CÔNG TY TNHH

TƯ VẤN - THƯƠNG MẠI KHÁNH LINH (WINCA)

QUY CHẾ VÀ CHÍNH SÁCH
CHỨNG THƯ SỐ

Phiên bản: 01

OID:

WINCA

MỤC LỤC

I. Giới thiệu.

I.1 Tổng quan

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

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

I.2 Tên tài liệu và nhận dạng

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

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

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

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

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

I.3 Các bên tham gia

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

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

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

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

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

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

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

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

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

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

I.4 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 WINCA cấp được phân ra các loại sau đây:

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

Chứng thư số cho cá nhân có thời hạn không được vượt quá thời hạn của chứng thư số WINCA.

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

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

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

Chứng thư số cho tổ chức doanh nghiệp có thời hạn không được vượt quá thời hạn của chứng thư số WINCA.

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 và chỉ được sử dụng theo đúng phạm vi quy định trong hợp đồng giữa WINCA và thuê bao.

Trong mọi trường hợp, cấm sử dụng chứng thư số do WINCA 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.

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

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

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

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

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

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

I.5 Quản lý chính sách

I.5.1 Tổ chức quản lý tài liệu

Tên cơ quan: Công ty TNHH Tư Vấn Thương Mại Khánh Linh

Địa chỉ: 16-18 Xuân Diệu, Quận Tân Bình, Tp.HCM

Điện thoại: 028 38116723

E-mail: info@ketoanvn.com.vn

Website: www.ketoanvn.com.vn

I.5.2 Người liên hệ

Người quản lý tài liệu

Họ và tên: Đào Cao Bích Ngọc

Điện thoại: 0933030678

Hỗ trợ kỹ thuật:

Họ và tên: Hứa Anh Chương

Điện thoại: 0918856738

I.5.3 Công nhận sự phù hợp của CPS

Bộ Thông tin và Truyền Thông và Công ty TNHH TƯ VẤN - THƯƠNG MẠI KHÁNH LINH xác nhận sự phù hợp của quy chế chứng thực này.

I.5.4 Thủ tục phê chuẩn CPS

Công ty TNHH TƯ VẤN - THƯƠNG MẠI KHÁNH LINH sẽ phê chuẩn CPS. Mỗi phiên bản của CPS có một bộ định danh đối tượng duy nhất (OID). Các thay đổi, cập nhật của CPS được ghi trong một tài liệu chứa các sửa đổi của CPS hay các thông tin về quá trình cập nhật và được công bố tại http://www.winca.org/cps.

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

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

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

http://www.winca.org/cps/version/

I.6 Các Định nghĩa và viết tắt

I.6.1 Các định nghĩa

Thuật ngữ	Giải thích
Chứng thư số WINCA	Là một dạng chứng thư điện tử do WINCA số cấp.
Chứng thư số có hiệu lực	Là chứng thư số chưa hết hạn, không bị tạm dừng hoặc bị thu hồi.
Chữ ký số	Là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng theo đó người có được thông điệp dữ liệu ban đầu và khoá công khai của người ký có thể xác định được chính xác:

	a. Việc biến đổi nêu trên được tạo ra bằng đúng khoá bí mật tương ứng với khoá công khai trong cùng một cặp khóa; b. Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.
Dịch vụ chứng thực chữ ký số	Là một loại hình dịch vụ chứng thực chữ ký điện tử, do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp. Dịch vụ chứng thực chữ ký số bao gồm: a. Tạo cặp khóa bao gồm khóa công khai và khóa bí mật cho thuê bao; b. Cấp, gia hạn, tạm dừng, phục hồi và thu hồi chứng thư số của thuê bao; c. Duy trì trực tuyến cơ sở dữ liệu về chứng thư số; d. Những dịch vụ khác có liên quan theo quy định.
Hệ thống mật mã không đối xứng	Là hệ thống mật mã có khả năng tạo được cặp khóa bao gồm khoá bí mật và khóa công khai.
Khoá	Là một chuỗi các số nhị phân (0 và 1) dùng trong các hệ thống mật mã.
Khóa bí mật	Là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được dùng để tạo chữ ký số.
Khóa công khai	Là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được sử dụng để kiểm tra chữ ký số được tạo bởi khoá bí mật tương ứng trong cặp khoá.
Ký số	Là việc đưa khóa bí mật vào một chương trình phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu.

Người ký	Là thuê bao dùng đúng khoá bí mật của mình để ký số vào một thông điệp dữ liệu dưới tên của mình.
Người nhận	Là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng chứng thư số của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.
Thuê bao	Là tổ chức, cá nhân được cấp chứng thư số, chấp nhận chứng thư số và giữ khoá bí mật tương ứng với khoá công khai ghi trên chứng thư số được cấp đó.
Tạm dừng chứng thư số	Là làm mất hiệu lực của chứng thư số một cách tạm thời từ một thời điểm xác định.
Thu hồi chứng thư số	Là làm mất hiệu lực của chứng thư số một cách vĩnh viễn từ một thời điểm xác định.

I.6.2 Từ viết tắt

ARLs	Authority Revocation Lists
CA	Certificate Authority
CMS	Cryptographic Message Syntax
CP	Certificate Policy
CPS	Certification Practice Statement
CRLs	Certificate Revocation Lists
CRR	Certificate Revocation Request
CSP	Certification Service Provider

DAP	Directory Access Protocol
DES	Data Encryption Standard
DNS	Domain Name System
HTTPS	Secure Hypertext Transaction Standard
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5 Hash Algorithm
OCSP	Online Certificate Status Protocol
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Extended Public Key Infrastructure
RA	Registration Authorities
RFC	Request For Comments
RSA	Rivest Shamir Adleman
S/MIME	Secure Multipurpose Internet Mail Extensions
SHA-1	Secure Hash Standard
SSL	Secure Socket Layer
TLS	Transport Layer Security
X.500	X.500 The ITU-T (International Telecommunication Union-T) standard that establishes a distributed,

	hierarchical directory protocol organized by country, region, Organization, etc.
X.501	The ITU-T (International TelecommuniCAtion Union-T) standard for use of Distinguished Names in an X.500 directory.
X.509	ITU-T standard for Certificates format

II. Trách nhiệm công bố và lưu trữ

II.1 Lưu trữ

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

II.2 Công bố thông tin chứng thư

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

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

Các kho lưu trữ trực tuyến được công bố tại địa chỉ URL sau: crl.winca.org

Địa chỉ công bố truy cập trả lời OCSP: ocsp.winca.org

LDAP được công bố trên: ldap.winca.org

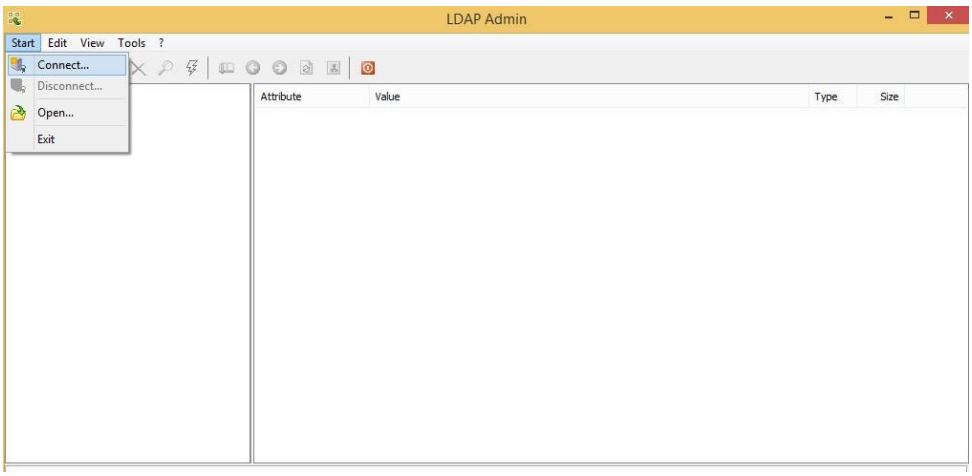
Để đảm bảo an toàn cơ sở dữ liệu LDAP thì WINCA không cho phép truy cập LDAP trên website mà có công cụ để kiểm tra.

Cách kiểm tra như sau:

Bước 1: Download Ldap admin tại:

http://www.winca.org/download/ldapadmin

Bước 2: Chạy Ldap admin vào mục Start -> connect.



Bước 3: Chọn new connect và điền các thông số như sau:

Mục host: ldap.winca.org, ấn nút Fetchs DNs, rồi chọn Base và ấn OK.

Bước 4: chọn Connect tới và xem được thông tin LDAP.

II.3 Tần số công bố thông tin

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

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

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

II.4 Kiểm soát truy cập vào kho lưu trữ

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

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

III. Nhận dạng và Xác thực

III.1 Tên

Trường “subject” của chứng thư số tuân theo chuẩn X.509 v3. Nội dung của trường "subject" của chứng thư số chứa tên các thành phần sau đây:

- EmailAddress (E): Định dạng của thành phần EmailAddress tuân theo chuẩn IETF RFC 2822.
- CommonName (CN): Phân biệt cho mỗi cá nhân, mỗi host, mỗi dịch vụ.
- LocalityName (L): Danh sách LocalityName được định nghĩa trước dựa trên các quy định quản trị của WINCA.
- OrganizationalUnitName (OU): Tên của tổ chức.
- OrganizationName (O): Giá trị của thành phần OrganizationName được định nghĩa trước (WINCA) và nó cũng là thành phần gốc của LDAP.
- CountryName (C): Giá trị của thành phần CountryName được định nghĩa trước (VN) và nó cũng là thành phần gốc của LDAP.

- Trong trường hợp chứng thư số cấp cho cá nhân nội dung trường “subject” phải bao gồm Họ và tên của thuê bao.
- Trong trường hợp chứng thư số cấp cho host/server nội dung trường “subject” phải bao gồm FQDN (Fully Qualified Domain Name) của host/server.

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

E=tungnx@.winca.org, CN= Nguyễn Xuân Tùng, L=Hanoi, OU=Administrator Dept, O=WINCA, C=VN.

III.1.1 Cần thiết cho tên trở nên có ý nghĩa

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

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

Thuộc tính	Giá trị
Quận, huyện (L)	Địa chỉ quận/huyện của thuê bao
Tỉnh, thành phố (ST)	Địa chỉ tỉnh, thành phố của thuê bao
Quốc gia (C)	Tên quốc gia của thuê bao
Mã định danh của thuê bao – UID	CMND: Đối với khách hàng cá nhân

Tên thường gọi (CN)	Tên thuê bao sở hữu chứng thư số (Theo như giấy CMND và một số giấy tờ khác)
Địa chỉ email (E)	Địa chỉ email giao dịch của thuê bao sở hữu chứng thư số

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

III.1.2 Tính duy nhất của tên

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

III.2 Xác minh danh tính ban đầu

III.2.1 Cách thức chứng minh sở hữu khóa bí mật

Người đăng ký cấp chứng thư số được yêu cầu phải chứng minh tính sở hữu khóa bí mật của họ thích hợp với khóa công khai trong một yêu cầu chứng thư số thông qua việc ký yêu cầu với khóa bí mật. WINCA sẽ xác minh rằng người nộp đơn có phải là người sở hữu khóa bí mật tương ứng với khóa công khai đã được đưa ra cùng với các ứng dụng phù hợp với một giao thức an toàn hay không.

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

III.2.2 Nhận dạng và xác thực đối với chủ thể cá nhân

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

a) Tài liệu nhận dạng danh tính

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

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

b) Thực hiện nhận dạng cá nhân

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

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

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

III.2.3 Nhận dạng và xác thực đối với tổ chức

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

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

Nhận dạng và xác thực được thực hiện bởi RA, được tiến hành trên cơ sở quy định "Thông tin về khách hàng" của tổ chức và các thủ tục tương tự khác, chúng có thể bao gồm một báo cáo của cơ quan chính phủ, và/hoặc sự tham gia của bên thứ ba có uy tín về thông tin kinh doanh để cung cấp thông tin có hiệu lực về tổ chức đề nghị cấp chứng thư số như:

- Tên hợp pháp của công ty;
- Loại hình hoạt động;
- Năm thành lập;

- Tên của giám đốc và cán bộ;
- Địa chỉ;
- Số điện thoại;
- Bằng chứng chắc chắn đơn vị nộp đơn đang trong thời gian sát nhập hoặc tổ chức.

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

III.3 Nhận dạng và xác thực trong yêu cầu cấp lại khoá (RE-KEY)

III.3.1 Nhận dạng và xác thực trong thủ tục cấp lại khoá

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

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

III.3.2 Nhận dạng và xác thực việc cấp lại khoá sau khi đã bị thu hồi

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

III.4 Nhận dạng và xác thực đối với yêu cầu thu hồi chứng thư số

Thuê bao có thể yêu cầu thu hồi chứng thư số của mình tại bất kỳ thời điểm nào với bất kỳ lý do nào. WINCA khi gặp phải những yêu cầu như vậy, cần phải có cơ chế xác thực

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

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

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

IV. Các yêu cầu trong vòng đời của chứng thư số

IV.1 Đơn xin cấp chứng thư số

IV.1.1 Ai có thể đệ trình đơn xin cấp chứng thư số

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

IV.2 Quá trình xử lý cấp chứng thư

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

- Hoàn thành bản kê khai và cung cấp các thông tin đúng, chính xác
- Tự tạo khoá hoặc yêu cầu tạo cặp khoá
- Cung cấp khoá công khai đến RA
- Chứng minh sự tương thích giữa khoá bí mật và khoá công khai cho RA
- Hồ sơ xin cấp chứng thư số bao gồm

- Đơn xin cấp chứng thư theo mẫu;
- Đối với Khách hàng là cá nhân: Bản sao hợp lệ giấy CMND/Hộ chiếu/Căn cước công dân.
- Đối với Khách hàng là cá nhân thuộc tổ chức doanh nghiệp: Bản sao hợp lệ Giấy ĐKKD của tổ chức, bản sao hợp lệ giấy CMND/Thẻ căn cước công dân/Hộ chiếu của cá nhân. Xác nhận của tổ chức về chức danh đăng ký trên chứng thư; hoặc giấy giới thiệu của tổ chức doanh nghiệp, hợp đồng lao động.
- Đối với khách hàng là tổ chức doanh nghiệp: Bản sao hợp lệ Giấy ĐKKD/Quyết định thành lập/Giấy phép đầu tư của tổ chức; bản sao giấy CMND/Hộ chiếu của người đại diện theo pháp luật, giấy tờ ủy quyền (nếu người ký trên văn bản đăng ký không phải là người đại diện theo pháp luật).
- Đối với khách hàng đăng ký chứng thư số cho máy chủ: Tương tự như hồ sơ cấp chứng thư số cho cá nhân hoặc tổ chức, doanh nghiệp.
- Cá nhân hoặc tổ chức có quyền lựa chọn bản sao công chứng còn thời hạn hoặc bản sao đi kèm bản gốc để đối chiếu đối với các giấy tờ văn bản sau: Chứng minh thư nhân dân, Thẻ căn cước công dân, Hộ chiếu, Giấp phép đăng ký kinh doanh, Giấy phép đầu tư, Quyết định thành lập.

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

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

IV.2.1 Thời gian xử lý yêu cầu cấp chứng thư

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

IV.3 Cấp phát chứng thư

IV.3.1 Hoạt động trong suốt quá trình phát hành chứng thư

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

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

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

IV.3.2 Thông báo của WINCA đến người dùng về việc cấp chứng thư

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

WINCA 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 ký vào bản xác nhận đã nhận đầy đủ chứng thư số của mình và gửi lại cho WINCA.

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

Thông tin tiếp nhận: Công ty TNHH Tư Vấn- Thương Mại Khánh Linh

Địa chỉ: 232/17 Cộng Hòa, Phường 12, Quận Tân Bình, Tp.HCM

Điện thoại: (028) 38116723

E-mail: info@winca.org

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

IV.4 Chấp nhận chứng thư

IV.4.1 Điều kiện chứng minh việc chấp nhận chứng thư

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

IV.4.2 Việc công khai chứng thư của WINCA

Sau khi nhận được chấp nhận chứng chỉ WINCA công bố chứng thư số đã phát hành, WINCA công bố tất cả các chứng thư hợp lệ trong kho lưu trữ trực tuyến trên cả web lẫn kho lưu trữ LDAP. (Xem mục II.2 Công bố thông tin chứng thư).

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

IV.4.3 Thông báo sự phát hành chứng thư đến các đối tượng khác

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

IV.5 Sử dụng cặp khoá của chứng thư

IV.5.1 Sử dụng chứng thư và khoá bí mật của thuê bao

Chứng thư số phát hành bởi WINCA và khoá bí mật tương ứng với khoá công khai trong chứng thư được sử dụng hợp pháp theo bản thoả thuận của thuê bao với các điều khoản có trong CP/CPS của nhà cung cấp chứng thư. Chứng thư sử dụng phải khớp với đuôi mở rộng trong trường KeyUsage có trong chứng thư (Trường KeyUsage được định nghĩa trước trong chứng thư và xác định một số chức năng và hoạt động của giao thức như SSL, TLS). Thuê bao có trách nhiệm bảo vệ khoá bí mật khỏi việc truy cập bất hợp pháp và sẽ không được sử dụng khoá bí mật khi chứng thư hết hạn hay bị thu hồi.

IV.5.2 Sử dụng chứng thư và khoá công khai của đối tác tin cậy

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

- Kiểm tra có đúng chứng thư số do WINCA phát hành;
- Kiểm tra chứng thư số chưa bị thu hồi;

- Chứng thư số được sử dụng theo đúng phần mở rộng của trường KeyUsage và extKeyUsage trong chứng thư;
- Việc sử dụng chứng thư cho các mục đích phù hợp và xác định rằng chứng thư sẽ được sử dụng đúng mục đích không bị ngăn cấm hoặc bị giới hạn bởi CP/CPS của WINCA.

IV.6 Khôi phục chứng thư

IV.6.1 Trường hợp khi cần khôi phục chứng thư

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

IV.6.2 Đối tượng yêu cầu khôi phục chứng thư

Chủ sở hữu của chứng thư có thể yêu cầu khôi phục chứng thư trước khi nó hết hạn bằng cách gửi cho RA tương ứng một e-mail ký với khóa bí mật của chứng thư yêu cầu khôi phục.

IV.6.3 Quy trình xử lý các yêu cầu khôi phục chứng thư

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

IV.6.4 Điều kiện chấp nhận khôi phục chứng thư

Tuân theo mục IV.4.1

IV.6.5 Công bố các chứng thư được khôi phục

Tuân theo mục IV.4.2

IV.6.6 Thông báo việc cấp chứng thư củaWINCA đến các đối tượng khác

Tuân theo mục IV.4.3

IV.7 Cấp khoá mới cho chứng thư

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

IV.7.1 Trường hợp cấp lại khoá chứng thư

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

IV.7.2 Đối tượng yêu cầu cấp khoá mới cho chứng thư

Chỉ có thuê bao của chứng thư mới có thể yêu cầu cấp khoá cho chứng thư.

Nếu chứng thư đã hết hạn thì thủ tục yêu cầu chứng thư tuân theo như yêu cầu cấp chứng thư đầu tiên.

IV.7.3 Xử lý các yêu cầu cấp khoá mới cho chứng thư

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

IV.7.4 Thông báo phát hành chứng thư mới tới thuê bao

Tuân theo mục IV.3.2

IV.7.5 Thông báo chấp nhận cấp mới khoá chứng thư

Tuân theo mục IV.4.1

IV.7.6 Phát hành chứng thư đã được cấp mới khoá của WINCA

Tuân theo mục IV.4.2

IV.7.7 Thông báo cấp chứng thư của WINCA tới các đối tượng khác

Tuân theo mục IV.4.3

IV.8 Sửa đổi chứng thư

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

IV.8.1 Các trường hợp sửa đổi chứng thư

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

IV.8.2 Đối tượng yêu cầu sửa đổi chứng thư

Không áp dụng

IV.8.3 Quá trình xử lý yêu cầu sửa đổi chứng thư

Không áp dụng

IV.8.4 Thông báo phát hành chứng thư mới tới thuê bao

Không áp dụng

IV.8.5 Điều kiện chấp nhận sửa đổi thuê bao

Không áp dụng

IV.8.6 Phát hành chứng thư đã được sửa đổi từ WINCA

Không áp dụng

IV.8.7 Thông báo phát hành chứng thư của WINCA tới các đổi tượng khác

Không áp dụng

IV.9 Thu hồi và tạm dừng chứng thư

WINCA không cung cấp tạm dừng chứng thư.

IV.9.1 Các trường hợp thu hồi

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

IV.9.2 Đối tượng có thể yêu cầu thu hồi

Yêu cầu thu hồi chứng thư được thực hiện bởi:

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

IV.9.3 Thủ tục yêu cầu thu hồi chứng thư

Thuê bao chứng thư số gửi một e-mail ký với khóa bí mật của chứng thư (chưa hết hạn) yêu cầu thu hồi.

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

IV.9.4 Thời gian cho một yêu cầu thu hồi chứng thư

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

IV.9.5 Thời gian WINCA xử lý yêu cầu thu hồi chứng thư

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

IV.9.6 Yêu cầu kiểm tra việc thu hồi cho đối tác tin cậy

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

IV.9.7 Tần số cấp phát CRL

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

IV.9.8 Thời gian trễ tối đã cho các CRL

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

IV.9.9 Dịch vụ hỗ trợ kiểm tra trạng thái thu hồi trực tuyến

Thông tin trạng thái chứng thư và thông tin thu hồi chứng thư được lưu trữ trực tuyến trên kho của WINCA truy cập qua nền tảng LDAP và web và có thể truy cập qua OCSP.

WINCA sẽ cho phép đối tác tin cậy truy vấn trực tuyến các thông tin thu hồi và trạng thái chứng thư.

IV.9.10 Những yêu cầu kiểm tra trạng thái chứng thư trực tuyến

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

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

IV.10 Dịch vụ trạng thái chứng thư số

IV.10.1 Các đặc tính hoạt động

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

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

IV.10.2 Tính sẵn sàng của dịch vụ

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

IV.10.3 Các đặc tính tuỳ chọn

OCSP có thể sẽ thu phí.

IV.11 Kết thúc hợp đồng

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

- Có yêu cầu dừng sử dụng chứng thư số hoặc dừng toàn bộ hệ thống WINCA hoặc WINCA 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.12 Cam kết và khôi phục khoá

IV.12.1 Chính sách và thực hiện cam kết khôi phục khoá

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

IV.12.2 Chính sách và thực hiện phục hồi và đóng gói khoá phiên

Xem mục IV.12.1.

V. Phương tiện, vấn đề quản lý và điều hành hoạt động

V.1 Kiểm soát mức vật lý

V.1.1 Cấu trúc và khoanh vùng

CA WINCA được đặt tại địa chỉ của tổ chức được quản lý trong tài liệu này (xem mục I.5.1).

V.1.2 Truy cập vật lý

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

V.1.3 Điều hoà và nguồn điện

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

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

V.1.4 Tiếp xúc với nước

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

V.1.5 Phòng cháy chữa cháy

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

V.1.6 Phương tiện lưu trữ

Một số các bản sao khoá bí mật của WINCA được lưu giữ trên thiết bị lưu trữ ngoài (SMARTCARD, USB, CD-ROM) ở vị trí an toàn đảm bảo tránh được những rủi ro bất ngờ (nước, lửa, điện từ trường).

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

V.1.7 Xử lý rác

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

V.1.8 Dự phòng từ xa

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

V.2 Các kiểm soát thủ tục

V.2.1 Những thành viên được tin cậy

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

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

V.2.2 Số lượng người yêu cầu cho mỗi công việc

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

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

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

V.2.3 Nhận dạng và xác thực cho từng thành viên

Tất cả các nhân viên CA phải được xác minh nhận dạng và xác thực trước khi họ: (i) có trong danh sách truy cập tới các vị trí CA; (ii) có trong danh sách truy cập đến hệ thống CA; (iii) được cung cấp một chứng thư số để thực hiện nhiệm vụ CA; hoặc (iv) được cung cấp một tài khoản trên hệ thống PKI.

V.2.4 Vai trò yêu cầu phân chia trách nhiệm

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

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

V.3 Kiểm soát nhân sự

V.3.1 Năng lực, kinh nghiệm và các yêu cầu khác

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

V.3.2 Thủ tục kiểm tra lai lịch

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

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

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

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

V.3.3 Yêu cầu về đào tạo

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

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

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

V.3.4 Chu kỳ tái đào tạo

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

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

V.3.5 Kỷ luật đối với các hoạt động không hợp pháp

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

V.3.6 Yêu cầu đối với các nhà thầu độc lập

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

V.3.7 Cung cấp tài liệu cho nhân viên

WINCA cung cấp tất cả các tài liệu cần thiết để họ hoàn thành tốt công việc của mình.

V.4 Thủ tục kiểm tra truy cập

V.4.1 Các loại bản ghi sự kiện

Những sự kiện sau đây được ghi lại:

- Trên các máy chủ lưu trữ chứng thư offline

- Khởi động và tắt;
- Đăng nhập, đăng xuất;
- Tạo và ký chứng thư.

- Trên các máy chủ trực tuyến của WINCA
- Nhận yêu cầu chứng thư từ một RA;
- Thêm một bản ghi trong cơ sở dữ liệu của CA;
- Ghi các yêu cầu cấp chứng thư ra thiết bị lưu trữ ngoài;
- Truyền các chứng thư cho yêu cầu bên liên quan;
- Lưu trữ chứng thư trong kho trực tuyến;
- Nhận được yêu cầu thu hồi;
- Phát hành CRL.

V.4.2 Tần suất xử lý bản ghi sự kiện

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

V.4.3 Thời gian duy trì cho kiểm định bản ghi

Khoảng thời gian lưu giữ tối thiểu đối với các bản ghi kiểm toán là 07 năm.

V.4.4 Bảo vệ các bản ghi kiểm định

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

V.4.5 Thủ tục sao lưu dự phòng cho các bản ghi kiểm định

Các bản ghi kiểm định sẽ được lưu trên một phương tiện di động mỗi đêm, trừ những ngày cuối tuần và ngày lễ khi các hoạt động không xảy ra trên các máy chủ offline và truy cập đọc vào các kho trực tuyến xảy ra trên máy chủ trực tuyến.

V.4.6 Hệ thống thu thập kiểm định (bên trong và bên ngoài)

Không quy định.

V.4.7 Thông báo về nguyên nhân sự kiện

Không quy định.

V.4.8 Đánh giá điểm yếu

Không chỉ định.

V.5 Lưu trữ các bản ghi

V.5.1 Những kiểu bản ghi được lưu trữ

Xem V.4.1.

V.5.2 Thời gian duy trì tài liệu lưu trữ

Khoảng thời gian lưu giữ tối thiểu là 07 năm.

V.5.3 Bảo mật tài liệu lưu trữ

Các lưu trữ chỉ được truy cập bởi các nhân viên điều hành và quản lý của WINCA.

V.5.4 Thủ tục sao lưu và dự phòng dữ liệu

Các bản ghi được sao lưu trên phương tiện lưu trữ di động và được cất giữ trong phòng với truy cập bị hạn chế.

V.5.5 Yêu cầu nhãn thời gian cho dữ liệu

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

V.5.6 Hệ thống thu thập dữ liệu lưu trữ (nội bộ và bên ngoài)

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

V.5.7 Thủ tục thu thập và kiểm tra thông tin lưu trữ

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

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

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

V.6 Thay đổi khoá

Không có quy định.

V.7 Lộ khóa và khôi phục sau thảm hoạ

V.7.1 Các thủ tục xử lý vấn đề lộ khoá và sự cố

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

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

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

V.7.2 Hành vi tiêu cực đối với tài nguyên máy tính, phần mềm và dữ liệu

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

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

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

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

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

Hệ thống sẽ được khởi động lại dựa trên phần cứng dự phòng bằng cách sử dụng phần mềm sao lưu dữ liệu được sao lưu tại DRDC của WINCA, 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.

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

WINCA thông báo với Trung tâm Chứng thực điện tử quốc gia về sự cố này không muộn quá 01 ngày làm việc kể từ khi sự cố xảy ra, theo các quy định của Thông tư

06/2015/TT-BTTTT về Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số do Bộ Thông tin truyền thông ban hành.

V.7.3 Khả năng phục hồi hoạt động sau thảm họa.

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

WINCA 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

WINCA dự phòng các thiết bị phần cứng và phần mềm cung cấp dịch vụ. Khóa bí mật của WINCA 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 hay RA

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

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

Thông báo tạm dừng dịch vụ không ít hơn 60 ngày trong trường hợp chấm dứt bình thường. Các CA quản lý tại thời điểm chấm dứt có trách nhiệm lưu trữ tất cả các hồ sơ theo yêu cầu trong phần V.5.2. Thực hiện chuyển giao cần thiết của dịch vụ CA tới các CA đang hoạt động theo thỏa thuận.

VI. Kiểm soát bảo mật kỹ thuật

VI.1 Tạo cặp khoá và cài đặt

VI.1.1 Tạo cặp khoá

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

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

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

VI.1.2 Chuyển giao khoá bí mật cho thuê bao

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

VI.1.3 Chuyển giao khoá công khai tới tổ chức ban hành chứng thư

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

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

VI.1.4 Chuyển giao khoá công khai của CA tới các đối tác tin cậy

Chứng thư số của CA (có chứa khoá công khai) được chuyển giao cho thuê bao bằng giao dịch trực tuyến từ Server website trực tuyến. Chứng thư của CA cũng có thể tải về từ kho lưu trữ (xem mục II.1)

VI.1.5 Kích thước khoá

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

Khoá của WINCA có chiều dài là 2048 bits.

VI.1.6 Tạo các tham số cho khoá công khai và kiểm tra chất lượng

Không có quy định.

VI.1.7 Mục đích sử dụng khoá (như trong X.509 v3 lĩnh vực sử dụng khoá)

Khoá được sử dụng theo mỗi loại chứng thư:

- Với thuê bao:
- Chứng thực;
- Chống chối bỏ;
- Mã hoá dữ liệu;
- Thiết lập phiên giao dịch;
- Kiểm tra tính toàn vẹn của dữ liệu.
- Với chứng thư tự ký của CA
- Ký chứng thư;
- Ký CRL;
- Thu hồi chứng thư.

VI.2 Bảo vệ khoá bí mật và kiểm soát phương thức mã hoá

VI.2.1 Kiểm soát và chuẩn hoá mô đun mã hoá

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

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

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

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

VI.2.2 Đa kiểm soát khoá bí mật

Kiểu điều khiển này chưa được cài đặt.

VI.2.3 Bản cam kết khoá bí mật

Không triển khai dịch vụ cam kết khoá bí mật.

VI.2.4 Sao lưu dự phòng khoá bí mật

Các thuê bao chịu trách nhiệm sao lưu dự phòng khoá bí mật của họ.

Các khoá mã của thuê bao sẽ được sao lưu dự phòng.

WINCA sao lưu các khóa bí mật của CA cho mục đích khôi phục và khắc phục sau thảm hoạ.

VI.2.5 Lưu trữ khoá bí mật

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

VI.2.6 Cách thức sao lưu khoá bí mật

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

VI.2.7 Phương thức kích hoạt khoá bí mật

Khoá bí mật của CA được kích hoạt bằng cách điều hành viên CA nhập cụm từ mật khẩu cá nhân của mình.

VI.2.8 Phương thức dừng hiệu lực của một khoá bí mật

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

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

VI.2.9 Phương thức huỷ khoá bí mật

Xem phần V.1.7.

VI.3 Các khía cạnh khác của việc quản lý cặp khoá

VI.3.1 Lưu trữ khoá công khai

WINCA phải lưu trữ tất cả các chứng thư đã phát hành trên thiết bị lưu trữ ngoài và được cất offline ở một nơi an toàn.

VI.3.2 Thời gian hoạt động của chứng thư và của cặp khoá

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

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

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

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

VI.4 Kích hoạt dữ liệu

VI.4.1 Quá trình tạo và cài đặt dữ liệu kích hoạt.

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

VI.4.2 Bảo vệ dữ liệu kích hoạt

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

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

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

VI.4.3 Những khía cạnh khác của dữ liệu kích hoạt.

Không có quy định.

VI.5 Kiểm soát bảo mật máy tính

VI.5.1 Các yêu cầu về kỹ thuật bảo mật máy tính

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

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

VI.5.2 Đánh giá bảo mật máy tính

Không có quy định.

VI.6 Kiểm soát chu kỳ kỹ thuật

VI.6.1 Kiểm soát về phát triển hệ thống

Không có quy định.

VI.6.2 Kiểm soát vấn đề quản lý bảo mật

Không có quy định.

VI.6.3 Kiểm soát về mặt bảo mật đối với một chu kỳ sống

Không có quy định.

VI.7 Kiểm soát bảo mật mạng

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

Máy chủ ký của WINCA được hoạt động offline.

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

VI.8 Nhãn thời gian

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

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

VII. Khuôn dạng của chứng thư, CRL và OCSP

VII.1 Khuôn dạng của chứng thư

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

Tên trường	Giá trị
Số hiệu chứng thư/ Serial Number	Do WINCA gán, là định dạng duy nhất của chứng thư số
Tên của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng/ Issuer	WINCA
Thời điểm chứng thư bắt đầu có hiệu lực/ Not Before	Thời điểm chứng thư bắt đầu có hiệu lực. Được đồng bộ với NTP Server.
Thời điểm chứng thư hết hiệu lực/ Not After	Thời điểm chứng thư hết hiệu lực. Được đồng bộ với NTP Server.
Tên của thuê bao/ Subject	Tên của thuê bao
Khóa công khai của thuê bao/ Subject Public Key Info	Khóa công khai của thuê bao. Được mã hóa theo tiêu chuẩn RFC 3280; Xác định thuật toán RSA được sử dụng cùng với khoá
Thuật toán chữ ký số áp dụng/ Signature Algorithm	Thuật toán WINCA sử dụng để ký số chứng thư
Chữ ký số của trung tâm chứng thư số / Signature	Chữ ký số của trung tâm chứng thư số WINCA
Các thông tin khác cho mục đích quản lý, sử dụng, an toàn, bảo mật	

do tổ chức cung cấp dịch vụ chữ ký số quy định.	

VII.1.1 Phiên bản

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

VII.1.2 Phần mở rộng của chứng thư

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

Chứng thư số dùng cho cá nhân

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

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

Chứng thư số dùng cho dịch vụ / Máy chủ

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

VII.1.3 Thuật toán nhận biết đối tượng

Các OID cho các thuật toán được sử dụng cho chữ ký của chứng thư phát hành bởi WINCA theo:

- hash function: id-sha1 — 1.3.14.3.2.26
- encryption: rsaEncryption — 1.2.840.113549.1.1.1
- signature: sha-1WithRSAEncryption —1.2.840.113549.1.1.5

VII.1.4 Cấu trúc tên

Mỗi chứng thư có một tên duy nhất và rõ ràng. Tên phân biệt trong tất cả các chứng thư phát hành bởi WINCA và tuân theo cấu trúc được định nghĩa trong tiêu chuẩn ITU-T Standards Recommendation X.501 (Xem mục III.1.1).

VII.1.5 Ràng buộc tên

Không có những ràng buộc khác hơn so với quy định tại mục VII.1.4, và III.1.1, III.1.2.

VII.1.6 Chính sách nhận biết đối tượng

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

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

VII.1.7 Cách dùng của sự mở rộng chính sách ràng buộc

Không có ràng buộc nào

VII.1.8 Chính sách hạn định cấu trúc và ngữ nghĩa

Không có quy định

VII.1.9 Xử lý ngữ nghĩa cho phần mở rộng của các chứng thư quan trọng

Không có quy định

VII.1.10 Khuôn dạng của danh sách thu hồi chứng thư CRL

Version	V2
Signature	sha1WithRSAEncryption
Issuer	WINCA

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

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

VII.1.11 Phiên bản

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

VII.1.12 CRL và phần mở rộng đầu vào CRL

Không có quy định

VII.2 Profile của OCSP

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

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

VII.2.1 Phiên bản

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

VII.2.2 Phần mở rộng của OCSP

Chưa được xác định

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

VIII.1 Tần suất và các trường hợp đánh giá

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

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

VIII.2 Danh tính và khả năng của người kiểm toán

Chưa được xác định.

VIII.3 Mối quan hệ giữa kiểm toán viên và thực thể được kiểm toán

Việc kiểm toán được thực hiện bởi hãng kiểm toán đóng vai trò bên thứ ba sẽ được tiến hành kiểm tra bởi các hãng độc lập với thực thể được kiểm toán. Không có bất kỳ tranh cãi nào về lợi ích gây cản trở tới việc thực hiện các dịch vụ kiểm toán.

VIII.4 Những chủ thể trong quá trình đánh giá

Chưa được xác định.

VIII.5 Các hoạt động phải được thực hiện khi kết quả đánh giá là thiếu sót.

WINCA phải hành động ngay lập tức nếu đánh giá cho thấy một sự vi phạm các quy định trong CP/CPS. Nếu phát hiện vi phạm trực tiếp tới sự tin cậy của chứng thư, Chứng thư được phát hành vi phạm sẽ bị thu hồi ngay lập tức.

VIII.6 Thông báo kết quả

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

IX. Các vấn đề thương mại và pháp lý khác

IX.1 Lệ phí

IX.1.1 Lệ phí cấp Chứng thư hoặc gia hạn chứng thư

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

IX.1.2 Lệ phí sử dụng chứng thư

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

IX.1.3 Phí truy cập thông tin về trạng thái chứng thư và việc thu hồi chứng thư

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

IX.1.4 Lệ phí sử dụng cho các dịch vụ khác

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

IX.1.5 Chính sách hoàn trả phí

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

IX.2 Trách nhiệm tài chính

IX.2.1 Đăng thông tin bảo hiểm

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

IX.2.2 Các trường hợp WINCA tiến hành đền bù bảo hiểm

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

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

IX.2.3 Các trường hợp không được đền bù bảo hiểm

WINCA không chịu trách nhiệm trong các trường hợp:

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

IX.2.4 Các tài sản khác

Không được đề cập.

IX.3 Tính bảo mật thông tin kinh doanh

IX.3.1 Phạm vi của thông tin cần bảo mật

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

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

IX.3.2 Thông tin không nằm trong phạm vi của quá trình đảm bảo tính mật

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

IX.4 Bí mật thông tin cá nhân

IX.4.1 Kế hoạch đảm bảo tính riêng tư

Không có quy định.

IX.4.2 Những thông tin được coi là riêng tư

Tất cả các thông tin về người đăng ý mà không được trích trong chứng thư và CRL được coi là riêng tư và không được công khai với bên ngoài CA và RA thực thi việc đăng ký.

IX.4.3 Thông tin không được coi là riêng tư

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

IX.4.4 Trách nhiệm bảo vệ thông tin riêng tư

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

IX.4.5 Thông báo và cho phép sử dụng thông tin bí mật

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

IX.4.6 Cung cấp thông tin riêng theo yêu cầu của pháp luật hay cho quá trình quản trị

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

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

IX.4.7 Những trường hợp làm lộ thông tin khác

Không có quy định.

IX.5 Quyền sở hữu trí tuệ

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

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

IX.6 Vấn đề đại diện và bảo lãnh

IX.6.1 Đại diện của CA và vấn đề bảo lãnh

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

IX.6.2 Đại diện của RA và vấn đề bảo lãnh

Tất cả các RA thực hiện nhiệm vụ của họ về nhận dạng và xác thực của các bên yêu cầu như được mô tả trong III.2.3 và III.2.2 với trách nhiệm và khả năng tốt nhất. Không có bảo lãnh khác được đưa ra.

IX.6.3 Đại diện của khách hàng và sự bảo lãnh

Khi yêu cầu WINCA cấp chứng thư khách hàng đã chấp nhận sử dụng và bảo vệ chứng thư và khoá của chứng thư tuân theo quy định trong CP/CPS có hiệu lực tại thời điểm

nhận phát hành chứng thư. Tuy nhiên thuê bao có thể áp dụng những quy tắc nghiêm ngặt hơn.

Cụ thể là các thuê bao sẽ thông báo ngày cho WINCA nếu khoá bí mật của chứng thư bị mất hoặc bị xâm hại để CA thu hồi chứng chỉ đó và các bên tin tưởng từ chối chấp nhận chứng thư đó.

Trong trường hợp vi phạm quy định của CP/CPS các thuê bao đã đồng ý theo yêu cầu thu hồi chứng thư của WINCA. Không có một bảo lãnh thêm được yêu cầu từ các thuê bao.

IX.6.4 Đại diện các đối tác tin cậy và vấn đề bảo lãnh

Thoả thuận với đối tác tin cậy yêu cầu đối tác tin cậy phải có đủ thông tin để đưa ra một quyết định dựa vào các thông tin trong chứng thư. Họ có trách nhiệm quyết định tin tưởng hay không vào các thông tin trong chứng thư. Các đối tác tin cậy sẽ chịu trách nhiệm pháp lý nếu vi phạm các điều khoản về nghĩa vụ của đối tác tin cậy có trong CP/CPS.

IX.6.5 Đại diện cho các bên liên quan khác và vấn đề bảo lãnh

Không có quy định.

IX.7 Từ chối bảo lãnh

Không quy định.

IX.8 Giới hạn trách nhiệm pháp lý

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

- Trách nhiệm của các bên được quy định và giới hạn theo hợp đồng đã ký kết
- Các điều khoản có tính độc lập: Trong trường hợp một điều khoản hay sự sửa đổi bổ sung của CPS được giữ lại không thể thi hành được bởi một phiên toàn hay một cuộc xét xử có thẩm quyền, phần còn lại của CPS vẫn có hiệu lực.

IX.9 Bồi thường

IX.9.1 Vấn đề bồi thường của khách hàng

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

- Những thông tin không hợp lệ do khách hàng cung cấp trên đơn vị cấp chứng thư.

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

IX.9.2 Vấn đề bồi thường của đại lý

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

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

IX.10 Thời hạn và sự kết thúc

IX.10.1 Thời hạn

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

IX.10.2 Kết thúc

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

IX.10.3 Ảnh hưởng của sự kết thúc và những tổn hại

Khi CP/CPS hết hiệu lực, các thành phần của dịch vụ WINCA sẽ không bị giới hạn bởi các điều khoản còn hiệu lực của chứng thư đã được ban hành.

IX.11 Thông báo riêng và giao tiếp giữa các bên

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

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

IX.12 Sửa đổi

IX.12.1 Các thủ tục sửa đổi

Những sửa đổi của CP/CPS sẽ được thực hiện bởi Cấp quản lý chính sách có thẩm quyền (xem mục I.5.4).

IX.12.2 Các trường hợp cần sửa đổi nhận diện đối tượng (OID)

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

IX.13 Giải quyết tranh chấp

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

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

IX.14 Luật hội đồng

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

IX.15 Tuân thủ luật

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

IX.16 Các điều khoản hỗn hợp

Không áp dụng.

IX.17 Các điều khoản khác

Không áp dụng.

X. Phụ lục

X.1 Quyền của Đại Lý

- Được hưởng thù lao đại lý theo qui định được ký kết giữa Đại Lý và WINCA.
- Được tham gia các chương trình khuyến mãi, quảng cáo của WINCA khi cung cấp dịch vụ theo hợp đồng.
- Yêu cầu WINCA cung cấp các tài liệu và tổ chức tập huấn về dịch vụ, các quy trình, quy định liên quan đến việc cung cấp dịch vụ cho khách hàng và việc thực hiện cho hợp đồng này.
- Chấm dứt hợp đồng khi không có nhu cầu làm đại lý hoặc khi WINCA vi phạm các điều khoản đã cam kết trong hợp đồng.

X.2 Nghĩa vụ của Đại Lý

- Không tiết lộ bí mật kinh doanh của WINCA cho bất kỳ người nào khi chưa được WINCA cho phép;
- Đại Lý có nghĩa vụ phải cung cấp dịch vụ đúng như trong hợp đồng đã ký và theo quy định pháp luật.
- Chịu trách nhiệm bán đúng giá theo bảng giá WINCA ban hành và không được bán giá cao hơn cho khách hàng.
- Tiếp nhận và bảo quản account truy vấn thông tin hệ thống WINCA. Đảm bảo bảo mật và chịu hoàn toàn trách nhiệm về các thông tin khai báo do account quản trị này thực hiện trên hệ thống.
- Tiếp nhận mẫu hợp đồng dịch vụ, biên bản bàn giao, nghiệm thu do WINCA cung cấp để thực hiện thủ tục ký kết hợp đồng và nghiệm thu với khách hàng.
- Bàn giao đầy đủ và đúng hạn các hồ sơ khách hàng cho WINCA, bao gồm: Hợp đồng và biên bản nghiệm thu với khách hàng và các giấy tờ liên quan đến thủ tục ký kết hợp đồng theo qui định.
- Cung cấp đúng và đầy đủ chính sách giá cước, chính sách dịch vụ cho khách hàng do WINCA quy định. Không được thu thêm bất kỳ chi phí nào khi giao dịch với khách hàng trong quá trình tiếp xúc giới thiệu, tư vấn, xúc tiến ký kết hợp đồng và cài đặt nghiệm thu dịch vụ.
- Phối hợp với WINCA thực hiện quảng cáo, tiếp thị, triển khai các đợt khuyến mãi, chăm sóc khách hàng tuỳ theo từng chương trình cụ thể do các bên thoả thuận.
- Tiếp nhận và chuyển các khiếu nại hoặc ý kiến phản hồi của khách hàng cho WINCA, phối hợp với WINCA giải quyết và trả lời cho khách hàng.
- Đối soát số liệu hàng tuần/ hàng tháng để làm căn cứ thanh toán tiền thù lao đại lý.

- Khi nhận tiền thù lao đại lý, WINCA phải xuất hoá đơn tài chính cho Đại Lý.
- Lắp đặt biển hiệu, tiếp nhận tờ rơi do WINCA cung cấp để thực hiện công tác quảng bá, tiếp thị dịch vụ cho khách hàng.
- Thông báo cho WINCA trước 07 ngày khi có sự thay đổi về địa chỉ, số điện thoại, số fax, email hoặc các yêu cầu khác.
- Không được chuyển nhượng hợp đồng đại lý này cho bất kỳ một bên thứ 3 nào khi chưa có sự đồng ý trước bằng văn bản của WINCA.
- Tự chịu trách nhiệm về các khoản thuế có liên quan theo quy định của pháp luật.

X.3 Các trách nhiệm khác của Đại Lý

X.3.1 Tiếp thị và giới thiệu dịch vụ chứng thư số của Công ty

- Đại Lý có trách nhiệm chủ động thực hiện các biện pháp marketing tiếp thị để tìm kiếm khách hàng trong những quy định về chính sách marketing của WINCA.

- Đại Lý có trách nhiệm giới thiệu đầy đủ, tận tình các dịch vụ giá trị gia tăng của Công ty cho khách hàng và hướng dẫn khách hàng các thông tin, thủ tục cần thiết để đăng ký và sử dụng các dịch vụ đó.

X.3.2 Kiểm tra điều kiện pháp lý của khách hàng

Đại Lý có trách nhiệm kiểm tra điều kiện pháp lý, khả năng tài chính của khách hàng để ký kết hợp đồng sử dụng dịch vụ giá trị gia tăng. Cụ thể:

Khách hàng là Tổ chức, doanh nghiệp:

- Hợp đồng, bản khai phải được ký và đóng dấu. Hợp đồng phải đầy đủ các thông tin của Khách hàng như: Người đại diện pháp lý ký hợp đồng (trường hợp uỷ quyền phải có giấy uỷ quyền kèm theo), Điện thoại, địa chỉ, tài khoản thanh toán, mã số thuế…
- Bản sao CMND hoặc Hộ chiếu của người đại diện pháp lý của tổ chức, doanh nghiệp có công chứng.
- Bản sao Giấy phép thành lập/Đăng ký kinh doanh có công chứng
- Bản sao Giấy chứng nhận đăng ký thuế của doanh nghiệp có công chứng (nếu có)
- Khách hàng là cá nhân:
- Hợp đồng, bản khai phải được ký và đầy đủ các thông tin của Khách hàng như: Tên khách hàng, Số CMTND (hộ chiếu), ngày cấp CMTND (hộ chiếu), Điện thoại, địa chỉ, tài khoản thanh toán, mã số thuế…
- Bản sao CMND có công chứng của cá nhân
- Bản sao có công chứng của cơ quan nhà nước Giấy ĐKKD hoặc Quyết định thành lập, Giấy phép đầu tư (đối với khách hàng cá nhân thuộc doanh nghiệp)

- Bản sao có công chứng của cơ quan nhà nước giấy CMND của người đại diện hợp pháp của tổ chức/doanh nghiệp (đối với khách hàng cá nhân thuộc doanh nghiệp)

X.3.3 Hướng dẫn khách hàng làm Hợp đồng các và thủ tục cần thiết

Nếu khách hàng đủ điều kiện pháp lý và đồng ý sử dụng dịch vụ, Đại Lý nhận hồ sơ và thẩm định lại trước khi cấp chứng thư số, hướng dẫn khách hàng điền đầy đủ và nộp lại các nội dung vào các mẫu do WINCA cung cấp sau:

- Giấy đăng ký xin cấp chứng thư số
- Hợp đồng cung cấp và sử dụng dịch vụ chứng thư số.
- Biên bản bàn giao thiết bị, có xác nhận của khách hàng

Đại Lý cũng có trách nhiệm hướng dẫn khách hàng thực hiện các nghĩa vụ trong Hợp đồng cung cấp dịch vụ.

X.3.4 Bàn giao Hồ sơ

Đại Lý phải đảm bảo thực hiện nhận đầy đủ hồ sơ của thuê bao trước khi cung cấp chứng thư số, và trước ngày mùng 5 hàng tháng Đại Lý có trách nhiệm bàn giao tất cả các hồ sơ thuê bao cho WINCA. Cụ thể:

- 01 Giấy đăng ký xin cấp chứng thư số
- 01 Hợp đồng (bản chính) và các hồ sơ, giấy tờ pháp lý liên quan của khách hàng sử dụng dịch vụ cho WINCA.
- 01 Biên bản bàn giao thiết bị với khách hàng

WINCA có trách nhận tiếp nhận Hồ sơ của khách hàng nhanh chóng và ký Biên bản bàn giao khách hàng với Đại Lý.

Đại Lý bàn giao Hợp đồng dịch vụ cho WINCA phải đảm bảo hợp đồng có đầy đủ thông tin của nhân viên đại lý trực tiếp tham gia vào quy trình cấp chứng thư số trên cụ thể bao gồm các thông tin sau:

- Họ tên nhân viên:
- Số CMND:
- Điện thoại liên hệ:
- Nếu trong thời gian cung cấp dịch vụ Đại Lý có thay đổi nhân sự thì phải thông báo bằng văn bản cho WINCA biết.

X.3.5 Hoàn thành thủ tục thanh toán cho khách hàng và đối soát quyết toán giữa Đại Lý và WINCA

Đại Lý có trách nhiệm theo dõi việc thực hiện trách nhiệm thanh toán của khách hàng (cước phí cài đặt và duy trì dịch vụ thanh toán lần đầu theo giá trị hợp đồng) đã quy định cụ thể trong Hợp đồng cung cấp dịch vụ cụ thể như sau:

- Đối với hợp đồng hai bên giữa Công ty và khách hàng cuối, khi Đại Lý nhận thiết bị đã có chữ ký số từ WINCA, Đại Lý phải thanh toán cước phí dịch vụ và phí thiết bị (nếu có) cho WINCA, lấy hoá đơn của WINCA để giao cho khách hàng (Công ty không chịu trách nhiệm về số tiền Đại Lý thu của khách hàng và chưa nộp cho Công ty). Nếu khách hàng thanh toán qua ngân hàng Đại Lý có trách nhiệm đôn đốc khách hàng đến khi tiền của khách hàng được chuyển về tài khoản của WINCA và chuyển hoá đơn của WINCA cho khách hàng.
- Đối với hợp đồng ba bên giữa WINCA, Đại Lý và khách hàng cuối, Đại Lý sẽ thu cước phí dịch vụ và thiết bị từ khách hàng và xuất hóa đơn cho khách hàng. Đối với thiết bị Token trắng, WINCA sẽ bàn giao trước cho Đại Lý theo thỏa thuận tại từng thời điểm, và Đại Lý phải thanh toán cho WINCA phí thiết bị này. Đại Lý và Công ty sẽ đối soát một tháng một lần vào từ ngày 01 đến ngày 05 hàng tháng bao gồm cả phí thiết bị.
- Đại Lý phải đảm bảo phương thức thanh toán, hoàn thành thủ tục thanh toán và đối soát quyết toán giữa WINCA và Đại Lý nhanh chóng, đầy đủ để đảm bảo thuê bao nhận được dịch vụ thông suốt.
- Đại Lý có trách nhiệm theo dõi việc thực hiện trách nhiệm thanh toán của khách hàng (cước phí cài đặt và duy trì dịch vụ thanh toán lần đầu theo giá trị hợp đồng) đã quy định cụ thể trong Hợp đồng cung cấp dịch vụ.

X.3.6 Hỗ trợ khách hàng

- Đại Lý có trách nhiệm tiếp nhận tất cả các yêu cầu hỗ trợ từ phía khách hàng, thực hiện hỗ trợ khách hàng tốt nhất trong khả năng và theo quy trình hướng dẫn của WINCA đã huấn luyện cho Đại Lý.
- Đại Lý có trách nhiệm phối hợp với WINCA hỗ trợ khách hàng.

X.3.7 Chăm sóc khách hàng

- Đại lý có trách nhiệm phối hợp với Công ty thực hiện các hoạt động chăm sóc khách hàng do Công ty đề xuất.
- Đại lý có thể chủ động thực hiện các hoạt động chăm sóc đối với khách hàng do Đại lý phát triển nhằm tăng uy tín của dịch vụ và không ảnh hưởng đến uy tín của Công ty.

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).