Phiên bản 1.0 ngày 18/06/2021

QUY CHẾ CHỨNG THỰC
Certificate Practices Statement (CPS)

DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG TỪ XA

*****

Người chịu trách nhiệm chính:

1. *Nguyễn Thanh Tùng*
2. *Nguyễn Ngọc Long*
3. *Tô Thị Hòa*

MỤC LỤC

THUẬT NGỮ VÀ TỪ VIẾT TẮT

TT	Định nghĩa/Từ viết tắt	Giải thích
1	CA	Certificate Authority – Nhà chứng thực chữ ký số, có chức năng ban hành, gia hạn, thu hồi và quản lý chứng thư số.
2	CP	Certificate Policy – Chính sách chứng thư số
3	CPS	Certification Practices Statement – Quy chế chứng thực
4	CRL	Certificate Revocation List – Danh sách các chứng thư số bị thu hồi
5	DC	Digital Certificate – Chứng thư số
6	DES	Data Encryption Standard – Chuẩn mã hóa dữ liệu đối xứng được sử dụng rộng rãi
7	PKI	Public Key Infrastructure - Hạ tầng khóa công khai
8	MISA	Công ty cổ phần MISA
9	MISA-CA	Hệ thống cung cấp dịch vụ chứng thực chữ ký số của Công ty cổ phần MISA
10	HSM	Hardware Security Module – Thiết bị phần cứng bảo mật dùng để tạo, lưu trữ và bảo vệ các khóa sử dụng trong mã hóa. Trong hệ thống PKI, HSM thường được dùng để bảo vệ các cặp khóa quan trọng như các cặp khóa của RootCA và SubCA
11	RSA	Thuật toán mật mã khóa công khai dùng để sinh cặp khóa

12	RootCA	Root Certification Authority – Hệ thống cấp phát chứng thư số mức gốc
14	OCSP	Online Certificate Status Protocol – Giao thức kiểm tra trạng thái chứng thư số trực tuyến
15	LDAP	Lightweight Directory Access Protocol – Giao thức chuẩn truy cập thư mục.
16	Ứng viên	Là một người, một tổ chức hay một thực thể đã đăng ký nhưng chưa được cấp chứng thư số
17	Thuê bao	Là một người, một tổ chức hay một thực thể đã được cấp chứng thư số
18	Đối tác tin tưởng	Là một người, một tổ chức hay một thực thể sử dụng chứng thư số của MISA-CA và các thông tin khác từ kho lưu trữ chứng thư số để xác thực chữ ký số của thuê bao
19	Remote QSCD	Thiết bị lưu khóa bí mật được đặt tại nhà cung cấp dịch vụ được sử dụng để sinh khóa và sử dụng khóa bí mật của thuê bao

1. GIỚI THIỆU

1.1. Tổng quan

MISA-CA là tên gọi của dịch vụ chứng thực chữ ký số công cộng do Công ty cổ phần MISA cung cấp, các quy định về chính sách chứng thư số của dịch MISA-CA được trình bày trong tài liệu này gồm có: Phát hành chứng thư, quản lý, thu hồi và cấp lại chứng thư số cho các thuê bao đầu cuối.

1.2. Nhận dạng tài liệu

Văn bản này là được gọi là quy chế chứng thực (CPS) tuyên bố về mặt nguyên tắc các chính sách quản trị của MISA-CA trong quá trình cung cấp dịch vụ chứng thực chữ ký số. Bản Quy chế chứng thực này đưa ra các yêu cầu luật pháp, các yêu cầu về kỹ thuật, cũng như yêu cầu kinh doanh cho quá trình chấp thuận, cấp phát, quản lý, sử dụng, thu hồi và cấp lại chứng thư số trong hệ thống MISA-CA. Các yêu cầu của Quy chế chứng thực đảm bảo tính bảo mật và toàn vẹn cho dịch vụ MISA-CA, được áp dụng cho tất cả các thành phần tham gia dịch vụ chứng thực chữ ký số.

Mục tiêu của văn bản này là:

◦ Công bố để các bên liên quan biết được nhà cung cấp dịch vụ MISA-CA hoạt động và tuân thủ theo các yêu cầu trong Quy chế chứng thực này.

◦ Giúp cho khách hàng sử dụng dịch vụ MISA-CA biết được quá trình xác thực và trách nhiệm của họ.

◦ Cung cấp thông tin cho đối tác về mức độ đảm bảo của chứng thư MISA-CA cung cấp.

Bản Quy chế chứng thực này được viết dựa theo RFC 3647 về "Khung quy chế chứng thực và chính sách chứng thư số", đáp ứng theo Thông tư 16/2019/TT-BTTTT ngày 05/12/2019 về Quy định Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số.

1.3. Các thành phần tham gia

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

Tổ chức cung cấp dịch vụ – CA là thành phần quan trọng nhất trong hệ thống PKI. CA xác thực thông tin thuê bao cũng như đảm bảo tính bảo mật và toàn vẹn nội dung thông tin mà các thành phần tham gia dịch vục chứng thực chữ ký số công cộng trao đổi thông qua hệ thống của CA.

Mỗi CA là tổng thể hệ thống thiết bị (phần cứng, phần mềm) và những người quản trị hệ thống đó nhằm thực hiện các chức năng chính sau:

- Thẩm định tất cả các yêu cầu cấp phát chứng thư
- Cấp mới, gia hạn, thay đổi thông tin và thu hồi chứng thư số của thuê bao theo quy định của pháp luật và CPS
- Duy trì trực tuyến cơ sở dữ liệu về chứng thư số (còn hiệu lực, hết hạn, gia hạn, cấp mới, thu hồi)
- Cung cấp các dịch vụ khác có liên quan cho người sử dụng
- CA nhất thiết phải đảm bảo thực hiện các chức năng trên một cách trực tiếp

1.3.2. Thuê bao

Thuê bao là tổ chức, cá nhân (đủ điều kiện theo quy định của pháp luật và CPS này) được MISA-CA cấp, chấp nhận chứng thư số và giữ khóa bí mật tương ứng với khóa công khai ghi trên chứng thư số đó.

1.3.3. Người nhận

Người nhận là các tổ chức, cá nhân sử dụng các chức năng của hệ thống MISA-CA để xác thực một chữ ký số và/hoặc giải mã một tài liệu hoặc thông điệp đã được mã hóa nhận được từ thuê bao của MISA-CA.

1.3.4. Các thành phần khác

Không có quy định

1.4. Sử dụng chứng thư số

1.4.1. Chứng thư số hợp lệ

Chứng thư số hợp lệ là tất cả các chứng thư số hợp lệ được sử dụng theo quy định của pháp luật và CPS này.

1.4.1.1. Các loại chứng thư số

Danh sách dưới đây liệt kê tất cả các trường hợp chứng thư dựa trên các thiết lập như sử dụng khoá, chỉ định và giới hạn tính hợp lệ sử dụng một chứng thư số, sử dụng thẻ, tên các thành phần của trường "Key Usage":

- Chứng thư số cho người dùng cá nhân hoặc tổ chức, doanh nghiệp: Chứng thư số được sử dụng cá nhân, cơ quan, tổ chức nhằm mục đích xác nhận danh tính của cá nhân, cơ quan tổ chức đó phục vụ cho các hoạt động như: ký số, xác thực đăng nhập, xác thực tài liệu điện tử.
- Chứng thư số SSL Server, SSL Client: Chứng thư số được sử dụng cho việc xác thực Web Server, mã hóa phiên giao dịch giữa client và server.
- Chứng thư số Code Signing: Chứng thư số được sử dụng để đảm bảo an ninh, an toàn nội dung của mã nguồn được phân phối qua Internet.

Định dạng các loại chứng thư số được mô tả trong mục 7.1 Đặc tả chứng thư số.

1.4.1.2. Thời gian có hiệu lực của chứng thư số

- Chứng thư số cho MISA-CA có hiệu lực theo thời gian quy định của Trung tâm chứng thực điện tử quốc gia.
- Chứng thư số cho thuê bao có hiệu lực từ khi thuê bao được cấp chứng thư.

Tùy theo từng loại chứng thư, thời gian có hiệu lực được quy định theo các mức 1 năm, 2 năm, 3 năm… khác nhau. Mức thời gian hiệu lực của chứng thư số được ghi trên chứng thư số.

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

Ngoài các trường hợp sử dụng chứng thư số hợp lệ và các trường hợp khác vi phạm pháp luật đều không được sử dụng.

1.5. Chính sách quản trị

1.5.1. Tổ chức quản lý văn bản

Công ty cổ phần MISA, Tầng 9 – Tòa nhà TECHNOSOFT, phố Duy Tân, phường Dịch Vọng Hậu, Quận Cầu Giấy, Thành phố Hà Nội.

1.5.2. Địa chỉ liên hệ

Mọi thông tin liên hệ, phản hồi về bản quy chế chứng thực có thể liên hệ với Công ty cổ phần MISA - Tầng 9 – Tòa nhà TECHNOSOFT, phố Duy Tân, Quận Cầu Giấy, Thành phố Hà Nội.

- Email: contact@misaca.vn
- Điện thoại: 024 3795 9595

Các thông tin cập nhật, bổ sung bản quy chế chứng thực sẽ được thông báo trên trang web của MISA-CA tại http://www.misaca.vn.

1.5.3. Đơn vị quyết định tính hợp pháp của CPS

Bộ Thông tin và 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 chứng thực này.

1.5.4. Thủ tục phê chuẩn CPS

Khi có sự thay đổi thông tin trong quy chế chứng thực, MISA-CA phải thông báo bằng văn bản đến Bộ Thông tin và Truyền thông (Trung tâm Chứng thực điện tử quốc gia - RootCA) và phải được sự đồng ý bằng văn bản của Trung tâm Chứng thực điện tử quốc gia đối với các nội dung thay đổi.

1.6. Các định nghĩa và tên viết tắt

Xem ở bảng THUẬT NGỮ VÀ TỪ VIẾT TẮT.

2. TRÁCH NHIỆM CÔNG BỐ VÀ LƯU TRỮ

2.1. Lưu trữ

MISA-CA 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 sau khi chứng thư số hết hiệu lực 7-10 năm . MISA-CA lưu trữ đầy đủ, chính xác, cập nhật danh sách các chứng thư số có hiệu lực và đã hết hiệu lực. Cho phép người sử dụng Internet truy nhập trực tuyến danh sách chứng thư này 24 giờ trong ngày và 7 ngày trong tuần.

2.2. Công bố thông tin chứng thư số

Cơ sở dữ liệu thông tin về chứng thư số của MISA-CA được đảm bảo duy trì thường xuyên, liên tục và công bố các địa chỉ lưu trữ cho phép thuê bao và các thành phần tham gia vào dịch vụ MISA-CA có thể kiểm tra, tra cứu được trạng thái chứng thư số cũng như thông tin về chính sách, Quy chế chứng thực của MISA-CA.

Các thông tin bao gồm:

- Thông tin về chính sách, Quy chế chứng thực chữ ký số công cộng MISA-CA và chứng thư số công khai của MISA-CA tại địa chỉ: http://www.misaca.vn.
- MISA-CA cung cấp dịch vụ để tra cứu thông tin, tình trạng, download chứng thư số do MISA-CA cấp tại địa chỉ: http://tracuucts.misaca.vn bằng giao thức HTTP tuân thủ theo chuẩn X.509 của thông tư 06/2015/TT-BTTTT.
- MISA-CA cung cấp dịch vụ truy xuất thông tin về danh sách chứng thư số đã bị thu hồi tại địa chỉ: http://www.misaca.vn/misaca1.crl bằng giao thức HTTP tuân thủ theo chuẩn RFC 2585 của thông tư 06/2015/TT-BTTTT. Dịch vụ CRL của MISA-CA được cung cấp để truy cập liên tục 24/7.
- MISA-CA cung cấp dịch vụ kiểm tra trạng thái chứng thư số trực tuyến OCSP của MISA-CA tại địa chỉ: http://ocsp1.misaca.vn tuân thủ theo chuẩn RFC 2560 của thông tư 06/2015/TT-BTTTT.
- Các thông tin khác có liên quan (mẫu hợp đồng, chính sách,…) tại địa chỉ: http://www.misaca.vn.

2.3. Thời gian và tần suất công bố

MISA-CA cập nhật các thông tin công bố như sau:

- Quy chế chứng thực chữ ký số, chính sách, thỏa thuận…: được cập nhật khi có sự thay đổi.

2.4. Quản lý truy cập tại các kho lưu trữ

- Các thông tin về chính sách, Quy chế chứng thực chữ ký số được cập nhật và công bố công khai nhưng không cho phép sửa đổi, thay thế tại địa chỉ http://www.misaca.vn. Mọi thay đổi của Quy chế chứng thực chỉ được phép thực hiện bởi cấp có thẩm quyền của MISA-CA và phải được phê duyệt bằng văn bản bởi Bộ Thông tin và Truyền thông (Trung tâm Chứng thực điện tử Quốc gia).
- Sau khi được phê duyệt, Quy chế chứng thực được công bố ngay lập tức bởi hệ thống MISA-CA
- Các thông tin về chứng thư số được cập nhật tự động bởi hệ thống MISA-CA và chỉ cho phép người sử dụng được quyền xem, download và không được phép chỉnh sửa, bổ sung.

3. ĐỊNH DANH VÀ XÁC THỰC

3.1. Tên và các loại tên

3.1.1. Các loại tên

Chứng thư số của thuê bao chứa tên (Distinguished Names) theo chuẩn X.501 trong trường Subject dùng để phân biệt với các chứng thư số của thuê bao khác. Distinguished Names trong chứng thư số là duy nhất đối với một thuê bao. Một thuê bao có thể có nhiều chứng thư số với cùng một Distinguished Names.

Các thuộc tính trong Distinguished Names mà MISA-CA sử dụng được mô tả trong bảng dưới đây:

Thuộc tính	Giá trị
Country (C)	Tên quốc gia theo chuẩn ISO 3166, Việt Nam được ký hiệu là VN
Organization (O)	Tên của tổ chức đối với chứng thư số của tổ chức hoặc chứng thư số của cá nhân thuộc tổ chức. Đối với chứng thư số của cá nhân không thuộc tổ chức nào thì không có trường này.
Organizational Unit (OU)	Tên của đơn vị hoặc phòng ban trong tổ chức. Đối với chứng thư số của cá nhân không thuộc tổ chức nào thì không có trường này.
State or Province (S)	Tên tỉnh, thành phố trực thuộc trung ương nơi cư trú hoặc đóng trụ sở của thuê bao.
Locality (L)	Tên địa phương cấp dưới tỉnh/thành phố trực thuộc trung ương nơi cư trú hoặc đóng trụ sở của thuê bao.
Common Name (CN)	Tên thuê bao sở hữu chứng thư số, tên miền nếu là chứng thư số SSL
E-Mail Address (E)	Địa chỉ email của thuê bao sở hữu chứng thư số

Title (T)	Chức vụ (đối với chứng thư số cá nhân thuộc doanh nghiệp)
UniqueIdentifier(UID)	Mã định danh của thuê bao sở hữu chứng thư số. ● Đối với cá nhân, UID sẽ là số chứng minh thư, căn cước công dân hoặc hộ chiếu ● Đối với doanh nghiệp, UID là Mã số thuế ● Đối với cơ quan tổ chức nhà nước, UID là Mã quan hệ ngân sách

3.1.2. Tính rõ ràng và ý nghĩa của tên trong chứng thư

Tên trong chứng thư số do MISA-CA ban hành cho phép xác định được nhận dạng của đối tượng sở hữu của chứng thư số.

3.1.3. Trường hợp thuê bao sử dụng tên ẩn danh hay biệt hiệu

Chứng thư số không được sử dụng biệt hiệu hoặc nặc danh cho tên. Việc sử dụng biệt hiệu hoặc nặc danh cho tên trong chứng thư số chỉ được thực hiện khi có yêu cầu của pháp luật. Khi này, nội dung tên sẽ không phải kiểm tra.

3.1.4. Quy tắc diễn giải các mẫu tên

Không có quy định.

3.1.5. Tính duy nhất của tên thuê bao

MISA-CA đảm bảo rằng tên của thuê bao là duy nhất trong miền định danh của một CA. Một thuê bao có thể có hai hay nhiều chứng thư số có cùng tên.

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

Người gửi đơn xin cấp chứng thư số không được sử dụng những tên vi phạm quyền sở hữu trí tuệ. Tuy nhiên MISA-CA không tổ chức phân xử bất cứ tranh chấp về sở hữu trí tuệ đối với tên miền, thương hiệu, nhãn hiệu của dịch vụ. Nếu có sự tranh chấp xảy ra về sở hữu thì MISA-CA sẽ có quyền thu hồi, tạm dừng chứng thư số hay loại bỏ đơn xin cấp chứng thư số.

3.2. Xác thực trong quá trình cấp mới

3.2.1. Phương pháp chứng minh sở hữu khóa bí mật

Để chứng minh thuê bao được cấp chứng thư số sở hữu khóa bí mật của họ, MISA-CA đảm bảo các thuê bao gửi yêu cầu cấp chứng thư số theo chuẩn PKCS#10 chứa các thông tin định danh của thuê bao được ký bởi khóa bí mật của thuê bao đó.

3.2.2. Xác thực định danh cho tổ chức

Tổ chức khi tiến hành xin cấp chứng thư số do MISA-CA cấp phải chịu trách nhiệm về tính chính xác của các tài liệu, thông tin do mình cung cấp.

MISA-CA sẽ xác thực các thông tin bắt buộc sau:

- Tổ chức xin cấp chứng thư số phải nộp các văn bản chứng minh định danh bao gồm:

o 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; thông tin về website,

o 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

o Căn cứ các thông tin của tổ chức trong các văn bản trên, MISA-CA xác minh sự tồn tại của tổ chức và người đại diện theo pháp luật của tổ chức bằng cách: Kiểm tra, đối chiếu với các thông tin được các cơ quan ban hành các văn bản trên như Tổng cục/Cục thuế, Bộ/Sở Kế hoạch và Đầu tư đối với tổ chức là doanh nghiệp hoặc cơ quản chủ quản đối với các tổ chức nhà nước hoặc tổ chức xã hội; Kiểm tra trụ sở của tổ chức đảm bảo sự hiện diện tại địa điểm được ghi trong hồ sơ xin cấp chứng thư số ở trên. Trong một số trường hợp cần làm rõ, MISA-CA sẽ xác thực bổ sung bằng cách gọi điện hoặc xác thực trực tiếp tại tổ chức.

- Khi chứng thư số của tổ chức có chứa tên cá nhân làm đại diện, cần thực hiện các thủ tục xác thực sự ủy quyền như quy định tại mục 3.2.5

3.2.3. Xác thực định danh cá nhân

Người sử dụng khi đăng ký cấp chứng thư số tại MISA-CA phải chịu trách nhiệm về tính chính xác của các tài liệu, thông tin do mình cung cấp.

Định danh của cá nhân bao gồm các thông tin: Tên cá nhân, địa chỉ, chứng minh nhân dân hoặc căn cước công dân hoặc hộ chiếu, địa chỉ thư điện tử; thông tin về website, quyền sở hữu tên miền của cá nhân (dùng cho việc cấp chứng thư số SSL). MISA-CA thực hiện xác thực thông tin định danh trên đúng với cá nhân sử dụng chứng thư số bằng cách gặp trực tiếp hoặc các biện pháp tương đương.

3.2.4. Thông tin thuê bao không được xác minh

Mọi thông tin trong hồ sơ thuê bao đều được xác minh theo quy định tại điểm a khoản 1 Điều 25 Nghị định số 130/2018/NĐ-CP.

3.2.5. Xác thực ủy quyền

Khi chứng thư số của tổ chức có chứa tên cá nhân làm đại diện, MISA-CA cần thực hiện các thủ tục xác thực sự ủy quyền như sau:

- Xác thực sự tồn tại của tổ chức như 3.2.2
- Xác thực cá nhân như 3.2.3 và xác thực sự ủy quyền của tổ chức đối với cá nhân đó bằng giấy ủy quyền. Người uỷ quyền trong giấy ủy quyền phải là người chịu trách nhiệm trước pháp luật đối với doanh nghiệp, hoặc quyết định bổ nhiệm hoặc quyết định giao nhiệm vụ hoặc giấy tờ tương đương đối với tổ chức không phải là doanh nghiệp.
- Trong một số trường hợp cần làm rõ, MISA-CA sẽ xác thực bổ sung bằng cách gọi điện hoặc xác thực trực tiếp tại tổ chức về cá nhân đó

3.2.6. Quy định về việc liên thông

MISA-CA tuân thủ các quy định về liên thông do Bộ Thông tin và Truyền thông ban hành.

3.3. Xác thực định danh cho yêu cầu thay đổi khóa

3.3.1. Xác thực định danh yêu cầu thay đổi khóa thông thường

Xác thực định danh yêu cầu thay đổi khóa thông thường giống như xác thực định danh cấp mới quy định tại mục 3.2.

3.3.2. Xác thực định danh yêu cầu thay đổi khóa sau khi thu hồi

Đối với các thuê bao sau khi bị thu hồi chứng thư số nếu muốn xin cấp mới chứng thư số khác để sử dụng thì ngoài các nội dung tài liệu phải cung cấp theo quy định

đối với trường hợp cấp chứng thư số mới, thuê bao phải cung cấp thêm các thông tin như sau:

- Lý do bị thu hồi chứng thư số
- Cam kết thực hiện các yêu cầu về giải quyết các lý do bị thu hồi

Việc xác thực định danh sẽ giống như xác thực định danh cấp mới quy định tại mục 3.2.

Các trường hợp sau sẽ không được cấp lại chứng thư số sau khi đã bị thu hồi:

- Thuê bao sử dụng chứng thư số đã được cấp vào các mục đích trái pháp luật
- Thuê bao sử dụng các thông tin giả mạo để xin cấp chứng thư số
- Thuê bao sử dụng chứng thư số do MISA-CA cấp vào các hoạt động có thể ảnh hưởng tới uy tín của MISA-CA

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

Thủ tục thu hồi ưu tiên cho những trường hợp thuê bao yêu cầu thu hồi chứng thư số. Trong một số trường hợp chứng thu số bị thu hồi với lý do từ MISA-CA hoặc các cơ quan công quyền như:

- MISA-CA có căn cứ để khẳng định rằng chứng thư số được cấp không tuân theo các quy định trong Quy chế chứng thực hoặc khi phát hiện ra bất cứ sai sót nào có ảnh hưởng đến quyền lợi của thuê bao và người nhận
- Khi có yêu cầu của cơ quan công quyền
- Theo điều kiện thu hồi chứng thư số đã được quy định trong hợp đồng giữa 2 bên
- Thủ tục duyệt cho xác thực yêu cầu thu hồi của một đăng ký bao gồm:
- Thuê bao cần chứng tỏ được quyền sở hữu khóa bí mật và chứng thư số của mình bằng các phương pháp xác thực đã nêu ở trên
- MISA-CA cũng có thể xác thực yêu cầu thu hồi chứng thư số từ thuê bao thông qua việc gọi điện thoại, fax, gửi email hoặc gặp trực tiếp (nếu có thể)

MISA-CA cũng có thể thực hiện thu hồi khi nhận được một thông điệp từ thuê bao yêu cầu thu hồi và chứa một chữ ký điện tử có thể được kiểm tra bằng chứng thư số bị thu hồi.

3.5. Xác thực khi mất phương tiện xác thực

Trong trường hợp thuê bao bị mất phương tiện xác thực: số điện thoại, email … thì liên hệ vào tổng đài tư vấn của MISA-CA và xác thực bằng câu hỏi bảo mật hoặc sử dụng hình thức khác để xác thực.

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

4.1. Cấp chứng thư số

4.1.1. Đối tượng được phép yêu cầu cấp chứng thư số

Đối tượng được phép yêu cầu cấp chứng thư số gồm:

- Bất cứ cá nhân nào đủ điều kiện theo quy định của pháp luật và CPS này có nhu cầu sử dụng chứng thư số
- Đại diện theo pháp luật của tổ chức đủ điều kiện theo quy định của pháp luật và CPS này có nhu cầu sử dụng chứng thư số

4.1.2. Quy trình đăng ký và trách nhiệm các bên

Các yêu cầu đăng ký chứng thư số là biểu hiện sự đồng ý với thỏa thuận giữa thuê bao và MISA-CA. Quá trình đăng ký gồm các bước sau:

- Thuê bao nộp đơn cấp chứng thư số theo mẫu của MISA-CA và gửi kèm các giấy tờ theo yêu cầu ở mục 3.2
- Cá nhân, 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
- Thuê bao sử dụng ứng dụng mobile gửi thông tin đăng ký đến MISA-CA
- MISA-CA tiếp nhận thẩm định hồ sơ, xử lý và gửi thông tin xác nhận đến khách hàng thông qua ứng dụng mobile
- Khách hàng kiểm tra và xác nhận thông tin đăng ký chứng thư số qua ứng dụng mobile để thực hiện việc tạo khóa và cấp chứng thư
- MISA-CA tạo cặp khóa thông qua thiết bị phần cứng mã hóa an toàn HSM CP5 và tạo CSR tương ứng với thông tin đăng ký của khách hàng.
- Hệ thống MISA-CA sẽ thực hiện tạo chứng thư số mới cho thuê bao.

4.2. Quy trình xử lý cấp chứng thư số

4.2.1. Thực hiện các chức năng nhận dạng và xác thực

MISA-CA sẽ thực hiện nhận dạng và xác thực trong quá trình cấp chứng thư số

MISA-CA sẽ không cấp chứng thư số cho đến khi mọi thông tin cần thiết của thuê bao cung cấp theo mục 3.2 là chính xác.

4.2.2. Chấp nhận hay từ chối các yêu cầu đăng ký

MISA-CA sẽ chấp nhận một yêu cầu đăng ký nếu các tiêu chuẩn sau đây thỏa mãn:

- Nhận dạng và xác thực thành công mọi thông tin trong yêu cầu đăng ký theo mục 3.2.2 và 3.2.3
- Nhận được các khoản phí cần thiết

MISA-CA sẽ từ chối một yêu cầu đăng ký nếu:

- Không thể xác minh thông tin thuê bao theo mục 3.2.2 và 3.2.3
- Thuê bao không hoàn thành hồ sơ theo như yêu cầu
- Thuê bao không thanh toán theo quy định
- Có lý do tin tưởng rằng cung cấp chứng thư số cho thuê bao này được sử dụng trong các hoạt động phạm pháp hoặc các hoạt động có thể gây hại cho hệ thống MISA-CA

4.2.3. Thời gian xử lý một yêu cầu đăng ký

MISA-CA bắt đầu xử lý những yêu cầu cấp chứng thư số trong một khoảng thời gian được xác nhận hợp lý và không muộn hơn 03 ngày, trừ khi xảy ra sự cố và phải khắc phục theo quy định hoặc xảy ra sự kiện bất khả kháng theo quy định của pháp luật. Không có quy định về thời gian hoàn thành xử lý của một yêu cầu cấp chứng thư số trừ khi nó được quy định trong thỏa thuận liên quan, Quy chế chứng thực hay các thỏa thuận khác giữa các thành viên của hệ thống MISA-CA.

4.3. Phát hành chứng thư số

4.3.1. Hoạt động của MISA-CA khi phát hành chứng thư số

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

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

MISA-CA sẽ thông báo cho thuê bao về việc đã tạo xong chứng thư số và cho phép thuê bao truy xuất chứng thư số bằng cách thông báo với họ rằng chứng thư số đã có hiệu lực và cách thức để lấy.

4.4. Chấp nhận chứng thư số

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

Sau khi nhận được thông báo từ MISA-CA, thuê bao thực hiện xác nhận các thông tin trong chứng thư số được cấp là chính xác.

4.4.2. Công bố chứng thư số

MISA-CA sẽ công bố chứng thư số đã cấp cho thuê bao trên cơ sở dữ liệu về chứng thư số của mình sau khi có xác nhận của thuê bao về tính chính xác của thông tin trên chứng thư số đó, thời hạn để công bố chậm nhất là 24 giờ sau khi đã có xác nhận của thuê bao, trừ trường hợp có thỏa thuận khác.

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

Thông báo việc cấp phát chứng thư số thuê bao đến các tổ chức, cá nhân khác được thực hiện bằng cách công bố chứng thư số thuê bao trên hệ thống trực tuyến về chứng thư số của MISA-CA.

4.5. Sử dụng cặp khóa và chứng thư số

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

Khóa bí mật tương ứng với chứng thư số sẽ lưu trong thiết bị phần cứng an toàn HSM và được phép sử dụng nếu thuê bao đã đồng ý tham gia vào thỏa thuận với MISA-CA và đã chấp nhận chứng thư số được cấp. Chứng thư số sẽ được sử dụng hợp pháp phù hợp với thỏa thuận với MISA-CA và các điều khoản của MISA-CA/Quy chế chứng thực. Mục đích sử dụng chứng thư số phải nhất quán với trường Key Usage trong chứng thư số.

Các thuê bao phải bảo vệ khóa bí mật khỏi việc sử dụng trái phép và ngừng sử dụng khóa bí mật nếu chứng thư số bị hết hạn hay bị thu hồi.

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

Trước khi chấp nhận chữ ký số của người ký, người nhận phải kiểm tra các thông tin sau:

- Trạng thái chứng thư số, phạm vi sử dụng, giới hạn trách nhiệm và các thông tin trên chứng thư số của người ký
- Chữ ký số phải được tạo bởi khóa bí mật tương ứng với khóa công khai trên chứng thư số của người ký

Người nhận phải thực hiện quy trình kiểm tra như sau:

- Kiểm tra trạng thái chứng thư số của người ký tại thời điểm thực hiện ký số, phạm vi sử dụng (trường KeyUsage trên chứng thư), giới hạn trách nhiệm và các thông tin trên chứng thư số đó nhằm đảm bảo chứng thư số của người ký còn hiệu lực thông qua dịch vụ tra cứu thông tin, tình trạng chứng thư số do MISA-CA cấp tại địa chỉ: http://tracuucts.misaca.vn/, danh sách chứng thư số đã bị thu hồi tại địa chỉ http://tracuucts.misaca.vn/misaca1.crl hoặc dịch vụ kiểm tra trạng thái chứng thư số trực tuyến tại địa chỉ http://ocsp1.misaca.vn.
- Kiểm tra trạng thái chứng thư số của MISA-CA tại thời điểm thực hiện ký số trên hệ thống của Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia (RootCA) tại địa chỉ: http://www.rootca.gov.vn/.

Chữ ký số trên thông điệp dữ liệu chỉ có hiệu lực khi kết quả kiểm tra tại các mục trên đồng thời có hiệu lực.

Người nhận phải chịu trách nhiệm khi không tuân thủ quy trình kiểm tra trên hoặc đã thực hiện kiểm tra và biết rằng chứng thư số không còn hiệu lực tại thời điểm ký mà vẫn chấp nhận thông điệp dữ liệu được ký số đó.

4.6. Gia hạn chứng thư số

Gia hạn chứng thư số là việc cấp phát một chứng thư số mới cho thuê bao mà không thay đổi cặp khóa và thông tin khác trong chứng thư số.

Trường hợp thay đổi khóa công khai trên chứng thư số được gia hạn được thực hiện như trường hợp cấp mới chứng thư số.

4.6.1. Điều kiện gia hạn chứng thư số

Trước khi hết hạn ít nhất 30 ngày MISA-CA sẽ thông báo về thời gian còn hiệu lực của chứng thư số cho khách hàng để khách hàng có thể biết thông tin và thực hiện gia hạn chứng thư số khi có nhu cầu tiếp tục sử dụng dịch vụ. Nếu thuê bao vẫn muốn tiếp tục sử dụng thì có thể thực hiện các thủ tục để tiến hành gia hạn chứng thư số trước khi hết hiệu lực.

4.6.2. Đối tượng được phép yêu cầu gia hạn

Các thành phần sau đây có thể yêu cầu gia hạn chứng thư số, bao gồm:

- Đối với thuê bao là cá nhân: chính cá nhân đó mới có quyền đề nghị gia hạn chứng thư số.
- Đối với thuê bao là tổ chức: chỉ có người đại diện hợp pháp cho tổ chức hoặc người được uỷ quyền hợp pháp của tổ chức mới có quyền gia hạn chứng thư số.

4.6.3. Xử lý yêu cầu gia hạn chứng thư số

Sau khi thuê bao điền đầy đủ các thông tin yêu cầu gia hạn chứng thư số, MISA-CA có trách nhiệm tiếp nhận, xác thực thông tin của thuê bao.

Trường hợp xác thực thông tin của thuê bao là chính xác thì MISA-CA thực hiện gia hạn cho thuê bao.

Trường hợp thông tin thuê bao chưa chính xác thì MISA-CA sẽ thông báo cho khách hàng biết để sửa và gửi lại yêu cầu gia hạn.

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

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

4.6.5. Điều khoản chấp nhận gia hạn chứng thư số

Tương tự như sự chấp nhận chứng thư số được cấp mới.

4.6.6. Công bố chứng thư số được gia hạn

Tương tự như công bố chứng thư số được cấp mới.

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

Tương tự như thông báo chứng thư số được cấp mới.

4.7. Thay đổi khóa chứng thư số

Đổi khóa là quá trình ban hành chứng thư số mới với một cặp khóa mới, thông tin khác trong chứng thư số không bị thay đổi.

4.7.1. Điều kiện thay đổi khóa

Một chứng thư số có thể được đổi khóa sau khi đã hết hạn hoặc trong trường hợp cần đổi khóa khẩn cấp đối với chứng thư (bị lộ khóa bí mật, bị mất khóa bí mật hoặc khóa bí mật bị sử dụng trái phép, thay đổi thông tin chứng thư…).

4.7.2. Đối tượng được phép yêu cầu thay đổi khóa

Chỉ đối tượng đăng ký chứng thư số mới có quyền yêu cầu đổi khóa của chứng thư số đó.

Đối với thuê bao là cá nhân: chính cá nhân đó mới có quyền đề nghị yêu cầu thay đổi cặp khoá chứng thư số.

Đối với thuê bao là tổ chức: chỉ có người đại diện hợp pháp cho tổ chức hoặc người được uỷ quyền hợp pháp của tổ chức mới có quyền yêu cầu thay đổi cặp khoá cho chứng thư số.

4.7.3. Xử lý yêu cầu thay đổi khóa

Sau khi thuê bao điền đầy đủ các thông tin yêu cầu thay đổi khoá, MISA-CA có trách nhiệm tiếp nhận, xác thực thông tin của thuê bao.

Trường hợp xác thực thông tin của thuê bao là chính xác thì MISA-CA thực hiện thay đổi khoá cho thuê bao.

Trường hợp thông tin thuê bao chưa chính xác thì MISA-CA sẽ thông báo cho khách hàng biết để sửa và gửi lại yêu cầu thay đổi khoá.

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

Tương tự như thông báo chứng thư số được cấp mới.

4.7.5. Điều khoản chấp nhận thay khóa chứng thư số

Tương tự như sự chấp nhận chứng thư số được cấp mới.

4.7.6. Công bố chứng thư số đã thay khóa

Tương tự như công bố chứng thư số được cấp mới.

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

Tương tự như thông báo chứng thư số được cấp mới.

4.8. Thay đổi thông tin chứng thư số

4.8.1. Điều kiện thay đổi thông tin chứng thư số

Khi thuê bao có nhu cầu thay đổi thông tin trên chứng thư số đang sử dụng của thuê bao mà không thay đổi khóa chứng thư số.

4.8.2. Đối tượng được phép yêu cầu thay đổi thông tin chứng thư số

Chỉ thuê bao của một chứng thư số cá nhân hay được ủy quyền đại diện cho tổ chức mới có thể yêu cầu thay đổi thông tin chứng thư số.

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

Sau khi thuê bao điền đầy đủ các thông tin yêu cầu thay đổi thông tin chứng thư số theo mẫu do MISA-CA ban hành và gửi đến bộ phận MISA-CA thì bộ phận MISA-CA có trách nhiệm tiếp nhận, xác thực thông tin của thuê bao.

Trường hợp xác thực thông tin của thuê bao là chính xác thì MISA-CA sẽ chuyển yêu cầu này về bộ phận MISA-CA để tiến hành thay đổi thông tin chứng thư số cho thuê bao.

Trường hợp thông tin thuê bao chưa chính xác thì sẽ có trách nhiệm thông báo cho khách hàng biết lý do từ chối cho khách hàng.

4.8.4. Thông báo cho thuê bao về việc thay đổi thông tin chứng thư số

Tương tự như thông báo chứng thư số được cấp mới.

4.8.5. Điều khoản chấp nhận thay đổi thông tin chứng thư số

Tương tự như sự chấp nhận chứng thư số được cấp mới.

4.8.6. Công bố chứng thư số đã thay đổi

Tương tự như sự công bố chứng thư số được cấp mới.

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

Tương tự như thông báo chứng thư số được cấp mới.

4.9. Tạm dừng và thu hồi chứng thư số

4.9.1. Các trường hợp thu hồi chứng thư số

Chứng thư số bị thu hồi khi có yêu cầu của chính thuê bao, MISA-CA hoặc các cơ quan nhà nước có thẩm quyền (như cơ quan tố tụng, cơ quan công an hoặc Bộ Thông tin và Truyền thông). Nếu chứng thư số bị thu hồi, thông tin chứng thư số bị thu hồi sẽ được công bố lên danh sách chứng thư số bị thu hồi (CRL) và cập nhật vào dịch vụ cung cấp trạng thái chứng thư số trực tuyến (OCSP) của MISA-CA.

Chứng thư số bị thu hồi trong những trường hợp sau:

- Khi thuê bao yêu cầu bằng văn bản và yêu cầu này đã được MISA-CA 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 MISA-CA

4.9.2. Đối tượng có thể yêu cầu thu hồi chứng thư số

- Đối với thuê bao là cá nhân: chính cá nhân đó mới có quyền đề nghị yêu cầu thu hồi chứng thư số.
- Đối với thuê bao là tổ chức: chỉ có người đại diện cho tổ chức đã được uỷ quyền đứng tên trên chứng thư số mới có quyền yêu cầu thu hồi chứng thư số.
- MISA-CA có thể thu hồi chứng thư số trong trường hợp phát hiện thuê bao thực hiện không đúng hợp đồng, vi phạm pháp luật
- Cơ quan nhà nước có thẩm quyền (như cơ quan tố tụng, cơ quan công an hoặc Bộ Thông tin và Truyền thông).

4.9.3. Thủ tục yêu cầu thu hồi chứng thư số

Ngay khi có những yêu cầu cần thu hồi chứng thư số, MISA-CA tiến hành xác minh trực tiếp với thuê bao, hồ sơ thuê bao và phía yêu cầu thu hồi để đảm bảo đúng đối tượng cần thu hồi trước khi MISA-CA thực hiện chính thức thu hồi.

4.9.4. Thời gian tiến hành yêu cầu thu hồi

Yêu cầu thu hồi sẽ được thực hiện càng sớm càng tốt.

4.9.5. Thời gian xử lý đề nghị thu hồi

Chứng thư số bị thu hồi ngay lập tức, sau khi MISA-CA xác thực các thông tin thu hồi.

4.9.6. Yêu cầu kiểm tra việc thu hồi cho người nhận

Sử dụng các chứng thư số của thuê bao bị thu hồi có thể làm tổn hại hoặc gây hậu quả đến nghiêm trọng tùy theo từng ứng dụng và mục đích sử dụng. Vì vậy, trước khi tin vào chứng thư số của một thuê bao, người nhận phải thực hiện kiểm tra tình trạng chứng thư số thông qua danh sách chứng thư số bị thu hồi (CRL) hoặc dịch vụ kiểm tra trạng thái chứng thư số trực tuyến (OCSP) của MISA-CA quy định tại Mục 2.2. MISA-CA sẽ cung cấp cho người nhận thông tin kiểm tra danh bạ, CRL và OCSP trực tuyến hỗ trợ kiểm tra trạng thái một chứng thư số.

Nếu thông tin thu hồi cho thấy một chứng thư số tạm thời không được sử dụng thì bên nhận phải từ chối sử dụng chứng thư số đó hoặc có quyết định đúng đắn và chấp nhận rủi ro xảy ra.

4.9.7. Tần suất cập nhật chứng thư số bị thu hồi

Tần suất MISA-CA sẽ cập nhật CRL như sau:

- Tự động cập nhật CRL mỗi ngày 1 lần tính từ thời điểm cập nhật trước đó khi không có sự thay đổi.

4.9.8. Thời gian trễ lớn nhất của CRL

Thời gian trễ giữa việc cập nhật CRL và công bố CRL là không quá 24 giờ.

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

MISA-CA hỗ trợ kiểm tra trực tuyến trạng thái chứng thư số bị thu hồi OCSP ở mục 2.2.

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

MISA-CA cung cấp dịch vụ kiểm tra trực tuyến chứng thư số bị thu hồi OCSP theo quy chuẩn RFC 2560.

4.9.11. Mẫu quảng bá chứng thư số bị thu hồi khác

Không có quy định.

4.9.12. Các điều kiện đặc biệt khi khóa bị xâm phạm

Các thuê bao của MISA-CA sẽ được thông báo trong trường hợp khóa bí mật của CA bị lộ. MISA-CA có trách nhiệm báo cho RootCA và tiến hành xin cấp lại khóa mới để đảm bảo an toàn, bảo mật cho dịch vụ.

4.9.13. Các trường hợp tạm dừng

MISA-CA sẽ tạm dừng chứng thư số của thuê bao khi đang xử lý việc thu hồi chứng thư số của thuê bao

MISA-CA có thể tạm dừng chứng thư số trong trường hợp phát hiện thuê bao thực hiện không đúng hợp đồng, vi phạm pháp luật

4.9.14. Đối tượng được phép yêu cầu tạm dừng

Đối với thuê bao là cá nhân: chính cá nhân đó mới có quyền đề nghị yêu cầu tạm dừng chứng thư số.

Đối với thuê bao là tổ chức: chỉ có người đại diện cho tổ chức đã được uỷ quyền đứng tên trên chứng thư số mới có quyền yêu cầu thu hồi chứng thư số.

MISA-CA có thể tạm dừng chứng thư số trong trường hợp phát hiện thuê bao thực hiện không đúng hợp đồng, vi phạm pháp luật

Cơ quan nhà nước có thẩm quyền (như cơ quan tố tụng, cơ quan công an hoặc Bộ Thông tin và Truyền thông).

4.9.15. Thủ tục yêu cầu tạm dừng

Chứng thư số bị tạm dừng ngay lập tức, sau khi MISA-CA xác thực các thông tin tạm dừng.

4.9.16. Giới hạn về thời gian tạm dừng

Ngay sau khi kết thúc thẩm định yêu cầu.

4.10. Dịch vụ kiểm tra trạng thái chứng thư số

4.10.1. Đặc điểm hoạt động

Trạng thái của chứng thư số được công bố qua CRL và OCSP.

4.10.2. Tính sẵn sàng của dịch vụ

Dịch vụ kiểm tra trạng thái chứng thư số được duy trì 24/7. Nếu có gián đoạn sẽ có thông báo trước.

4.10.3. Các tính năng tùy chọn

Không có quy định.

4.11. Kết thúc thuê bao

Sự kết thúc thuê bao có hiệu lực trong các trường hợp sau:

- Thuê bao đã hết hạn mà không gia hạn
- Thu hồi chứng thư số xảy ra mà không xin cấp một chứng thư số mới

4.12. Ủy thác và phục hồi khóa

4.12.1. Chính sách ủy thác và khôi phục khóa

Không có quy định.

4.12.2. Chính sách và thực hiện phục hồi và đóng gói khóa phiên.

Không có quy định.

5. VẤN ĐỀ AN TOÀN, AN NINH CƠ SỞ

5.1. An toàn về mặt vật lý

5.1.1. Vị trí đặt và xây dựng hệ thống

Hệ thống thiết bị MISA-CA được đặt tại Trung tâm dữ liệu được trang bị nhiều lớp bảo vệ khác nhau: bảo vệ vật lý vòng ngoài của tòa nhà, bảo vệ khu đặt thiết bị, bảo vệ tủ đặt thiết bị, bảo vệ chống cháy nổ nhằm ngăn ngừa và phát hiện truy nhập trái phép vào hệ thống hoặc tiết lộ các thông tin hệ thống một cách bất hợp pháp.

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

5.1.2. Truy cập vật lý

- Khi vào TTDL thì nhân viên phải xuất trình giấy tờ cho bảo vệ tòa nhà TTDL như CMND, thẻ căn cước, hộ chiếu để làm thủ tục vào.
- Nhân viên được phân công quản trị hệ thống CA chỉ được quyền truy cập phòng máy đã được phân quyền ra vào ở khu vực đó và phải có người của TTDL dẫn đi.
- Khi đưa thiết bị vào/ra khỏi TTDL thì phải xuất trình giấy đề nghị mang tài sản vào/ra TTDL đã được lãnh đạo có thẩm quyền của MISA-CA phê duyệt.
- Toàn bộ khu vực xung quanh đặt thiết bị của hệ thống MISA-CA đều được lắp đặt hệ thống camera an ninh 24/7.
- Mỗi tủ rack chứa thiết bị của MISA-CA tách riêng với các hệ thống khác và đều có khóa tủ rack riêng bằng chìa khóa vật lý.
- Quyền truy nhập hệ thống chỉ được trao cho những người có trách nhiệm quản trị và theo dõi hệ thống. Do đó, những người không đủ thẩm quyền, nếu có vượt qua được hệ thống bảo vệ cũng không có khả năng truy nhập vào hệ thống.
- Tất cả mọi truy cập đều được ghi nhận.

5.1.3. Điều kiện về nguồn điện và hệ thống làm mát

Hệ thống nguồn điện cung cấp cho hệ thống MISA-CA đảm bảo luôn liên tục, không bị gián đoạn truy cập, được thực hiện theo:

- Sử dụng hệ thống UPS có khả năng duy trì nguồn điện tối thiểu 30 phút
- Có máy phát điện dự phòng, tự động chuyển từ điện lưới sang điện máy phát, hệ thống máy phát điện được kiểm tra bảo dưỡng định kỳ để đảm bảo tính sẵn sàng cao nhất
- Có đầy đủ các hệ thống làm mát chuyên dụng để kiểm soát nhiệt độ và độ ẩm

5.1.4. Phòng chống nước

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

5.1.5. Phòng cháy, chữa cháy

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

5.1.6. Phương tiện lưu trữ

Phương tiện lưu trữ dữ liệu của MISA-CA được bảo vệ tương đương với mức độ quan trọng của dữ liệu mà hệ thống đó lưu trữ.

Phương tiện lưu trữ dữ liệu tại hệ thống dự phòng cũng được bảo vệ tương tự như hệ thống chính.

5.1.7. Tiêu huỷ rác

Các tài liệu và tài nguyên nhạy cảm cần được cắt thành từng miếng vụn trước khi hủy. Các phương tiện thu thập hay truyền các thông tin nhạy cảm cần được làm cho không thể truy cập được trước khi tiêu hủy. Các thiết bị dùng để mã hóa được phá hủy về mặt vật lý theo hướng dẫn của nhà sản xuất trước khi tiêu hủy. Các loại rác khác được tiêu hủy đạt yêu cầu về tiêu hủy rác thông thường của MISA-CA.

5.1.8. Hệ thống dự phòng

Hệ thống dự phòng cho dịch vụ MISA-CA được xây dựng về mặt chức năng giống như hệ thống chính thức và được đặt cách xa hệ thống chính thức tối thiểu 30 km.

Hệ thống này duy trì hoạt động thông suốt và đồng bộ thường xuyên với hệ thống chính.

5.2. Các thủ tục kiểm soát

5.2.1. Người tin cậy

Các thành viên của MISA-CA đều được sử dụng nhân sự đảm bảo tin cậy và được đào tạo kiểm tra thường xuyên.

Người được tin cậy là những người có thể truy cập hay điều khiển các thao tác xác thực, mã hóa, liên quan đến:

- Xác minh các thông tin trong hồ sơ cấp chứng thư số
- Chấp nhận, từ chối, hay các xử lý khác đối với yêu cầu cấp chứng thư số, yêu cầu thu hồi hoặc gia hạn chứng thư số
- Chuyển giao, thu hồi chứng thư số
- Quản lý thông tin thuê bao, thông tin yêu cầu từ thuê bao

Người được tin tưởng bao gồm nhưng không giới hạn các đối tượng sau:

- Người đứng đầu hệ thống CA
- Người vận hành, cấp chứng thư số
- Người quản trị hệ thống
- Người đảm bảo an toàn, an ninh hệ thống
- Người kiểm toán hệ thống kỹ thuật
- Người chuyển giao, thu hồi chứng thư số

Những người được tin tưởng đều được xác minh về nhân thân, khả năng chuyên môn và kinh nghiệm cần thiết để đảm bảo đáp ứng yêu cầu công việc cũng như các bằng chứng trong sạch không tiền án, tiền sự, thông thường, cần thiết thực hiện các dịch vụ chứng thực cá nhân dựa vào chính quyền sở tại.

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

MISA-CA thiết lập, duy trì và có các yêu cầu nghiêm ngặt về thủ tục điều khiển để đảm bảo sự phân công nhiệm vụ dựa trên khả năng làm việc và đảm bảo rằng nhiều người được tin cậy sẽ cùng thực hiện các công việc có tính chất nhạy cảm.

Chính sách và thủ tục được thực hiện để đảm bảo sự phân công nhiệm vụ dựa trên khả năng làm việc. Những công việc mang tính nhạy cảm cao, chẳng hạn truy cập

và quản lý hệ thống phần cứng mã hoá và các công việc liên quan đến khóa, yêu cầu nhiều người được tin tưởng tham gia.

Những thủ tục điều khiển ở bên trong được thiết kế để đảm bảo ít nhất 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 huỷ về logic và/hoặc về vật lý. Mỗi một lần module này được kích hoạt trong các thao tác liên quan đến khóa, các truy cập xa hơn nữa sẽ bị thu hồi để duy trì việc phân cách giữa điều khiển các truy cập ở mức vật lý và mức logic tới thiết bị. Những người có truy cập vật lý tới các module không giữ thông tin cho phép truy cập vào hệ thống và ngược lại.

5.2.3. Xác thực định danh các vai trò

Mọi cá nhân trước khi trở thành người được tin tưởng trong hệ thống MISA-CA đều phải được xác minh nhân thân, nhận dạng và trình độ theo các thủ tục được đưa ra trong Quy chế chứng thực.

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

5.2.4. Phân chia trách nhiệm giữa các vị trí

Các vị trí nhân sự phải được phân công trách nhiệm, bao gồm nhưng không giới hạn bởi các vai trò công việc sau:

- Xác minh thông tin trong hồ sơ đăng ký chứng thư số của thuê bao
- Chấp nhận, từ chối hay các xử lý khác đối với yêu cầu cấp chứng thư số, yêu cầu thu hồi, gia hạn chứng thư số
- Chuyển giao chứng thư số cho thuê bao
- Quản lý thông tin của thuê bao
- Tư vấn, hỗ trợ khách hàng trong quá trình sử dụng

5.3. Kiểm soát nhân sự

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

MISA yêu cầu những nhân viên đang mong muốn được trở thành người được tin tưởng chứng minh được lai lịch tốt, có năng lực tốt và kinh nghiệm cần thiết để thực hiện tốt các yêu cầu công việc trong tương lai, cũng như việc được tin tưởng, nếu có, cần thiết để thực hiện các dịch vụ về chứng thư theo hợp đồng quản lý.

5.3.2. Các thủ tục kiểm tra về lý lịch và trình độ

Trước khi cấp vai trò được tin tưởng cho một nhân viên, MISA thực hiện việc kiểm tra lai lịch gồm các yếu tố sau:

- Giấy xác nhận của địa phương về cá nhân, gia đình
- Kiểm tra tham khảo đồng nghiệp
- Sự xác nhận của mức độ đào tạo cao nhất đã đạt được
- Kiểm tra các tiền án tiền sự (ở địa phương, thành phố)

Báo cáo bao gồm các thông tin trên được đánh giá bởi bộ phận quản trị nguồn nhân lực và các nhân viên an ninh, những người sẽ đưa ra các biện pháp thích hợp cho mỗi trường hợp, mức độ, và tần suất không được đề cập đến trong quá trình kiểm tra lai lịch. Những hành động này có thể bao gồm việc kiểm tra và loại bỏ các ứng viên cho vị trí được tin tưởng hoặc chấm dứt công việc của những người đang được tin tưởng. Việc sử dụng các thông tin thu thập được từ trong quá trình kiểm tra lai lịch để đưa ra các hành động thích hợp với luật pháp.

Việc kiểm tra lai lịch sẽ được lặp lại 5 năm một lần.

5.3.3. Yêu cầu về đào tạo

MISA-CA thực hiện các chương trình đào tạo nội bộ cho đội ngũ nhân viên, quá trình đào tạo được thực hiện theo quy trình, có ghi lại nhật ký đào tạo cho từng cá nhân.

Chương trình huấn luyện của MISA-CA hướng tới trách nhiệm cụ thể của mỗi nhân viên, nội dung huấn luyện bao gồm:

- Các khái niệm PKI cơ bản
- Trách nhiệm công việc

- Các chính sách và thủ tục an ninh của hoạt động MISA-CA
- Sử dụng và vận hành các thiết bị phần cứng và phần mềm
- Xử lý các sự cố
- Các thủ tục duy trì tính liên tục của dịch vụ khi có thảm họa.

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

5.3.4. Tần suất và yêu cầu đào tạo lại

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

5.3.5. Tần suất luân chuyển công việc

MISA-CA thực hiện chính sách luân chuyển cán bộ trong phạm vi nội bộ của mình tuy nhiên không quy định cụ thể về tần suất luân chuyển công việc.

5.3.6. Kỷ luật đối với các hoạt động bất hợp pháp

MISA-CA thiết lập, duy trì và áp đặt các chính sách đối với hành động bất hợp pháp. Các biện pháp kỷ luật có thể bao gồm đánh giá, và có thể chấm dứt hợp đồng phụ thuộc vào tần suất và mức độ nghiêm trọng của các hành động bất hợp pháp.

5.3.7. Các yêu cầu ký kết độc lập

Trong một số trường hợp, các cố vấn độc lập có thể được thuê để thực hiện một số công việc cần sự tin tưởng của MISA-CA. Những người này cũng phải tuân theo các tiêu chuẩn an ninh như nhân viên của MISA-CA. Nếu các cố vấn không đáp ứng đủ các tiêu chí đã quy định, họ chỉ được phép thực hiện công việc khi có sự giám sát của người được tin tưởng của MISA-CA.

5.3.8. Tài liệu được cung cấp cho nhân viên

MISA-CA cung cấp các tài liệu cần thiết cho nhân viên, đảm bảo các nhân viên có thể thực hiện tốt công việc với các tài liệu được cung cấp.

5.4. Các thủ tục ghi nhật ký

5.4.1. Các loại sự kiện được ghi lại

Các sự kiện có thể kiểm định phải được ghi lại. Mọi bản ghi, điện tử hay bằng tay, chứa thời gian của sự kiện, và nhận dạng của đơn vị thực hiện. MISA-CA đưa ra các loại bản ghi sự kiện trong Quy chế chứng thực này. Các dạng sự kiện có thể kiểm định bao gồm:

- Các sự kiện:

1. Tạo khóa CA,

2. Bật tắt các hệ thống và ứng dụng,

3. Thay đổi khóa CA,

4. Sự kiện có liên quan đến quản lý chu kỳ mã hoá,

5. Quá Trình xử lý dữ liệu kích hoạt cho khóa bí mật của CA, các bản ghi truy cập vật lý,

6. Bảo trì và thay đổi cấu hình hệ thống,

7. Bản ghi huỷ bỏ các phương tiện chứa khóa, dữ liệu kích hoạt, hoặc thông tin thuê bao.

8. Việc sử dụng khóa của thuê bao

- Các sự kiện về vòng đời của chứng thư (bao gồm cấp mới, gia hạn, thu hồi)
- Sự kiện liên quan tới nhân viên tin cậy bao gồm:

1. Hành động truy cập hay thoát ra;

2. Tạo và xóa bỏ mật khẩu hay thay đổi đặc quyền của người sử dụng,

3. Thay đổi nhân sự.

- Báo cáo về việc truy nhập vào mạng và các hệ thống không được cấp quyền
- Lỗi trong việc đọc và ghi của chứng thư và kho lưu trữ
- Thay đổi chính sách tạo chứng thư, thời gian hợp lệ của chứng thư số
- Lỗi phát sinh liên quan đến chứng thư số và dịch vụ chứng thực chữ ký số do thuê bao thông báo hoặc do MISA-CA phát hiện

5.4.2. Tần suất xử lý nhật ký

Các nhật ký sẽ được lưu lại tức thời khi có sự kiện liên quan đến hệ thống CA và các sự kiện sẽ được xử lý hằng ngày hoặc hàng tuần tùy theo mức độ quan trọng. Ngoài ra, MISA-CA sẽ tiến hành kiểm tra bất thường dựa theo các cảnh báo và hiện tượng của hệ thống.

5.4.3. Thời gian lưu trữ nhật ký giám sát

Nhật ký sẽ được giữ tại hệ thống ít nhất 2 tháng sau khi xử lý và sau đó được chuyển sang khu vực lưu trữ.

5.4.4. Bảo vệ các nhật ký giám sát

Nhật ký giám sát được bảo vệ chỉ được phép xem, ngăn chặn tất cả các thao tác khác như các hành động thay đổi, xóa hay can thiệp bất hợp pháp.

5.4.5. Các thủ tục sao lưu nhật ký kiểm tra

Nhật ký kiểm tra được sao lưu theo chế độ sao lưu dữ liệu chung của MISA-CA.

5.4.6. Hệ thống thu thập nhật ký

Các log ứng dụng, hệ điều hành và mạng được ghi lại tự động. Một số log được ghi bằng tay bởi nhân viên.

Chi tiết về nơi lưu nhật ký và cơ chế lưu được mô tả trong Hồ sơ kỹ thuật.

5.4.7. Thông báo khi có sự kiện xảy ra

MISA-CA có hệ thống cảnh báo cho người quản trị khi có một sự kiện cần phải xử lý.

5.4.8. 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.

Ngoài ra MISA có quy trình đánh giá hệ thống và trên kết quả đánh giá sẽ phân tích và tìm ra các lỗ hổng và sự cố có thể xảy ra trong tương lai.

5.5. Lưu trữ các bản ghi

5.5.1. Các loại bản ghi được lưu trữ

MISA-CA sẽ lưu trữ các thông tin sau:

- Thông tin đơn xin cấp chứng thư số
- Các thông tin bổ sung của đơn xin cấp chứng thư số
- Thông tin vòng đời chứng thư số như: thu hồi, đổi khóa, làm mới…
- Và các thông tin khác theo quy định của RootCA
- Các dữ liệu nhật ký trong phần 5.4

5.5.2. Thời gian duy trì của các dữ liệu lưu trữ

Các dữ liệu và thông tin liên quan sẽ được lưu trong một khoảng thời gian nhất định kể từ ngày chứng thư số hết hạn hoặc bị huỷ bỏ tối thiểu là 5 năm.

5.5.3. Bảo vệ dữ liệu lưu trữ

Các dữ liệu lưu trữ được bảo vệ để không bị truy cập bất hợp pháp, xem, thay đổi, xóa, sửa hay phá hoại bên trong hệ thống tin cậy. Phương tiện lưu trữ dữ liệu và các ứng dụng được yêu cầu xử lý dữ liệu sẽ được duy trì nhằm đảm bảo các dữ liệu lưu trữ có thể được truy cập trong khoảng thời gian đã được thiết lập trong Quy chế chứng thực.

5.5.4. Các thủ tục sao lưu dữ liệu lưu trữ

Dữ liệu lưu trữ được sao lưu theo chế độ sao lưu chung của MISA-CA.

5.5.5. Nhãn thời gian của các bản ghi

Các bản ghi thông tin về chứng thư số và toàn bộ sự kiện liên quan đến việc thu hồi chứng thư số đều chứa thông tin về thời gian xảy ra sự kiện.

5.5.6. Hệ thống chứa dữ liệu lưu trữ

MISA-CA có hệ thống chứa dữ liệu lưu trữ được mô tả chi tiết trong Hồ sơ kỹ thuật.

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

Chỉ những cá nhân được tin tưởng và có thẩm quyền mới có quyền truy cập vào các dữ liệu lưu trữ. Khi có nhu cầu truy cập vào các thông tin lưu trữ, phải thực hiện theo quy trình mà MISA đề ra.

5.6. Thay đổi khóa của CA

Chứng thư số của MISA-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 MISA-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 MISA-CA hết hạn, MISA-CA sẽ tiến hành quy trình gia hạn nhằm đảm bảo hệ thống hoạt động thông suốt. MISA-CA sẽ xin gia hạn chứng thư số từ RootCA không chậm hơn 60 ngày trước thời điểm hết hạn.

Trước khi hết hạn chứng thư số của MISA-CA, các thủ tục được ban hành cho phép chuyển tiếp từ cặp khóa cũ sang cặp khóa mới cho các thực thể thuộc phạm vi quản lý của MISA-CA. Quá trình chuyển tiếp khóa của MISA-CA đảm bảo rằng:

- MISA-CA chỉ ban hành chứng thư số mới cho thuê bao trước thời điểm nhất định so với ngày hết hạn cặp khóa. Thời điểm này là thời điểm tạm dừng ban hành chứng thư số, do pháp luật quy định.
- Khi nhận được yêu cầu ban hành chứng thư số sau thời điểm tạm dừng ban hành chứng thư số trên, MISA-CA sử dụng cặp khóa mới để ban hành chứng thư số cho thuê bao.

5.7. Xử lý khi bị lộ thông tin và khôi phục thảm họa

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

Các thông tin sau được backup đề phòng có sự cố và thảm họa: dữ liệu về đơn xin cấp chứng thư số, dữ liệu nhật ký, và các bản ghi chứng thư số được tạo ra.

Khi có sự cố, các dữ liệu được phục hồi theo các thủ tục đã có. MISA-CA đào tạo quy trình kiểm soát sự cố và thảm họa đến từng nhân viên.

5.7.2. Xử lý các hỏng hóc về máy tính, phần mềm và dữ liệu

Khi có sự cố xảy ra, tùy theo từng trường hợp sẽ xử lý và đảm bảo thời gian khắc phục là nhanh nhất. Mỗi sự cố sẽ có các quy trình xử lý khác nhau. Nếu sự cố nghiêm trọng thì sẽ thực hiện các thủ tục phục hồi lại hệ thống theo kịch bản sẵn có.

5.7.3. Mất/Lộ khoá bí mật

Khi khóa bí mật của MISA-CA nghi ngờ bị mất/lộ, MISA-CA sẽ thực hiện thủ tục xử lý khi khóa bị lộ. Đội xử lý sự cố an ninh của MISA-CA chịu trách nhiệm điều phối thực hiện các bước trong thủ tục này. Đội xử lý sự cố bao gồm người đứng đầu MISA-CA, người phụ trách kỹ thuật và người phụ trách cấp phát chứng thư số.

Nêu chứng thư số của MISA-CA bị thu hồi, các thủ tục sau sẽ được thực hiện:

- Trạng thái thu hồi chứng thư số của MISA-CA sẽ được công bố bởi RootCA.
- MISA-CA cố gắng thông báo cho toàn bộ người nhận trong hệ thống MISA-CA dừng sử dụng các chứng thư số do MISA-CA ban hành.

MISA-CA xin cấp chứng thư số mới từ RootCA và ban hành chứng thư số cho các thuê bao của mình để họ tiếp tục sử dụng.

5.7.4. Khả năng duy trì liên tục trong kinh doanh sau thảm hoạ

MISA-CA xây dựng hệ thống dự phòng cách vị trí hệ thống chính tối thiểu 30km.

MISA-CA sẽ lập kế hoạch, triển khai và thử nghiệm kế hoạch dự phòng, đảm bảo hoạt động liên tục kể cả có thảm họa. Kế hoạch này thường xuyên được kiểm tra xem xét và cập nhật cho phù hợp với thực tế.

MISA-CA có khả năng phục hồi những hoạt động quan trọng trong vòng 24 giờ sau khi một thảm họa xảy ra. Ít nhất các hoạt động sau sẽ được phục hồi:

- Ban hành chứng thư số
- Thu hồi chứng thư số
- Công bố thông tin thu hồi chứng thư số

Cơ sở dữ liệu của MISA-CA phục hồi thảm họa sẽ được đồng bộ với cơ sở dữ liệu chính trong thời gian phù hợp.

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

5.7.5. Kiểm tra hệ thống

CA thực hiện việc kiểm tra cấu hình hệ thống định kỳ 01 tháng một lần và kiểm tra bất thường khi có sự cố

5.8. Kết thúc sự hoạt động CA

Trong trường hợp MISA-CA không còn hoạt động, MISA-CA dùng mọi biện pháp cố gắng thông báo cho thuê bao, người nhận và các đối tượng trước khi dừng hoạt

động. Công ty Cổ phần MISA sẽ thực hiện chuyển tất cả các thuê bao qua nhà cung cấp dịch vụ khác hoặc thực hiện đền bù và thu hồi các chúng thư cần thiết.

MISA-CA sẽ thực hiện theo các hướng dẫn của Trung tâm chứng thực điện tử quốc gia (NEAC) để đảm bảo toàn bộ khách hàng sử dụng chứng thực số vẫn tiếp tục được duy trì theo quy định của pháp luật.

Trong trường hợp bị chấm dứt, CA sẽ thực hiện kế hoạch chấm dứt sau: Ít nhất 30 ngày trước ngày dự kiến chấm dứt, CA sẽ:

- Thông báo cho Trung tâm chứng thực điện tử quốc gia (NEAC) tất cả các thuê bao sử dụng dịch vụ CA và tất cả các bên có liên quan khác;
- Hợp tác với NEAC để chuyển giao dịch vụ chứng thực chữ ký số sang CA khác, bao gồm cả việc sử dụng số tiền ký quỹ trong ngân hàng để thanh toán các nghĩa vụ về tài chính, chi phí chuyển giao và các chi phí khác;
- Thông báo cho thuê bao rằng tất cả các chứng thư số không hết hạn tại thời điểm ngừng hoạt động sẽ bị thu hồi;
- Lưu giữ hồ sơ và thông tin liên quan đến giấy chứng thư số trong ít nhất 01 năm kể từ thời điểm cấp, ngoài ra còn có thể cung cấp bằng chứng xác nhận trong các thủ tục pháp lý, hành chính;
- Lập kế hoạch phá hủy các khóa riêng được sử dụng để ký ở chế độ từ xa và các mô – đun mật mã liên quan;
- Tuân thủ với các quy định của NEAC để cung cấp thông tin về các chứng thư số đã bị thu hồi.

Vào ngày chấm dứt MISA sẽ:

- Thu hồi các chứng thư số đang hoạt động thuộc CA đã chấm dứt;
- Phá hủy các khóa bí mật và các mô – đun mật mã liên quan để tránh khả năng tái tạo. Có truy vết được thực hiện về hoạt động này;
- Cập nhật danh sách tạm dừng và thu hồi chứng thư số lần cuối và vô hiệu hóa cặp khóa CA đảm bảo không sử dụng được.

6. VẤN ĐỀ AN TOÀN, AN NINH KỸ THUẬT

6.1. Tạo cặp khóa và cài đặt

6.1.1. Tạo cặp khóa (Sinh cặp khóa)

Hệ thống MISA-CA sử dụng hệ thống mật mã không đối xứng (thuật toán RSA) cho việc tạo khóa của hệ thống MISA-CA và thuê bao. Mỗi cặp khóa bao gồm khóa bí mật và khóa công khai được sinh ngẫu nhiên và đúng một lần duy nhất trong thiết bị mã hóa an toàn như HSM, đảm bảo khóa bí mật không bị phát hiện khi có khóa công khai tương ứng đáp ứng theo nghị định 130/2018/NĐ-CP và khóa bí mật sau khi sinh được lưu trữ trên thiết bị đạt chuẩn FIPS 140-2 Level 3 đáp ứng theo thông tư 16/2015/TT-BTTTT .

Việc tạo khóa cho MISA-CA được thực hiện theo quy trình như sau:

1. Cặp khóa của MISA-CA sẽ được sinh trong thiết bị HSM phần cứng chuyên dụng FIPS 140-2 Level 3 và sử dụng thuật toán sinh số ngẫu nhiên (Random Number Generator (RNG)) theo chuẩn AIS-31 để sinh khóa. Hệ thống MISA-CA sử dụng HSM của những nhà cung cấp đáp ứng tiêu chuẩn FIPS 140-2 Level 3 được thể hiện trong phụ lục **Đặc tả thiết bị HSM** là một phần của hồ sơ này.

2. Đối với khóa của thuê bao:

- Sau khi hồ sơ cấp chứng thư của khách hàng được MISA-CA thẩm định thông tin là chính xác. Thuê bao cần xác nhận lại trước khi gửi yêu cầu cấp chứng thư đến MISA-CA. Khóa của khách hàng sẽ được sinh ra ở HSM CP5 tương ứng với thông tin đã đăng ký, cặp khóa này sẽ được sinh theo thuật toán mã hóa phù hợp với các tiêu chuẩn về tính duy nhất và bảo mật cho cặp khóa đáp ứng thông tư 16/2019/TT-BTTTT.

6.1.2. Phân phối khóa bí mật cho thuê bao

Khóa của thuê bao được sinh ra trên phần cứng mã hóa an toàn HSM CP5 sau khi khách hàng xác nhận cấp chứng thư như mô tả tại mục 6.1.1

6.1.3. Cung cấp khóa công khai cho tổ chức phát hành chứng thư

Khóa công khai được tạo cùng với khóa bí mật và được quản lý trên HSM CP5 theo quy trình tạo khóa như mô tả tại mục 6.1.1

6.1.4. Phân phối khóa công khai của CA

Khóa công khai của hệ thống MISA-CA được công bố truy xuất theo điều khoản trong mục 2.2.

6.1.5. Kích thước khóa

Các cặp khóa cần có chiều dài thích hợp để ngăn việc lộ khóa bí mật trong thời gian sử dụng cặp khóa. Chuẩn độ dài cặp khóa của MISA-CA và thuê bao yêu cầu tối thiểu là RSA độ dài khóa 2048 bit trở lên hoặc ECDSA 256 bit trở lên .

6.1.6. Tạo tham số khóa công khai và kiểm tra chất lượng

MISA-CA sinh khóa với các tham số theo chuẩn được quy định tại Thông tư số 16/2019/TT-BTTTT ngày 05/12/2019.

6.1.7. Mục đích sử dụng khóa (quy định trong bản ghi X.509 v3 Key Usage)

Xem trong phần 7.1.2.1.

6.2. Bảo vệ khóa bí mật và kiểm soát phương thức mã hóa

6.2.1. Kiểm soát và chuẩn hóa mô đun mã hóa

Khóa bí mật nằm trong hệ thống MISA-CA sẽ được bảo vệ bởi hệ thống tin cậy và người nắm giữ khóa bí mật sẽ giữ chức năng phòng ngừa để ngăn chặn sự mất mát, bị tiết lộ, sửa đổi và sử dụng bất hợp pháp khóa bí mật phù hợp với Quy chế chứng thực này, nghĩa vụ hợp đồng và yêu cầu được cung cấp nằm trong văn kiện bảo mật riêng của MISA-CA.

MISA-CA sử dụng thiết bị mã hóa phần cứng an toàn chuyên dụng HSM (Hardware Security Module) để lưu trữ khóa bí mật của MISA-CA. Thiết bị mã hóa phần cứng an toàn của MISA-CA đáp ứng chuẩn FIPS 140-2 Level 3.

MISA-CA sẽ tạo khóa bí mật của thuê bao trong phần cứng mã hóa an toàn đạt chuẩn PP CEN 419 221-5 (Protection Profiles for TSP Cryptographic modules – Part 5: Cryptograhic Module for Trust Sevices) và được bảo vệ tuyệt đối bằng khóa MBK.

6.2.2. Biện pháp kiểm soát khóa bí mật nhiều người (M out of N)

Khóa bí mật được kiểm soát theo cơ chế (M,N).

Cơ chế kiểm soát khóa bí mật được MISA-CA sử dụng là cơ chế chia sẻ mã. Cơ chế này tách dữ liệu kích hoạt khóa bí mật thành (N) phần khác nhau, các phần này được giữ bởi nhiều (N) người khác nhau.

Với mỗi chức năng nhất định, cần có (M) phần (M nhỏ hơn hoặc bằng N) mã chia sẻ để kích hoạt chức năng đó.

Tại MISA-CA, M >= 2.

6.2.3. Ủy thác giữ khóa bí mật

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

MISA-CA sẽ lưu trữ khóa bí mật của thuê bảo khi có sự ủy thác và xác nhận của thuê bao. Khóa bí mật sẽ được lưu trữ phần cứng mã hóa an toàn đạt chuẩn PP CEN 419 221-5 (Protection Profiles for TSP Cryptographic modules – Part 5: Cryptograhic Module for Trust Sevices)

6.2.4. Sao lưu khóa bí mật

MISA-CA sẽ sao lưu (backup) khóa bí mật của mình để đề phòng thảm họa và trục trặc thiết bị. Khóa bí mật của MISA-CA được sao lưu dự phòng trong các thiết bị phần cứng mã hóa an toàn dự phòng được đặt ở trung tâm dữ liệu dự phòng cách vị trí lưu trữ khóa bí mật chính tối thiểu 30km.

Khóa bí mật của Thuê bao được tạo và lưu trữ trong HSM CP5 của Utimaco và bảo vệ bởi Remote QSCD (ADSS SAM Appliance v6.0) phục vụ cho mục đích khôi phục định kỳ và khắc phục sự cố. Các khóa như vậy được lưu trữ ở dạng mã hóa trong các mô đun mã hóa phần cứng và các thiết bị lưu trữ khóa liên quan. Các mô đun mã hóa được sử dụng để lưu trữ Khóa bí mật đáp ứng các yêu cầu CPS này.

Khóa bí mật của thuê bao không thể trích xuất hoặc khôi phục từ QSCD.

6.2.5. Lưu trữ khóa bí mật

Sau khi chứng thư số của MISA-CA hết hạn, cặp khóa tương ứng vẫn được lưu trữ (archive) an toàn với thời hạn ít nhất 5 năm trong thiết bị phần cứng mã hóa an toàn. Những cặp khóa đó sẽ không còn được sử dụng cho bất kỳ hoạt động của MISA-CA.

Khóa bí mật của thuê bao được lưu trữ trong HSM và nằm trong môi trường QSCD đạt tiêu chuẩn bảo mật Common Criteria EAL 4+(AVA_VAN.5)

6.2.6. Chuyển khóa bí mật vào/ra

MISA-CA giữ khóa trên một thiết bị phần cứng mã hóa an toàn và một bản sao khóa để dự phòng phục vụ cho trường hợp phục hồi hệ thống trên một thiết bị phần cứng mã hóa an toàn khác. Khóa bí mật sẽ được mã hóa trong quá trình chuyển giữa 2 thiết bị phần cứng mã hóa an toàn.

6.2.7. Lưu trữ khóa bí mật trong thiết bị phần cứng mã hóa an toàn

MISA-CA giữ khóa bí mật trong các thiết bị phần cứng mã hóa an toàn, khóa bí mật được lưu trong dạng được mã hóa, theo chuẩn do Bộ Thông tin và Truyền thông ban hành.

6.2.8. Phương thức kích hoạt khóa bí mật

Tất cả các thành phần tham gia MISA-CA sẽ có các biện pháp bảo vệ để kích hoạt khóa bí mật phù hợp, cụ thể:

- Đối với thuê bao: Khóa bí mật được lưu trữ và mã hóa trong thiết bị HSM CP5 đạt tiêu chuẩn, việc kích hoạt khóa bí mật yêu cầu có tài khoản đăng nhập, mã PIN bảo vệ, sinh trắc học hoặc mã OTP gửi về số điện thoại, email của khách hàng. Thuê bao có trách nhiệm bảo vệ mật khẩu để kích hoạt khóa bị mật khỏi bị mất, đánh cắp, sửa đổi, để lộ hoặc sử dụng trái phép.Trong trường hợp thuê bao nhập sai tên truy cập, mật khẩu và mã OTP 5 lần liên tiếp, tài khoản Remote QSCD sẽ bị khóa.
- Đối với MISA-CA: sử dụng thiết bị phần cứng mã hóa an toàn để lưu trữ khóa bí mật, để kích hoạt khóa bí mật yêu cầu phải có (M) mã chia sẻ kết nối vào thiết bị phần cứng mã hóa an toàn.

6.2.9. Phương pháp ngừng kích hoạt khóa bí mật

Khóa bí mật của MISA-CA bị ngừng kích hoạt ngay lập tức khi không đủ (M) mã chia sẻ kết nối với thiết bị phần cứng mã hóa an toàn.

Khóa bí mật của thuê bao có thể bị ngừng kích hoạt sau khi hết phiên làm việc, đăng xuất hệ thống.

6.2.10. Phương pháp huỷ khóa bí mật

Việc hủy khóa bí mật của MISA-CA và thuê bao được thực hiện theo phương pháp an toàn theo chuẩn do Bộ Thông tin và Truyền thông ban hành, đảm bảo không thể phục hồi lại khóa đã huỷ bằng bất cứ hình thức nào.

6.2.11. Đánh giá thiết bị mã hóa

MISA-CA sử dụng các thiết bị mã hóa đáp ứng theo quy định tại phần 6.2.1.

Các thiết bị này đều đã được Ban Cơ yếu Chính phủ đánh giá đáp ứng các tiêu chuẩn kỹ thuật về sản phẩm dịch vụ mật mã dân sự được sử dụng tại Việt Nam.

6.3. Các khía cạnh khác của quản lý cặp khóa

6.3.1. Lưu trữ khóa công khai

Tất cả các thông tin về khóa công khai được lưu trữ trong hệ thống cơ sở dữ liệu quan hệ và hệ thống danh bạ (LDAP).

6.3.2. Thời gian hoạt động của chứng thư số và thời gian sử dụng cặp khóa

- Thời gian hoạt động của chứng thư số do MISA-CA cấp tuân theo quy định của Bộ Thông tin và Truyền thông, các chứng thư số được cấp cho thuê bao sẽ có thời gian hiệu lực tùy thuộc vào thỏa thuận với thuê bao, thông thường sẽ là từ 1 đến 3 năm
- Thời hạn sử dụng của chứng thư số sẽ kết thúc khi chứng thư số đó hết hạn hoặc bị thu hồi
- MISA-CA không ban hành các chứng thư số có thời hạn sử dụng vượt quá thời hạn sử dụng chứng thư số của MISA-CA

6.4. Dữ liệu kích hoạt

6.4.1. Quá trình sinh và cài đặt dữ liệu kích hoạt

Dữ liệu kích hoạt được sử dụng để bảo vệ HSM có chứa Khóa bí mật của MISA-CA, Cơ chế kiểm soát khóa bí mật được MISA-CA sử dụng là cơ chế chia sẻ mã. Cơ chế này tách dữ liệu kích hoạt khóa bí mật thành (N) phần khác nhau, các phần này được giữ bởi nhiều (N) người khác nhau.

Với mỗi chức năng nhất định, cần có (M) phần (M nhỏ hơn hoặc bằng N) mã chia sẻ để kích hoạt chức năng đó.

Dữ liệu kích hoạt sử dụng (tên truy cập, mật khẩu và OTP) để bảo vệ Remote QSCD có chưa khóa bí mật của đối tượng sử dụng, được tạo ra theo tiêu chuẩn tuân thủ của QSCD

6.4.2. Bảo vệ dữ liệu kích hoạt

Người giữ và bảo vệ dữ liệu kích hoạt này phải là người tin tưởng và được ký cam kết bảo mật thông tin.

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

Thuê bao đăng ký sẽ phải ghi nhớ thông tin xác thực kích hoạt(PIN, PUK, tên truy cập, mật khẩu, OTP) và không chia sẽ với bất kỳ ai.

6.4.3. Các khía cạnh khác của dữ liệu kích hoạt

6.4.3.1. Vấn đề chuyển tải dữ liệu kích hoạt

Để chuyển giao các dữ liệu kích hoạt cho các khoá bí mật, các thành viên thuộc dịch vụ MISA-CA sẽ sử dụng các biện pháp chống lại các nguy cơ mất mát, bị đánh cắp, bị sửa đổi, bị tiết lộ hoặc bị sử dụng trái phép đối với khóa bí mật.

6.4.3.2. Huỷ dữ liệu kích hoạt

Khi hết hạn sử dụng hoặc khi cần thiết, dữ liệu kích hoạt khóa bí mật sẽ được MISA-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 cho hệ thống máy tính

6.5.1. Yêu cầu kỹ thuật bảo mật máy tính

MISA-CA đảm bảo rằng các máy chủ cài đặt hệ thống CA và dữ liệu được bảo vệ trước các truy nhập không được phép. MISA-CA giới hạn quyền truy nhập tới CA server theo vai trò của quản trị. Trên các máy chủ cài đặt hệ thống CA, không có ứng dụng nào khác được cài đặt thêm.

Hệ thống mạng của MISA-CA được cách ly với các thành phần khác, bảo vệ khỏi sự truy cập bất hợp pháp. Sự cách ly này được thực hiện bằng hệ thống tường lửa đa lớp. Lớp tường lửa bên ngoài bảo vệ cả hệ thống khỏi các truy nhập từ ngoài. Lớp tường lửa bên trong cách ly các server CA ra khỏi hệ thống mạng chung của MISA-CA. Các quản trị viên của MISA-CA chỉ truy nhập và quản trị hệ thống thông qua một số giới hạn các máy tính quản trị được xác định sẵn.

MISA-CA yêu cầu sử dụng mật khẩu mạnh, mật khẩu được định kỳ được thay đổi.

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

6.5.2. Đánh giá an ninh hệ thống

Hệ thống máy chủ cung cấp dịch vụ của MISA-CA đang hoạt động theo chuẩn ISO 27001, chứng nhận ISO 9001:2015 được đánh giá định kỳ một năm một lần.

Chứng chỉ CMMi đánh giá định kỳ ba năm một lần.

Hệ thống đạt chứng nhận QTSP theo quy định của Liên minh châu Âu số 910/2014

6.6. Các biện pháp kỹ thuật quản lý vòng đời

6.6.1. Biện pháp quản lý phát triển hệ thống

Theo quy trình/quy định giám sát nội bộ của Công ty cổ phần MISA đề ra.

6.6.2. Biện pháp quản lý giám sát an ninh

Theo quy trình/quy định giám sát nội bộ của Công ty cổ phần MISA đề ra. Các thủ tục và biện pháp này tuân theo tiêu chuẩn quản lý an ninh thông tin ISO 27001.

6.6.3. Giám sát an ninh vòng đời chứng thư số

Theo quy trình/quy định giám sát nội bộ của Công ty cổ phần MISA đề ra.

6.7. Kiểm soát bảo mật mạng

MISA-CA dựa trên các tiêu chuẩn an toàn như ISO 27001 để thiết kế hệ thống, bao gồm:

- Chính sách an ninh thông tin

- Hệ thống Firewall lớp trong (Internal Firewall): bảo vệ vành đai lớp ngoài, phân chia truy cập từ ngoài Internet vào hệ thống các dịch vụ cung cấp ra ngoài Internet
- Hệ thống Firewall lớp ngoài (External Firewall): phân tách và quản lý truy cập giữa các lớp mạng nội bộ
- Hệ thống Firewall tích hợp sẵn với hệ thống phát hiện và chống thâm nhập mạng IPS.
- Hệ thống Web Application Firewall phòng chống tấn công ở mức chuyên sâu trong lớp ứng dụng Web.
- Hệ thống Load Balancer: phân tải các yêu cầu truy cập vào hệ thống và năng cao khả năng sẵn sàng của dịch vụ.
- Hệ thống phòng chống Antivirus tập trung: Client/server, quản lý tập trung.
- Hệ thống cập nhật bản vá cho các máy chủ/máy trạm.
- Hệ thống giám sát an ninh: giám sát an ninh tập trung, các thành phần dò tìm các lỗ hổng, thành phần thiết lập chính sách an ninh mạng, thành phần phân tích an ninh và báo cáo, thành phần cập nhật các bản vá, thành phần quản lý và phân tích băng thông của mạng.

6.8. Dán nhãn thời gian

MISA-CA không cung cấp dịch vụ này.

7. ĐẶC TẢ VỀ CHỨNG THƯ SỐ, CRL VÀ OCSP

7.1. Đặc tả chứng thư số

Các chứng thư MISA-CA tuân theo ITU-T Recommendation x.509 (1997): Information Technology – Open Systems Interconnection-The Directory: Authentication Framework, June 1997 and (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008 ("RFC 5280 ").

Tối thiểu, các chứng thư X.509 bao gồm các trường cơ bản và các giá trị bắt buộc được chỉ ra hoặc phải tuân theo các ràng buộc trong bảng dưới đây:

Tên trường	Giá trị
Version	Phiên bản 3 (version 3) tiêu chuẩn X.509
Serial Number	Số hiệu chứng thư số Giá trị của trường này là duy nhất Quy tắc sinh ra tên serial number này có thể theo thứ tự hoặc theo nguyên tắc nhất định do MISA-CA đặt ra
Signature Algorithm	Thuật toán mật mã. Định danh thuật toán được sử dụng để ký chứng thư
Issuer	Đơn vị cung cấp chứng thư
Valid From	Thời điểm có hiệu lực của chứng thư số (tuân thủ theo tiêu chuẩn RFC 5280)
Valid To	Thời điểm hết hiệu lực của chứng thư số (tuân thủ theo tiêu chuẩn RFC 5280)
Subject	Thông tin về người nhận chứng thư (tuân thủ theo tiêu chuẩn RFC 5280) Chi tiết xem tại mục 3.1.1

Public Key	Khoá công cộng tương ứng với khóa bí mật của chứng thư số (tuân thủ theo tiêu chuẩn RFC 5280)
Signature	Chữ ký số của tổ chức cung cấp dịch vụ chứng thực chữ ký số. Được sinh và mã hoá phù hợp với tiêu chuẩn RFC 5280

7.1.1. Số hiệu phiên bản

Các chứng thư MISA-CA tuân theo phiên bản 3 tiêu chuẩn X.509.

Chứng thư số của thuê bao tuân theo phiên bản 3 tiêu chuẩn X.509.

7.1.2. Các thành phần mở rộng

MISA-CA tạo ra chứng thư X.509 phiên bản 3 với sự mở rộng được yêu cầu trong các mục dưới đây:

Tên trường	Giá trị
Key Usage	Mục đích, phạm vi sử dụng của chứng thư số.
Basic Constraints	Cho biết chủ thể của chứng thư số có phải là CA hay thuê bao.
Certificate Policies Extension	Chứa các điều khoản thông tin chính sách về chứng thư số được sinh ra và mục đích sử dụng của chứng thư số đó
Subject Alternative Names	Các tên thay thế của thuê bao có thể là: otherName, rfc822Name, dNSName, x400Address, directoryName, ediPartyName, uniformResourceIdentifier, iPAddress, registeredID
Extended Key Usage	Các giá trị của trường "Extended Key Usage" trong chứng thư số được sử dụng theo thỏa thuận trong hợp đồng với thuê bao.
CRL Distribution Points	Các giá trị của trường "CRL Distribution Points" trong chứng thư số có chứa địa chỉ URL để người dùng có thể truy cập tới file CRL để kiểm tra trạng thái của chứng thư số.

Authority Key Identifier	Giá trị của trường "Authority Key Identifier" định danh chứng thư số của MISA-CA.
Subject Key Identifier	Giá trị của trường "Subject Key Identifier" định danh chứng thư số của thuê bao mà do MISA-CA ban hành.

7.1.3. Số hiệu thuật toán

MISA-CA ký lên chứng thư số sẽ sử một trong các thuật toán sau:

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

7.1.4. Định dạng tên

Tên trong chứng thư số của thuê bao được khởi tạo theo định dạng tiêu chuẩn X.509.

7.1.5. Các ràng buộc về tên

Tên trên chứng thư số phải đúng với tên của thuê bao quy định tại các giấy tờ có giá trị pháp lý nhằm xác định nhân thân của thuê bao.

7.1.6. Định danh đối tượng chính sách chứng thư

Việc sử dụng chứng thư số phải tuân thủ theo các quy định về chính sách và quy chế chứng thư số.

7.1.7. Sử dụng phần mở rộng ràng buộc chính sách

Không có quy định

7.1.8. Cú pháp và ngữ nghĩa quy chế

MISA-CA ban hành chứng thư số tuân theo các quy định trong quy chế chứng thực này và các thỏa thuận với thuê bao.

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

Không có quy định

7.2. Đặc tả danh sách chứng thư số thu hồi

7.2.1. Số phiên bản

MISA-CA hỗ trợ định dạng CRL theo phiên bản 2 và tuân theo tiêu chuẩn RFC 5280.

7.2.2. CRL và các mở rộng

7.2.2.1. Khuôn dạng của CRL

Về cơ bản, khuôn dạng thông tin trong danh sách của CRL do MISA-CA công bố tuân theo tiêu chuẩn ITU-T X.509 và các quy định của RFC 5280. CRL do MISA-CA sẽ có tối thiểu các trường sau:

Tên trường	Giá trị
Version	Phiên bản của CRL (version 2).
Issuer	Tên của CA phát hành CRL.
Effective Date	Ngày phát hành (cập nhật) hiện tại của CRL.
Next update	Ngày sẽ cập nhật tiếp theo (trong tương lai) của CRL
Revoked certificates	Trường này chứa thông tin về các chứng thư bị thu hồi bao gồm: ● Serial number: Số serial number của chứng thư số bị thu hồi ● Revocation Date: Thời gian chứng thư bị thu hồi ● Revocation entry: Các thông tin mở rộng của chứng thư số bị thu hồi. Chi tiết xem tại bảng: Các trường mở rộng của CRL Entry Extension bên dưới
Signature algorithm	Thuật toán sử dụng để ký vào CRL
Signature hash algorithm	Thuật toán băm
Signature	Giá trị ký số (dạng bit) bởi MISA-CA

CRL Extension	Các thông tin mở rộng khác (trường tùy chọn). Chi tiết xem bảng: Các trường mở rộng của CRL Extensions bên dưới

7.2.2.2. Các trường mở rộng của CRL

Tên trường	Giá trị của trường
CRL number	Số hiệu của CRL
Authority key identifier	Định danh dùng để xác định khóa công khai tương ứng khóa bí mật dùng để ký chứng thư số
Issuer alternative name	Các kiểu tên khác của MISA-CA (email, tên miền, địa chỉ IP, URI)
Certificate issuer	Thông tin về CA phát hành (chỉ sử dụng trong trường hợp MISA-CA tiếp nhận quản lý chứng thư số từ một CA khác)

7.2.2.3. Các trường mở rộng của CRL Entry Extendsion

Bảng các giá trị của trường Reason Code:

Tên	Giá trị
unspecified	0
keyCompromise	1
cACompromise	2
affiliationChanged	3
superseded	4
cessationOfOperation	5
certificateHold	6

removeFromCRL	8
privilegeWithdrawn	9
aACompromise	10

7.3. Đặc tả OCSP

MISA-CA cung cấp dịch vụ OCSP tuân theo RFC 2560.

7.3.1. Số phiên bản

Sử dụng phiên bản 1.

7.3.2. Phần mở rộng OCSP

Không có quy định.

8. KIỂM ĐỊNH TÍNH TUÂN THỦ VÀ CÁC ĐÁNH GIÁ

MISA-CA sẽ tiến hành kiểm toán định kỳ nhằm đảm bảo việc tuân thủ các tiêu chuẩn của dịch vụ MISA-CA sau khi đi vào hoạt động.

Bên cạnh đó, các tiêu chuẩn của dịch vụ MISA-CA sẽ được dùng để tiến hành đánh giá và thanh tra nhằm đảm bảo tính trung thực của MISA-CA, bao gồm những điều sau:

Các tiêu chuẩn của dịch vụ MISA-CA sẽ được dùng để thanh tra hay đánh giá MISA-CA, hay thuê bao. Trong trường hợp kết quả đánh giá cho thấy các thực thể không đạt các tiêu chuẩn của dịch vụ MISA-CA, sẽ được tiếp tục hoạt động hoặc không được hoạt động tuỳ thuộc vào mức độ và hậu quả của tổn thất gây ra. Những lỗi hay những tổn thất, cho thấy mối đe doạ tiềm ẩn và thực sự đối với an ninh hay tính toàn vẹn của MISA-CA .

Các tiêu chuẩn của dịch vụ MISA-CA sẽ được dùng để tiến hành các đánh giá về quản lý rủi ro bổ sung của chính MISA-CA hay của thuê bao theo những phát hiện về việc không tuân thủ đầy đủ hoặc có những ngoại lệ trong kết quả cuộc kiểm toán quá trình tuân thủ và đó cũng là một phần của quá trình quản lý rủi ro tổng thể.

8.1. Tần suất thực hiện kiểm tra

Các bộ phận của MISA-CA sẽ bị kiểm tra định kỳ mỗi năm một lần để đảm bảo hoạt động đúng với các điều khoản quy định trong Quy chế chứng thực.

8.2. Đặc điểm và trình độ chuyên môn của người kiểm tra

Người thực hiện kiểm tra các bộ phận thành viên của MISA-CA là một bộ phận phải chứng minh năng lực trong lĩnh vực kiểm tra, kiểm soát sự hoạt động của CA.

8.3. Mối quan hệ của người kiểm tra và đơn vị được kiểm toán

Sẽ có một đơn vị độc lập thực hiện kiểm tra việc tuân thủ quy chế của các đơn vị thuộc MISA-CA. Đồng thời kiểm soát năng lực của các đơn vị này về lĩnh vực an toàn và bảo mật thông tin nói chung và về hạ tầng khóa công khai nói riêng.

8.4. Các vấn đề phải kiểm tra

Kiểm tra sự chấp hành các đơn vị của MISA-CA chính là sự kiểm tra về sự tuân thủ các điều khoản trong Quy chế chứng thực, bao gồm:

- Môi trường hoạt động của Công ty
- Hệ thống kỹ thuật cung cấp dịch vụ của Công ty
- Đánh giá việc tuân thủ theo các chuẩn của Công ty
- Quy trình quản lý, cung cấp và sử dụng chứng thư số của Công ty
- Các nội dung khác

8.5. Xử lý khi phát hiện sai sót

Sau khi có kết quả đánh giá kiểm tra, nếu phát hiện sai sót có nguy cơ ảnh hưởng đến chất lượng dịch vụ, MISA-CA sẽ phải triển khai ngay các biện pháp khắc phục.

Đối với các sai sót nhỏ lẻ, MISA-CA sẽ xây dựng kế hoạch triển khai hợp lý tuỳ theo mức độ sai sót và ảnh hưởng đến dịch vụ, quyền lợi của khách hàng.

Trong trường hợp xảy những sai sót nghiêm trọng và ảnh hưởng tới an ninh và tính toàn vẹn của hệ thống MISA-CA thì:

- MISA-CA và các đơn vị cấp trên cũng như các đơn vị liên quan có thể quyết định thu hồi các chứng thư số liên quan
- MISA-CA và các đơn vị cấp trên cũng như các đơn vị liên quan có thể quyết định tạm dừng quá trình hoạt động của các đơn vị gây lỗi
- MISA-CA và các đơn vị cấp trên cũng như các đơn vị liên quan có thể quyết định kết thúc các dịch vụ của đơn vị gây lỗi, tùy thuộc vào các quy định của pháp luật, quy định trong Quy chế chứng thực và hợp đồng với đơn vị gây lỗi nêu trên

8.6. Công bố kết quả

Các kết quả của các cuộc kiểm tra của các đơn vị thành viên của MISA-CA sẽ được công bố tại website của dịch vụ.

9. CÁC VẤN ĐỀ PHÁP LÝ VÀ KINH DOANH KHÁC

9.1. Phí dịch vụ

9.1.1. Phí cấp mới, gia hạn, thay đổi cặp khóa, thay đổi chứng thư

Khách hàng sử dụng dịch vụ MISA-CA phải trả phí khi xin cấp, gia hạn, thay đổi cặp khóa, thay đổi chứng thư số. Biểu giá sẽ được niêm yết trên website chính thức của dịch vụ.

9.1.2. Phí dịch vụ cung cấp thông tin về chứng thư số

Các thuê bao của dịch vụ MISA-CA không phải trả phí để truy cập thông tin chứng thư hay dịch vụ cung cấp thông tin chứng thư trực tuyến cho đối tác tin cậy.

9.1.3. Phí dịch vụ cung cấp thông tin về trạng thái chứng thư và việc thu hồi chứng thư

MISA-CA không thu phí dịch vụ duy trì trạng thái kiểm tra chứng thư số (OCSP).

9.1.4. Lệ phí sử dụng cho các dịch vụ khác

Các thành phần tham gia dịch vụ MISA-CA không phải trả phí khi truy cập Quy chế chứng thực. Việc sử dụng văn bản với các mục đích khác như sao chép, phân bổ lại sẽ phải được sự chấp thuận bằng văn bản của MISA-CA.

9.1.5. Quy chế hoàn trả phí

MISA-CA sẽ đưa ra phạm vi cho việc áp dụng chính sách hoàn trả phí. Chính sách này sẽ được đưa lên website hoặc đưa vào bản thoả thuận với khách hàng trong hợp đồng dịch vụ.

9.1.6. Phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số

MISA-CA phải có trách nhiệm nộp đầy đủ phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số cho Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia để duy trì trực tuyến cơ sở dữ liệu về chứng thư số và các thông tin khác phục vụ việc kiểm tra trạng thái chứng thư số, hiệu lực chữ ký số tuân theo các quy định tại Nghị định số 130/2018/NĐ-CP, Thông tư số 305/2016/TT-BTC và Thông tư số 17/2018/TT-BTC.

9.2. Trách nhiệm tài chính

9.2.1. Bảo hiểm

MISA-CA sẽ duy trì tính thương mại hợp lý cho các mức bảo hiểm đối với các lỗi hay thiếu sót thông qua các chương trình bảo hiểm của các công ty bảo hiểm hoặc tự cam kết bảo hiểm.

9.2.1.1. Các trường hợp MISA-CA tiến hành đền bù bảo hiểm và mức đền bù bảo hiểm

MISA-CA tiến hành đền bù bảo hiểm cho các trường hợp sau:

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

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

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

- Các trường hợp sử dụng chứng thư không được đề cập đến trong Quy chế chứng thực này
- Các trường hợp giả mạo chứng thư số
- Các trường hợp sử dụng, cấu hình thiết bị không phù hợp, không nằm trong; trách nhiệm của CA được sử dụng trong quá trình xử lý chứng thư
- Khách hàng đánh mất hoặc để lộ code PIN bảo vệ khoá bí mật

9.2.2. Các tài sản khác

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

9.2.3. Bảo hiểm hoặc bảo hành cho các đơn vị cuối

Không có quy định

9.3. Vấn đề an toàn và bảo mật thông tin

Không có một đơn vị thành viên nào của MISA-CA được phép cung cấp cho đơn vị khác tên thuê bao và các thông tin cá nhân của người đăng ký và thuê bao trừ khi có

một điều khoản trong Quy chế chứng thực quy định vấn đề này. Nếu có vi phạm nào trong các đơn vị về vấn đề rò rỉ thông tin thì sẽ có chế tài xử lý hành chính hoặc thương mại. Các thông tin được cung cấp sẽ được chỉ rõ trong Quy chế chứng thực và trong các hợp đồng song phương khác.

9.3.1. Các loại thông tin được giữ bí mật

Thông tin được cung cấp bởi các thuê bao, hoặc đối tác tin tưởng của các thuê bao sử dụng hay dựa trên chứng thư số của MISA-CA, các dữ liệu chi tiết liên quan đến kiểm tra kỹ thuật, các thông tin về đảm bảo an toàn, khắc phục sự cố thảm họa, … một số thông tin khác theo thoả thuận giữa thuê bao và MISA-CA, không bao gồm các thông tin mô tả trong Mục 9.3.2 dưới đây, sẽ được coi là là thông tin mật. Thông tin này được coi là bí mật và không được tiết lộ, trừ các trường hợp sau:

- Các đơn vị thành viên của MISA-CA sẽ có quyền trao đổi các thông tin này với nhau theo quy định nội bộ của công ty
- Các thông tin này cũng có thể được trao đổi với các đơn đơn vị hỗ trợ MISA-CA trong quá trình xác minh đối tác
- Các thông tin cũng phải tiết lộ khi bắt buộc theo thủ tục tố tụng pháp luật, tư pháp hoặc hành chính hoặc theo yêu cầu của cơ quan pháp luật
- Các đơn vị của MISA-CA cũng có quyền được tiết lộ thông tin đó với các cố vấn pháp lý và tài chính hỗ trợ trong việc liên kết với cơ quan luật pháp, tư pháp, hành chính hoặc các thủ tục như yêu cầu của pháp luật để chứng minh năng lực, tư vấn pháp luật, kế toán, ngân hàng và các nguồn tài trợ và cố vấn của họ trong kết nối với các vụ sáp nhập, mua lại hoặc tái tổ chức

9.3.2. Các loại thông tin không được coi là bí mật

Các thông tin sau đây không được coi là bí mật:

- Thông tin trong chứng thư số của MISA-CA hay danh sách chứng thư số bị thu hồi
- Thông tin trong các Quy chế chứng thực
- Thông tin được tiết lộ không phải do lỗi của các thành viên trong MISA-CA
- Thông tin đã bị cơ quan pháp luật thu thập từ các thành viên trong MISA-CA
- Thông tin được công bố khi đã thông qua chủ sở hữu của nó.

9.3.3. Trách nhiệm bảo vệ thông tin bí mật

MISA-CA đảm bảo các thông tin riêng tư không bị tiết lộ với bên thứ 3 khi chưa có sự đồng ý của thuê bao.

9.4. Tính riêng tư của thông tin cá nhân

9.4.1. Chính sách đảm bảo tính riêng tư

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

9.4.2. Những thông tin coi là riêng tư

Tất cả những thông tin về thuê bao không được công bố công khai đều được coi là riêng tư. Những thông tin công bố công khai bao gồm chứng thư số của thuê bao, danh sách chứng thư số đã ban hành, danh mục chứng thư số bị thu hồi (CRL) và dịch vụ cung cấp trạng thái chứng thư số trực tuyến (OCSP).

9.4.3. Thông tin không được coi là riêng tư

Tất cả các thông tin được công khai trong chứng thư số và những thông tin công bố công khai bao gồm danh sách chứng thư số đã ban hành, danh mục chứng thư số bị thu hồi (CRL) và dịch vụ cung cấp trạng thái chứng thư số trực tuyến (OCSP) được coi như không phải là thông tin riêng tư.

9.4.4. Trách nhiệm bảo vệ thông tin riêng tư

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

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

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

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

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

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

9.4.7. Các trường hợp làm lộ thông tin khác

Không có quy định.

9.5. Quyền sở hữu trí tuệ

9.5.1. Quyền sở hữu những thông tin chứng thư và thông tin thu hồi chứng thư.

MISA-CA có quyền sở hữu trí tuệ liên quan đến các chứng thư số mà Công ty đã cấp và chứng thư số thu hồi.

MISA-CA được quyền sao chép và phân phối chứng thư số mà không cần phải trả phí.

MISA-CA và thuê bao cho phép người nhận sử dụng các thông tin về tình trạng thu hồi chứng thư số cũng như các thông tin về khóa công khai của chứng thư số để thực hiện các công việc theo thoả thuận của mình.

9.5.2. Quyền sở hữu quy chế chứng thực

MISA-CA có quyền sở hữu trí tuệ đối với các nội dung và bản thân Quy chế chứng thực này.

9.5.3. Quyền sở hữu tên

Thuê bao có quyền sở hữu đối với các thương hiệu, tên dịch vụ, tên chứng thư số. Việc đăng ký và thực hiện các quyền sở hữu này tuân thủ theo quy định của pháp luật về sở hữu trí tuệ.

9.5.4. Quyền sở hữu khoá và các tài liệu của khoá

Cặp khóa bí mật và công khai tương ứng với chứng thư số của thuê bao thuộc quyền sở hữu của MISA-CA và thuê bao, được bảo vệ theo quy định của pháp luật về sở hữu trí tuệ.

9.6. Vấn đề đại diện và bảo lãnh

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

MISA-CA đảm bảo rằng:

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

9.6.2. Đại diện cho thuê bao và vấn đề bảo lãnh

Thuê bao đảm bảo rằng:

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

9.6.3. Đại diện cho người nhận và vấn đề bảo lãnh

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

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

9.6.4. Đại diện và bảo lãnh cho các bên liên quan khác

Ngoài MISA-CA, RA, thuê bao và người nhận không có tuyên bố và cam kết của đối tượng nào khác được MISA-CA quy 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 MISA-CA từ chối bảo lãnh.

9.8. Giới hạn về trách nhiệm pháp lý

Trong giới hạn của luật pháp, hợp đồng thuê bao và người nhận có thể có giới hạn khả năng chịu trách nhiệm pháp lý của MISA-CA. Trách nhiệm pháp lý của thuê bao và MISA-CA sẽ được thiết lập trong hợp đồng cung cấp dịch vụ.

MISA-CA sẽ không chịu trách nhiệm pháp lý đối với các hoạt động nằm ngoài phạm vi cung cấp dịch vụ chứng thực chữ ký số.

9.9. Vấn đề bồi thường cho MISA-CA

9.9.1. Vấn đề bồi thường của thuê bao

Trong trường hợp xảy ra sự cố mà do lỗi của MISA mà phải bồi thường thì MISA sẽ sử dụng tiền ký quỹ để thực hiện việc bồi thường này.

Trong giới hạn được cho phép bởi pháp luật, thuê bao phải bồi thường cho MISA-CA và người nhận (nếu có giao dịch) khi xảy ra những trường hợp sau:

- Thuê bao cung cấp thông tin không đúng với thực tế trên yêu cầu cấp chứng thư. Trong từng trường hợp sự miêu tả này là sai hay bỏ quên, được làm cẩu thả hoặc với mục đích lừa đảo.
- Lỗi của thuê bao trong việc bảo vệ khóa bí mật, sử dụng hệ thống không tin cậy, hoặc không thực hiện các biện pháp phòng ngừa cần thiết để tránh gây hậu quả.

- Việc sử dụng tên của khách hàng (kể cả việc không giới hạn tên chung, tên miền, hoặc địa chỉ thư điện tử) vi phạm quyền sở hữu trí tuệ của bên thứ 3.

Hợp đồng với khách hàng có thể có những bổ sung phù hợp.

9.9.2. Vấn đề bồi thường của người nhận

Trong phạm vi cho phép của pháp luật, người nhận có trách nhiệm bồi thường cho MISA-CA trong các trường hợp sau:

- Không thực hiện những bắt buộc đối với người nhận và làm thiệt hại cho MISA-CA hoặc các bên liên quan.
- Sử dụng không đúng phương pháp hoặc sử dụng sai mục đích các dịch vụ do MISA-CA cung cấp gây thiệt hại hoặc phá huỷ dữ liệu của MISA-CA

Thỏa thuận với người nhận có thể có thêm một số nghĩa vụ khác.

9.10. Thời hạn và kết thúc

9.10.1. Thời hạn

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

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

9.10.2. Kết thúc

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

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

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

9.11. Thông báo cho các bên liên quan

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

9.12. Những điều sửa đổi

9.12.1. Thủ tục sửa đổi

Quy chế này được bổ sung, sửa đổi bởi MISA-CA. Nội dung sửa đổi được lưu tại mục 2.2

9.12.2. Cơ chế và thời gian thông báo

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

9.12.3. Các trường hợp OID cần phải thay đổi

Các trường hợp OID cần phải thay đổi tuân theo quy định của bộ Thông tin và truyền thông.

9.13. Các điều khoản tranh chấp

9.12.1. Tranh chấp giữa MISA-CA, đối tác và thuê bao

Việc giải quyết tranh chấp giữa MISA-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.

9.12.2. Tranh chấp với thuê bao hay người nhận

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

9.14. Áp dụng luật

Quy chế chứng thực này được xây dựng theo quy định của pháp luật của nước Cộng hòa xã hội chủ nghĩa Việt Nam. Trong quá trình cung cấp, sử dụng dịch vụ MISA-CA cũng như giải quyết các tranh chấp phát sinh các thành phần tham gia dịch vụ MISA-CA cũng như các bên liên quan sẽ áp dụng pháp luật của nước Cộng hòa xã hội chủ nghĩa Việt Nam.

Hệ thống pháp luật chính có liên quan bao gồm:

- Luật giao dịch điện tử;
- Luật công nghệ thông tin;

- Luật viễn thông;
- Luật thương mại;
- Luật doanh nghiệp;
- ….

9.15. Chấp hành theo hệ thống pháp luật phù hợp

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

9.16. Các điều khoản chung

9.16.1. 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 Quy chế chứng thực được giữ lại không thể thi hành được bởi một phiên tòa hay một cuộc xét xử có thẩm quyền, phần còn lại của Quy chế chứng thực vẫn có hiệu lực.

9.16.4.Sự thực thi

Bất kỳ một bên nào chiếm ưu thế trong những tranh cãi nảy sinh ra 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

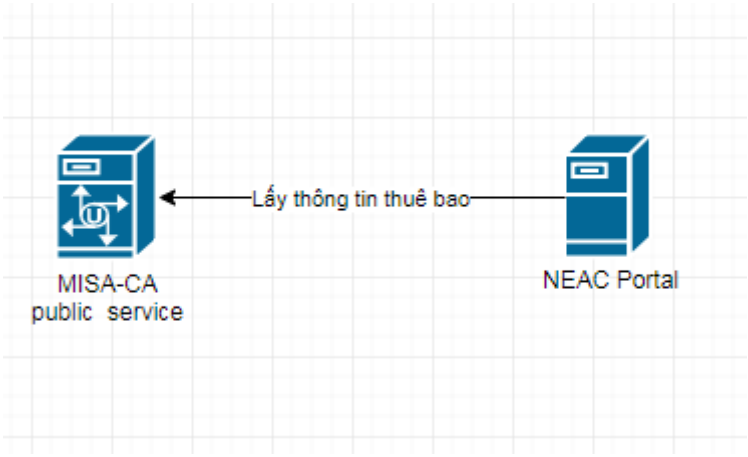
Trong phạm vi luật pháp cho phép, thỏa thuận của thuê bao và thỏa thuận bên liên quan bắt buộc phải tuân theo các điều khoản bảo vệ dịch vụ MISA-CA.

9.17. Các điều khoản khác

9.17.1. Phương án cung cấp trực tuyến thông tin thuê bao cho Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia

Hệ thống MISA-CA được thiết kế có thể cung cấp thông tin thuê bao trực tuyến cho NEAC theo một trong hai cách dưới đây:

- Phương án 1: MISA sẽ cung cấp service public internet để NEAC có thể chủ động lấy thông tin thuê bao từ hệ thống MISA-CA khi cần.



- Phương án 2: NEAC cung cấp cổng service để MISA chủ động đồng bộ dữ liệu thông tin thuê bao lên định kỳ.