CÔNG TY CỔ PHẦN DỊCH VỤ T-VAN HILO

***

QUY CHẾ CHỨNG THỰC

HÀ NỘI 2021

CÔNG TY CỔ PHẦN DỊCH VỤ T-VAN HILO

_____***_____

QUY CHẾ CHỨNG THỰC

HÀ NỘI-08/2021

QUY CHẾ CHỨNG THỰC

1. THÔNG TIN CHUNG

1.1 Khái quát

HILO-CA là tên gọi dịch vụ chứng thực chữ ký số công cộng do Công ty cổ phần Dịch vụ T-Van Hilo cung cấp. Các quy định về chính sách chứng thư số của HILO-CA được trình bày trong tài liệu này gồm có các quy trình quản lý cấp phát, gia hạn, thu hồi, tạm dừng, khôi phục, hủy bỏ chứng thư số cho các thuê bao là cá nhân, tổ chức doanh nghiệp...

Bản quy chế chứng thực mô tả các thủ tục và cơ chế thực thi của nhà cung cấp chứng thư số của hệ thống HILO-CA. Quy chế chứng thực mô tả các điều khoản và điều kiện thực hiện của nó nhằm cung cấp tới các cơ quan quản lý cũng như người sử dụng những mô tả rõ ràng về các dịch vụ của hệ thống và các điều kiện để sử dụng chúng. Ngoài ra, nó cũng đưa ra những đảm bảo về mặt an toàn bảo mật và an toàn thông tin của hệ thống HILO-CA và các dịch vụ chứng thực chữ ký số cung cấp cho khách hàng.

Hệ thống HILO-CA được tuân thủ theo luật giao dịch điện tử số 51/2005/QH11 Ngày 29 tháng 11 năm 2005; Nghị định số 130/2018/NĐ-CP ngày 27 tháng 09 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; Thông tư sô 31/2020/TT-BTTTT ngày 30 tháng 10 năm 2020; 31/2020/TT-BTTTT;

1.2 Nhận dạng tài liệu

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

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

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

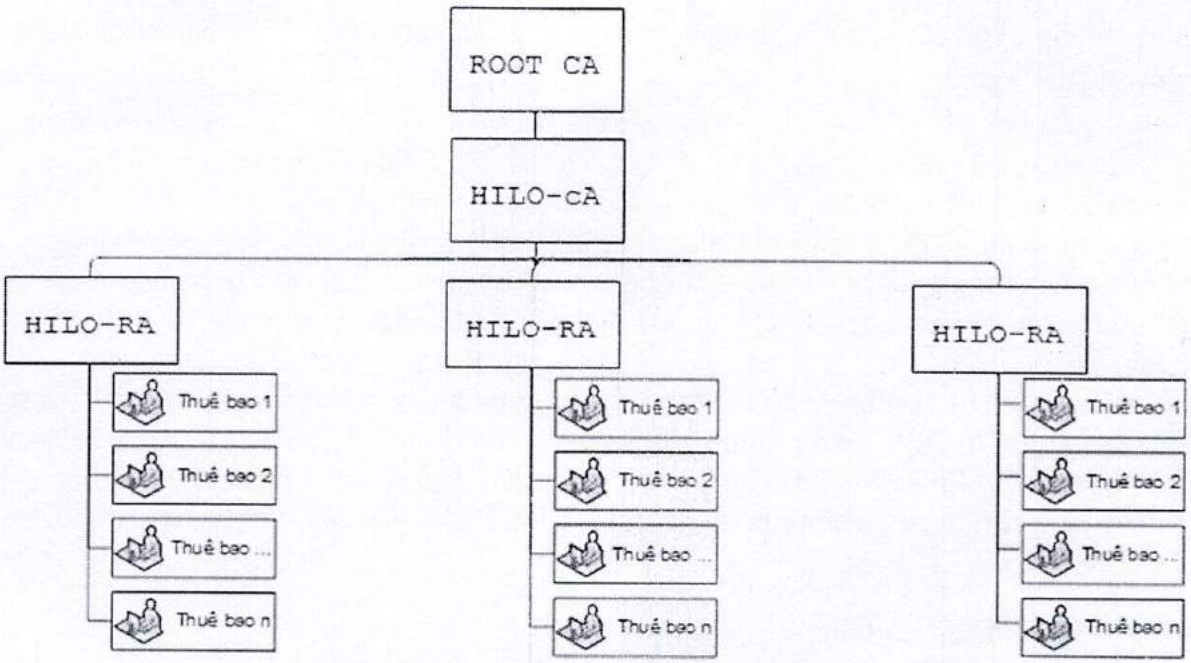
Mục tiêu của văn bản này là:

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

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

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

1.3 Các thành phần tham gia dịch vụ HILO-CA



Hình 1 – Sơ đồ tổ chức hệ thống HILO-CA

Hệ thống HILO-CA hoạt động có các thành phần tham gia gồm:

- Hệ thống dịch vụ chứng thực chữ ký số Quốc gia do Bộ Thông tin và Truyền thông quản lý là hệ thống RootCA Quốc gia (ROOT-CA).
- Hệ thống HILO-CA được tổ chức theo quy định của pháp luật Việt Nam, trực thuộc ROOT-CA (Trung tâm Chứng thực điện tử Quốc gia) do Bộ Thông tin và Truyền thông quản lý. HILO-CA được Bộ Thông tin và Truyền thông cấp phép cung cấp dịch vụ chứng thực chữ ký số công cộng, do đó có quyền cấp chứng thư số cho các tổ chức, doanh nghiệp, cá nhân (đủ điều kiện theo quy định của pháp luật và CPS này), có yêu cầu cấp chứng thư số.
- HILO-RA (registration authority) là tổ chức được CA tin cậy, uỷ quyền tiếp nhận yêu cầu cung cấp dịch vụ và xác thực thông tin của thuê bao nhằm đảm bảo tính chính xác các thông tin trong chứng thư số của thuê bao trên toàn hệ thống. HILO-RA là toàn bộ các chi nhánh trên toàn quốc và đối tác của HILO-CA có khả năng kiểm tra, xác thực định danh các thuê bao. Nhiệm vụ của HILO-RA là gồm:
    - Tiếp nhận yêu cầu cấp chứng thư số và báo cho CA thông qua hệ thống thiết bị (phần cứng, phần mềm) và người vận hành hệ thống đó;
    - Xác thực thông tin thuê bao theo yêu cầu quy định tại CPS này nhằm đảm bảo tính chính xác các thông tin trong chứng thư số trên toàn hệ thống.
- Thuê bao là tổ chức, cá nhân (đủ điều kiện theo quy định của pháp luật và CPS này) được HILO-CA cấp chứng thư số.
- Người nhận là các tổ chức, cá nhân sử dụng các chức năng của hệ thống HILO-CA để giải mã/xác thực thông tin nhận được từ thuê bao của HILO-CA.

1.4 Sử dụng chứng thư số

1.4.1 Chứng thư số hợp pháp

Chứng thư số HILO-CA được cấp bởi RootCA quốc gia với mục đích sử dụng chính như sau: digitalSignature, nonrepudiation, keyAgreement, dataEncipherment và keyEncipherment (các trường trong Key Usage của chứng thư số).

Chứng thư số HILO-CA được sử dụng để ký phát hành chứng thư số cho thuê bao, các danh sách chứng thư số thu hồi CRLs của HILO-CA, chứng thư số cho hệ thống kiểm tra chứng thư số trực tuyến OCSP; để xác thực các chứng thư số do HILO-CA cấp và xác thực dữ liệu đã ký số.

Chứng thư được cấp cho cá nhân: chứng thư được sử dụng với mục đích cá nhân, xác định danh tính. Phục vụ ký số, xác thực tài liệu điện tử, xác thực đăng nhập, SSL, mail…

Chứng thư được cấp cho tổ chức: chứng thư được cấp cho một tổ chức, doanh nghiệp. Chứng thư số cho thiết bị Usbtoken, HSM, SSL server, mail server…

Chứng thư số CodeSigning.

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

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

Sử dụng chứng thư số sai mục đích, sử dụng để thực hiện các hành vi vi phạm pháp luật sẽ bị cấm.

1.5 Chính sách quản trị

1.5.1 Tổ chức quản lý văn bản

Công ty cổ phần Dịch vụ T-Van Hilo là đơn vị viết, cập nhật CPS này.

CPS này có thể được tải tại *https://hilo-ca.vn/tailieu*

1.5.2 Địa chỉ liên hệ

Công ty cổ phần Dịch vụ T-Van Hilo.

Địa chỉ: Số 18 Đoàn Trần Nghiệp, Phường Bùi Thị Xuân, Quận Hai Bà Trưng, Thành phố Hà Nội.

Văn phòng giao dịch: Tầng 6, tòa HEC, số 2 ngõ 95 Chùa Bộc, Quận Đống Đa, Thành phố Hà Nội.

Điện thoại: 1900 29 29 62

Email: nguyenductung.ct@hilo.com.vn

1.5.3 Đơn vị quyết định tính hợp pháp của CPS

Bộ Thông tin truyền thông (Trung tâm chứng thực điện tử quốc gia – RootCA) là cơ quan có thẩm quyền quyết định tính hợp pháp của quy chế này.

1.5.4 Thủ tục phê chuẩn CPS

Trong quá trình hoạt động, khi có thay đổi nội dung trong quy chế chứng thực, HILO-CA sẽ báo cáo và được sự đồng ý của Bộ Thông tin truyền thông (Trung tâm chứng thực điện tử quốc gia – RootCA) chấp nhận.

Các thay đổi phải được thể hiện bằng văn bản dưới dạng một tài liệu chứa các sửa đổi mẫu của CPS hay các thông tin về quá trình cập nhật.

Tất cả những phiên bản đã sửa đổi hoặc cập nhật thông tin được công bố tại đại chỉ https://hilo-ca.vn/tailieu.

1.6 Các định nghĩa và tên viết tắt

Chi tiết trong Phụ lục

2. TRÁCH NHIỆM LƯU TRỮ, CÔNG BỐ VÀ SỬ DỤNG THÔNG TIN

2.1 Lưu trữ thông tin

HILO-CA thực hiện lưu trữ và sử dụng thông tin của thuê bao một cách bí mật, an toàn và chỉ sử dụng thông tin này vào mục đích liên quan đến chứng thư số.

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

HILO-CA thực hiện lưu trữ đầy đủ, chính xác và cập nhật danh sách các chứng thư số có hiệu lực, đang tạm dừng và đã hết hiệu lực và cho phép, hướng dẫn người sử dụng Internet truy nhập trực tuyến 24 giờ trong ngày và 7 ngày trong tuần. Tài liệu hướng dẫn người dùng và các tài liệu khác được HILO-CA ban hành, lưu trực tuyến tại địa chỉ https://hilo-ca.vn/tailieu).

HILO-CA thực hiện lưu trữ toàn bộ thông tin liên quan đến việc tạm đình chỉ hoặc thu hồi giấy phép và các cơ sở dữ liệu về thuê bao, chứng thư số trong thời gian ít nhất 05 (năm) năm, kể từ khi giấy phép bị tạm đình chỉ hoặc thu hồi.

Việc lưu trữ thông tin sẽ gồm 02 phần là lưu trữ hồ sơ khách hàng và lưu trữ thông tin khách hàng.

a. Lưu hồ sơ khách hàng

- Bộ hồ sơ lưu trữ bao gồm:
    - Phiếu đăng ký cấp chứng thư số
    - Đăng ký kinh doanh (Quyết định thành lập và giấy cấp mã số thuế)
    - Chứng minh thư nhân dân/Căn cước công dân/Hộ chiếu của người đại diện doanh nghiệp hoặc của cá nhân đăng ký.
    - Giấy xác nhận thông tin khách hàng.
    - Giấy ủy quyền, giấy bổ nhiệm và các giấy tờ liên quan khác.
- Hồ sơ khách hàng được HILO-CA lưu theo hai hình thức:
    - Hồ sơ giấy: Là hồ sơ bản cứng, có dấu và chữ ký tay của khách hàng. Hồ sơ khách hàng sau khi thẩm định sẽ được chỉnh lý, đánh số và scan số hóa.
        - Bản hồ sơ cứng được lưu trữ tại 01 tủ riêng cùng kho lưu trữ tại bộ phận văn thư. Tủ có khóa và đặt trong phòng văn thư có khóa riêng.
        - Bản hồ sơ Scan được HILO-CA tổ chức và lưu trữ trên cơ sở dữ liệu khách hàng tại Server RA. Việc lưu các bản scan hồ sơ sẽ phục vụ việc tra cứu, tìm kiếm được nhanh chóng và thuận lợi hơn.
    - Hồ sơ điện tử: Là hồ sơ bản điện tử, được ký số bởi chứng thư số hợp lệ và còn hiệu lực của tổ chức/cá nhân.
        - Hồ sơ điện tử sẽ được tổ chức và lưu trữ trên RA server, phục vụ việc tra cứu, tìm kiếm được nhanh chóng.

- Hiện tại, việc áp dụng chữ ký số đã khá phổ biến và tính pháp lý của chữ ký số ngày càng được khẳng định rõ ràng hơn nên HILO-CA khuyến khích khách hàng thực hiện các hồ sơ điện tử do tính tiện lợi của nó.

b. Tổ chức lưu thông tin thuê bao

Thông tin thuê bao sau khi được thẩm định sẽ được lưu trữ gồm:

- *Với tổ chức đề nghị cấp chứng thư số:*
  - Tên tổ chức
  - Mã số thuế/Mã số tổ chức hợp lệ
  - Địa chỉ theo Giấy phép đăng ký kinh doanh
  - Email
  - Số điện thoại
  - Thông tin về website, tên miền của tổ chức (sử dụng cho chứng thư SSL)
  - Thông tin về người đại diện pháp luật của tổ chức
  - Thông tin liên hệ khác
- *Với cá nhân đại diện cho tổ chức đề nghị cấp chứng thư số:*
  - Họ và tên cá nhân
  - Thông tin tổ chức
  - Số chứng minh thư nhân dân/ Thẻ căn cước công dân/Hộ chiếu/Số chứng thực cá nhân (CMND)
  - Địa chỉ theo CMND
  - Số điện thoại
  - Email
  - Thông tin sở hữu tên miền (sử dụng cho chứng thư SSL)
- *Với cá nhân đề nghị cấp chứng thư số:*
  - Họ và tên cá nhân
  - Số chứng minh thư nhân dân/ Thẻ căn cước công dân/Hộ chiếu/Số chứng thực cá nhân (CMND)
  - Địa chỉ theo CMND
  - Số điện thoại
  - Email
  - Thông tin sở hữu tên miền (sử dụng cho chứng thư SSL)

2.2 Công bố thông tin chứng thư số

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

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

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

- Các chứng thư số do HILO-CA cấp;
- CRL do HILO-CA quản lý;
- Tất cả các phiên bản cũ và hiện tại của CPS;
- Mẫu Hợp đồng dịch vụ giữa HILO-CA với thuê bao.
- Tài liệu hướng dẫn tra cứu thông tin dành cho thuê bao.

Nhằm đảm bảo tính công khai, CPS và các tài liệu khác được HILO-CA duy trì lưu trữ trực tuyến tại địa chỉ **https://hilo-ca.vn/tailieu**.

2.3 Thời gian và tần suất công bố

Quy chế chứng thực: được cập nhật theo phần 9.12.

Thỏa thuận thuê bao, thỏa thuận người nhận: được cập nhật khi cần thiết.

Chứng thư số: được công bố khi chứng thư số được ban hành và xác nhận của thuê bao và không quá 24 giờ.

Trạng thái chứng thư số: được công bố ngay lập tức lên OCSP Responder và duy trì 24 giờ trong ngày và 7 ngày trong tuần.

Danh sách chứng thư số bị thu hồi: được cập nhật hằng ngày.

2.4 Quản lý truy cập tại các kho lưu trữ

CRL, CPS được công bố công khai nhưng không cho phép sửa đổi hoặc thay thế tại địa chỉ **https://hilo-ca.vn/tailieu**.

Cập nhật CRL được thực hiện tự động bởi hệ thống HILO-CA;

Mọi thay đổi của CPS chỉ được phép thực hiện bởi cấp có thẩm quyền của HILO-CA sau khi được phê duyệt bằng văn bản của Bộ Thông tin truyền thông (Trung tâm chứng thực điện tử quốc gia – RootCA).

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

3.1 Đặt tên trong chứng thư số

3.1.1 Các kiểu tên

HILO-CA cung cấp các chứng thư số được phân loại theo:

- Chứng thư số tổ chức
- Chứng thư số cá nhân
- Chứng thư số cho cá nhân thuộc tổ chức
- Chứng thư số SSL

Chứng thư số chứa một tên dùng để phân biệt với các chứng thư số khác (Distinguished Names – DN) theo chuẩn X.501 trong trường Issuer và Subject. Các thuộc tính trong một DN mà HILO-CA sử dụng được mô tả trong bảng dưới đây:

Thuộc tính	Giá trị
Quốc gia (C)	Hai chữ cái chỉ tên quốc gia theo ISO, Việt Nam được ký hiệu là "VN"
Tổ chức (O)	Tên tổ chức, cá nhân được cấp chứng thư số hoặc tên miền đối với chứng thư số được cấp cho tên miền
Bộ phận tổ chức (OU)	Tên đơn vị nằm trong tổ chức.
Tỉnh/Thành Phố (S)	Tên Tỉnh, Thành phố là nơi cư trú hoặc đặt trụ sở của thuê bao
Tên của thuê bao (CN)	Các loại giá trị của thuộc tính này: - Tên tổ chức - Tên cá nhân - Tên miền
Địa chỉ email (E)	Địa chỉ email của thuê bao sở hữu chứng thư số
Định danh của thuê bao (UID)	MST:[mã số thuế] hoặc MNS:[mã quan hệ ngân sách] hoặc BHXH:[mã số bảo hiểm xã hội] hoặc CMND:[số chứng minh nhân dân] hoặc HC:[số hộ chiếu] hoặc CCCD:[số thẻ căn cước công dân] *Các trường hợp khác theo thỏa thuận giữa thuê bao và tổ chức cung cấp dịch vụ chứng thực chữ ký số.*

3.1.2 Quy định yêu cầu đối với tên trong chứng thư

Tên trong chứng thư là tên hoặc tên viết tắt đã được sở hữu và đăng ký bởi thuê bao theo quy định pháp luật.

Nguyên tắc đặt tên với nghĩa dễ hiểu cho phép nhận dạng được cá nhân, tổ chức, doanh nghiệp sở hữu chứng thư số đó.

Tên có ý nghĩa của 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.

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

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

3.1.4 Quy tắc diễn giải các mẫu tên

Không có quy định.

3.1.5 Tính duy nhất của tên thuê bao

Tên thuê bao sẽ là duy nhất gắn với một cấp chứng thư số xác định trong dịch vụ HILO-CA.

Một thuê bao có thể có hai hoặc nhiều chứng thư số có cùng tên thuê bao.

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

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

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

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

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

3.2 Xác minh đề nghị cấp chứng thư số

3.2.1 Quy trình tiếp nhận đề nghị cấp chứng thư số.

Bước 1: Thuê bao đề nghị cấp chứng thư số

- Thuê bao (có thể là một cá nhân hoặc một đơn vị) đến trung tâm đăng ký chứng thư (HILO-RA), thực hiện yêu cầu cung cấp dịch vụ chữ ký số HILO-CA.
- Thuê bao điền thông tin vào đơn cấp chứng thư số theo mẫu và cung cấp các giấy tờ liên quan.
- Thuê bao có 02 lựa chọn:
    - Thuê bao tự sinh khóa: Điền đơn cấp chứng thư số theo mẫu do HILO-CA cung cấp.
    - Thuê bao yêu cầu CA sinh khóa: Điền đơn cấp chứng thư số theo mẫu do HILO-CA cung cấp có tích vào phần yêu cầu HILO-CA sinh khóa cho thuê bao.
- HILO-CA tiếp nhận thông tin thuê bao đăng ký.

Bước 2: Xác minh thông tin yêu cầu cấp chứng thư số

- HILO-CA thực hiện việc kiểm tra tính chính xác của thông tin được người sử dụng khai báo trên đơn cấp chứng thư số (quá trình kiểm tra có thể dựa trên cơ sở dữ liệu lưu hồ sơ của ngành, các nguồn thông tin tin cậy như tại website: http://tracuunnt.gdt.gov.vn/ do Tổng Cục thuế cung cấp hoặc cũng có thể thông qua các giấy tờ người đó mang theo). Việc xác minh chi tiết theo từng trường hợp được mô tả ở các phần tiếp theo.
- Nếu thông tin thuê bao không hợp lệ, HILO-CA thông báo từ chối tiếp (ghi rõ lý do) và hướng dẫn thuê bao thực hiện lại đề nghị cấp chứng thư số..
- Nếu thông tin thuê bao hợp lệ, HILO-CA chuyển sang bước tạo khóa cho thuê bao.

3.2.2 Thủ tục xác minh, kiểm tra hồ sơ đề nghị cấp chứng thư số của thuê bao

a. Xác minh thuê bao sở hữu khóa bí mật

Thuê bao đăng ký chứng thư số trong trường hợp thuê bao tự sinh khóa cần phải chứng minh đang sở hữu khóa bí mật hợp lệ.

Phương pháp chứng minh sở hữu khóa bí mật sẽ tuân theo chuẩn PKCS#10 chứa thông tin định danh của thuê bao và được ký sử dụng khóa bí mật của thuê bao.

Thuê bao cần cung cấp các thông tin liên quan cấu hình thiết bị phần cứng, phần mềm, thông tin thuê bao tương ứng với file request (.csr) cung cấp cho HILO-CA.

b. Xác thực định danh cho tổ chức

HILO-CA thực hiện xác thực định danh của tổ chức thông qua bộ hồ sơ cấp chứng thư số gồm:

- Phiếu đề nghị cấp chứng thư số:
  - Đơn có đúng mẫu do HILO-CA ban hành.
  - Thông tin doanh nghiệp điền trong phiếu có chính xác.
  - Người đại diện pháp luật của tổ chức ký và đóng dấu tổ chức.
  - Trường hợp người ủy quyền ký thay cần kiểm tra thêm giấy ủy quyền có hợp lệ không.
- Giấy tờ kèm theo để xác thực gồm:
  - Quyết định thành lập hoặc quyết định quy định về chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức hoặc giấy chứng nhận đăng ký doanh nghiệp hoặc giấy chứng nhận đầu tư;
  - Chứng minh nhân dân, hoặc căn cước công dân hoặc hộ chiếu của người đại diện theo pháp luật của tổ chức.
  - Các giấy tờ khác (nếu có): Giấy ủy quyền, sổ hộ khẩu…
- Tổ chức có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc nộp bản sao xuất trình kèm bản chính để đối chiếu.

Sau quá trình xác thực định danh cho tổ chức, bộ phận nghiệp vụ HILO-CA phải trả kết quả xác thực hồ sơ là hợp lệ hay không hợp lệ (ghi rõ lý do).

c. Xác thực định danh cá nhân thuộc tổ chức

Việc xác thực định danh để cấp cá nhân thuộc tổ chức thực hiện như việc xác thực định danh tổ chức và thêm các thủ tục sau:

- Xác thực thông tin cá nhân (theo giấy tờ tùy thân và thông tin tin cậy được công bố).
- Xác thực vị trí công tác (Phòng ban, chức vụ, quyền hạn) của cá nhân trong tổ chức.

Sau quá trình xác thực định danh cho tổ chức, bộ phận nghiệp vụ HILO-CA phải trả kết quả xác thực hồ sơ là hợp lệ hay không hợp lệ (ghi rõ lý do).

d. Xác thực định danh cho cá nhân

HILO-CA thực hiện xác thực định danh của cá nhân thông qua bộ hồ sơ cấp chứng thư số. Các thông tin cần xác thực gồm:

- Phiếu đề nghị cấp chứng thư số:
  - Phiếu có nguyên vẹn mẫu của HILO-CA cung cấp.
  - Thuê bao điền đã đầy đủ thông tin trong phiếu.
  - Chủ thuê bao đã ký xác nhận vào mẫu.
- Giấy tờ kèm theo để xác thực gồm:
  - Chứng minh nhân dân hoặc căn cước công dân hoặc hộ chiếu;
  - Giấy ủy quyền (nếu có) và các giấy tờ khác
- Thuê bao có quyền lựa chọn nộp bản sao từ giấy tờ gốc, bản sao có chứng thực hoặc nộp bản sao xuất trình kèm bản chính để đối chiếu.
- Một số thông tin khác cá nhân có thể bổ sung để việc xác thực được tốt hơn gồm: Địa chỉ thư điện tử; Thông tin về website, quyền sở hữu tên miền của cá nhân (dùng cho việc cấp chứng thư số SSL).

e. Thông tin thuê bao không xác minh

Các thông tin thuê bao không xác minh bao gồm:

- Thông tin phòng ban trong tổ chức của thuê bao.
- Các thông tin không cần xác thực trong chứng thư.

3.2.3 Các quy định về liên thông

HILO-CA tuân thủ theo các quy định về liên thông giữa các hệ thống chứng thực chữ ký số do Bộ Thông tin truyền thông ban hành.

3.3 Xác minh đề nghị thay đổi khóa

3.3.1 Quy trình tiếp nhận đề nghị thay đổi khóa.

Để thực hiện thủ tục thay đổi khóa, Thuê bao cần đến gặp HILO-RA và thực hiện các bước sau:

- Điền thông tin vào phiếu đề nghị thay đổi khóa và nộp lại cho HILO-RA.
- HILO-RA tiến hành tiếp nhận và xác minh đề nghị thay đổi khóa.
- Thuê bao chờ HILO-RA xác minh đề nghị thay đổi khóa.

Đối với trường hợp thuê bao không đến trực tiếp có thể gửi hồ sơ đầy đủ theo đường bưu điện đến cho HILO-RA.

3.3.2 Thủ tục xác minh đề nghị thay đổi cặp khóa của thuê bao

- Sau khi HILO-RA tiếp nhận phiếu đề nghị thay đổi cặp khóa của thuê bao. HILO-RA cần xác minh để đảm bảo rằng cá nhân/tổ chức đề nghị thay đổi cặp khóa là chủ thuê bao của chứng thư số đó.
- Thuê bao cần cung cấp thêm thông tin để xác minh đủ thẩm quyền yêu cầu thay đổi cặp khóa:
    - Thuê bao cung cấp hợp đồng đã ký với HILO-CA (hoặc hóa đơn VAT do HILO-CA xuất), giấy đăng ký kinh doanh để chứng minh thuê bao là hợp lệ.
    - Ngoài ra, thuê bao cần cung cấp thêm giấy tờ tùy thân (CMTND/CCCD/HC), giấy ủy quyền (trong trường hợp được ủy quyền).
- Phần HILO-RA xác minh các thông tin trên phiếu đề nghị thay đổi cặp khóa tương tự phần 3.2 Xác minh đề nghị cấp chứng thư số.
- HILO-RA tra cứu hệ thống theo thông tin thuê bao cung cấp để tìm thông tin thuê bao.
    - Nếu tồn tại chứng thư số của thuê bao hợp lệ: Trả kết quả xác minh thông tin thành công, chuyển bước tiếp theo.

Nếu không tồn tại chứng thư số của thuê bao hoặc thông tin thuê bao không hợp lệ hoặc hợp đồng với thuê bao đã hết hiệu lực (chứng thư số hết hạn) thì trả kết quả xác minh không thành công, ghi rõ lý do và hướng dẫn thuê bao các thủ tục khác.

3.3.3 Nhận dạng và xác minh yêu cầu thay cặp khóa của thuê bao

Thuê bao không được phép thay cặp khóa nếu thuộc một trong các trường hợp sau:

- HILO-CA phát hiện ít nhất 1 thông tin cần xác minh trong chứng thư số không đúng.
- Chứng thư số được sử dụng trong các hoạt động phạm pháp, các hoạt động có thể ảnh hưởng tới uy tín của HILO-CA.

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

3.4.1 Quy trình đề nghị thu hồi chứng thư số.

Chứng thư số của thuê bao bị thu hồi trong những trường hợp sau đây:

- Thuê bao có đề nghị thu hồi chứng thư số của thuê bao hợp lệ gửi tới HILO-CA.
- Khi có yêu cầu của cơ quan tiến hành tố tụng, cơ quan công an hoặc Bộ Thông tin và Truyền thông.
- Khi thuê bao là cá nhân đã chết hoặc mất tích theo tuyên bố của tòa án hoặc thuê bao là tổ chức giải thể hoặc phá sản theo quy định của pháp luật;
- HILO-CA phát hiện sự cố, truy cập, sử dụng bất hợp pháp cần thu hồi/tạm dừng

Để thực hiện thu hồi chứng thư số, thuê bao cần thực hiện các bước như sau:

- Thuê bao gửi đề nghị thu hồi chứng thư số đến HILO-CA.
- HILO-RA tiến hành xác minh đề nghị thu hồi chứng thư số.
- Thuê bao đợi HILO-RA trả kết quả và hướng dẫn thủ tục tiếp theo.

3.4.2 Thủ tục xác minh đề nghị thu hồi chứng thư số

- Xác minh tính hợp lệ của hồ sơ:
  - Hồ sơ đúng thẩm quyền của các cơ quan.
  - Hồ sơ của thuê bao đề nghị đúng mẫu do HILO-CA cung cấp.
  - Chủ thuê bao đã điền đủ thông tin, ký và xác nhận vào phiếu đề nghị thu hồi chứng thư số
  - Người thực hiện đề nghị thu hồi chứng thư số là chủ hợp pháp của thuê bao (hoặc người ủy quyền hợp pháp).
    - Người thực hiện cung cấp hợp đồng (hoặc hóa đơn VAT do HILO-CA xuất), đăng ký kinh doanh của doanh nghiệp.
    - Người thực hiện cung cấp giấy tờ tùy thân (CMTND, CCCD, HC), giấy ủy quyền (nếu thực hiện theo ủy quyền).

⇨ Nếu xác minh hồ sơ đề nghị thu hồi chứng thư số hợp lệ thì HILO-RA thực hiện chuyển bước tiếp theo. Nếu không hợp lệ thì trả đề nghị lại thuê bao, ghi rõ lý do từ chối.

- Xác minh thông tin thuê bao trong hệ thống: HILO-CA thực hiện tìm kiếm chứng thư số của thuê bao trong hệ thống.
  - Tìm thấy chứng thư số của thuê bao hợp lệ: Trả kết quả xác minh cho kết quả thành công. Chuyển bước tiếp theo.
  - Nếu không thấy chứng thư số hoặc thông tin người thực hiện cung cấp bị sai hoặc chứng thư số hết hạn: Trả kết quả xác minh không thành công, ghi rõ lý do và hướng dẫn thực hiện bước tiếp theo.

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

4.1 Cấp chứng thư số

4.1.1 Đối tượng đề nghị cấp chứng thư số

Đối tượng đề nghị cấp chứng thư số gồm:

- Tổ chức, cá nhân sống và làm việc tại Việt Nam, đáp ứng đủ điều kiện theo quy định của pháp luật và CPS này có nhu cầu sử dụng chứng thư số;

- Đại diện theo pháp luật của tổ chức đủ điều kiện theo quy định của pháp luật và CPS này có nhu cầu sử dụng chứng thư số.
- Người được ủy quyền (nếu có).

4.1.2 Hồ sơ đề nghị cấp chứng thư số

Hồ sơ đề nghị cấp chứng thư số bao gồm:

- Phiếu đề nghị cấp chứng thư số.
  - Giấy đăng ký kinh doanh, Quyết định thành lập hoặc quyết định quy định về chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức hoặc giấy chứng nhận đầu tư và giấy chứng nhận mã số thuế/
  - Chứng minh nhân dân, hoặc căn cước công dân hoặc hộ chiếu của người đại diện theo pháp luật của tổ chức.
  - Các giấy tờ khác (nếu có): Giấy ủy quyền, sổ hộ khẩu…
- Tổ chức có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc nộp bản sao xuất trình kèm bản chính để đối chiếu.

4.2 Xử lý yêu cầu cấp chứng thư số

4.2.1 Thực hiện xác thực định danh

Hilo-CA tiến hành xác thực định danh tất cả các thông tin của thuê bao yêu cầu cấp chứng thư số theo phần 3..

4.2.2 Chấp nhận hoặc từ chối cấp chứng thư số

HILO-CA chỉ chấp nhận yêu cầu cấp chứng thư số nếu thỏa mãn tất cả các điều kiện xác minh thông tin, ký hợp đồng và nộp đầy đủ phí dịch vụ cấp chứng thư số cho HILO-CA.

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

- Xác thực định danh không thành công ít nhất một trong các thông tin về đối tượng yêu cầu cấp chứng thư số theo phần 3;
- Đối tượng yêu cầu cấp chứng thư số không cung cấp đủ tài liệu theo yêu cầu;
- Đối tượng yêu cầu cấp chứng thư số không trả lời yêu cầu liên lạc trong hạn thời gian xác định;
- Đối tượng yêu cầu cấp chứng thư số chưa thanh toán phí dịch vụ cấp chứng thư số;
- Có căn cứ cho rằng việc HILO-CA cấp chứng thư số cho đối tượng yêu cầu có thể ảnh hưởng tới uy tín và độ tin cậy của HILO-CA.

4.2.3 Thời gian xử lý yêu cầu cấp chứng thư số

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

4.3 Cấp chứng thư số

Để cấp chứng thư số, thuê bao đều phải ký *Hợp đồng dịch vụ* với HILO-CA sau khi thực hiện quy trình đăng ký bao gồm:

Bước 1: Đăng ký cấp chứng thư số

- Thuê bao (có thể là một cá nhân hoặc một đơn vị) đến văn phòng giao dịch/ủy quyền của HILO-CA hoặc tải danh mục hồ sơ cấp chứng thư số trên website http://hilo-ca.vn/tailieu.
- Thuê bao điền thông tin vào đơn cấp chứng thư số theo mẫu và cung cấp các giấy tờ liên quan gửi cho HILO-CA theo quy định tại 4.1.2
- Trong phiếu đăng ký cấp chứng thư số thuê bao có 02 lựa chọn:
    - Thuê bao tự sinh khóa: Điền đơn cấp chứng thư số theo mẫu do HILO-CA cung cấp.
    - Thuê bao yêu cầu CA sinh khóa: Điền đơn cấp chứng thư số theo mẫu do HILO-CA cung cấp có tích vào phần yêu cầu HILO-CA sinh khóa cho thuê bao.
- HILO-CA tiếp nhận thông tin thuê bao đăng ký, thuê bao đợi kết quả xác minh yêu cầu cấp chứng thư số.

Bước 2: HILO-CA xác minh thông tin thuê bao trên phiếu đề nghị cấp chứng thư số

- HILO-CA thực hiện việc xác minh thông tin thuê bao theo quy định tại phần 3.
- Nếu thông tin thuê bao không hợp lệ, HILO-CA thông báo từ chối cấp chứng thư số (ghi rõ lý do).
- Nếu thông tin thuê bao hợp lệ:
    - HILO-CA bàn giao thiết bị Usb Token đạt chuẩn cho thuê bao và hướng dẫn thuê bao cách tạo khóa hoặc tài liệu yêu đối bảo mật với thiết bị HSM nếu thuê bao chọn tự sinh khóa.
    - HILO-CA nhập thông tin thuê bao, đính kèm cái tài liệu lên hệ thống quản lý khách hàng.
    - HILO-CA gửi yêu cầu cấp chứng thư số tới hệ thống, chuyển sang bước tạo khóa cho thuê bao.

Bước 3: Tạo khoá và chứng thư

Để tạo khóa và chứng thư số thì HILO-CA có 02 cách tương ứng với lựa chọn là thuê bao tự tạo khóa và thuê bao yêu cầu sinh khóa hộ như sau:

- Trường hợp thuê bao tự tạo khóa:
    - Thuê bao tạo khóa từ thiết bị Usb Token/HSM theo hướng dẫn.

- Thuê bao gửi yêu cầu cấp chứng thư số về cho HILO-CA (định dạng file .csr) theo chuẩn PKCS#10.
- HILO-CA tiếp nhận CSR của thuê bao.
- HILO-CA kiểm tra thông tin trên yêu cầu cấp CTS. Các thông tin cần xác minh gồm:
    - Các trường quy định tên như quy định tại phần 1.
    - Xác minh thông tin trong file .csr với thông tin thuê bao đã được xác minh từ bộ phận thẩm định. Kiểm tra, so khớp thông tin trong hệ thống và thông tin trên hồ sơ đăng ký.
    - Cấu hình thiết bị phần cứng đáp ứng tiêu chuẩn mật mã.
    - Hệ thống HILO-CA tạo dữ liệu chứng thư số dưới dạng chuẩn X509 v3. Hệ thống HILO-CA gửi yêu cầu ký chứng thư số tới HSM, HSM sẽ thực hiện ký chứng thư số cho thuê bao tạo ra chứng số chuẩn X509.
    - Hệ thống HILO-CA sẽ lưu trữ vào cơ sở dữ liệu của HILO-CA các thông tin của thuê bao: Hồ sơ thông tin thuê bao; Request yêu cầu cấp phát chứng thư PKCS#10; Chứng thư số của thuê bao. Hệ thống cập nhật dữ liệu chứng thư số vào LDAP. Hệ thống cập nhật trạng thái chứng thư số vừa được cấp phát vào Database OCSP của HILO-CA

- Trường hợp thuê bao yêu cầu CA tạo khóa:
    - HILO-CA kiểm tra lại thông tin thuê bao trong hệ thống, gói cước yêu cầu.
    - HILO-CA tạo khóa và chứng thư số cho thuê bao trong thiết bị USB Token đạt chuẩn (như trên).

Bước 4: Lưu và công bố thông tin chứng thư số quy định ở phần tiếp theo.

Lưu ý:

- Đối với các tệp, vì trong đó có khoá bí mật đã được mã hoá (sử dụng mật khẩu khi tạo tệp này), do vậy khi gửi đến máy ghi cần gửi kèm danh sách mật khẩu tương ứng.
- Sau mỗi lần ghi xong một USB Token, trung tâm quản lý chứng thư thực hiện điền vào một danh sách thông tin về chứng thư được lưu trên USB Token đó và gửi về cho trung tâm đăng ký để chuyển đến thuê bao.

4.4 Xác nhận và công khai chứng thư số

4.4.1 Thuê bao xác nhận các thông tin trên chứng thư số được cấp

Thuê bao sẽ xác nhận thông tin trên chứng thư số được cấp là chính xác qua hai bước.

Về mặt kỹ thuật, trong quá trình tạo chứng thư số, hệ thống HILO-CA có màn hình hiển thị thông tin thuê bao để tạo chứng thư số. Thuê bao kiểm tra thông tin thuê bao:

- Nếu thông tin thuê bao đúng: Thuê bao chấp nhận và chuyển bước tiếp theo để tạo chứng thư số.
- Nếu thông tin thuê bao không đúng: Thuê bao hủy quá trình tạo chứng thư số và thực hiện lại.
- Đồng thời, các quá trình tạo khóa, tạo chứng thư số, HILO-CA đều gửi email ghi đầy đủ thông tin, gói cước để thông báo cho thuê bao về việc cấp chứng thư số. Thuê bao cần gửi email xác nhận thông tin là đúng đối với HILO-CA. Nếu thuê bao không phản hồi với HILO-CA trong khoảng thời gian 3 ngày, chứng thư số coi như được thuê bao chấp nhận.

Về mặt hồ sơ, sau khi nhận được chứng thư số, thuê bao cần kiểm tra thông tin chứng thư số và điền thông tin vào phiếu xác nhận thông tin. Người đại diện hợp lệ của thuê bao tiến hành ký, đóng dấu (đối với tổ chức) và gửi phiếu xác nhận thông tin về HILO-CA. Thủ tục này là yêu cầu bắt buộc. Nếu thuê bao không thực hiện (trong 01 tháng), HILO-CA có thể tiến hành tạm dừng chứng thư số của thuê bao để hạn chế rủi ro cho chủ thể của thuê bao.

4.4.2 Tổ chức cung cấp dịch vụ chứng thực chữ ký số công bố công khai chứng thư số của thuê bao theo quy định.

HILO-CA sẽ thực hiện công bố công khai và quản lý hệ thống danh bạ về chứng thư số của thuê bao ngay sau khi hoàn thành thủ tục cấp chứng thư số cho thuê bao tại website *https://hilo-ca.vn*. Hệ thống danh bạ chứng thư số HILO-CA công bố bao gồm:

- Chứng thư số của HILO-CA: truy cập chức năng theo đường dẫn *http://hilo-ca.vn/hilocert*
- Chứng thư số của thuê bao: truy cập chức năng theo đường dẫn *http://hilo-ca.vn/danhsachcts*
- Danh sách Chứng thư số thu hồi (CRL): truy cập chức năng theo đường dẫn *http://hilo-ca.vn/crl*
- Quy chế chứng thực chữ ký số HILO-CA và các thông tin khác: truy cập chức năng theo đường dẫn http://hilo-ca.vn/tailieu

Đồng thời, HILO-CA công bố thông tin tới các thành phần liên quan tới hệ thống như sau:

- Email công bố thông tin chứng thư số tới thuê bao theo email thuê bao đăng ký.

- Cung cấp thông tin tới ROOT-CA theo quy định.

HILO-CA thực hiện công bố tài liệu hướng dẫn thuê bao tra cứu thông tin chứng thư số trực tuyến tại địa chỉ website: https://hilo-ca.vn/TaiLieu.

4.5 Sử dụng cặp khóa và chứng thư số

Sau khi thuê bao được tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp chứng thư số thì có thể sử dụng cặp khóa cũng như chứng thư số của mình một cách hợp pháp theo các quy định của pháp luật.

4.5.1 Cách sử dụng chứng thư số và khóa bí mật của thuê bao

Việc sử dụng khóa bí mật tương ứng với khoá công khai trong chứng thư số chỉ được cho phép khi thuê bao chấp nhận chứng thư số. Chứng thư số sẽ được sử dụng hợp pháp dựa trên các điều khoản của Hợp đồng dịch vụ, các điều khoản trong CPS này cũng như quy định của pháp luật.

Cách sử dụng chứng thư số phải tương ứng với giá trị quy định của trường KeyUsage bên trong chứng thư số (Ví dụ nếu giá trị Digital Signature không có trong trường KeyUsage thì chứng thư số này không thể được dùng để ký điện tử) .

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

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

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

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

4.6 Gia hạn chứng thư số

4.6.1 Các trường hợp được gia hạn chứng thư số của thuê bao.

Chỉ có thuê bao của HILO-CA mới có thể được gia hạn chứng thư số.

Chỉ có các chứng thư số đang hoạt động hợp lệ (không bị tạm dừng, thu hồi) mới có thể thực hiện yêu cầu gia hạn.

Chỉ có thuê bao cá nhân hoặc đại diện theo pháp luật của tổ chức đối với thuê bao tổ chức mới được phép yêu cầu gia hạn chứng thư số.

Thuê bao cần gửi yêu cầu HILO-CA gia hạn trước 30 ngày tính đến ngày hết hạn sử dụng chứng thư số đó.

4.6.2 Xử lý yêu cầu gia hạn chứng thư số

Thuê bao cần tiến hành điền đủ thông tin yêu cầu trong Phiếu yêu cầu gia hạn chứng thư số theo mẫu do HILO-CA ban hành và nộp về HILO-CA để tiến hành gia hạn.

Sau khi nhận được yêu cầu gia hạn chứng thư số, HILO-CA tiến hành xác minh thông tin đề nghị như quy định tại phần 3.

Nếu thông tin xác thực, việc gia hạn được tiến hành. Nếu thông tin sai lệch, yêu cầu bị từ chối.

Ngoài ra, HILO-CA sẽ yêu cầu người thực hiện chứng minh mình đủ thẩm quyền để thực hiện việc gia hạn và những yêu cầu cho xác thực yêu cầu cấp chứng thư số gốc sẽ được sử dụng để gia hạn.

4.6.3 Thông báo cho thuê bao về việc phát hành chứng thư số mới

Việc thông báo cho thuê bao về việc phát hành chứng thư số mới tuân theo quy định ghi tại phần 4.2

4.6.4 Điều khoản chấp nhận gia hạn chứng thư số

Điều kiện cấu thành điều khoản gia hạn chứng thư số tuân theo phần 4.3

4.6.5 Công bố chứng thư số được gia hạn

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

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

HILO-CA có trách nhiệm thông báo tới ROOT-CA, HILO-RA về việc gia hạn chứng thư số do họ xác thực định danh.

4.7 Thay đổi khóa của thuê bao

4.7.1 Đối tượng được gửi yêu cầu thay đổi khóa

Chỉ có thuê bao của HILO-CA mới có thể được gửi yêu cầu thay đổi khóa.

Chỉ có thuê bao cá nhân hoặc đại diện theo pháp luật của tổ chức đối với thuê bao tổ chức mới được phép yêu cầu thay đổi cặp khóa.

Thuê bao còn hạn hợp đồng hoặc gia hạn/ký mới hợp đồng mới có thể gửi yêu cầu thay đổi khóa.

4.7.2 Các trường hợp được thay đổi khóa của thuê bao

Thuê bao được thay đổi khóa trong các trường hợp sau:

- Thiết bị chứa khóa bị hư hỏng.
- Thuê bao mất thiết bị chứa khóa.
- Thuê bao/HILO-CA phát hiện khóa có dấu hiệu bị lộ.
- Thay đổi khóa theo nhu cầu sử dụng của thuê bao.
- Thuê bao thay đổi thông tin dẫn đến phải thay đổi khóa tương ứng với thông tin mới.
- Các trường hợp khác theo quy định của pháp luật.

Chỉ có thuê bao cá nhân hoặc đại diện theo pháp luật của tổ chức đối với thuê bao tổ chức mới được phép yêu cầu thay đổi khóa chứng thư số.

4.7.3 Xử lý yêu cầu thay đổi khóa

Thuê bao cần tiến hành các thủ tục theo phần 4.1 và điền đủ thông tin yêu cầu trong bản Phiếu yêu cầu thay đổi khóa theo mẫu do HILO-CA ban hành.

HILO-CA hoặc Hilo-CA tiến hành xác thực thông tin cung cấp của thuê bao theo phần 3.3. Nếu thông tin xác thực, việc thay khóa được tiến hành. Nếu thông tin sai lệch, yêu cầu bị từ chối.

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

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

4.7.5 Điều khoản chấp nhận thay khóa chứng thư số

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

4.7.6 Công bố chứng thư số đã thay khóa

HILO-CA có trách nhiệm công bố chứng thư số được thay khóa trên kho lưu trữ công khai theo phần 2.2

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

HILO-CA có trách nhiệm thông báo cho Hilo-RA và các đơn vị quản lý theo quy định về việc thay khóa chứng thư số do họ xác thực định danh.

4.8 Thay đổi thông tin chứng thư số

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

4.8.1 Đối tượng được thay đổi thông tin chứng thư số

Chỉ có thuê bao của HILO-CA mới có thể được gửi yêu cầu thay thông tin chứng thư số.

Chỉ có thuê bao cá nhân hoặc đại diện theo pháp luật của tổ chức đối với thuê bao tổ chức mới được phép yêu cầu thay đổi chứng thư số.

Thuê bao còn hạn hợp đồng hoặc gia hạn/ký mới hợp đồng mới có thể gửi yêu cầu thay thông tin chứng thư số.

4.8.2 Các trường hợp được thay đổi thông tin chứng thư số.

Thuê bao được thay đổi thông tin chứng thư số trong các trường hợp sau:

- Phát hiện thông tin chứng thư số không đúng thông tin của chủ thể thuê bao.
- Chủ thể thuê bao thay đổi thông tin dẫn đến phải thay đổi chứng thư số. Các thông tin khi thay đổi phải đổi thông tin chứng thư số được quy định tại phần 3.1.

4.8.3 Xử lý yêu cầu thay đổi thông tin chứng thư số

Thuê bao điền phiếu yêu cầu thay đổi thông tin chứng thư số do HILO-CA ban hành.

HILO-CA tiến hành xác minh tính hợp lệ của thông tin yêu cầu từ thuê bao theo phần 3.2.

Quá trình xác minh trả kết quả hồ sơ hợp lệ, HILO-CA tiến hành thay cấp chứng thư số mới cho thuê bao theo thông tin mới theo phần 4.3

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

Xem phần 4.2.

4.8.5 Điều khoản chấp nhận sửa đổi chứng thư số

Xem phần 4.2.

4.8.6 Công bố chứng thư số đã sửa đổi

Xem phần 4.4.

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

Xem phần 4.4.

4.9 Tạm dừng và thu hồi chứng thư số

4.9.1 Đối tượng được phép yêu cầu tạm dừng và thu hồi chứng thư số.

Chỉ có thuê bao của HILO-CA mới có thể được gửi yêu cầu tạm dừng, thu hồi chứng thư số.

Chỉ có thuê bao cá nhân hoặc đại diện theo pháp luật của tổ chức đối với thuê bao tổ chức mới được phép yêu cầu thay đổi chứng thư số.

Thuê bao còn hạn hợp đồng mới có thể gửi yêu cầu thay thông tin chứng thư số.

Cơ quan tiến hành tố tụng, cơ quan công an hoặc Bộ Thông tin truyền thông;

HILO-CA thu hồi, tạm dừng chứng thư số của thuê bao theo yêu cầu của cơ quan quản lý hoặc đảm bảo quyền lợi cho thuê bao, HILO-CA.

4.9.2 Các trường hợp được phép thu hồi, tạm dừng chứng thư số

Chứng thư số của thuê bao bị thu hồi, tạm dừng trong những trường hợp sau đây:

- Khi thuê bao yêu cầu bằng văn bản và yêu cầu này đã được tổ chức cung cấp dịch vụ chứng thực chữ ký số của mình xác minh là chính xác;
- Khi thuê bao là cá nhân đã chết hoặc mất tích theo tuyên bố của tòa án hoặc thuê bao là tổ chức giải thể hoặc phá sản theo quy định của pháp luật;

- 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 thu hồi chứng thư số đã được quy định trong hợp đồng giữa thuê bao và tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.

4.9.3 Quy trình, thủ tục thu hồi, tạm dừng chứng thư số

Cơ quan, tổ chức có thẩm quyền gửi công văn yêu cầu việc thu hồi, tạm dừng chứng thư số hoặc chủ thuê bao gửi yêu cầu thu hồi, tạm dừng chứng thư số theo mẫu HILO-CA ban hành tới HILO-CA.

HILO-CA tiếp nhận yêu cầu thu hồi và tiến hành xác minh đề nghị thu hồi, tạm dừng sẽ được tiến hành theo nội dung trong phần 3.4.

Trường hợp kết quả trả xác minh không thành công, HILO-CA sẽ từ chối đề nghị và gửi kết quả tới trả lời ghi rõ lý do;

Trường hợp kết quả xác minh thành công, HILO-CA tiến hành thu hồi, tạm dừng chứng thư số của thuê bao.

HILO-CA công bố trên cơ sở dữ liệu về chứng thư số việc thu hồi, tạm dừng.

4.9.4 Thông báo, công bố việc thu hồi chứng thư số của thuê bao.

HILO-CA cập nhật thông tin chứng thư số bị thu hồi, tạm dừng vào danh sách CRL và công bố tại địa chỉ *http://hilo-ca.vn/crl*.

HILO-CA gửi thông báo về việc thu hồi, tạm dừng chứng thư số tới email thuê bao đã đăng ký về việc thu hồi, tạm dừng chứng thư số.

4.9.5 Tần suất phát hành chứng thư số bị thu hồi

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

4.9.6 Thời gian trễ lớn nhất của CRL

CRL được phát hành công khai và quá trình này được tiến hành tự động ngay sau khi danh sách CRL được cập nhật.

4.9.7 Hỗ trợ kiểm tra trực tuyến trạng thái chứng thư số bị thu hồi

Kiểm tra trạng thái chứng thư số trực tuyến (OCSP) truy cập tại địa chỉ: *http://hilo-ca.vn/ocsp*;

4.9.8 Điều kiện kiểm tra trực tuyến chứng thư số bị thu hồi

Người nhận phải kiểm tra trạng thái chứng thư số trước khi tin tưởng.

4.9.9 Mẫu quảng bá chứng thư số bị thu hồi khác

Không có quy định.

4.9.10 Các điều kiện đặc biệt khi khóa bị xâm phạm

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

4.9.11 Giới hạn thời gian của yêu cầu thu hồi, tạm dừng chứng thư số.

Chứng thư số bị tạm dừng, thu hồi ngay lập tức sau khi HILO-CA xác thực thông tin tạm dừng là hợp lệ.

Thời gian tạm dừng không được vượt quá thời hạn của chứng thư số. Nếu thời gian yêu cầu tạm dừng quá thời hạn của chứng thư số, HILO-CA hướng dẫn thuê bao chuyển sang yêu cầu thu hồi chứng thư số.

4.10 Kiểm tra trạng thái chứng thư số

4.10.1 Các hình thức kiểm tra trạng thái chứng thư số của thuê bao.

Thuê bao có thể kiểm tra trạng thái chứng thư số thông qua CRL tại trang web của HILO-CA (https://hilo-ca.vn), dịch vụ LDAP hoặc thông qua dịch vụ OCSP (nếu có thể).

4.10.2 Tính sẵn sàng của dịch vụ

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

Trường hợp nâng cấp, bảo trì, phát sinh vấn đề cần xử lý, HILO-CA sẽ thông báo kế hoạch xử lý trên website của HILO-CA.

4.10.3 Các tùy chọn khác

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

4.11 Chấm dứt dịch vụ của thuê bao

4.11.1 Các trường hợp thuê bao chấm dứt dịch vụ.

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

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

4.11.2 Thủ tục chấm dứt dịch vụ

- Thủ tục chấm dứt dịch vụ được thực hiện tự động bởi hệ thống HILO-CA khi chứng thư số hết hạn.

4.12 Lưu trữ và phục hồi khóa bí mật của thuê bao

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

4.12.1. Dịch vụ lưu trữ khóa bí mật của thuê bao

HILO-CA không có quy định.

4.12.2. Quy trình phục hồi khóa bí mật của thuê bao

HILO-CA không có quy định.

5. KIỂM SOÁT, QUẢN LÝ VÀ VẬN HÀNH

5.1 Kiểm soát an toàn, an ninh vật lý

5.1.1 Quy trình, thủ tục kiểm soát vào ra trụ sở, nơi đặt máy móc thiết bị của tổ chức cung cấp dịch vụ chứng thực chữ ký số.

a. Kiểm soát an toàn tại Trụ sở/ Phòng vận hành (NOC)

Phòng NOC của HILO-CA đặt tại trụ sở tại tầng 6, tòa HEC, số 2 ngõ 95 Chùa Bộc, Phường Trung Liệt, Quận Đống Đa, TP. Hà Nội. Để truy vào được phòng NOC cần thực hiện các bước sau:

- Đăng ký sử dụng phòng NOC, ghi rõ nội dung sử dụng, trang thiết bị mang vào ra phòng NOC với bộ phận quản trị vận hành hệ thống HILO-CA.
- Bộ phận quản trị vận hành hệ thống xác minh thông tin, mục đích đăng ký của nhân sự, nếu hợp lệ thì xác nhận và cấp giấy sử dụng phòng NOC.
- Nhân sự tới tòa HEC, khai báo với bảo vệ tòa nhà về mục đích làm việc, để lại giấy tờ tùy thân và nhận thẻ từ vào tòa nhà.
- Nhân sự trình giấy đăng ký sử dụng phòng NOC và giấy tờ cá nhân để xác minh.
- Nhân sự sử dụng phòng NOC theo quy định.
- Bộ phận quản trị vận hành hệ thống giám sát và cập nhật thông tin sử dụng phòng NOC vào sổ.

b. Kiểm soát an toàn tại DC (FPT 17 Duy Tân)/DRC (ViettelIDC Láng Hòa Lạc)

Quy trình để nhân sự vào hệ thống DC/DRC của HILO-CA gồm các bước:

- HILO gửi yêu cầu ra vào hệ thống ghi rõ thông tin người sẽ thực hiện (Họ tên, số chứng minh thư nhân dân…), thời gian, trang thiết bị mang theo (nếu có) và mục đích vào hệ thống. Người gửi yêu cầu phải là người đại diện pháp luật hoặc quản trị hệ thống (đã đăng ký với trung tâm từ trước).
- Trung tâm dữ liệu xếp lịch và xác nhận lịch làm việc bằng phiếu đăng ký vào trung tâm dữ liệu.
- Nhân sự HILO nhận phiếu đăng ký và mượn khóa tủ rack để lên trung tâm làm việc.
- Nhân sự đến Data Center, khai báo lý do lên Data Center để qua cửa an ninh của trung tâm.
- Nhân sự đến cửa trung tâm và gặp nhân sự quản lý trung tâm, xuất trình phiếu đăng ký, giấy tờ tùy thân (CMTND) để xác minh.
- Sau khi xác minh thông tin, nhân sự quản lý trung tâm dữ liệu sẽ cấp thẻ từ ra vào trung tâm dữ liệu (thẻ từ có 2 cấp truy cập (vào data center và vào khu vực máy chủ) tùy vào mục đích làm việc đã đăng ký).

Nhân sự thực hiện cần có chìa khóa rủ rack để mở tủ thực hiện các thao tác cơ bản. Thao tác vào hệ thống chỉ giới hạn nhân sự nhất định mới được phép truy cập.

5.1.2 Các điều kiện nguồn điện, điều hoà, phòng chống cháy nổ...

Trung tâm vận hành HILO-CA (NOC) đặt tại vị trí trung tâm thành phố nên điều kiện về nguồn điện được đảm bảo tốt. Hệ thống HILO-CA đi vào vận hành sẽ hoạt động với độ ổn định cao nên việc sử dụng phòng NOC cũng ít xảy ra. Trường hợp sử dụng gấp, nhân sự vận hành hệ thống đăng ký và thực hiện trực tiếp tại DC/DRC.

Phòng NOC được trang bị hệ thống điều hòa và hạn chế tối đa thiết bị nhằm giảm thiểu nguy cơ cháy nổ có thể xảy ra.

Hệ thống thiết bị chính của HILO-CA đặt tại trung tâm dữ liệu của Viettel (IDC Viettel Láng Hòa Lạc) và FPT (IDC FPT 17 Duy Tân.

Hai trung tâm dữ liệu đáp ứng đầy đủ điều kiện về nguồn điện, điều hòa, phòng chống cháy nổ… đảm bảo hệ thống HILO-CA vận hành ổn định và liên tục 24.7.

5.1.3 Thiết bị lưu trữ dữ liệu.

Tất cả các sản phẩm lưu trữ thông tin về phần mềm và dữ liệu, kiểm toán, tư liệu hay thông tin dự phòng được lưu trữ đảm bảo an ninh thông qua các triển khai an ninh vật lý và điều khiển truy cập nhằm ngăn ngừa truy cập trái phép và bảo vệ phương tiện lưu trữ không bị phá hủy (do nước, lửa, điện từ trường…)

5.1.4 Hệ thống dự phòng.

Hệ thống dự phòng (DRC) HILO-CA đặt tại trung tâm dữ liệu IDC Viettel tại Láng Hòa Lạc.

Hệ thống dự phòng cách hệ thống chính (IDC FPT 17 Duy Tân) trên 30km nên đảm bảo điều kiện khoảng cách tối thiểu hai hệ thống.

HILO-CA xây dựng hệ thống dự phòng có thiết kế gần giống với hệ thống chính. Hệ thống chính và dự phòng kết nối với nhau qua kênh truyền riêng và có cơ chế back up dữ liệu đảm bảo hệ thống dự phòng có thể hoạt động nhanh nhất thay thế hệ thống chính khi có sự cố xảy ra.

5.1.5 Quy trình xử lý rác, tiêu hủy thông tin nhạy cảm.

Các tài liệu và tài nguyên nhạy cảm được cắt vụn trước khi hủy.

Các phương tiện thu thập hay truyền thông tin nhạy cảm được xử lý để đảm bảo các thông tin này không bị truy cập bất hợp pháp trước khi tiêu hủy.

Các thiết bị dùng để mã hóa phải được phá hủy về mặt vật lý theo hướng dẫn của nhà sản xuất trước khitiêu hủy.

Các loại rác khác phải tiêu hủy đạt yêu cầu về tiêu chuẩn tiêu hủy rác thông thường của HILO-CA.

5.2 Quy trình kiểm soát

5.2.1 Kiểm soát người có quyền truy nhập, thao tác đối với hệ thống

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

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

- Quá trình kiểm tra thông tin trong ứng dụng chứng thư số;
- Quá trình cung cấp dịch vụ chứng thực chữ ký số;
- Ban hành, thu hồi quyền truy cập tới các phần bị hạn chế của hệ thống;

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

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

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

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

5.2.2 Nhận dạng và xác thực cho từng thành viên

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

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

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

5.2.3 Phân chia nhân sự cho mỗi công việc; vai trò, trách nhiệm của từng thành viên

Những vai trò yêu cầu phân chia trách nhiệm bao gồm nhưng không giới hạn. Một nhân sự có thể kiêm nhiệm nhiều vị trí:

Tên vị trí	Số lượng nhân sự tối thiểu	Vai trò	Trách nhiệm
Quản trị hệ thống	1	Quản trị vận hành hệ thống	Chịu trách nhiệm về tất cả các hoạt động, vận hành của hệ thống.
Vận hành hạ tầng	1	Vận hành kỹ thuật	Đảm bảo hệ thống hoạt động ổn định và liên tục

Kinh doanh	10	Phát triển kinh doanh	Ký hợp đồng và tiếp nhận thông tin khách hàng đưa vào hệ thống.
Thẩm định	2	Xác thực thông tin	Xác thực thông tin hồ sơ. Kiểm tra tính hợp lệ của hồ sơ
Vận hành hệ thống cấp phát	2	Vận hành hệ thống cấp phát chứng thư số	Xác thực thông tin nhập vào hệ thống (yêu cầu kĩ thuật). Cấp, điều chỉnh, thu hồi chứng thư số.
Pháp chế	1	Quản lý pháp chế	Soạn điều khoản hợp đồng và tư vấn các giấy tờ khác.
Kế toán	1	Quản lý tài chính, công nợ	Đối soát thuê bao với nhân viên kinh doanh, đại lý. Đối soát, thúc đẩy thu hồi công nợ
Số hóa	1	Đảm bảo giấy tờ, hồ sơ được đầy đủ	Thu hồ sơ, chỉnh lý và số hóa hồ sơ.

5.3 Kiểm soát nhân sự

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

5.3.1 Kinh nghiệm, bằng cấp, chứng chỉ của đội ngũ nhân sự liên quan đến quản lý và vận hành hệ thống.

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

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

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

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

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

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

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

5.3.2 Yêu cầu về đào tạo cho cán bộ vận hành, quản lý hệ thống

HILO-CA đào tạo nhân viên sau tuyển dụng cũng như trong quá trình làm việc để đảm bảo nhân viên có thể hoàn thành công việc của mình.

HILO-CA sẽ lưu giữ các tư liệu của những lần đào tạo này đồng thời thường xuyên xem xét lại và nâng cấp các chương trình đào tạo khi thấy cần thiết.

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

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

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

Ngoài ra, HILO-CA sẽ thường xuyên tham gia các hội thảo về chữ ký số, an toàn bảo mật tại Việt nam và các diễn đàn trên thế giới.

HILO-CA khuyến khích cán bộ thi thêm các chứng chỉ, bằng cấp liên quan đến chứng thư số và an toàn bảo mật thông tin.

5.3.3 Yêu cầu đào tạo lại thường xuyên

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

5.3.4 Hình thức xử lý các trường hợp vi phạm

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

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

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

Các trường hợp khác hình thức xử lý các trường hợp vi phạm theo quy định của pháp luật có liên quan và thỏa thuận.

5.4 Các quy trình ghi nhật ký hệ thống

5.4.1 Các sự kiện HILO-CA cần ghi nhận

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

Các dạng sự kiện được ghi tự động tại file log hệ thống trên máy chủ FileServer bao gồm:

- Các sự kiện tới hệ thống:
  - Tạo khóa CA;
  - Bật tắt các hệ thống và ứng dụng;
  - Thay đổi khóa CA;
  - Sự kiện có liên quan đến quản lý chu kỳ mã hóa;
  - Quá trình xử lý dữ liệu kích hoạt cho khóa bí mật của CA, các bản ghi truy cập vật lý;
  - Bảo trì và thay đổi cấu hình hệ thống;
  - Bản ghi hủy bỏ các phương tiện chứa khóa, dữ liệu kích hoạt, hoặc thông tin thuê bao.
- Các sự kiện về vòng đời của chứng thư số, bao gồm: phát hành, cấp lại, cấp mới, thu hồi, tạm dừng;
- Sự kiện lên quan tới người tin cậy, bao gồm:
  - Hành động truy cập hay thoát ra;
  - Tạo và xóa bỏ mật khẩu hay thay đổi đặc quyền của người sử dụng;
  - Thay đổi nhân sự;
- Báo cáo về việc truy nhập vào mạng và các hệ thống không được cấp quyền;
- Lỗi trong việc đọc và ghi chứng thư số và kho lưu trữ;
- Thay đổi chính sách tạo chứng thư số, thời gian hợp lệ;
- Lỗi phát sinh liên quan đến chứng thư số và dịch vụ chứng thực chữ ký số do thuê bao thông báo hoặc do HILO-CA phát hiện.

5.4.2 Quy định việc sử dụng nhật ký hệ thống

a. Tần suất xử lý bản ghi kiểm tra

Các bản ghi kiểm tra được xử lý tối thiểu hàng tuần đối với các sự kiện an ninh và vận hành quan trọng. Ngoài ra, HILO-CA sẽ tiến hành kiểm tra bất thường dựa theo các cảnh báo và hiện tượng của hệ thống.

b. Thời gian lưu trữ bản ghi kiểm tra

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

c. Bảo vệ bản ghi kiểm tra

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

d. Thủ tục sao lưu bản ghi kiểm tra

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

e. Hệ thống thu thập nhật ký (Bên trong và bên ngoài)

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

f. Thông báo cho đối tượng gây ra sự kiện

Khi một sự kiện được ghi nhật ký, không có thông báo cho đối tượng gây ra sự kiện đó.

g. Đánh giá lỗ hổng hệ thống

Dữ liệu nhật ký sẽ được đưa vào phân tích, kết quả phân tích sẽ cho biết các lỗ hổng tiềm tàng trong hệ thống, từ đó có phương án khắc phục.

5.5 Lưu trữ các bản ghi

5.5.1 Các loại hình, thông tin bản ghi cần lưu trữ

HILO-CA sẽ lưu trữ các thông tin sau

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

5.5.2 Thời gian lưu trữ

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

5.5.3 Bảo vệ bản ghi lưu trữ

Chỉ nhân sự tin tưởng được cấp phép bởi HILO-CA mới có khả năng truy cập và sử dụng dữ liệu lưu trữ.

Phương tiện lưu trữ dữ liệu thường xuyên được bảo trì và quản lý, luôn sẵn sàng phục vụ truy cập.

Thông tin lưu trữ sẽ được kiểm tra tính toàn vẹn khi được lấy ra.

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

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

5.6 Thay đổi khóa

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

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

5.7 Xử lý sự cố, thảm họa và phục hồi

Việc dự phòng và sao lưu cần tiến hành tại địa điểm, thiết bị khác nhằm phòng ngừa khả năng sự cố.

Các dữ liệu cần sao lưu gồm: dữ liệu đăng ký chứng thư số, dữ liệu kiểm tra, cơ sở dữ liệu của các chứng thư số đã phát hành.

Sao lưu dự phòng khóa bí mật của CA tuân theo quy định trong phần 6.2.4.

5.7.1 Sự cố liên quan tài nguyên máy tính, phần mềm và dữ liệu

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

5.7.2 Thủ tục xử lý sự cố bị lộ khóa bí mật

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

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

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

5.7.3 Khả năng khôi phục hoạt động sau sự cố

HILO-CA xây dựng hệ thống dự phòng cách vị trí hệ thống chính thức tối thiểu 30 km. HILO-CA sẽ lập kế hoạch, triển khai và thử nghiệm phương án phục hồi sau sự cố nhằm giảm tối đa các hậu quả gây ra do yếu tố tự nhiên hay con người. Kế hoạch này thường xuyên được kiểm tra, xem xét và cập nhật cho phù hợp với tình hình thực tế.

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

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

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

Cơ sở dữ liệu dùng cho phục hồi sau sự cố được đồng bộ với hệ thống đang vận hành trong khoảng thời gian cho phép. Các thiết bị sử dụng cho kế hoạch phục hồi được bảo vệ theo quy định ở phần 5.1.

HILO-CA bảo quản các thiết bị phần cứng và sao lưu dự phòng tại khu vực quản lý trang thiết bị phục hồi sau sự cố. Khóa bí mật của HILO-CA được sao lưu vào bảo quản cho nhiệm vụ phục hồi sau thảm họa theo quy định ở phần 6.2.

5.8 Ngừng dịch vụ của HILO-CA hoặc HILO-RA

HILO-CA sẽ thông báo khi HILO-CA hoặc một Hilo-RA chấm dứt hoạt động cho các đối tác, thuê bao bằng các phương tiện truyền thông hợp lý có thể sử dụng. Khi

chấm dứt hoạt động, HILO-CA sẽ thực hiện quy trình chấm dứt nhằm giảm thiểu các thiệt hại tới thuê bao, người nhận. Quy trình này có thể bao gồm các bước sau:

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

6. ĐẢM BẢO AN TOÀN AN NINH VỀ KỸ THUẬT

6.1 Tạo và phân phối khóa

6.1.1 Sinh cặp khóa

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

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

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

Cặp khóa của thuê bao được sinh ra tại PKI Smartcard, PKI token theo tiêu chuẩn FIPS 140-2 Level 2 trở lên, sử dụng sinh khóa ký số phải có Token và mã PIN xác thực truy xuất vào thiết bị.

Trong một số trường hợp khách hàng có nhu cầu đặt biệt, khách hàng sử dụng thiết bị HSM đạt chuẩn FIPS 140-2 Level 3, cặp khóa được sinh ra trong thiết bị HSM của khách hàng.

6.1.2 Quy trình phân phối khóa tới thuê bao

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

Trường hợp thuê bao ủy quyền cho HILO-CA sinh khóa hộ: Khóa bí mật được lưu trong USB Token. HILO-CA chịu trách nhiệm và đảm bảo giao USB Token và mật khẩu sử dụng đến tận tay thuê bao một cách an toàn theo quy trình chuyển giao khóa bí mật:

- Mật khẩu sử dụng cho USB Token được tạo ngẫu nhiên cho từng thuê bao.
- USB Token và mật khẩu sử dụng được đóng gói và niêm phong trong phong bì của HILO-CA.
- HILO-CA cung cấp dịch vụ chuyển USB Token đến tận nơi cho thuê bao thông qua dịch vụ chuyển phát của HILO-CA hoặc đối tác. Để đảm bảo an toàn của khóa bí mật đối với trường hợp này, PINCODE (mật khẩu sử dụng) được gửi cho thuê bao thông qua SMS hoặc email đã đăng ký trước đó.
- Thuê bao chỉ ký vào biên bản giao nhận khi USB Token và mật khẩu sử dụng nằm trong phong bì vẫn còn niêm phong.

Các hoạt động này được HILO-CA theo dõi và ghi lại.

6.1.3 Gửi khóa công khai tới đơn vị phát hành

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

6.1.4 Chuyển giao khóa công khai của CA tới bên tin cậy.

Các bên tin cậy có thể tải và cài đặt khóa công khai của HILO-CA, RootCA từ website của HILO-CA.

Khóa công khai của HILO-CA có thể truy xuất theo điều khoản trong phần 2.1.

6.1.5 Kích thước khóa

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

6.1.6 Sinh các tham số khóa và kiểm tra chất lượng

Không có quy định.

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

Xem trong phần 7.1.2.1.

6.2 Kiểm soát và bảo vệ khóa bí mật

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

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

6.2.1 Tiêu chuẩn kỹ thuật đối với thiết bị mật mã

HILO-CA sử dụng thiết bị mật mã phần cứng để sinh khóa và lưu trữ khóa bí mật gốc của CA. Thiết bị HILO-CA sử dụng đạt tiêu chuẩn tối thiểu như sau:

- Ký hiệu tiêu chuẩn: FIPS PUB 140-2 Level 3
- Tên đầy đủ của tiêu chuẩn: Security Requirements for Cryptographic Modules

6.2.2 Cơ chế kiểm soát, bảo vệ các khoá bí mật

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

Để kích hoạt khóa cần ít nhất một số lơn hơn 1 (m) mảnh khóa (m =< n).Tại HILO-CA, m >= 2.

6.2.3 Ủy thác giữ khóa bí mật

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

Khóa bí mật của thuê bao được ủy thác theo điều khoản phần 4.1.

6.2.4 Dự phòng khóa bí mật

Cặp khóa bí mật của HILO-CA được sao lưu dự phòng trên thiết bị phần cứng an toàn và được đặt cách xa vị trí lưu trữ bản chính tối thiểu 30 km.

6.2.5 Lưu trữ khóa bí mật

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

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

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

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

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

6.2.8 Phương pháp kích hoạt sử dụng khóa bí mật

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

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

6.2.9 Phương pháp hủy khóa bí mật

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

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

6.2.10 Đánh giá thiết bị mật mã

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

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

6.3.1 Lưu trữ cặp khóa

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

6.3.2 Thời hạn có hiệu lực của chứng thư số và thời hạn sử dụng cặp khóa

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

Thời gian hoạt động của cặp khóa trong chứng thư số HILO-CA tuân theo quy định của Bộ Thông tin và Truyền thông. Thời gian hoạt động của cặp khóa trong chứng thư số thuê bao không được quá 4 năm.

6.4 Kích hoạt dữ liệu

6.4.1 Khởi tạo và cài đặt dữ liệu kích hoạt khóa bí mật.

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

- Được một cá nhân tạo ra;
- Có ít nhất tám ký tự;
- Có ít nhất một ký tự là chữ cái và một ký tự là chữ số;
- Có ít nhất một ký tự chữ thường;
- Một ký tự bất kỳ không lặp lại từ 3 lần trở lên;
- Không trùng tên với tên của người vận hành;
- Không chứa một phần tên trong tên của người vận hành;

6.4.2 Bảo vệ dữ liệu kích hoạt

HILO-CA khuyến cáo thuê bao tuân theo các yêu cầu trên. Ngoài ra để tăng cường an toàn, HILO-CA khuyến khích sử dụng các cơ chế đa xác thực (token và passphrase, sinh trắc và token, sinh trắc và passphrase) cho quá trình kích hoạt khóa bí mật.

6.4.3 Quy trình kích hoạt dữ liệu

- Tạo dữ liệu theo nguyên tắc phần 6.4.1.
- Kích hoạt dữ liệu
- Gửi dữ liệu kích hoạt: Khi tiến hành gửi dữ liệu kích hoạt khóa bí mật cho thuê bao, Hilo– CA sử dụng các phương pháp đảm bảo không để bị mất mát, đánh cắp, sửa đổi, để lộ hoặc sử dụng trái phép khóa bí mật.
- Hủy dữ liệu kích hoạt: Khi cần thiết, dữ liệu kích hoạt khóa bí mật sẽ được HILO-CA hủy bỏ bằng các phương pháp thích hợp, đảm bảo dữ liệu không bị mất mát, đánh cắp, sửa đổi, để lộ hoặc sử dụng trái phép khóa bí mật được bảo vệ bởi dữ liệu kích hoạt đó.

6.5 Kiểm soát an ninh máy tính

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

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

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

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

6.5.2 Đánh giá an ninh hệ thống máy tính

HILO-CA tuân theo chuẩn an toàn hệ thống máy tính ISO 27001. Công việc đánh giá và kiểm tra được tiến hành theo định kỳ và đột xuất căn cứ theo tình hình thực tế.

Bộ phận quản lý hệ thống chịu trách nhiệm xử lý các báo cáo kiểm tra khảo sát và đưa ra biện pháp, kế hoạch và triển khai giải quyết các vấn đề trong báo cáo kiểm tra.

6.6 Kiểm soát an ninh quy trình sử dụng

6.6.1 Điều khiển quy trình phát triển hệ thống

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

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

6.6.2 Kiểm soát việc quản lý an toàn, an ninh

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

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

6.7 Giám sát an ninh mạng hệ thống

HILO-CA đều có các biện pháp bảo mật tương ứng với các tiêu chuẩn quy định trong chính sách về bảo mật nhằm ngăn chặn các truy cập trái phép và các hoạt động tấn công khác.

HILO-CA xây dựng hệ thống giao diện quản lý và phần mềm giám sát an ninh đảm bảo được an ninh theo quy định.

6.8 Dán nhãn thời gian

Không sử dụng.

7. ĐỊNH DẠNG CHỨNG THƯ SỐ, DANH SÁCH THU HỒI CHỨNG THƯ SỐ (CRL), GIAO THỨC KIỂM TRA TRẠNG THÁI CHỨNG THƯ SỐ TRỰC TUYẾN (OCSP)

7.1 Định dạng của chứng thu số

Chứng thư số có định dạng X.509 phiên bản 3 (1997) và RFC 5280 - Internet X.509 Public Key Infrastructure Certificate, theo Thông tư 06/2015/TT-BTTTT.

Tối thiểu thành phần chứng thư số phải có như sau:

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

Bảng 2 – Thành phần chứng thư số

7.1.1 Số hiệu phiên bản

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

7.1.2 Các thành phần mở rộng

Cách sử dụng khóa (Key Usage)

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

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

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

Tên thay thế của thuê bao (Subject Alternative Names)

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

Các ràng buộc cơ bản (Basic Constraints)

Không có quy định

Cách sử dụng khóa mở rộng (Extended Key Usage)

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

Điểm công bố danh sách chứng thư số bị thu hồi

Trường cRLDistributionPoints của chứng thư số X.509 phiên bản 3 có chứa địa chỉ URL để người dùng truy cập tới CRL nhằm kiểm tra trạng thái chứng thư số.

Định danh khóa cho HILO-CA

Sẽ xác định sau, theo quy định của RootCA.

Định danh khóa cho thuê bao

Sẽ xác định sau, theo quy định của RootCA.

7.1.3 Số hiệu thuật toán

Chứng thư số của Hilo– CA sử dụng thuật toán sau đây:

+) sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

7.1.4 Định dạng tên

Định dạng tên của chứng thư số tuân theo quy định trong phần 3.1.1

7.1.5 Các ràng buộc về tên

Không có quy định.

7.1.6 Số hiệu của quy chế chứng thực

Số hiệu (OID) của CPS này sẽ được đăng ký khi hệ thống của HILO-CA chính thức đi vào hoạt động.

7.1.7 Sử dụng các ràng buộc quy chế mở rộng

Không có quy định.

7.1.8 Cú pháp và ngữ nghĩa quy chế

Không có quy định.

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

Không có quy định.

7.2 Định dạng danh sách thu hồi chứng thư số (CRL)

CRL cần chứa các giá trị sau đây:

Trường	*Giá trị hoặc yêu cầu*
Version	Xem phần 7.2.1
Signature Algorithm	Thuật toán dùng để ký danh sách chứng thư số bị thu hồi.
Issuer	Thực thể thi hành ký và phát hành danh sách chứng thư số bị thu hồi.
Effective Date	Ngày có hiệu lực của danh sách chứng thư số bị thu hồi. Các CRL có hiệu lực ngay khi phát hành.
Next Update	Ngày cập nhật phiên bản tiếp theo của danh sách chứng thư số bị thu hồi.
Revoked Certificates	Danh các các chứng thư số bị thu hồi, bao gồm số hiệu (Serial Number) của chứng thư số bị thu hồi và ngày thu hồi.

Bảng 3 – Thành phần của CRL

7.2.1 Số hiệu phiên bản của CRL

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

7.2.2 CRL và các mở rộng

Không có quy định.

7.3 Định dạng giao thức kiểm tra trạng thái chứng thư số trực tuyến (OCSP)

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

7.3.1 Số hiệu phiên bản của OCSP

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

7.3.2 Các mở rộng OCSP

Không có quy định.

8. KIỂM ĐỊNH TÍNH TUÂN THỦ VÀ CÁC ĐÁNH GIÁ KHÁC

8.1 Tần suất và các tình huống kiểm tra kỹ thuật

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

Các tình huống kiểm tra kỹ thuật theo kịch bản kiểm tra tùy theo từng thời kỳ hoạt động.

8.2 Đơn vị thực hiện đánh giá chất lượng

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

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

8.3 Các nội dung kiểm tra kỹ thuật

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

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

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

8.4 Xử lý khi phát hiện sai sót

Căn cứ theo kết quả đánh giá và kiểm định, các vấn đề sự cố và thiếu sót phải được chỉ ra và xử lý bởi bộ phận quản lý của HILO-CA.

Nếu vấn đề là do thiết bị không đảm bảo: Lên phương án thay thế ngay thiết bị đáp ứng yêu cầu vận hành hệ thống.

Nếu sai sót ở quy trình quản lý khóa: Rà soát lại toàn bộ quy trình phân công và thực hiện quản lý khóa, ngay lập tức đưa quy trình về hoạt động đúng như CPS quy định.

Nếu sai sót ở quy trình vận hành: Tiến hành rà soát, tư vấn, nâng cấp quy trình vận hành ngay lập tức.

Đối với các nội dung không quá nguy hiểm cho hệ thống: Rà soát và khắc phục ngay khi phát hiện.

HILO-CA cam kết tuân theo các quy trình đề ra để đảm bảo tính an toàn, toàn vẹn và liên tục của hệ thống. Bất kì tổ chức, cá nhân nào gây nguy hại có hệ thống HILO-CA đều phải chịu trách nhiệm trước pháp luật và HILO-CA.

8.5 Công bố kết quả kiểm tra kỹ thuật

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

8.6 Tần suất và các trường hợp đánh giá

Hàng năm, HILO-CA sẽ lên kế hoạch về tần suất và các trường hợp đánh giá để phù hợp với tình hình hoạt động thực tế và quy định của pháp luật.

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

Danh tính và khả năng của đơn vị, người kiểm tra được HILO-CA công bố trong phần công bố kết quả kiểm tra kỹ thuật.

9. CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC

9.1 Phí/Giá

Phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số theo quy định tại Thông tư số 17/2018/TT-BTC ngày 09/02/2018 của Bộ Tài chính sửa đổi, bổ sung một số điều của Thông tư số 305/2016/TT-BTC và Thông tư số 305/2016/TT-BTC ngày 15/11/2016 của Bộ Tài chính 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: HILO-CA thu phần phí này từ thuê bao và có trách nhiệm nộp về cơ quan quản lý có thẩm quyền theo quy định.

Giá cấp, gia hạn, thu hồi chứng thư số: Bảng giá HILO-CA sẽ công bố công khai trên website và các tài liệu kinh doanh. HILO-CA sẽ công bố và gửi email thông báo tới thuê bao hiện hữu trước tối thiểu 30 ngày khi có thay đổi bảng giá.

Các loại chi phí khác (nếu có):

- Thuế VAT mức 10% theo quy định.
- Phí USB Token
- Phí theo thỏa thuận với khách hàng.

9.2 Trách nhiệm tài chính

9.2.1 Nghĩa vụ nộp phí trong quá trình cung cấp dịch vụ

HILO-CA cam kết tuân thủ nghĩa vụ nộp các loại phí trong quá trình cung cấp dịch vụ theo quy định của pháp luật.

9.2.2 Nghĩa vụ tài chính trong trường hợp bị thu hồi giấy phép.

Trường hợp HILO-CA bị thu hồi giấy phép, khoản tiền ký quỹ do HILO-CA thực hiện sẽ được dùng để đền bù thiệt hại cho các bên liên quan và xử lý tiếp quá trình cung cấp dịch vụ.

- Đền bù cho thuê bao: Theo quy định trong hợp đồng
- Đền bù cho các đơn vị khác: Theo kết quả đánh giá thực tế.

9.3 Bảo mật các thông tin nghiệp vụ

9.3.1 Phạm vi của nghiệp vụ cần bảo vệ

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

- Các dữ liệu ứng dụng CA, được phê chuẩn hoặc không phê chuẩn;
- Các dữ liệu ứng dụng chứng thư số;
- Các dữ liệu chuyển đổi (dữ liệu đầy đủ và các dữ liệu kiểm toán của quá trình chuyển đổi);
- Các dữ liệu kiểm định được tạo hoặc lưu giữ bởi HILO-CA hoặc một thuê bao;
- Các báo cáo kiểm định tạo bởi HILO-CA hay thuê bao (cho việc đánh giá những báo cáo này), hoặc những kiểm định viên (nội bộ hoặc bên ngoài);
- Các dự án khôi phục do tai nạn hay khôi phục sau sự cố;
- Quản lý mức độ an ninh trong hoạt động của phần cứng, phần mềm, các quản trị viên của dịch vụ chứng thư số và của các dịch vụ khác.
- Tài liệu hướng dẫn, chuyển giao, đào tạo liên quan đến xây dựng, vận hành hệ thống và quy trình thẩm định của HILO-CA.

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

Chứng thư số, thu hồi chứng thư số và các thông tin về trạng thái của chứng thư số, nơi lưu giữ của HILO-CA cùng các thông tin chứa bên trong chúng không được coi là các thông tin mật/riêng tư. Các thông tin mật/riêng tư trong phần 9.3.1 sẽ không được coi là riêng tư hoặc không được coi là bí mật nếu pháp luật có quy định khác.

9.3.3 Trách nhiệm bảo mật thông tin nghiệp vụ

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

Các đơn vị liên quan khi sử dụng tài liệu trong danh mục bảo mật của HILO-CA cần được sự cho phép của HILO-CA và cam kết không tiết lộ cho bất kì bên nào khác.

9.4 Bảo mật thông tin cá nhân

9.4.1 Phạm vi thông tin bí mật cần bảo vệ

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

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

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

9.4.2 Trách nhiệm bảo mật thông tin cá nhân

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

9.4.3 Thông báo và cho phép sử dụng thông tin riêng tư

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

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

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

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

9.5 Quyền sở hữu trí tuệ

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

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

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

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

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

9.5.2 Quyền sở hữu trong CPS

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

9.5.3 Quyền sở hữu tên

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

9.5.4 Quyền sở hữu khóa và các tài liệu của khóa

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

9.6 Tuyên bố và cam kết

9.6.1 Đại diện của HILO-CA và vấn đề bảo lãnh

Các dịch vụ HILO-CA bảo đảm:

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

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

9.6.2 Đại diện của Hilo-RA và vấn đề bảo lãnh

Các HILO-CA bảo đảm:

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

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

9.6.3 Đại diện cho thuê bao và vấn đề bảo lãnh

Thuê bao cam kết rằng:

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

Hợp đồng dịch vụ giữa HILO-CA với thuê bao có thể có thêm các thỏa thuậnvà cam kết khác.

9.6.4 Đại diện cho người nhận và vấn đề bảo lãnh

Thỏa thuận với người nhận yêu cầu người nhận phải có đủ thông tin để đưa ra một quyết định dựa vào các thông tin trong chứng thư số. Họ có trách nhiệm quyết định tin tưởng hay không vào các thông tin trong chứng thư số. Người nhận phải chịu trách nhiệm pháp lý nếu vi phạm các điều khoản về nghĩa vụ của người nhận quy định trong CPS này.

Thỏa thuận giữa HILO-CA và người nhận có thể bao gồm thêm các tuyên bố và cam kết khác.

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

Không có qui định.

9.7 Từ chối bảo lãnh

Trong giới hạn cho phép của luật pháp, hợp đồng thuê bao và người nhận có thể bị HILO-CA từ chối bảo lãnh nếu lỗi không phải do HILO-CA gây ra.

9.8 Giới hạn trách nhiệm

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

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

9.9 Bồi thường thiệt hại

9.9.1 Vấn đề bồi thường của thuê bao

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

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

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

9.9.2 Vấn đề bồi thường của người nhận

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

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

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

9.10 Hiệu lực của CPS

9.10.1 Hiệu lực của CPS

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

Các điều sửa đổi bổ sung cho CPS này cần được sự đồng ý của ROOT-CA và có hiệu lực khi có sự công bố từ kho lưu trữ của dịch vụ HILO-CA.

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

9.10.2 Kết quả của kết thúc hiệu lực và các tồn tại

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

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

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

Các phiên bản của CPS được HILO-CA lưu và công bố đầy đủ trên website của mình tại link: https://hilo-ca.vn/tailieu

9.12 Bổ sung và sửa đổi

9.12.1 Thủ tục sửa đổi

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

9.12.2 Quy trình sửa đổi, bổ sung quy chế

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

Những đề xuất thay đổi CPS sẽ được nêu ra trong tài liệu của HILO-CA tại địa chỉ: http://www.hilo-ca.vn/tailieu sau khi được Bộ Thông tin truyền thông chấp nhận.

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

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

9.12.3 Thời điểm có hiệu lực

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

9.12.4 Cơ chế xử lý đề xuất

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

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

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

9.12.5 Các trường hợp OID thay đổi

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

9.13 Thủ tục giải quyết tranh chấp

9.13.1 Tranh chấp giữa HILO-CA, đối tác và thuê bao

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

9.13.2 Tranh chấp với thuê bao hay người nhận

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

9.14 Hệ thống pháp lý điều chỉnh

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

- Luật giao dịch điện tử năm 2005;
- Nghị định số 130/2018/NĐ-CP ngày 27/9/2018 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;

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

9.15 Phù hợp với pháp luật hiện hành

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

9.16 Các điều khoản khác

9.16.1 Điều khoản thỏa thuận chung

Không có quy định.

9.16.2 Trách nhiệm

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

9.16.3 Tính độc lập của các điều khoản

Trong trường hợp một điều khoản hay sự sửa đổi bổ sung của CPS được giữ lại không thể thi hành được bởi quy định của pháp luật hoặc quyết định của cơ quan nhà nước có thẩm quyền thì phần còn lại của Quy chế vẫn có hiệu lực.

9.16.4 Sự thực thi (quyền ủy nhiệm và quyền khước từ)

Bất kỳ một bên nào chiếm ưu thế trong những tranh cãi nảy sinh ngoài hợp đồng đều được quyền ủy nhiệm hoặc quyền khước từ do sự vi phạm một trong các điều khoản trong hợp đồng.

9.16.5 Chính sách bắt buộc thực thi

Trong phạm vi luật pháp cho phép, thỏa thuận của thuê bao và thỏa thuận bên liên quan bắt buộc phải tuân theo các điều khoản bảo vệ dịch vụ HILO-CA.

9.17 Các điều khoản khác

Không có quy định.

PHỤ LỤC

Danh mục định nghĩa và thuật ngữ viết tắt

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

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

HILO-CA	Dịch vụ chứng thực chữ ký số công cộng do Công ty cổ phần Dịch vụ T-Van Hilo cung cấp/và Công ty cổ phần Dịch vụ T-Van (Hilo) với tư cách là nhà cung cấp dịch vụ chứng thực chữ ký số công cộng.
Hilo-RA	Tổ chức tiếp nhận yêu cầu cung cấp dịch vụ và xác thực thông tin thuê bao HILO-CA ủy quyền.
Xác thực định danh	là hoạt động nhằm chứng minh thông tin định danh của thuê bao, người yêu cầu cấp chứng thư số.