sẽ công bố trạng thái chứng thư số ngay sau khi chứng thư số được gia hạn thành công và công khai trạng thái chứng thư số thông qua dịch vụ web, CRLs và OCSP theo quy định.

Thuê bao và bên tin tưởng có thể tải CRLs để kiểm tra trạng thái của chứng thư số, hoặc sử dụng dịch vụ OCSP để kiểm tra trạng thái chứng thư số. Thuê bao có thể dùng cho các ứng dụng khác thông qua máy chủ web.

Bước 8: Công bố chứng thư số

Hệ thống NEWTEL-CA sẽ công bố công khai chứng thư số thông qua kho lưu trữ LDAP.

Thuê bao và bên tin tưởng có thể tải chứng thư số về sử dụng thông qua web hoặc LDAP.

IV.6.1 Các tình huống gia hạn chứng thư số

Trước khi hết hạn, để đảm bảo hoạt động ký số, thuê bao cần phải gia hạn chứng thư số.

Chứng thư số của thuê bao được kiểm tra và định danh theo mục IV.6 Gia hạn chứng thư số:

Một chứng thư số có thể được gia hạn với điều kiện các thông tin ghi trong chứng thư số cũ không thay đổi và thời gian trước khi hết hạn không ít hơn 30 ngày.

IV.6.2 Đối tượng có thể yêu cầu gia hạn chứng thư số

Chỉ đối tượng đăng ký chứng thư số mới có quyền yêu cầu gia hạn chứng thư số.

IV.6.3 Xử lý yêu cầu gia hạn chứng thư số

NEWTEL-CA tiến hành xác minh yêu cầu gia hạn chứng thư số như trong phần cấp chứng thư số mới.

Chỉ trong trường hợp thông tin thuê bao không thay đổi, chứng thư số mới có thể được gia hạn

IV.6.4 Thông báo sự tạo chứng thư số mới cho thuê bao

Thông bao về việc ban hành chứng thư số mới khi gia hạn chứng thư số cũng giống như thông báo khi chứng thư số được cấp mới.

IV.6.5 Công bố chứng thư số mới được gia hạn

Tương tự phần IV.4

IV.6.6 Thông báo tạo chứng thư số mới được gia hạn cho các đối tượng khác

Tương tự phần IV.4

IV.6.7 Tổ chức bàn giao và xác nhận chứng thư số được gia hạn

Tương tự phần IV.4

IV.7 Thu hồi và đình chỉ chứng thư số

IV.7.1 Các tình huống thu hồi chứng thư số

Yêu cầu thu hồi chứng thư số sẽ được xử lý khi thuê bao đề nghị, do NEWTEL-CA 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 NEWTEL-CA.

IV.7.2 Ai có thể yêu cầu thu hồi chứng thư số

- Thuê bao đề nghị thu hồi chứng thư số của mình
- Về an toàn thông tin, NEWTEL-CA có quyền yêu cầu thu hồi chứng thư số.
- Theo yêu cầu của pháp luật.

IV.7.3 Thủ tục thu hồi chứng thư số

Khi có thông báo khẩn cấp, tạm dừng chứng thư số (Supsend). Khi thuê bao có đơn hợp lệ thì chính thức thu hồi chứng thư số.

Trước khi thu hồi chứng thư số, NEWTEL-CA xác thực yêu cầu thu hồi chứng thư số bằng cách:

- Thu hồi theo yêu cầu: Khi nhận yêu cầu thu hồi từ một thuê bao cho chứng thư số của mình, NEWTEL-CA 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, NEWTEL-CA mới chính thức thu hồi và công bố thông tin thu hồi chứng thư số.
- Xác minh quyết định yêu cầu thu hồi chứng thu số của đơn vị có thẩm quyền.
- Nếu NEWTEL-CA có đủ sơ sở để xác minh khách hàng bị lộ khoá bí mật gây mất an toàn, NEWTEL-CA 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.

IV.7.4 Quy trình thu hồi chứng thư số

Bước 1: Yêu cầu tạm dừng chứng thư số

Khi có lý do phải thu hồi chứng thư số, thuê bao bằng các phương tiện liên lạc có thể gửi yêu cầu tạm dừng chứng thư số đại lý hoặc RA theo số điện thoại hoặc email đã đăng ký trước. Sau đó thuê bao phải hoàn thiện các thủ tục theo quy định của NEWTEL-CA

Quản trị cấp phát chứng thư số phải thực hiện các biện pháp xác minh định danh thuê bao theo hồ sơ xin cấp chứng thư số của thuê bao và các biện pháp định danh khác theo quy định, để đảm bảo yêu cầu tạm dừng là đúng từ thuê bao trước khi thực hiện

Bước 2: Lập hồ sơ xin thu hồi chứng thư số

Thuê bao tới đại lý hoặc RA làm hồ sơ theo mẫu, nêu rõ lý do thu hồi chứng thư số có chữ ký xác nhận của tổ chức, doanh nghiệp, văn bản ủy quyền nếu là tổ chức doanh nghiệp. Sau đó gửi hồ sơ để đề nghị thu hồi chứng thư số.

Bước 3: Nhập thông tin thu hồi chứng thư số

RA tiếp nhận thông tin từ đại lý, xác minh hồ sơ và nhập vào hệ thống để thực hiện việc thu hồi chứng thư số.

Bước 4: Thực hiện thu hồi chứng thư số CA kiểm tra lại hồ sơ yêu cầu, nếu hồ sơ hợp lệ thì phê duyệt thu hồi chứng thư số (Approve):

- Thực hiện thu hồi chứng thư số
- RA thực hiện kiểm tra lại trạng thái của chứng thư số sau khi thực hiện. Nếu chứng thư số có trạng thái bị thu hồi thì việc thu hồi chứng thư số của thuê bao là thành công; Thông tin về việc thu hồi của thuê bao sẽ được hệ thống lưu trữ theo quy định.

Bước 5: Công bố chứng thư số bị thu hồi

NEWTEL-CA thông báo tới thuê bao qua email, hoặc điện thoại, SMS, fax về việc đã thu hồi thành công chứng thư số.

Hệ thống NEWTEL-CA sẽ công bố công khai chứng thư số bị thu hồi ngay sau khi bị thu hồi thông qua dịch vụ web, CRL và OCSP theo quy định.

Trường hợp có yêu cầu thu hồi chứng thư số từ các cơ quan chức năng có thẩm quyền thì thực hiện xác minh yêu cầu và thực hiện bước 4, bước 5.

IV.7.5 Quy trình tạm dừng chứng thư số

Chứng thư số được tạm dừng trong các trường hợp sau đây:

- Khi NEWTEL-CA có căn cứ khẳng định rằng chứng thư số của thuê bao được cấp không theo các quy tắc của bản Quy chế chứng thực này.
- Khi có yêu cầu của cơ quan tiến hành tố tụng, cơ quan công an hoặc Bộ Thông tin và Truyền thông;
- Theo điều kiện tạm dừng chứng thư số đã được quy định trong hợp đồng giữa thuê bao và NEWTEL-CA.

Trong các trường hợp trên thì NEWTEL – CA sẽ tiến hành tạm dựng chứng thư số của thuê bao ngay, sau đó thông tin cho thuê bao biết.

- Khi có yêu cầu tạm dừng từ thuê bao. Các bước thực hiện như sau:

Bước 1: Lập hồ sơ xin tạm dừng chứng thư số

Thuê bao làm hồ sơ yêu cầu tạm dừng theo mẫu và phải nêu rõ lý do tạm dừng, có xác nhận tổ chức, doanh nghiệp đối với tổ chức doanh nghiệp. Sau đó gửi hồ sơ về đại lý, RA để đề nghị tạm dừng chứng thư số.

Bước 2: Nhập thông tin tạm dừng chứng thư số

RA sẽ xem xét, xác minh lại hồ sơ tạm dừng chứng thư số và nhập thông tin vào hệ thống.

Bước 3: Phê duyệt tạm dừng chứng thư số.

CA kiểm tra lại hồ sơ và thực hiện các bước phê duyệt tạm dừng chứng thư số:

- Thực hiện phê duyệt tạm thời chứng thư số

- RA kiểm tra lại trạng thái của chứng thư số sau khi thực hiện. Nếu chứng thư số bị tạm dừng thì thông báo lại cho thuê bao biết. Thông tin về việc tạm dừng chứng thư số sẽ được hệ thống lưu trữ theo quy định.

Bước 4: Công bố trạng thái chứng thư số

Thuê bao phải kiểm tra trạng thái chứng thư số của mình thông qua giao thức OCSP và xác nhận chứng thư số của mình đã bị tạm dừng với NEWTEL-CA

Hệ thống NEWTEL-CA sẽ công bố công khai trạng thái chứng thư số ngay khi bị tạm dừng thông qua dịch vụ OCSP, CRL theo quy định.

IV.7.6 Thay đổi nội dung thông tin Chứng thư số

Điều kiện thay đổi nội dung thông tin Chứng thư số:

- Chứng thư số phải còn hạn sử dụng ít nhất 60 ngày;
- Cơ quan, tổ chức, cá nhân phải có văn bản đề nghị được cơ quan, tổ chức quản lý trực tiếp xác nhận đề nghị thay đổi nội dung thông tin chứng thư số.

Các tình huống thay đổi nội dung thông tin chứng thư số:

- Đối với chứng thư số của cá nhân:

  Thay đổi cơ quan, tổ chức công tác mà thông tin không phù hợp với thông tin trong chứng thư số; Thay đổi các thông tin về địa chỉ thư điện tử, số điện thoại.

- Đối với chứng thư số của cơ quan, tổ chức:

  Cơ quan, tổ chức đổi tên, số điện thoại đại diện hoặc địa chỉ hoạt động mà thông tin không phù hợp với thông tin trong chứng thư số;

- Đối với chứng thư số của thiết bị, dịch vụ, phần mềm:

  Thiết bị, dịch vụ, phần mềm đổi tên hoặc được nâng cấp phiên bản, bổ sung tính năng mà thông tin không phù hợp với thông tin trong chứng thư số.

Ai có thể yêu cầu thay đổi thông tin chứng thư số: Thuê bao đề nghị thay đổi thông tin chứng thư số của mình

Quy trình thay đổi thông tin chứng thư số

Bước 1: Yêu cầu thay đổi thông tin chứng thư

Thuê bao nộp hồ sơ thay đổi thông tin đến Đại lý hoặc NEWTEL-CA bao gồm các tài liệu hồ sơ của thuê bao như mục cấp mới Chứng thư số mục IV.1.3), cùng với đó là Phiếu yêu cầu Thay đổi thông tin chứng thư do người đại diện trước pháp luật của chứng thư ký/đóng dấu. Đại lý và RA kiểm tra thông tin như quy trình cấp mới chứng thư.

Bước 2: Nhập thông tin yêu cầu thay đổi thông tin Chứng thư số.

RA nhập thông tin yêu cầu thay đổi thông tin chứng thư số theo quy định và gửi hồ sơ đến CA

Bước 3: Phê duyệt yêu cầu thay đổi thông tin chứng thư số

Bộ phận CA thực hiện phê duyệt (Approve):

- Đối chiếu thông tin được RA nhập yêu cầu thay đổi thông tin chứng thư số với thông tin trong hồ sơ khách hàng và đồng thời có thể đối chiếu các nguồn thông tin khác (nếu cần). Khi thấy thông tin đúng và đầy đủ theo quy định, cán bộ quản trị cấp phát chứng thư số sẽ thực hiện phê duyệt thay đổi thông tin chứng thư số (Approve).
- Chứng thư số cũ được thu hồi
- Chứng thư số mới được sinh trong thiết bị chuyên dụng
- Dữ liệu liên quan đến hồ sơ thuê bao xin gia hạn chứng thư số sẽ được hệ thống lưu trữ có bảo mật theo quy định.

Bước 4: Thông báo chứng thư số được phê duyệt

- NEWTEL-CA sẽ gửi thư điện tử (email) tới thư điện tử của thuê bao (đã đăng ký trong hồ sơ), hoặc điện thoại, fax tới thuê bao với nội dung thư thông báo hoàn thành việc thay đổi thông tin chứng thư

Bước 5: Xác nhận đã nhận chứng thư số

- RA.Thuê bao ký vào bản xác nhận đã nhận được chứng thư số

Bước 6: Công bố trạng thái chứng thư số

- Hệ thống NEWTEL-CA sẽ công bố trạng thái chứng thư số ngay sau khi chứng thư số được thay đổi thông tin thành công và công khai trạng thái chứng thư số thông qua dịch vụ web, CRLs và OCSP theo quy định.
- Thuê bao và bên tin tưởng có thể tải CRLs để kiểm tra trạng thái của chứng thư số, hoặc sử dụng dịch vụ OCSP để kiểm tra trạng thái chứng thư số. Thuê bao có thể dùng cho các ứng dụng khác thông qua máy chủ web.

Bước 7: Công bố chứng thư số

- Hệ thống NEWTEL-CA sẽ công bố công khai chứng thư số thông qua kho lưu trữ LDAP.

IV.7.7 Quy trình phục hồi chứng thư số

Bước 1: Yêu cầu phục hồi chứng thư số

Thuê bao bằng các phương tiện liên lạc có thể gửi yêu cầu phục hồi chứng thư số đến đại lý, RA.

RA phải thực hiện các biện pháp xác minh định danh thuê bao và các biện pháp định danh khác theo quy định, để đảm bảo yêu cầu phục hồi là đúng từ thuê bao trước khi thực hiện.

Sau đó thuê bao phải hoàn thiện các thủ tục theo quy định của NEWTEL-CA.

Bước 2: Nhập thông tin phục hồi chứng thư số

RA sẽ xem xét, xác minh lại hồ sơ phục hồi chứng thư số và nhập thông tin vào hệ thống

Bước 3: Phê duyệt phục hồi chứng thư số

CA kiểm tra lại hồ sơ và thực hiện phê duyệt phục hồi chứng thư số:

- Thực hiện phê duyệt phục hồi chứng thư số
- RA kiểm tra lại trạng thái của chứng thư số sau khi thực hiện. Nếu chứng thư số đã được phục hồi thông báo lại cho thuê bao biết. Thông tin về việc phục hồi chứng thư số sẽ được hệ thống lưu trữ theo quy định.

Bước 4: Công bố trạng thái chứng thư số

Thuê bao phải kiểm tra trạng thái chứng thư số của mình thông qua giao thức OCSP và xác nhận chứng thư số của mình đã được phục hồi với NEWTEL-CA.

Hệ thống NEWTEL-CA sẽ công bố công khai trạng thái chứng thư số ngay sau khi phục hồi thông qua dịch vụ OCSP theo quy định.

IV.7.8 Thời hạn gửi yêu cầu thu hồi chứng thư số

- Thuê bao sẽ gửi yêu cầu thu hồi chứng thư số ngay lập tức khi phát hiện hay nghi ngờ khóa bí mật bị mất/lộ.
- Các yêu cầu thu hồi từ các cơ quan có thẩm quyền gửi yêu cầu thu hồi chứng thư số tối thiểu 03 ngày trước thời hạn cần thu hồi chứng thư số. Trong trường hợp khẩn cấp, cần liên lạc theo các phương tiện có thể với NEWTEL-CA để tạm ngưng chứng thư số.

IV.7.9 Thời gian bắt đầu xử lý yêu cầu thu hồi chứng thư số

NEWTEL-CA sẽ xử lý ngay khi nhận được yêu cầu thu hồi chứng thư số hợp lệ.

IV.7.10 Kiểm tra trạng thái thu hồi

Người tin tưởng sẽ có được thông tin trạng thái chứng thư số, thông qua CRL và OCSP.

IV.7.11 Tần suất công bố CRL mới

CRL được cập nhật ít nhất một ngày một lần

CRL được công bố ngay lập tức sau khi được tạo ra

Chứng thư số hết hạn bị loại bỏ khỏi CRL

IV.7.12 Kiểm tra trạng thái chứng thư số trực tuyến

Thông tin thu hồi và trạng thái chứng thư số được công bố qua OCSP hoặc trang web

IV.7.13 Yêu cầu kiểm tra trạng thái thu hồi trực tuyến

Người nhận phải kiểm tra trạng thái của một chứng thư số nếu muốn tin tưởng.

Việc kiểm tra trạng thái chứng thư số được thực hiện thông qua CRL hay dịch vụ OCSP.

IV.7.14 Các dạng thông tin trạng thái thu hồi khác

NEWTEL-CA Không sử dụng dạng công bố thông tin trạng thái thu hồi nào khác ngoài CRL và OCSP.

IV.7.15 Yêu cầu đặc biệt khi khóa CA, sub CA bị mất, bị lộ hoặc thu hồi

Khi khóa bí mật bị mất/lộ hoặc nghi ngờ mất/lộ NEWTEL-CA ngay lập tức thông báo cho thuê bao về sự mất/lộ này thông qua các tất cả các phương tiên liên lạc có thể.

IV.8 Dịch vụ về trạng thái chứng thư số

IV.8.1 Phương tiện công bố

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

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

IV.8.2 Tính sẵn sàng của dịch vụ

Dịch vụ trạng thái chứng thư số được duy trì 24/7. Nếu có gián đoạn NEWTEL-CA sẽ thông báo trước 24 giờ, 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.

IV.8.3 Tùy chọn đặc biệt

Không có quy định.

IV.9 Kết thúc thuê bao chứng thư số

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

- Có lệnh dừng sử dụng chứng thư số hoặc dừng toàn bộ hệ thống NEWTEL- CA hoặc NEWTEL-CA 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.

IV.10 Lưu khóa ở bên thứ ba và khôi phục khóa

Hiện tại, NEWTEL-CA không thực hiện việc lữu trữ khóa bí mật của thuê bao cũng như cung cấp dịch vụ phục hồi khóa (trừ trường hợp đặc biệt cơ quan có thẩm quyền yêu cầu).

Duy nhất trường hợp thuê bao đăng ký chứng thư số máy chủ được tự sinh cặp khóa bí mật theo quy trình của NEWTEL-CA

Thuê bao phải lưu trữ khóa bí mật vào thiết bị lưu trữ theo quy định của pháp luật về an toàn thông tin và pháp luật khác có liên quan, và tự chịu trách nhiệm về an toàn, bảo mật của khóa bí mật đó.

IV.11 Cấp bù chứng thư số

IV.11.1 Các tình huống cấp bù chứng thư số

- Thuê bao đang sử dụng chứng thư số còn hạn nhưng bị lộ khóa, phải tạo lại cặp khóa;
- Thuê bao đang sử dụng chứng thư số còn hạn nhưng bị mất, hỏng Token, SIM PKI;
- Thuê bao đang sử dụng chứng thư số còn hạn, nhưng tại thời điểm đó các thuật toán sinh chứng thư số được cập nhật, thay đổi theo yêu cầu của cơ quan quản lý nhà nước;
- Chứng thư số đang sử dụng hết hạn, nhưng hợp đồng cung cấp dịch vụ được ký giữa thuê bao và nhà cung cấp vẫn còn hiệu lực, thời gian cấp bù được tính bằng thời gian hiệu lực còn lại của hợp đồng.

IV.11.2 Ai có thể yêu cầu cấp bù chứng thư số

Thuê bao đề nghị cấp bù chứng thư số của mình

IV.11.3 Quy trình cấp bù chứng thư số

Bước 1: Gửi hồ sơ xin cấp bù

Thuê bao làm hồ sơ theo mẫu để xin cấp bù chứng thư.

Bước 2: Tiếp nhận, xác minh định danh của thuê bao xin cấp bù

- Nhân viên được giao nhiệm vụ tại RA tiếp nhận hồ sơ xin cấp bù chứng thư, và thực hiện:
- Kiểm tra Chứng thư số của thuê bao đã được cấp có còn hiệu lực hay không
- Kiểm tra hồ sơ và các minh định danh theo quy định như trường hợp xin cấp mới. Nếu không đúng và không đầy đủ theo quy định thì thông báo cho thuê bao biết và bổ sung hoặc từ chối cấp. Nếu đúng và đầy đủ thì hẹn thời gian xử lý yêu cầu cấp bù.
- Chỉ tiếp nhận hồ sơ khi thông tin về chứng thư không thay đổi
- Nếu đúng và đầy đủ theo quy định, RA nhập thông tin về thuê bao cấp bù và chuyển hồ sơ tới CA để thực hiện cấp bù.

Bước 3: Nhập thông tin cấp bù chứng thư số

RA sẽ nhận, kiểm tra các hồ sơ xin cấp bù chứng thư số, xác minh định danh. Nếu đúng và đầy đủ theo quy định, RA nhập thông tin về thuê bao cấp bù và chuyển hồ sơ tới CA để thực hiện cấp bù. Nếu hồ sơ không đúng và không đầy đủ theo quy định, RA thông báo tới các đại lý.

Bước 4: Phê duyệt cấp bù chứng thư số

Bộ phận CA thực hiện phê duyệt (Approve):

- Đối chiếu thông tin được RA nhập yêu cầu cấp bù chứng thư số với thông tin trong hồ sơ khách hàng và đồng thời có thể đối chiếu các nguồn thông tin khác (nếu cần). Khi thấy thông tin đúng và đầy đủ theo quy định, cán bộ quản trị cấp phát chứng thư số sẽ thực hiện phê duyệt cấp bù chứng thư số (Approve).

- Chứng thư số cấp bù được sinh trong thiết bị chuyên dụng
- Dữ liệu liên quan đến hồ sơ thuê bao xin cấp bù chứng thư số sẽ được hệ thống lưu trữ có bảo mật theo quy định.

Bước 5: Thông báo chứng thư số được phê duyệt

NEWTEL-CA sẽ gửi thư điện tử (email) tới thư điện tử của thuê bao (đã đăng ký trong hồ sơ), hoặc điện thoại, fax tới thuê bao với nội dung thư thông báo hoàn thành việc cấp bù và hẹn thời gian bàn giao chứng thư số

Bước 6: Xác nhận đã nhận chứng thư số

NEWTEL-CA sẽ bàn giao chứng thư số cho thuê bao, thuê bao nhận được chứng thư số sẽ kiểm tra tính chính xác của chứng thư số và nếu thông tin trong chứng thư số không phù hợp, người dùng thông báo lại cho đại lý hoặc RA của NEWTEL-CA trong thời gian quy định để được xử lý.

Thông tin tiếp nhận: Mục IV.3.3

Bước 7: Công bố trạng thái chứng thư số

Hệ thống NEWTEL-CA sẽ công bố trạng thái chứng thư số ngay sau khi chứng thư số được cấp bù thành công và công khai trạng thái chứng thư số thông qua dịch vụ web, CRLs và OCSP theo quy định.

Thuê bao và bên tin tưởng có thể tải CRLs để kiểm tra trạng thái của chứng thư số, hoặc sử dụng dịch vụ OCSP để kiểm tra trạng thái chứng thư số. Thuê bao có thể dùng cho các ứng dụng khác thông qua máy chủ web.

Bước 8: Công bố chứng thư số

V THIẾT BỊ, QUẢN LÝ VÀ KIỂM SOÁT VẬN HÀNH

Các yêu cầu đối với cơ sở hạ tầng, tổ chức, và các biện pháp an ninh của NEWTEL-CA được xác định dựa trên các loại hình dịch vụ được NEWTEL-CA cung cấp.

Tính năng của hệ thống được xem xét thông qua các giá trị cơ bản như tính sẵn sàng, tính toàn vẹn, bảo mật và xác thực, được dựa trên các quy tắc về an toàn và bảo mật thông tin.

V.1 Kiểm soát vật lý

Nhằm đảm bảo chất lượng dịch vụ, NEWTEL-CA thực hiện các biện pháp kiểm soát và các thủ tục kiểm soát nhằm đảm bảo an ninh vật lý của hệ thống.

V.1.1 Tính sẵn sàng của dịch vụ

Hệ thống thiết bị của NEWTEL-CA được đặt như sau: Trung tâm dữ liệu chính PDC được đặt tại Datacenter của Viettel IDC (địa chỉ: Khu công nghệ cao Hòa Lạc) và trung tâm khôi phục thảm họa (DRDC) được đặt tại VDC (địa chỉ: Khu công nghiệp Nam Thăng Long). DRDC tách biệt với PDC.

Trong hoạt động bình thường chỉ có PDC tương tác trực tiếp với người dùng cuối và thực hiện các dịch vụ quản lý, chứng thực chữ ký số . DRDC làm nhiệm vụ như một trung tâm backup của PDC. Trường hợp có các rủi ro mà PDC không thể tự phục hồi được thì DRDC sẽ được kích hoạt và tiếp tục cung cấp dịch vụ cho người dùng.

V.1.2 Truy cập vật lý

Địa điểm đặt thiết bị nằm trong khuôn viên của Datacenter của Viettel IDC và VDC.

Phòng đặt hệ thống CA và RA của NEWTEL-CA được ngăn cách với các hệ thống khác, với hệ thống Camera giám sát an ninh và bảo vệ 24/7.

Quyền ra vào nơi đặt thiết bị được kiểm soát bởi hệ thống khóa kết hợp sử dụng công nghệ sinh trắc học hoặc SmartCard. Nhân viên bảo vệ chuyên trách có trách nhiệm ngăn chặn các truy cập từ bên ngoài ở mức vật lý.

Cụ thể, kiểm soát vật lý của hệ thống NEWTEL-CA có 5 lớp bảo mật truy cập vật lý, mỗi lớp cung cấp thêm các biện pháp kiểm soát và thiết bị an ninh vật lý chống lại xâm nhập không được phép.

1. Cửa kiểm soát của cán bộ bảo vệ;
2. Cửa kiểm soát của bảo vệ Trung tâm dữ liệu;
3. Hệ thống cửa có bảo mật của Trung tâm dữ liệu;
4. Hệ thống kiểm soát truy nhập bằng sinh trắc học hoặc Smartcard, camera giám sát 24/24 tại phòng máy chủ CA;
5. Phòng an toàn được kiểm soát bởi sinh trắc học hoặc smartcard, để thực hiện các thao tác tạo khóa và cấp chứng thư số cần 03 cán bộ có thẩm quyền.

V.1.3 Điều kiện về nguồn điện, môi trường

Hệ thống cung cấp dịch vụ của NEWTEL-CA đặt tại Datacenter của Viettel IDC và VDC nên sử dụng nguồn điện ổn định có hệ thống UPS (online và dự phòng), có hệ thống máy phát điện. Hệ thống máy phát điện được kiểm tra bảo dưỡng định kỳ để đảm bảo tính sẵn sàng cao nhất.

Phòng đặt máy chủ của NEWTEL-CA trang bị hệ thống điều hòa có điều khiển chính xác nhiệt độ. Hệ thống cảnh báo khi nhiệt độ, độ ẩm và khói, bụi vượt ngưỡng cho phép.

V.1.4 Phòng chống thiên tai

Hệ thống thiết bị của NEWTEL-CA được bố trí trên tầng cao, hạn chế tối đa sự tiếp xúc với nước kể cả khi có lũ lụt.

V.1.4 Phương án phòng chống chữa cháy

NEWTEL-CA được trang bị phương án phòng ngừa để cảnh báo và dập tắt lửa hay các thảm họa có thể gây cháy hay khói. Hệ thống thiết kế phù hợp với tiêu chuẩn QCVN 06 : 2010/BXD Quy chuẩn kỹ thuật quốc gia về an toàn cháy cho nhà và công trình.

V.1.5 Phương tiện lưu trữ dữ liệu

NEWTEL-CA có phương tiện lữu trữ dữ liệu (máy chủ, hệ thống SAN và NAS) được bảo vệ khỏi nước, lửa hay môi trường hủy hoại và được bảo vệ tránh sử dụng truy cập trái phép hay phá hủy.

V.1.6 Xử lý rác

Các tài liệu chứa thông tin nhạy cảm được hủy bằng các biện pháp phù hợp trước khi được bỏ đi. Đảm bảo các thông tin nhạy cảm, ví dụ như các bản sao hồ sơ của các thuê bao, tài liệu quản lý thuê bao, phương tiện điện tử lưu dữ liệu,… khi bị hủy không thể đọc được.

V.1.7 Hệ thống dự phòng ở địa điểm khác

NEWTEL-CA thực hiện việc lưu trữ dữ liệu dự phòng tại DRDC. Có chế độ bảo dưỡng sao lưu dữ liệu quan trọng hay bất cứ thông tin nhạy cảm nào phục vụ cho hoạt động của hệ thống NEWTEL-CA.

V.2 Các thủ tục kiểm soát

V.2.1 Những cá nhân được tin tưởng

Người được tin tưởng là các cán bộ của NEWTEL-CA được quyền thực hiện các nhiệm vụ quan trọng như sau trong quá trình vận hành hệ thống NEWTEL-CA:

- Xác minh và kiểm tra tính đầy đủ của thông tin trong đơn xin cấp chứng thư số của các thuê bao.
- Chấp nhận, loại bỏ đơn xin cấp chứng thư số, yêu cầu thu hồi, làm mới, tạm ngưng, gia hạn chứng thư số.
- Tạo khóa, ban hành, thu hồi, tạm ngưng, gia hạn chứng thư số
- Quản lý thông tin thuê bao

Người được tin tưởng trong NEWTEL-CA bao gồm nhưng không giới hạn trong các đối tượng sau:

1. Người đứng đầu hệ thống
2. Những người quản lý khóa của hệ thống
3. Người quản trị hệ thống và bộ phận quản trị hệ thống
4. Người phụ trách cấp phát, quản lý chứng thư số và bộ phận phụ trách quản lý chứng thư số
5. Kiểm toán kỹ thuật
6. Quản lý lưu dữ liệu

Những người được tin tưởng đều được xác minh về nhân thân, khả năng đảm bảo đáp ứng yêu cầu công việc trước khi được giao nhiệm vụ.

Trong hệ thống còn có thể có các thành viên khác với các chức năng khác. Ví dụ như người phụ trách kiểm toán kỹ thuật.

V.2.2 Số người được yêu cầu trên một nhiệm vụ nhạy cảm

NEWTEL-CA đảm bảo có nhiều người được tin tưởng thực hiện một công việc nhạy cảm như truy cập, điều khiển thiết bị phần cứng mã hóa. Với các chức năng này, NEWTEL-CA có ít nhất 3 người để cùng thực hiện cùng một công việc nhạy cảm theo mô hình "M out of N" (Mô hình này đòi hỏi ít nhất M quản trị viên trong tổng số N người sử dụng Smartcard/token của mình để thực hiện các thao tác quản trị và vận hành quan trọng).

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.

V.2.3 Nhận dạng và xác thực trong mỗi vai trò

Mọi cá nhân trước khi trở thành người được tin tưởng trong hệ thống NEWTEL-CA phải được xác minh Sơ yếu lý lịch, ngoài việc đáp ứng các tiêu chuẩn chuyên môn. NEWTEL-CA phê duyệt danh sách các cán bộ này.

Quá trình kiểm tra lại được trình bày trong phần V.3.1.

V.2.4 Những vai trò yêu cầu phải phân tách nhiệm vụ

Nhằm đảm bảo an toàn thông tin, tránh các sự cố bảo mật liên quan đến nhân sự, một số vai trò cần phải có sự phân tách, bao gồm nhưng không giới hạn:

- Xác minh thông tin trong đơn xin cấp chứng thư số;
- Chấp nhận, từ chối hay các xử lý khác đối với đơn xin cấp chứng thư số, yêu cầu thu hồi, làm mới chứng thư số;
- Tạo khóa, ban hành, thu hồi chứng thư số;
- Quản lý thông tin, yêu cầu của thuê bao;
- Kiểm toán kỹ thuật của hệ thống (tùy chọn).

V.3 Kiểm soát nhân sự

V.3.1 Khả năng chuyên môn, kinh nghiệm và sự trong sạch

Những cán bộ được tin tưởng của NEWTEL-CA phải được xác minh dựa trên khả năng và kinh nghiệm chuyên môn đáp ứng các nhu cầu công việc và trong sạch về lý lịch.

V.3.2 Các thủ tục kiểm tra lý lịch, trình độ

Trước khi được bổ nhiệm, cán bộ được tin tưởng cần được kiểm tra các thông tin như sau:

- Xác minh lại trình độ học vấn cao nhất đạt được, chuyên nghành;
- Xem xét các thông tin tiền án/tiền sự/kỷ luật/tố cáo;
- Kiểm tra thông tin tài chính, tín dụng, sức khỏe;
- Bản xác minh sơ yếu lý lịch;
- Kiểm tra các nguồn thông tin tham khảo;
- Xác nhận việc làm trước đó.

V.3.3 Yêu cầu đào tạo vận hành hệ thống

Tất cả các cán bộ liên quan đến vận hành hệ thống NEWTEL-CA được đào tạo các nội dung liên quan đến chữ ký số và chứng thực chữ ký số.

Quá trình đạo tạo chuyên môn được ghi lại để đảm bảo nhân sự có được đầy đủ kiến thức về lĩnh vực được phân công phụ trách.

Chương trình huấn luyện của NEWTEL-CA hướng đến đảm bảo thực hiện được các nhiệm vụ mỗi cá nhân được giao, bao gồm nhưng không hạn chế trong các lĩnh vực sau đây:

- Các nội dung pháp lý cần thiết liên quan đến chữ ký số và giao dịch điện tử;
- Khái niệm và kiến thức PKI cơ bản;
- Các chính sách và quy chế của NEWTEL-CA;
- Sử dụng và vận hành các thiết bị;
- Xử lý các sự cố và thủ tục duy trì tính liên tục của hệ thống.
- Việc đào tạo được duy trì và đảm bảo cập nhật các kiến thức cần thiết để các nhân viên thành thạo và thực hiện tốt công việc được giao khi vận hành hệ thống NEWTEL-CA.

NEWTEL-CA đầu tư cung cấp các tài liệu cần thiết cho nhân viên để đảm bảo hoàn thành các nhiệm vụ được giao.

V.3.4 Tần suất luân chuyển công việc

Theo quy định luân chuyển cán bộ của CÔNG TY CỔ PHẦN VIỄN THÔNG NEW TELECOM.

V.3.5 Xử lý các hành động không được phép

Xử lý theo quy định của CÔNG TY CỔ PHẦN VIỄN THÔNG NEW TELECOM và các quy định của luật pháp liên quan.

V.3.6 Phối hợp với Trung tâm Chứng thực điện tử quốc gia

NEWTEL-CA duy trì hoạt động trao đổi thông tin, chuyên môn với Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia (do Trung tâm Chứng thực điện tử quốc gia vận hành) để đảm bảo được cập nhật các thông tin liên quan đến pháp lý, chuẩn, quy định của nhà nước nhằm vận hành hệ thống cấp và quản lý chứng thư số được an toàn, đáp ứng yêu cầu.

V.4 Quy trình lưu nhật ký kiểm toán hệ thống NEWTEL-CA

V.4.1 Các loại sự kiện được ghi lại

NEWTEL-CA ghi lại nhật ký (log) các sự kiện sau:

- Các sự kiện về quá trình sử dụng chứng thư số:
  - Tạo khóa, đăng ký, tạo mới, đổi khóa, thay đổi, và thu hồi chứng thư số cho các thuê bao
  - Kết quả khi xử lý những yêu cầu từ các tổ chức, cá nhân muốn đăng ký chứng thư số
  - Truyền các chứng thư cho yêu cầu bên liên quan;

- Nhận được yêu cầu thu hồi
- Ban hành CRL

- Các sự kiện có liên quan đến an toàn, an ninh:
  - Truy cập hệ thống bởi nhân viên vận hành của thuê bao (thành công/không thành công).
  - Hành động đọc, ghi hoặc xóa các file, bản ghi an ninh nhạy cảm.
  - Sự cố hệ thống và những hiện tượng bất thường.
  - Hoạt động của an ninh mạng.
  - Thiết bị giám sát an ninh vật lý.
- Hệ thống của NEWTEL-CA ghi lại các thông tin đăng ký bao gồm tài liệu nhận dạng được người/tổ chức xin cấp chứng thư số đưa ra, cụ thể:
  - Thông tin định danh (xem III.2.2)
  - Nơi lưu trữ các bản sao đơn đăng ký và tài liệu nhận dạng
  - Người trực tiếp xử lý, tiếp nhận đơn

V.4.2 Tần suất xử lý nhật ký kiểm toán

- Nhật ký kiểm toán của hệ thống NEWTEL-CA được kiểm tra khi có sự việc không bình thường xảy ra;
- Hàng tuần nhật ký kiểm tra cần được tổng kết bằng văn bản;
- Tổng kết nhật ký kiểm toán cần được gửi đến Lãnh đạo của CÔNG TY CỔ PHẦN VIỄN THÔNG NEW TELECOM.

V.4.3 Thời hạn giữ lại các nhật ký kiểm toán

- Nhật ký kiểm toán sẽ được giữ tại hệ thống ít nhất 6 tháng, sau đó được lưu bởi hệ thống lữu trữ (phần V.5.2).

V.4.4 Bảo vệ các nhật ký kiểm toán

- Nhật ký kiểm toán từng tháng được ký bởi lãnh đạo của CÔNG TY CỔ PHẦN VIỄN THÔNG NEW TELECOM, được bảo vệ với trước các hành động xem, thay đổi, xóa bởi các đối tượng không có thẩm quyền.

V.4.5 Các thủ tục dự phòng nhật ký kiểm toán

- Nhật ký kiểm toán được sao lưu chế độ sao lưu chung của NEWTEL-CA

V.4.6 Phương thức ghi nhật ký kiểm toán

- Hoạt động của hệ thống, hệ điều hành và mạng được ghi lại và có cơ chế để không thay đổi được nhật ký.
- Một số nhật ký được ghi bằng tay bởi nhân viên nếu cần bổ sung.

V.4.7 Thông báo cho đối tượng gây ra sự kiện

- Khi một sự kiện được ghi nhật ký kiểm toán, tùy vào bản chất sự kiện, người lãnh đạo cấp trên (xem V.4.4) có thể thông báo hoặc không thông báo cho đối tượng gây ra sự kiện đó.

V.4.8 Đánh giá lỗ hổng hệ thống

- Dữ liệu nhật ký kiểm toán của NEWTEL-CA được phân tích để có phướng án khắc phục nếu có sự cố.

V.5 Lưu trữ các bản ghi

V.5.1 Các loại bản ghi được lưu trữ

- Mọi dữ liệu nhật ký kiểm toán trong phần V.4
- Thông tin liên quan đến đơn xin cấp chứng thư số, và vòng đời chứng thư số như: thu hồi, đổi khóa, làm mới….
- Thông tin về sử dụng chứng thư số như việc truy cập để xác định tính hiệu lực của chứng thư số (tùy chọn)
- Thông tin về các hoạt động kiểm toán kỹ thuật của hệ thống.

V.5.2 Thời hạn giữ lại các lưu trữ

Thời gian lưu trữ các bản ghi theo quy định của pháp luật. Nếu không có quy định, thời gian lưu trữ ít nhất là 10 năm.

V.5.3 Bảo vệ lưu trữ

- Hệ thống lưu trữ dữ liệu của NEWTEL-CA được bảo vệ vả chỉ người được NEWTEL-CA chỉ định mới có thể truy cập.
- Dữ liệu lưu trữ được bảo vệ theo các phương pháp cần thiết, chống lại việc xem, thay đổi, xóa, hay các thao tác 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 hệ thống NEWTEL-CA được phép hoạt động.

V.5.4 Thủ tục sao lưu lưu trữ

Dữ liệu lưu trữ được tiến hành sao lưu theo chế độ sao lưu của NEWTEL-CA.

V.5.5 Nhãn thời gian của các bản ghi

Các bản ghi có chứa thông tin về thời gian, ngày tháng

Thông tin thời gian không cần được mã hóa

V.5.6 Hệ thống lưu trữ

Hệ thống lưu trữ của NEWTEL-CA là hệ thống tập trung, có dự phòng.

V.5.7 Thủ tục truy cập và kiểm tra thông tin lưu trữ

Chỉ những người được NEWTEL-CA cấp quyền mới được phép truy nhập tới thông tin lữu trữ của hệ thống NEWTEL-CA.

V.6 Thay đổi khóa của NEWTEL-CA

Trước khi chứng thứ số của NEWTEL-CA hết hạn, nếu trong thời gian được cấp phép, NEWTEL-CA sẽ đăng ký với RootCA để được gia hạn và sử dụng chứng thư số mới và cặp khóa mới để ban hành chứng thư số cho các thuê bao.

Chỉ có khóa mới nhất của NEWTEL-CA là được sử dụng cho mục đích ký các chứng thư số.

Các khóa trước vẫn cần được lưu trữ để kiểm tra các chữ ký và để ký CRL.

Thời gian hoạt động của chứng thư số của NEWTEL-CA và thời gian sử dụng cặp khóa được quy định trong phần IV.3.2.

V.7 Lộ khóa và khôi phục sự cố/thảm họa

V.7.1 Các thủ tục kiểm soát sự cố và thảm họa

NEWTEL-CA có một Hướng dẫn Xử lý các tình huống khẩn cấp khi có các sự cố về an toàn thông tin về việc lộ cặp khóa của NEWTEL-CA.

Tài liệu Hưỡng dẫn Xử lý các tình huống khẩn cấp cần được chuyển đến tay tất cả các cán bộ của NEWTEL-CA.

Các yếu tố cơ bản của thủ tục trong Hướng dẫn Xử lý các tình huống khẩn cấp được bao gồm các mục V.7.2, V.7.3.

V.7.2 Sự cố về máy tính, phần mềm và dữ liệu

Khi có các sự cố về máy tính, phần mềm và dữ liệu, các thủ tục xử lý sự cố được thực hiện.

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 NEWTEL-CA, 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.

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

NEWTEL-CA 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 số 37/2009/TT-BTTTT và Thông tư số 08/2011/TT-BTTTT do Bộ Thông tin truyền thông ban hành về hồ sơ và thủ tục liên quan đến cấp phép, đăng ký, công nhận các tổ chức cung cấp dịch vụ chứng thực chữ ký số.

V.7.3 Thủ tục xử lý khóa bí mật bị làm mất/lộ

Khi có nghi ngờ khóa bí mật của NEWTEL-CA bị lộ hay bị mất, ngay lập tức cần báo động cho toàn bộ nhân viên của NEWTEL-CA, từ người đứng đầu, người phụ trách kỹ thuật và người phụ trách cấp phát chứng thư số đến các nhân viên kỹ thuật khác. Các bước sau cần được tiến hành :

a. Thông báo ngay lập tức với lãnh đạo CÔNG TY CỔ PHẦN VIỄN THÔNG NEW-TELECOM (thông báo cho Trung tâm Chứng thực điện tử quốc gia và các cơ quan pháp luật có liên quan) để phối hợp loại bỏ các chứng thư số bị ảnh hưởng từ sự cố.

b. Thông báo ngay lập tức cho tất cả các thuê bao bị ảnh hưởng bằng mọi phương tiện có thể.

c. Thu hồi ngay lập tức tất cả chứng thư số đã phát hành. Rà soát các thông tin online, được lưu trữ hay các dữ liệu kiểm toán kỹ thuật. Khi cần, kho dữ liệu của NEWTEL-CA cần được ngắt off-line để hạn chế các thông tin không chính xác được công bố.

d. Tổ chức tạo một cặp khóa mới và chứng thư số mới cho NEWTEL-CA

e. Duy trì hoạt động cấp các chứng thư số mới cho thuê bao.

V.7.4 Khả năng phục hồi hoạt động sau thảm họa

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

NEWTEL-CA 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

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

V.8 Kết thúc CA và RA

Khi chấm dứt hoạt động, NEWTEL-CA hoặc RA sẽ báo cho thuê bao, người tin cậy và các đối tượng có liên quan trước khi dừng hoạt động 06 tháng.

Nếu vì lý do cần dừng để chuyển sang sử dụng dịch vụ của tổ chức cung cấp dịch vụ chứng thực chữ ký số khác, NEWTEL-CA sẽ:

- Thông báo cho các thuê bao bị ảnh hưởng;
- Thu hồi chứng thư số của thuê bao;
- Thực hiện các thủ tục chuẩn bị, hướng dẫn các thuê bao chuyển sang tổ chức cung cấp dịch vụ chứng thực chữ ký số khác;
- Bảo quản dữ liệu lưu trữ và bản ghi của NEWTEL-CA trong thời gian được quy định bởi quy chế này;

Tiếp tục dịch vụ hỗ trợ thuê bao tới khi các chứng thư số do NEWTEL-CA ban hành hết hạn, nếu cần thiết.

VI KIỂM SOÁT AN TOÀN KỸ THUẬT

VI.1 Tạo cặp khóa và cài đặt

VI.1.1 Sinh cặp khóa

- Cặp khóa cho NEWTEL-CA được sinh ra trong thiết bị phần cứng mã hóa chuyên dụng (Hardware Security Module) đạt chuẩn FIPS 140-2 Level 3 trở lên.
- Cặp khóa của thuê bao được sinh trực tiếp và lưu trên các thiết bị chuyên dụng do thuê bao giữ.

VI.1.2 Công bố chứng thư số của NEWTEL-CA

- Người nhận có thể tải về khóa công khai của NEWTEL-CA từ trang web của dịch vụ NEWTEL-CA.
- Đường dẫn SHA1 http://pub.newca.vn/newtel-ca.crt
- Đường dẫn SHA256 http://newtel-ca.vn/download

VI.1.3 Độ dài khóa của thuê bao

- NEWTEL-CA tạo các cặp khóa có độ dài tối thiểu 1024 bits RSA cho các chứng thư số của thuê bao.
- Cặp khóa của Root NEWTEL-CA có độ dài 2048 bits RSA

VI.1.4 Các tham số sinh cặp khóa mã công khai và kiểm tra chất lượng

- Quá trình sinh cặp khóa mã công khai được tiến hành tuân theo chuẩn PKCS#11 (Giao diện giao tiếp với các thẻ mật mã) theo Thông tư 06/2015/TT-BTTTT: Quy định danh mục tiêu chuẩn bắt buộc về chữ kỹ số và dịch vụ chứng thực chữ kỹ số.
- NEWTEL-CA tuân thủ tiêu chuẩn về chữ ký số và chứng thực chữ ký số do Bộ Thông tin và Truyền thông ban hành.

VI.1.5 Chuyển giao khóa bí mật cho thuê bao

- Cặp khóa của thuê bao được sinh ra tại thiết bị USB Token, SIM PKI do NEWTEl-CA cung cấp. NEWTEl-CA thực hiện thủ tục sinh cặp khóa trong thiết bị và phân phối thiết bị trực tiếp tới thuê bao hoặc qua RA, đại lý.
- Thiết bị USB Token, SIM PKI sẽ sinh cặp khóa cho người sử dụng sử dụng thuật toán sinh khóa RSA với các tham số an toàn và độ dài khóa ít nhất 1024bit

VI.1.6 Chuyển giao khóa công khai của thuê bao đến RA

NEWTEL-CA, RA, đại lý hoặc thuê bao chuyển giao tập tin đề nghị cấp chứng thư số cho thuê bao mã theo chuẩn PKCS#10 sinh từ SIM PKI đạt chuẩn EAL level 4 trở lên, USB Token đạt chuẩn FIPS 140-2 Level 2 trở lên, hoặc tương đương qua kênh bảo mật SSL.

VI.1.7 Mục đích sử dụng khóa

- Trường mở rộng về mục đích sử dụng khóa trong chứng thư số của thuê bao do NEWTEL-CA cấp quy định về hạn chế các mục đích sử dụng mà thuê bao được áp dụng;
- Cặp khóa ký số được sử dụng để cung cấp xác thực, tính toàn vẹn và chống từ chối;
- Cặp khóa mã hóa được sử dụng cho mục đích mã hóa dữ liệu, phục vụ bảo mật.

VI.2 Bảo vệ khóa bí mật và kiểm soát module mã hóa

VI.2.1 Tiêu chuẩn module mã hóa

Thiết bị phần cứng mã hóa chuyên dụng HSM được dùng để lưu trữ khóa bí mật của NEWTEL-CA. Thiết bị HSM của NEWTEL-CA đáp ứng tiêu chuẩn FIPS 140-2 level 3 trở lên.

VI.2.2 Cơ chế kiểm soát khóa bí mật

Khóa bí mật của NEWTEL-CA được tách thành N phần khác nhau, các phần này được giữ bởi các đối tượng khác nhau. Với mỗi chức năng, cần có M phần (M nhỏ hơn hay bằng N) mã chia sẻ để kích hoạt chức năng đó.

VI.2.3 Lưu giữ ngoài khóa bí mật của thuê bao

Quy định về lưu giữ ngoài khóa bí mật (Key escrow) của thuê bao được trình bày trong phần IV.10.

VI.2.4 Dự phòng khóa bí mật

NEWTEL-CA sẽ lưu dự phòng (backup) khóa bí mật của mình để đề phòng thảm họa và trục trặc thiết bị. Khóa bí mật của NEWTEL-CA được lưu trữ trong các thiết bị HSM.

VI.2.5 Lưu trữ khóa bí mật

Sau khi hết thời hạn hoạt động, cặp khóa của NEWTEL-CA vẫn được lưu trữ (archive) an toàn với thời hạn ít nhất 5 năm trong HSM nhằm mục đích tra cứu sau này theo yêu cầu của cơ quan có thẩm quyền.

VI.2.6 Chuyển khóa bí mật vào/ra HSM

Khóa bí mật ở ngoài HSM luôn ở trạng thái mã. NEWTEL-CA hạn chế lưu khóa ngoài HSM.

VI.2.7 Phương thức kích hoạt khóa bí mật

- NEWTEL-CA sẽ có các biện pháp kỹ thuật bảo vệ kích hoạt khóa bí mật phù hợp với yêu cầu của thuê bao. Khóa bí mật được lưu trong token/SIM PKI do thuê bao giữ. Việc kích hoạt khóa bí mật yêu cầu mật khẩu bảo vệ (PIN).
- Hệ thống NEWTEL-CA sử dụng HSM để lưu trữ khóa bí mật và việc kích hoạt khóa bí mật yêu cầu các mã chia sẻ theo cơ chế mã trong VI.2.2.

VI.2.8 Phương pháp ngừng kích hoạt khóa bí mật

- Các thành viên của NEWTEL-CA được yêu cầu phải đăng xuất khỏi hệ thống khi rời khỏi chỗ làm việc.

VI.2.9 Phương pháp hủy bỏ khóa 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 Token/SIM PKI được xóa bằng phần mềm quản trị chuyên dụng. NEWTEL-CA hướng dẫn cho các cán bộ vận hành và thuê bao cách thức hủy bỏ khóa bí mật khi cần thiết;
- Khóa bí mật của NEWTEL-CA lưu trên HSM được xóa bằng chức năng xóa khóa của HSM.

Các hoạt động hủy bỏ khóa bí mật, liên quan đến hệ thống CA hoặc của các cán bộ được giao vận hành hệ thống CA, được ghi lại trong nhật ký.

VI.2.10 Đánh giá thiết bị mã hóa phần cứng

Xem phần VI.2.1.

VI.3 Các vấn đề khác của việc quản lý cặp khóa

VI.3.1 Lưu trữ khóa công khai

NEWTEL-CA sẽ lưu trữ khóa công khai của mình và toàn bộ thuê bao.

VI.3.2 Thời hạn sử dụng chứng thư số và thời hạn sử dụng cặp khóa

Thời hạn sử dụng của chứng thư số sẽ kết thúc khi chứng thư số đó hết hạn hoặc bị thu hồi

Thời hạn sử dụng cặp khóa của thuê bao giống như thời hạn sử dụng của chứng thư số, ngoại trừ chức năng giải mã và kiểm tra chữ ký số sau khi chứng thư số hết hạn.

NEWTEL-CA không ban hành các chứng thư số có thời hạn sử dụng vượt quá thời hạn sử dụng chứng thư số của NEWTEL-CA.

VI.4 Dữ liệu khởi tạo

VI.4.1 Tạo và cài đặt dữ liệu kích hoạt

Dữ liệu kích hoạt bí mật của NEWTEL-CA được chia thành các mã được chia sẻ.

Các mã được chia sẻ này được tạo theo các yêu cầu trong phần VI.2.2 và tuân theo các thủ tục, quy định về Lễ sinh khóa của một CA.

Quá trình tạo và phân phối mã chia sẻ được ghi nhật ký.

Mật khẩu để bảo vệ, kích hoạt chia sẻ được đặt theo nguyên tắc mật khẩu mạnh.VI.4.2 Bảo vệ dữ liệu kích hoạt

Người giữ mã chia sẻ của NEWTEL-CA được yêu cầu bảo vệ an toàn mã chia sẻ của họ. Những người này phải ký một thỏa thuận với NEWTEL-CA về việc đảm bảo trách nhiệm trong việc bảo vệ mã chia sẻ mà họ giữ.

RA và quản trị hệ thống được yêu cầu phải giữ khóa bí mật ở dạng mã hóa sử dụng mật khẩu bảo vệ.

Thuê bao của NEWTEL-CA được yêu cầu lưu trữ khóa bí mật dưới dạng mã hóa sử dụng Token/SIM PKI và mật khẩu bảo vệ.

VI.4.3 Các vấn đề khác của dữ liệu kích hoạt

- Truyền, gửi dữ liệu kích hoạt
- Dữ liệu kích hoạt khi được truyền, gửi đi được bảo vệ chống lại việc mất, lộ, truy cập không được phép.
- Hủy bỏ dữ liệu kích hoạt
- Sau khi hết hạn sử dụng được quy định trong phần V.5.2, NEWTEL-CA sẽ loại bỏ dữ liệu kích hoạt khóa bí mật bằng cách ghi đè và/hoặc hủy bỏ vật lý.

VI.5 Kiểm soát an ninh cho hệ thống máy tính

Hệ thống NEWTEL-CA được vận hành với các biện pháp an ninh do CÔNG TY CỔ PHẦN VIỄN THÔNG NEW TELECOM quy định.

VI.5.1 Các yêu cầu an ninh hệ thống máy tính

Các máy chủ cài đặt hệ thống NEWTEL-CA và các dữ liệu được bảo vệ khỏi các truy nhập không được phép.

NEWTEL-CA giới hạn quyền truy nhập tới máy chủ CA theo vai trò của quản trị.

Trên các máy tạo cặp khóa của NEWTEL-CA, không kết nối vào mạng và không cài đặt các ứng dụng khác.

Hệ thống mạng của NEWTEL-CA được cách ly với các hệ thống khác, bảo vệ khỏi sự truy cập bất hợp pháp, được thiết kế theo mô hình 4 vùng (DMS, Service, CA và WAN-Internet). Sự cách ly này được thực hiện bằng hệ thống tường lửa. Lớp tường lửa và IPS bên ngoài bảo vệ cả hệ thống khỏi các truy nhập từ ngoài. Lớp tường lửa bên trong cách ly các máy chủ CA và hệ thống mạng chung của NEWTEL-CA.

NEWTEL-CA yêu cầu sử dụng mật mẩu mạnh, được định kỳ được thay đổi.

Việc truy nhập trực tiếp dữ liệu của CA chỉ được giới hạn cho những người có quyền và nhiệm vụ phù hợp.

VI.5.2 Đánh giá an ninh của hệ thống máy tính

Đánh giá theo quy định của CÔNG TY CỔ PHẦN VIỄN THÔNG NEW TELECOM.

VI.6 Kiểm soát kỹ thuật vòng đời chứng thư số

VI.6.1 Giám sát triển khai hệ thống

NEWTEL-CA đáp ứng các điều kiện được quy định trong 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.

Quá trình triển khai và khai thác hệ thống chịu sự giám sát chặt chẽ của NEWTEL-CA.

VI.6.2 Quản lý giám sát an ninh

NEWTEL-CA có các thủ tục và biện pháp kiểm soát an ninh trong quá trình thiết lập hệ thống phù hợp với các quy định nội bộ.

Các cấu hình của hệ thống CA cũng như bất kỳ sửa đổi và nâng cấp phải được ghi chép và kiểm soát. Có phương pháp phát hiện sửa đổi trái phép các phần mềm CA hay cấu hình.

VI.6.3 Giám sát an ninh vòng đời chứng thư số

NEWTEL -CA tuân thủ quy trình trong cả vòng đời chứng thư số.

VI.7 Kiểm soát an toàn mạng

Hệ thống mạng của NEWTEL-CA được bảo vệ thông qua việc lắp đặt và cấu hình các thiết bị để cho phép chỉ có các giao thức và lệnh cần thiết cho hoạt động của CA mới được chấp nhận.

VII CHỨNG THƯ SỐ, CRL, VÀ HỒ SƠ OCSP

VII.1 Hồ sơ chứng thư số

VII.1.1 Phiên bản

Chứng thư số do NEWTEL-CA ban hành tuân theo chuẩn ITU-T X.509 v3 và các quy định của RFC 5280.

VII.1.2 Trường cơ bản

Chứng thư số do NEWTEL-CA ban hành có các trường cơ bản theo bảng dưới đây.

Trường giá trị	Ý nghĩa
Serial Number	Giá trị là duy nhất với mỗi chứng thư số do NEWTEL-CA ban hành
Signature Algorithm	Định danh (OID) của thuật toán được sử dụng để ký tên lên chứng thư số
Issuer	NEWTEL-CA
Valid From	Thời điểm bắt đầu chứng thư số có hiệu lực, theo giờ Việt Nam
Valid To	Thời điểm hết hiệu lực của chứng thư số, theo giờ Việt Nam
Subject DN	Xem phần VII.1.5
Subject Public key	Khóa công khai, được mã hóa phù hợp với RFC 5280
Signature	Chữ ký số của NEWTEL-CA được mã hóa phù hợp với RFC 5280

VII.1.3 Trường mở rộng

NEWTEL-CA phải công bố các phần mở rộng của chứng thư số và các ứng dụng đã được phê duyệt phải xử lý các mở rộng này như quy định tại RFC 5280.

Phần mở rộng của chứng thư số được NEWTEL-CA hỗ trợ bao gồm:

- Basic Contraints (basicContraints): chứa thông tin xác định đây có phải là CA không và độ sâu lớn nhất của cấu trúc phân cấp chứng thư (certificate path).
- Key Usage (keyUsage): Mô tả mục đích sử dụng của khóa được lưu trong chứng thư.
- Certificate Policies (certificatePolicies): chứa một hoặc nhiều cụm các thông tin chính sách, mỗi cụm gắn kèm với nó là một OID và một bộ định tính tùy chọn (optional qualitiers).
- Authority Key Identifier (authorityKeyIdentifier): xác định khóa công khai tương ứng với khóa bí mật đã sử dụng để ký CRL.
- Subject Key Identifier (subjectKeyIdentifier): xác định các chứng thư chứa một khóa công khai cụ thể.
- CRL Distribution Points (crlDistributionPoints): chứa các thông tin về danh sách thu hồi chứng thư (CRL).
- Authority Information Access (authorityInformationAccess): đưa ra cách truy cập các thông tin và dịch vụ CA của nhà cung cấp theo các trường mở rộng chứng thư.

- Extended Key Usage (extendedKeyUsage): đưa ra một hoặc nhiều các mục đích sử dụng của khóa bổ sung cho mục đích sử dụng xác định trong mục Key Usage.

VII.1.4 Các thuật toán ký

Các thuật toán NEWTEL-CA đùng để ký chứng thư số và CRL như sau: shalwithRSAEncrytion (1 2 840 113549 1 1 5), sha256WithRSAEncryption (1 2 840 113549 1 1 1).

VII.1.5 Khuôn dạng tên

Chứng thư số của NEWTEL-CA chứa tên phân biệt (DN) dạng X.509 đầy đủ của NEWTEL-CA và certificate subject trong các trường hợp Issuer name và Subject name.

Tên phân biệt (DN) ở dạng một chuỗi ký tự in được của X.501.

VII.1.6 Giới hạn tên

Không quy định.

VII.1.7 Sử dụng ràng buộc mở rộng chính sách chứng thư số

OID của Quy chế chứng thực này được xác định
1.3.6.1.4.30339.1.[code-CA].3
[code-CA] do Bộ Thông tin và Truyền thông cấp.

VII.1.8 Cú pháp và ngữ nghĩa của chính sách phân loại
Không quy định.

VII.1.9 Xử lý ngữ nghĩa của các trường mở rộng chính sách chứng thư số

Không quy định.

VII.2 Hồ sơ CRL

CRL do NEWTEL-CA công bố tuân theo chuẩn ITU-T X.509 v3 và các quy định của RFC 5280. Tối thiểu, CRL do NEWTEL-CA công bố có các trường và giá trị theo bảng dưới đây:

Trường giá trị	Ý nghĩa
Serial Number	Xem phần VII.2.1
Signature Algorithm	Thuật toán được dùng để ký CRL. Sử dụng một trong các hàm băm sau SHA-256, SHA-384, SHA-512.
Issuer	Thực thể ký và ban hành CRL: NEWTEL-CA
Effective Date	Ngày có hiệu lực CRL.
Next Update	Thời gian mà CRL tiếp theo sẽ được công bố.
Revoked Certificates	Danh sách các chứng thư số bị thu hồi, bao gồm Serial Number của các chứng thư số bị thu hồi.

VII.2.1 Số phiên bản của CRL

NEWTEL-CA ban hành X.509 V3 CRL.

VII.2.2 CRL và các trường mở rộng CRL

Không quy định.

VII.3 Hồ sơ OCSP

VII.3.1 Phiên bản

Chứng thư số OCSP Responder sử dụng trong Hệ thống được NEWTEL-CA ban hành theo chuẩn X.509 v3 và các quy định của RFC 5280.

Hệ thống kiểm tra trạng thái các loại chứng thư sau theo chuẩn OCSP mô tả trong RFC2560:

- Chứng thư số cho cá nhân
- Chứng thư số cho các tổ chức, doanh nghiệp

VII.3.2 Trường cơ bản

Chứng thư số OCSP Responder bao gồm các trường sau:

Trường giá	**Ý nghĩa**
Serial Number	Giá trị là duy nhất với mỗi chứng thư số do NEWTEL-CA ban hành
Signature Algorithm	Định danh (OID) của thuật toán được sử dụng để ký tên lên chứng thư số
Issuer	NEWTEL-CA
Valid From	Thời điểm bắt đầu chứng thư số có hiệu lực, theo giờ Việt Nam
Valid To	Thời điểm hết hiệu lực của chứng thư số, theo giờ Việt Nam
Subject DN	Xem phần VII.1.4
Subject	Khóa công khai, được mã hóa phù hợp với RFC 5280
Signature	Chữ ký số của NEWTEL-CA được mã hóa phù hợp với RFC 5280

VII.3.3 Trường mở rộng

Chứng thư số OCSP Responder bao gồm các trường mở rộng sau:

Trường giá trị	**Ý nghĩa**
Basic Contraints (basicContraints)	Chứa thông tin xác định đây có phải là CA không và độ sâu lớn nhất của cấu trúc phân cấp chứng thư (certificate path)
Key Usage (keyUsage)	Mô tả mục đích sử dụng của khóa được lưu trong chứng thư
Subject Key Identifier (subjectKeyIdentifier)	Xác định các chứng thư chứa một khóa công khai cụ thể
Subject Alternative Name (subjectAltName)	Cho phép bổ sung thêm các định danh gắn với chủ thể của chứng thư cho được cấp phát
Extended Key Usage (extendedKeyUsage)	Đưa ra một hoặc nhiều các mục đích sử dụng của khóa bổ sung cho mục đích sử dụng xác định trong mục Key Usage

VIII KIỂM TOÁN MỨC TUÂN THỦ VÀ CÁC ĐÁNH GIÁ KHÁC

Việc kiểm toán kỹ thuật các hoạt động NEWTEL-CA được thực hiện định kỳ từ CÔNG TY CỔ PHẦN VIỄN THÔNG NEW TELECOM hoặc theo yêu cầu từ Trung tâm Chứng thực điện tử quốc gia.

VIII.1 Tần suất và các tình huống kiểm toán kỹ thuật

Kiểm toán kỹ thuật được thực hiện ít nhất một năm một lần, phí tổn thuộc về CÔNG TY CỔ PHẦN VIỄN THÔNG NEW TELECOM.

VIII.2 Đơn vị thực hiện kiểm toán kỹ thuật

Đơn vị kiểm toán kỹ thuật NEWTEL-CA được chỉ định bởi CÔNG TY CỔ PHẦN VIỄN THÔNG NEW TELECOM hoặc bởi Trung tâm Chứng thực điện tử quốc gia.

VIII.3 Mối quan hệ của đơn vị kiểm toán kỹ thuật với NEWTEL-CA

Kiểm toán kỹ thuật được thực hiện bởi những đơn vị không phụ thuộc vào NEWTEL-CA.

VIII.4 Các nội dung kiểm toán kỹ thuật

Các lĩnh vực được kiểm toán kỹ thuật bao gồm: hạ tầng hệ thống, các quy trình quản lý khóa, quy trình vận hành hệ thống và các nội dung khác theo yêu cầu của đơn vị kiểm toán kỹ thuật.

VIII.5 Xử lý khi phát hiện sai sót

Sau khi có báo cáo kiểm toán kỹ thuật, NEWTEL-CA sẽ làm việc với đơn vị kiểm toán về những nội dung chưa phù hợp.

NEWTEL-CA sẽ nghiên cứu, đề ra và thực hiện phương án xử lý những nội dung chưa phù hợp trong thời gian thống nhất đơn vị tiến hành kiểm toán và có báo cáo Trung tâm Chứng thực điện tử quốc gia.

Dịch vụ của NEWTEL-CA sẽ bị ngưng trong các tình huống sau:

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

VIII.6 Công bố kết quả kiểm toán kỹ thuật

Báo cáo kết quả kiểm toán kỹ thuật được NEWTEL-CA gửi Trung tâm Chứng thực điện tử quốc gia và nếu được phép công bố.

IX CÁC NỘI DUNG NGHIỆP VỤ PHÁP LÝ KHÁC

IX.1 Phí

NEWTEL-CA thực hiện thu phí với các thuê bao theo như hợp đồng cung cấp dịch vụ bao gồm các loại phí:

- Phí cập mới: theo hợp đồng cung cấp dịch vụ
- Phí gia hạn: theo hợp đồng cung cấp dịch vụ
- Phí thu hồi: miễn phí

- Phí truy cập OCSP: miễn phí
- Phí dịch vụ duy trì hệ thống kiểm tra trạng thái cho chứng thư số công bố ở NEAC: 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, mức 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

NEWTEL-CA sẽ tiến hành hoàn phí cung cấp dịch vụ cho thuê bao sử dụng dịch vụ theo các điều khoản Hoàn phí được quy định trong Hợp đồng cung cấp dịch vụ.

IX.2. Tính bí mật của thông tin nghiệp vụ

IX.2.1 Phạm vi các thông tin bí mật

Những thông tin sau sẽ được coi là thông tin bí mật:

- Các thông tin được yêu cầu bởi pháp luật.
- Hồ sơ đăng ký cấp chứng thư số.
- Nhật ký của NEWTEL-CA.
- Báo cáo kiểm toán kỹ thuật của NEWTEL-CA.
- Kế hoạch đối phó với sự cố và kế hoạch khôi phục lại sau thảm họa của NEWTEL-CA.
- Phương pháp điều khiển hoạt động các thành phần NEWTEL-CA: phần cứng, phầm mềm và quản trị của dịch vụ của NEWTEL-CA.

IX.2.2 Những thông tin ngoài phạm vi thông tin bí mật

Các thông tin không được coi là bí mật:

- Chứng thư số, trạng thái thu hồi của chứng thư số và thông tin trạng thái khác, địa chỉ website của NEWTEL-CA trên mạng và các thông tin trên đó.
- Không được chỉ rõ ràng trong phần IX.2.1.

IX.2.3 Trách nhiệm bảo vệ các thông tin bí mật

NEWTEL-CA thực hiện các biện pháp đảm bảo an ninh cho các thông tin bí mật.

IX.3 Tính riêng tư của thông tin cá nhân

IX.3.1 Kế hoạch bảo mật thông tin cá nhân

Chính sách bảo mật thông tin cá nhân được CÔNG TY CỔ PHẦN VIỄN THÔNG NEW TELECOM thông qua được công bố trên website của NEWTEL-CA và thông báo cho thuê bao khi tiến hành đăng ký chứng thư số.

IX.3.2 Phạm vi các thông tin cá nhân

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

IX.3.3 Những thông tin ngoài phạm vi thông tin cá nhân

Mọi thông tin được công bố trong một chứng thư số, dịch vụ thư mục và CRL được coi là không bí mật.

IX.3.4 Trách nhiệm bảo vệ các thông tin bí mật

NEWTEL-CA thực hiện các biện pháp đảm bảo an ninh cho các thông tin bí mật của thuê bao, tuân theo yêu cầu của luật pháp.

IX.3.5 Thông báo và sự đồng thuận sử dụng của thông tin mật

Thông tin bí mật sẽ không được sử dụng mà không có sự cho phép của người sở hữu thông tin hoặc đại diện sở hữu thông tin đó, trừ những trường hợp được quy định trong quy chế này hoặc trong các thỏa thuận cụ thể.

IX.3.6 Cung cấp thông tin theo yêu cầu của cơ quan pháp luật

NEWTEL-CA sẽ cung cấp thông tin bí mật nếu có yêu cầu của cơ quan pháp luật có thẩm quyền và tuân thủ theo quy định của pháp luật.

IX.3.7 Các tình huống cung cấp thông tin khác

NEWTEL-CA không cung cấp thông tin cho các đối tượng nào khác ngoài đại diện có thẩm quyền của pháp luật.

IX.4 Quyền sở hữu trí tuệ

IX.4.1 Quyền sở hữu những thông tin chứng thư số và thu hồi

NEWTEL-CA giữ mọi quyền sở hữu chứng thư số và thông tin thu hồi mà nó tạo ra.

NEWTEL-CA cho phép sử dụng thông tin thu hồi khi thực hiện chức năng của người nhận.

IX.4.2 Quyền sở hữu quy chế chứng thực

NEWTEL-CA giữ mọi quyền sở hữu trí tuệ quy chế chứng thực này.

IX.4.3 Quyền sở hữu tên

Không quy định.

IX.4.4 Quyền sở hữu khóa

Cặp khóa tương ứng với chứng thư số của NEWTEL-CA, RA, thuê bao được sở hữu bởi chính đối tượng là chủ thể của chứng thư số đó.

IX.5 Tuyên bố và cam kết

IX.5.1 Tuyên bố và cam kết của NEWTEL-CA

NEWTEL-CA 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 cấp phát chứng thư số
- Chứng thư số do NEWTEL-CA ban hành đáp ứng các yêu cầu trong quy chế này.

IX.5.2 Tuyên bố và cam kết của RA

NEWTEL-CA 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 cấp phát chứng thư số;
- Chứng thư số do NEWTEL-CA ban hành đáp ứng các yêu cầu trong quy chế này;
- Thực hiện nghĩa vụ Đại lý tại điều 35 Nghị định số 130/2018/NĐ-CP về quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số.

IX.5.3 Tuyên bố và cam kết của thuê bao

Thuê bao đảm bảo rằng:

- Khi ký, thuê bao 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.
- NEWTEL-CA khuyến cáo cần phải lưu trữ chứng thư số trong các thiết bị lưu trữ chuyên dụng.
- Thỏa thuận thuê bao có thể bao gồm thêm những điều khoản khác do NEWTEL-CA quy định.

Nếu thuê bao vi phạm các cam kết trên, thuê bao chịu hoàn toàn trách nhiệm và phải đền bù các thiệt hại gây ra theo quy định của pháp luật.

IX.5.4 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 NEWTEL-CA ban hành.

Người nhận phải chịu trách nhiệm cho những hành động của mình do không thực hiện theo các nội quy liên quan được quy định trong thỏa thuận người nhận hoặc quy chế chứng thực này.

IX.5.5 Tuyên bố và cam kết của các đối tượng khác

Ngoài các cam kết do NEWTEL-CA định ra , RA, thuê bao và người nhận, không có tuyên bố và cam kết của đối tượng nào khác được NEWTEL-CA chấp nhận.

IX.6 Tuyên bố về sự đảm bảo

Không quy định.

IX.7 Giới hạn về trách nhiệm

Không quy định.

IX.8 Bồi thường

Không quy định.

IX.9 Điều khoản và sự kết thúc

IX.9.1 Thời hạn bắt đầu có hiệu lực

Quy chế chứng thư số này có hiệu lực khi công bố trên website của NEWTEL-CA. Các nội dung bổ sung cho quy chế chứng thư số này có hiệu lực khi được công bố.

IX.9.2 Thời hạn hết hiệu lực

Quy chế này được còn hiệu lực cho đến khi nó được thay thế bằng một phiên bản mới.

IX.9.3 Ảnh hưởng của quy chế chứng thực số 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.

IX.10 Thông báo cho thuê bao và liên lạc với các bên có tham gia

Trừ khi được quy định rõ ràng, các thành viên NEWTEL-CA 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.

IX.11 Thay đổi Quy chế chứng thực

IX.11.1 Thủ tục bổ sung

Quy chế này được bổ sung, sửa đổi bởi tổ chuyên gia do CÔNG TY CỔ PHẦN VIỄN THÔNG NEW TELECOM phê chuẩn.

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.

IX.11.2 Cơ chế và thời hạn thông báo

Đối với các thay đổi không quan trọng như thay đổi URL, thông tin liên hệ, lỗi in ấn… NEWTEL-CA có quyền thay đổi quy chế mà không cần thông báo về sự thay đổi.

Trong trường hợp các thay đổi được phê duyệt có liên quan tới an ninh của hệ thống, NEWTEL-CA sẽ thực hiện sự thay đổi quy chế này lập tức, sau đó sẽ thông báo cho các tổ chức cá nhân có liên quan và Trung tâm Chứng thực điện tử quốc gia.

IX.11.3 Giải quyết các bất đồng, tranh chấp

Thực hiện theo quy định của CÔNG TY CỔ PHẦN VIỄN THÔNG NEW TELECOM và trong hợp đồng cung cấp dịch vụ.

IX.11.4 Luật điều chỉnh

Pháp luật Việt Nam sẽ được sử dụng trong mọi trường hợp để xử lý tranh chấp liên quan đến các dịch vụ và chứng thư số dô NEWTEL-CA cấp, kể cả trường hợp có liên quan đến các yếu tố nước ngoài.

IX.11.5 Tính tuân thủ với các luật pháp được áp dụng

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.

IX.11.6 Điều khoản chung

Quy chế chứng thực này là thỏa thuận mà mọi thành viên của NEWTEL-CA phải tuân thủ.

Không có quy định nào cho phép chuyển nhượng quyền sử dụng chứng thư số. NEWTEL-CA không quy định các trường hợp chuyển nhượng khác.

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.

IX.11.7 Điều khoản khác

Không quy định.

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).