QUY CHẾ CHỨNG THỰC
Certificate Practices Statement (CPS)

DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG TỪ XA

*****

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

13	OCSP	Online Certificate Status Protocol – Giao thức kiểm tra trạng thái chứng thư số trực tuyến
14	LDAP	Lightweight Directory Access Protocol – Giao thức chuẩn truy cập thư mục.
15	Ứng viên	Là một người, một tổ chức hay một thực thể đã đăng ký nhưng chưa được cấp chứng thư số
16	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
17	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
18	RAR Center	Trung tâm nghiên cứu, ứng dụng dữ liệu dân cư và căn cước công dân
19	VNeID	Là một ứng dụng trên thiết bị di động được phát triển bởi Trung tâm dữ liệu quốc gia về dân cư của Bộ Công An Việt Nam, với mục đích thay thế cho giấy tờ truyền thống. Ứng dụng này được xây dựng trên nền tảng cơ sở dữ liệu về định danh, dân cư và xác thực điện tử, cung cấp các tiện ích phát triển công dân số, chính phủ số, xã hội số.

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.

Tài liệu quy chế chứng thực tuân thủ quy định của Luật Giao dịch điện tử ngày 22 tháng 6 năm 2023, Nghị định số 23/2025/NĐ-CP ngày 21 tháng 02 năm 2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ tin cậy và các quy định pháp luật liên quan.

1.2. Tên và dấu hiệu nhận diện 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 theo mô hình ký số từ xa. 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. Quy chế này không phải thỏa thuận về mặt pháp lý giữa MISA-CA và các thực thể sử dụng dịch vụ cũng như bất kỳ thành phần khác tham gia vào dịch vụ chữ ký số và chứng thực chữ ký số theo mô hình ký số từ xa.

Mục tiêu của văn bản này là:

a) 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.

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

c) 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 theo mô hình ký số trên thiết bị di động và ký số từ xa.

1.3. Các thành phần trong hệ thống dịch vụ chứng thực chữ ký số

1.3.1. Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia (Trung tâm Chứng thực điện tử quốc gia)

- Trung tâm Chứng thực điện tử quốc gia (NEAC) là đơn vị trực thuộc Bộ Thông tin và Truyền thông có chức năng phát triển hạ tầng phục vụ hoạt động giao dịch điện tử, chữ ký điện tử và xác thực điện tử; đề xuất các chính sách, quy hoạch trong lĩnh vực giao dịch điện tử, chữ ký điện tử, xác thực điện tử. NEAC là Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia (Root Certification Authority).
- Tên giao dịch tiếng Anh: The National Electronic Authentication Centre.
- Tên viết tắt: NEAC.

1.3.2. 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 vụ 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:

a) Thẩm định tất cả các yêu cầu cấp phát chứng thư

b) 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

c) Duy trì trực tuyến cơ sở dữ liệu về chứng thư số (còn hiệu lực, hết hạn, gia hạn, cấp mới, thu hồi)

d) Cung cấp các dịch vụ khác có liên quan cho người sử dụng

e) CA nhất thiết phải đảm bảo thực hiện các chức năng trên một cách trực tiếp

1.3.3. Thuê bao

Thuê bao/Khách hàng 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.

1.3.4. Bên tin tưởng

Bên tin tưởng là một cá nhân hay một tổ chức được tin tưởng, kiểm tra chứng thư số của đối tác theo thỏa thuận và cam kết giữa hai bên. Người nhận có quyền xác nhận các thông tin của thuê bao trong chứng thư số là đúng sự thật. Người nhận căn cứ vào các thông tin trong chứng thư số là chính xác và các thông tin trong CPS để đưa ra quyết định thực hiện thỏa thuận và cam kết giữa hai bên.

1.3.5. Các bên khác

Trung tâm nghiên cứu, ứng dụng dữ liệu dân cư và căn cước công dân (RAR Center) thực hiện kết nối với MISA-CA thực hiện thí điểm giải pháp "Cổng ký số từ xa tập trung trên nền tảng định danh và xác thực điện tử VneID" theo Công văn số… nhằm thực hiện nhiệm vụ "*Đảm bảo 100% các giao dịch của Công dân số được định danh, ký số, xác thực, các hợp đồng điện tử được định danh, ký số"*.

1.4. Mục đích sử dụng chứng thư chữ ký số

1.4.1. Các trường hợp sử dụng chứng thư chữ ký 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.

Hệ thống MISA-CA cung cấp các loại chứng thư số như sau:

- Chứng thư số cho người dùng cá nhân, tổ chức, doanh nghiệp thông qua thiết bị tạo chữ ký đảm bảo (QSCD) đáp ứng 16/2019/TT-BTTTT Quy định Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa.
- Các chứng thư được cung cấp với các độ dài khóa: 2048 bit, 4096 bit. Tùy theo từng loại chứng thư, thời gian có hiệu lực được quy định tại 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 chữ ký số

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. Quản lý quy chế chứng thực

1.5.1. Tổ chức quản lý quy chế chứng thực

Công ty cổ phần MISA, Tầng 9 Tòa nhà Technosoft, phố Duy Tân, Phường Cầu Giấy, Thành phố Hà Nội.

1.5.2. Thông tin 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, Phường 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. Cơ quan, tổ chức đánh giá sự phù hợp của quy chế chứng thực với pháp luật

Bộ Khoa học và công nghệ (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 duyệt, ban hành quy chế chứng thực

Mọi thay đổi trong Quy chế chứng thực chữ ký số này đều phải đảm bảo tuân thủ đúng quy định của pháp luật Việt Nam về dịch vụ chứng thực chữ ký số công cộng và đảm bảo không ảnh hưởng đến quyền lợi của thuê bao.

Khi có sự thay đổi thông tin trong quy chế chứng thực, MISA-CA phải thông báo bằng văn bản đến Bộ Khoa học và công nghệ (Trung tâm Chứng thực điện tử quốc gia - RootCA).

Đồng thời, tất cả những phiên bản đã sửa đổi hoặc cập nhật thông tin được công bố tại địa chỉ https://esign.misa.vn/download/.

1.6. Các định nghĩa và tên viết tắt

Xem ở bảng THUẬT NGỮ VÀ TỪ VIẾT TẮT.

2. TRÁCH NHIỆM LƯU TRỮ VÀ CÔNG BỐ THÔNG TIN

2.1. Lưu trữ

a) MISA-CA cam kết xây dựng và duy trì hệ thống thông tin cung cấp dịch vụ tin cậy, bảo đảm các điểm tiếp nhận, phần mềm, ứng dụng đề nghị phát hành chứng thư số tuân thủ đầy đủ các quy định của pháp luật về xác thực và lưu trữ thông tin thuê bao. MISA-CA chịu hoàn toàn trách nhiệm trước pháp luật về tính chính xác, toàn vẹn của thông tin thuê bao được xác thực, lưu trữ và quản lý tại hệ thống.

MISA-CA thiết lập và duy trì cơ sở dữ liệu thông tin thuê bao tập trung để nhập, lưu trữ và quản lý thông tin trong suốt quá trình cung cấp dịch vụ. Thông tin lưu trữ bao gồm:

- Hồ sơ đề nghị phát hành chứng thư chữ ký số theo quy định pháp luật.
- Thông tin về ngày bắt đầu và ngày chấm dứt sử dụng dịch vụ của thuê bao.
- Danh sách các chứng thư chữ ký số có hiệu lực, hết hiệu lực, bị tạm dừng hoặc thu hồi.
- Các sự kiện, nhật ký hệ thống liên quan đến quá trình xác thực thuê bao.

Thời hạn lưu trữ

Thông tin thuê bao và dữ liệu liên quan được lưu trữ, bảo mật theo quy định của pháp luật về lưu trữ với thời hạn cụ thể như sau:

Trong thời gian thuê bao sử dụng dịch vụ: Lưu trữ đầy đủ, liên tục, chính xác và cập nhật.

Sau khi thuê bao chấm dứt sử dụng dịch vụ: Tiếp tục lưu trữ thông tin trong cơ sở dữ liệu tối thiểu 02 năm.

Trường hợp đặc biệt (Tạm đình chỉ/Thu hồi giấy phép CA): Lưu trữ toàn bộ hồ sơ, dữ liệu thuê bao tối thiểu 05 năm kể từ khi giấy phép bị tạm đình chỉ, thu hồi hoặc không được cấp lại.

Khả năng tra cứu và kết nối dữ liệu

MISA-CA đảm bảo hệ thống kỹ thuật cho phép người sử dụng truy nhập trực tuyến để tra cứu danh sách chứng thư chữ ký số, trạng thái chứng thư chữ ký số 24 giờ trong ngày và 7 ngày trong tuần.

MISA-CA thực hiện kết nối cơ sở dữ liệu thông tin thuê bao tập trung với:

Cơ sở dữ liệu của Bộ Khoa học và Công nghệ: Để phục vụ công tác quản lý nhà nước.

Cơ sở dữ liệu quốc gia về dân cư: Để tham chiếu, đối soát và xác thực thông tin thuê bao, đảm bảo định danh đúng chủ thể theo quy định của pháp luật về định danh và xác thực điện tử.

2.2. Công bố thông tin

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:

a) 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.

b) 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.

c) 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.

d) 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.

e) 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 thông tin

MISA-CA cập nhật các thông tin công bố bao gồm Quy chế chứng thực chữ ký số, chính sách, thỏa thuận…: được cập nhật khi có sự thay đổi.

2.4. Kiểm soát truy nhập thông tin

a) 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 Khoa học và công nghệ (Trung tâm Chứng thực điện tử Quốc gia).

b) Sau khi được phê duyệt, Quy chế chứng thực được công bố ngay lập tức bởi hệ thống MISA-CA

c) 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 YÊU CẦU ĐỀ NGHỊ PHÁT HÀNH CHỨNG THƯ CHỮ KÝ SỐ

3.1. Đặt tên

3.1.1. Các kiểu 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.
Common Name (CN)	Tên thuê bao sở hữu chứng thư số, tên miền nếu là chứng thư số SSL
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 hộ gia đình, hộ kinh doanh là số định danh cá nhân của người đại diện hộ gia đình, đại diện hộ kinh doanh, cá nhân kinh doanh ● 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. Cần tên có ý nghĩa

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. Ẩn danh hoặc bút danh

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 hình thức tên khác nhau

Không có quy định.

3.1.5. Tính duy nhất của tên

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 nhãn 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 minh đề nghị phát hành chứng thư chữ ký số

3.2.1. Phương pháp chứng minh quyền 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 minh danh tính đối với tổ chức

Trường hợp người sử dụng là tổ chức đăng ký cấp chứng thư chữ ký số, MISA-CA sẽ thực hiện quy trình đăng ký và xác thực bằng một trong hai phương thức: (i) xác thực định danh thủ công hoặc (ii) xác thực định danh điện tử.

a) *Phương pháp xác thực định danh thủ công*

i. Đối với thông tin của cá nhân thuộc tổ chức: MISA-CA thực hiện xác thực thông tin định danh của người đăng ký đúng với cá nhân sử dụng chứng thư chữ ký số bằng cách gặp trực tiếp hoặc các biện pháp tương đương.

ii. Đối với thông tin của tổ chức: 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 quan 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 chữ ký 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 hoặc các biện pháp tương đương.

iii. Tổ chức, cá nhân 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

b) *Phương pháp xác thực định danh điện tử*

Quy trình đăng ký cấp chứng thư chữ ký số bằng phương thức điện tử gồm các bước sau:

Bước	Mô tả yêu cầu
Bước 1	**Người sử dụng khởi tạo yêu cầu**
	● Trường hợp người sử dụng khởi tạo yêu cầu trực tiếp trên hệ thống của MISA-CA: - Người sử dụng tiến hành khởi tạo và gửi yêu cầu cấp chứng thư chữ ký số lên hệ thống MISA-CA.

	- MISA-CA tiếp nhận thông tin đăng ký và gửi email cho người sử dụng yêu cầu cung cấp hồ sơ thuê bao bản gốc và chuẩn bị để thực hiện xác thực định danh điện tử. - Trước khi xác thực định danh diện tử, MISA-CA yêu cầu người sử dụng xác nhận đọc và đồng ý với các điều khoản trong thỏa thuận được xác lập giữa MISA và người sử dụng để tiếp tục đăng ký cấp chứng thư chữ ký số trên ứng dụng của MISA cài đặt trên thiết bị di động của người sử dụng. Việc xác nhận đồng ý của người sử dụng được MISA-CA ghi nhận thành bản ghi trong cơ sở dữ liệu, bản ghi này chứa các thông tin xác nhận (thông tin người dùng, thời gian, thiết bị, thông tin trình duyệt…). Trường hợp người dùng sử dụng ứng dụng VNeID, người dùng đăng nhập vào ứng dụng VNeID bằng thông tin công dân đã xác minh, sử dụng tính năng Đăng ký chứng thư chữ ký số để khởi tạo yêu cầu cấp chứng thư chữ ký số gửi đến hệ thống MISA-CA
Bước 2	**Thu thập thông tin đăng ký của thuê bao và hồ sơ thuê bao**
	● Đối với thuê bao đăng ký trên hệ thống của MISA-CA Người sử dụng chuẩn bị hồ sơ đăng ký theo quy định tại Mục 3.2.2 và cung cấp trực tiếp thông tin và hồ sơ bản gốc cho MISA-CA thông qua ứng dụng của MISA trên thiết bị di động, trong đó: - Đơn đề nghị cấp chứng thư chữ ký số được Người sử dụng trực tiếp điền thông tin trên ứng dụng của MISA và ký xác nhận bằng phương thức điện tử; - Các hồ sơ, giấy tờ khác được thu thập trực tiếp tại thời điểm đăng ký ứng dụng của MISA. Thao tác quét các trường thông tin từ hồ sơ thuê bao được thực hiện tự động thông qua công nghệ quét quang học (OCR) và đảm bảo an toàn thông tin cá nhân theo quy định của pháp luật an toàn thông tin. ● Trường hợp người dùng sử dụng ứng dụng VNeID, thông tin đăng ký của thuê bao và hồ sơ thuê bao sẽ được gửi trực tiếp đến hệ thống MISA-CA sau khi được người dùng đồng ý với các Điều khoản sử dụng và Chính sách quyền riêng tư, xác nhận chia sẻ thông tin từ hệ thống định danh và xác thực điện tử cho MISA.
Bước 3	**Xác minh các thông tin đăng ký của thuê bao và hồ sơ thuê bao**

	● Đối với thuê bao đăng ký trên hệ thống của MISA-CA, MISA-CA tiếp nhận và xác minh thông tin và hồ sơ thuê bao của người sử dụng, cụ thể: - Người sử dụng thực hiện di chuyển chậm hồ sơ thuê bao bản gốc bao gồm mặt trước, mặt sau và góc cạnh để lấy được các góc thể hiện tính chất vật lý đặc biệt của hồ sơ thuê bao theo hướng dẫn và yêu cầu chi tiết trên ứng dụng của MISA. - Các hồ sơ thuê bao phải là bản gốc, đảm bảo tính toàn vẹn, không được chỉnh sửa và được xuất trình trực tiếp trước camera của thiết bị di động tại thời điểm đăng ký. Toàn bộ quá trình xuất trình hồ sơ thuê bao được thực hiện trên ứng dụng của MISA và được ghi lại dưới dạng video sequence nhằm mục đích lưu trữ và xác minh tính chân thực của hồ sơ thuê bao. Thuê bao có thể nộp giấy chứng nhận đăng ký doanh nghiệp hoặc giấy chứng nhận đầu tư hoặc giấy chứng nhận đăng ký hộ kinh doanh được cơ quan nhà nước cấp ở dạng điện tử. ● Trường hợp người dùng sử dụng ứng dụng VNeID, thông tin đăng ký của thuê bao và hồ sơ thuê bao sẽ được gửi trực tiếp đến hệ thống MISA-CA sau khi được người dùng xác nhận đúng thông tin và đồng ý để hệ thống xác nhận kích hoạt. Hồ sơ xác thực định danh đảm bảo đáp ứng quy định tại điều 3.2.2.
Bước 4	**Đối chiếu với người sử dụng**
	● Đối với thuê bao đăng ký trên hệ thống của MISA-CA, MISA-CA thực hiện so sánh gương mặt của người sử dụng với hình ảnh tương ứng trong hồ sơ thuê bao để đảm bảo người sử dụng chính là chủ sở hữu hồ sơ thuê bao, cụ thể: - Người sử dụng thực hiện quay video streaming về khuôn mặt theo hướng dẫn và yêu cầu chi tiết trên ứng dụng của MISA. - Toàn bộ quy trình quay video streaming về khuôn mặt được thực hiện trực tiếp tại thời điểm đăng ký bằng ứng dụng của MISA, không được ghi hình trước. Video streaming sẽ được ghi hình lại nhằm mục đích lưu trữ và xác minh tính chân thực của hồ sơ thuê bao. ● Trường hợp người dùng sử dụng ứng dụng VNeID, thông tin đăng ký của thuê bao và hồ sơ thuê bao sẽ được gửi trực tiếp đến hệ

	thống MISA-CA để thực hiện xác nhận dựa trên dữ liệu công dân đã được xác minh. Hồ sơ xác thực định danh đảm bảo đáp ứng quy định tại điều 3.2.2.
Bước 5	**Thông báo kết quả và lưu trữ thông tin đăng ký**
	● Đối với trường hợp người dùng đăng ký trực tiếp với MISA-CA Sau khi đã xác minh thông tin hồ sơ thuê bao, - MISA-CA trả kết quả (từ chối cấp hoặc cấp chứng thư chữ ký số) cho người sử dụng qua email/tài khoản người sử dụng đã đăng ký với MISA-CA. - Trường hợp xác minh thông tin hồ sơ thuê bao hợp lệ, MISA-CA yêu cầu người sử dụng xác nhận đọc và đồng ý với các điều khoản trong thỏa thuận xác lập với người dùng. MISA-CA trả kết quả (từ chối cấp hoặc cấp chứng thư chữ ký số) cho người sử dụng qua email/tài khoản người sử dụng đã đăng ký với MISA-CA. ● Đối với trường hợp người dùng đăng ký qua ứng dụng VNeID, sau khi đã xác minh hồ sơ thuê bao theo dữ liệu công dân: - MISA-CA trả kết quả (từ chối cấp hoặc cấp chứng thư chữ ký số) cho người sử dụng thông qua ứng dụng VNeID ● Toàn bộ thông tin, dữ liệu đăng ký của người sử dụng được lưu trữ an toàn, bảo mật, được sao lưu dự phòng, đảm bảo sự toàn vẹn của dữ liệu để phục vụ cho công tác kiểm tra, đối chiếu, giải quyết, tra soát, khiếu nại, tranh chấp và cung cấp thông tin khi có yêu cầu từ cơ quan quản lý nhà nước có thẩm quyền; đáp ứng quy định của pháp luật về dịch vụ chứng thực chữ ký số và an toàn thông tin.

c) Hồ sơ xác thực định danh

- Tổ chức, cá nhân 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.
- Hồ sơ đăng ký bao gồm:

i. Đơn đề nghị cấp dạng bản giấy hoặc điện tử theo mẫu của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng. Trường hợp tổ chức, cá nhân đăng ký sử dụng chữ ký số trên ứng dụng VneID thì sẽ cần đồng ý cho phép RAR Center chia sẻ, xác thực dữ liệu với mục đích đăng ký và sử dụng chữ ký số với MISA-CA.

ii. Hồ sơ, tài liệu kèm theo bao gồm:

- Đối với tổ chức: 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 hoặc giấy chứng nhận đăng ký hộ kinh doanh và giấy tờ tùy thân của người đại diện theo pháp luật của tổ chức, bao gồm thẻ căn cước công dân hoặc thẻ căn cước hoặc giấy chứng nhận căn cước hoặc tài khoản định danh điện tử mức độ 2 hoặc hộ chiếu; hoặc tài khoản định danh điện tử của tổ chức.
- Đối với cá nhân thuộc tổ chức: CCCD/Hộ chiếu của người xin cấp thuê bao; Văn bản ủy quyền cho cơ quan, tổ chức xin cấp .

iii. Cá nhân, tổ chức có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc nộp bản sao trình kèm bản chính để đối chiếu hoặc cung cấp dữ liệu điện tử để tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng sử dụng, khai thác theo quy định tại khoản iv Điều này.

iv. Trường hợp cá nhân, người đại diện theo pháp luật của tổ chức cung cấp hoặc sử dụng thông tin trong thẻ căn cước công dân hoặc thẻ căn cước hoặc căn cước điện tử hoặc giấy chứng nhận căn cước hoặc thông tin trong tài khoản định danh điện tử mức độ 2 của cá nhân hoặc thông tin trong tài khoản định danh của tổ chức thì tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng (đã có văn bản chấp thuận cho phép thực hiện kết nối với hệ thống định danh và xác thực điện tử theo quy định pháp luật về định danh và xác thực điện tử hoặc có đầy đủ phương tiện đọc dữ liệu trong chíp điện tử, dữ liệu trong tài khoản định danh điện tử mức độ 2) khai thác dữ liệu trong chíp điện tử, dữ liệu của tài khoản định danh điện tử mức độ 2 của cá nhân, tài khoản định danh điện tử của tổ chức, không yêu cầu cá nhân, người đại diện theo pháp luật của tổ chức nộp các hồ sơ, tài liệu theo quy định tại khoản iii Điều này.

3.2.3. Xác minh danh tính đối với cá nhân

Trường hợp người sử dụng là cá nhân đăng ký cấp , MISA-CA sẽ thực hiện quy trình đăng ký và xác thực bằng một trong hai phương thức: (i) xác thực định danh thủ công hoặc (ii) xác thực định danh điện tử.

a) Phương pháp xác thực định danh thủ công

i. Đối với thông tin của cá nhân: MISA-CA thực hiện xác thực thông tin định danh của người đăng ký đúng với cá nhân sử dụng bằng cách gặp trực tiếp hoặc các biện pháp tương đương.

ii. Cá nhân 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

b) Phương pháp xác thực định danh điện tử

Quy trình đăng ký cấp chứng thư chữ ký số bằng phương thức điện tử gồm các bước sau:

Bước	Mô tả yêu cầu
Bước 1	**Người sử dụng khởi tạo yêu cầu**
	● Trường hợp người sử dụng khởi tạo yêu cầu trực tiếp trên hệ thống của MISA-CA: - Người sử dụng tiến hành khởi tạo và gửi yêu cầu cấp chứng thư chữ ký số lên hệ thống MISA-CA. - MISA-CA tiếp nhận thông tin đăng ký và gửi email cho người sử dụng yêu cầu cung cấp hồ sơ thuê bao bản gốc và chuẩn bị để thực hiện xác thực định danh điện tử. - Trước khi xác thực định danh diện tử, MISA-CA yêu cầu người sử dụng xác nhận đọc và đồng ý với các điều khoản trong thỏa thuận được xác lập giữa MISA và người sử dụng để tiếp tục đăng ký cấp chứng thư chữ ký số trên ứng dụng của MISA cài đặt trên thiết bị di động của người sử dụng. Việc xác nhận đồng ý của người sử dụng được MISA-CA ghi nhận thành bản ghi trong cơ sở dữ liệu, bản ghi này chứa các thông tin xác nhận (thông tin người dùng, thời gian, thiết bị, thông tin trình duyệt…). ● Trường hợp người dùng sử dụng ứng dụng VNeID, người dùng đăng nhập vào ứng dụng VNeID bằng thông tin công dân đã xác minh, sử dụng tính năng Đăng ký chứng thư chữ ký số để khởi tạo yêu cầu cấp chứng thư chữ ký số gửi đến hệ thống MISA-CA
Bước 2	**Thu thập thông tin đăng ký của thuê bao và hồ sơ thuê bao**
	● Đối với thuê bao đăng ký trên hệ thống của MISA-CA Người sử dụng chuẩn bị hồ sơ đăng ký theo quy định tại Mục 3.2.3 và cung cấp trực tiếp thông tin và hồ sơ bản gốc cho MISA-CA thông qua ứng dụng của MISA trên thiết bị di động, trong đó: - Đơn đề nghị cấp chứng thư chữ ký số được Người sử dụng trực tiếp điền thông tin trên ứng dụng của MISA và ký xác nhận bằng phương thức điện tử; - Các hồ sơ, giấy tờ khác được thu thập trực tiếp tại thời điểm đăng ký ứng dụng của MISA.

	Thao tác quét các trường thông tin từ hồ sơ thuê bao được thực hiện tự động thông qua công nghệ quét quang học (OCR) và đảm bảo an toàn thông tin cá nhân theo quy định của pháp luật an toàn thông tin. Trường hợp người dùng sử dụng ứng dụng VNeID, thông tin đăng ký của thuê bao và hồ sơ thuê bao sẽ được gửi trực tiếp đến hệ thống MISA-CA sau khi được người dùng đồng ý với các Điều khoản sử dụng và Chính sách quyền riêng tư, xác nhận chia sẻ thông tin từ hệ thống định danh và xác thực điện tử cho MISA.
Bước 3	**Xác minh các thông tin đăng ký của thuê bao và hồ sơ thuê bao**
	● Đối với thuê bao đăng ký trên hệ thống của MISA-CA, MISA-CA tiếp nhận và xác minh thông tin và hồ sơ thuê bao của người sử dụng, cụ thể: - Người sử dụng thực hiện di chuyển chậm hồ sơ thuê bao bản gốc bao gồm mặt trước, mặt sau và góc cạnh để lấy được các góc thể hiện tính chất vật lý đặc biệt của hồ sơ thuê bao theo hướng dẫn và yêu cầu chi tiết trên ứng dụng của MISA. - Các hồ sơ thuê bao phải là bản gốc, đảm bảo tính toàn vẹn, không được chỉnh sửa và được xuất trình trực tiếp trước camera của thiết bị di động tại thời điểm đăng ký. Toàn bộ quá trình xuất trình hồ sơ thuê bao được thực hiện trên ứng dụng của MISA và được ghi lại dưới dạng video sequence nhằm mục đích lưu trữ và xác minh tính chân thực của hồ sơ thuê bao. ● Trường hợp người dùng sử dụng ứng dụng VNeID, thông tin đăng ký của thuê bao và hồ sơ thuê bao sẽ được gửi trực tiếp đến hệ thống MISA-CA sau khi được người dùng xác nhận đúng thông tin và đồng ý để hệ thống xác nhận kích hoạt. Hồ sơ xác thực định danh đảm bảo đáp ứng quy định tại điều 3.2.3
Bước 4	**Đối chiếu với người sử dụng**
	● Đối với thuê bao đăng ký trên hệ thống của MISA-CA, MISA-CA thực hiện so sánh gương mặt của người sử dụng với hình ảnh tương ứng trong hồ sơ thuê bao để đảm bảo người sử dụng chính là chủ sở hữu hồ sơ thuê bao, cụ thể: - Người sử dụng thực hiện quay video streaming về khuôn mặt theo hướng dẫn và yêu cầu chi tiết trên ứng dụng của MISA.

	- Toàn bộ quy trình quay video streaming về khuôn mặt được thực hiện trực tiếp tại thời điểm đăng ký bằng ứng dụng của MISA, không được ghi hình trước. Video streaming sẽ được ghi hình lại nhằm mục đích lưu trữ và xác minh tính chân thực của hồ sơ thuê bao. Trường hợp người dùng sử dụng ứng dụng VNeID, thông tin đăng ký của thuê bao và hồ sơ thuê bao sẽ được gửi trực tiếp đến hệ thống MISA-CA để thực hiện xác nhận dựa trên dữ liệu công dân đã được xác minh. Hồ sơ xác thực định danh đảm bảo đáp ứng quy định tại điều 3.2.3.
Bước 5	**Thông báo kết quả và lưu trữ thông tin đăng ký**
	● Đối với trường hợp người dùng đăng ký trực tiếp với MISA-CA Sau khi đã xác minh thông tin hồ sơ thuê bao, - MISA-CA trả kết quả (từ chối cấp hoặc cấp chứng thư chữ ký số) cho người sử dụng qua email/tài khoản người sử dụng đã đăng ký với MISA-CA. - Trường hợp xác minh thông tin hồ sơ thuê bao hợp lệ, MISA-CA yêu cầu người sử dụng xác nhận đọc và đồng ý với các điều khoản trong thỏa thuận xác lập với người dùng. MISA-CA trả kết quả (từ chối cấp hoặc cấp chứng thư chữ ký số) cho người sử dụng qua email/tài khoản người sử dụng đã đăng ký với MISA-CA. Đối với trường hợp người dùng đăng ký qua ứng dụng VNeID, sau khi đã xác minh hồ sơ thuê bao theo dữ liệu công dân: - MISA-CA trả kết quả (từ chối cấp hoặc cấp chứng thư chữ ký số) cho người sử dụng thông qua ứng dụng VNeID ● Toàn bộ thông tin, dữ liệu đăng ký của người sử dụng được lưu trữ an toàn, bảo mật, được sao lưu dự phòng, đảm bảo sự toàn vẹn của dữ liệu để phục vụ cho công tác kiểm tra, đối chiếu, giải quyết, tra soát, khiếu nại, tranh chấp và cung cấp thông tin khi có yêu cầu từ cơ quan quản lý nhà nước có thẩm quyền; đáp ứng quy định của pháp luật về dịch vụ chứng thực chữ ký số và an toàn thông tin.

c) Hồ sơ định danh

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

- Hồ sơ đăng ký bao gồm:

i. Đơn đề nghị cấp chứng thư chữ ký số dạng bản giấy hoặc điện tử theo mẫu của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng. Trường hợp cá nhân đăng ký sử dụng chữ ký số trên ứng dụng VneID thì sẽ cần đồng ý cho phép RAR Center chia sẻ, xác thực dữ liệu với mục đích đăng ký và sử dụng chữ ký số với MISA-CA

ii. Hồ sơ, tài liệu kèm theo bao gồm:

- Giấy tờ tùy thân bao gồm thẻ căn cước công dân hoặc thẻ căn cước hoặc căn cước điện tử hoặc giấy chứng nhận căn cước hoặc tài khoản định danh điện tử mức độ 2 hoặc hộ chiếu còn thời hạn; thị thực nhập cảnh còn thời hạn hoặc giấy tờ chứng minh được miễn thị thực nhập cảnh (đối với cá nhân là người nước ngoài).

iii. Cá nhân có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc nộp bản sao trình kèm bản chính để đối chiếu hoặc cung cấp dữ liệu điện tử để tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng sử dụng, khai thác theo quy định tại khoản iv Điều này.

iv. Trường hợp cá nhân cung cấp hoặc sử dụng thông tin trong thẻ căn cước công dân hoặc thẻ căn cước hoặc căn cước điện tử hoặc giấy chứng nhận căn cước hoặc thông tin trong tài khoản định danh điện tử mức độ 2 của cá nhân thì tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng (đã có văn bản chấp thuận cho phép thực hiện kết nối với hệ thống định danh và xác thực điện tử theo quy định pháp luật về định danh và xác thực điện tử hoặc có đầy đủ phương tiện đọc dữ liệu trong chíp điện tử, dữ liệu trong tài khoản định danh điện tử mức độ 2) khai thác dữ liệu trong chíp điện tử, dữ liệu của tài khoản định danh điện tử mức độ 2 của cá nhân, không yêu cầu cá nhân, người đại diện theo pháp luật của tổ chức nộp các hồ sơ, tài liệu theo quy định tại khoản iii Điều này.

3.2.4. Thông tin 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 35 Nghị định số 23/2025/NĐ-CP.

3.2.5. Xác minh thẩm quyền

Khi tên của cá nhân trong chứng thư số có liên quan tới một tổ chức, MISA- CA cần thực hiện:

- Xác định sự tồn tại của tổ chức thông qua ít nhất một bên thứ ba;

- Xác thực các thông tin ghi trong Phiếu yêu cầu cấp chứng thư số thông qua các tài liệu cần thiết và có thể thu thập;

- Xác định danh tính và vị trí của cá nhân trong tổ chức có tương ứng với các thông tin đã đăng ký hay không.

3.2.6. Tiêu chí liên thông

MISA-CA tuân thủ các quy định về liên thông do Bộ Khoa học và công nghệ ban hành.

3.3. Xác minh đề nghị thay đổi cặp khóa

3.3.1. Xác minh danh tính và xác thực đối với yêu cầu thay đổi cặp khóa định kỳ

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 danh tính và xác thực đối với yêu cầu thay đổi cặp 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:

a) Lý do bị thu hồi chứng thư số

b) 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:

a) Thuê bao sử dụng chứng thư số đã được cấp vào các mục đích trái pháp luật

b) Thuê bao sử dụng các thông tin giả mạo để xin cấp chứng thư số

c) 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 thư số bị thu hồi với lý do từ MISA-CA hoặc các cơ quan công quyền như:

a) 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

b) Khi có yêu cầu của cơ quan công quyền

c) Theo điều kiện thu hồi chứng thư số đã được quy định trong hợp đồng giữa 2 bên

d) Thủ tục duyệt cho xác thực yêu cầu thu hồi của một đăng ký bao gồm:

e) 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

f) 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)

g) 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 CHỮ KÝ SỐ

4.1. Yêu cầu đề nghị phát hành chứng thư chữ ký số

4.1.1. Đối tượng đề nghị phát hành chứng thư chữ ký số

Đối tượng đề nghị phát hành chứng thư chữ ký số gồm:

a) 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

b) 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. Trách nhiệm và quy trình đăng ký

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:

a) Thuê bao đề nghị cấp chứng thư chữ ký số và gửi kèm các thông tin theo yêu cầu tại mục 3.2

b) MISA-CA tiếp nhận, xử lý và gửi thông tin xác nhận đến khách hàng thông qua ứng dụng mobile

c) 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

d) 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.

e) Hệ thống MISA-CA sẽ thực hiện tạo chứng thư số mới cho thuê bao.

4.2. Xử lý yêu cầu đề nghị phát hành chứng thư chữ ký số

4.2.1. Thực hiện các chức năng xác minh danh tính 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. Phê duyệt hoặc từ chối hồ sơ đề nghị phát hành chứng thư chữ ký số

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

a) Nhận dạng và xác thực thành công mọi thông tin trong yêu cầu đăng ký theo mục 3.2.2 và 3.2.3

b) Nhận được các khoản phí cần thiết

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

d) Không thể xác minh thông tin thuê bao theo mục 3.2.2 và 3.2.3

e) Thuê bao không hoàn thành hồ sơ theo như yêu cầu

f) Thuê bao không thanh toán theo quy định

g) 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 hồ sơ đề nghị phát hành chứng thư chữ ký số

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 chữ ký số

4.3.1. Quy trình phát hành chứng thư chữ ký 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 việc phát hành chứng thư chữ ký 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. Xác nhận và công bố công khai chứng thư chữ ký số

4.4.1. Xác nhận các thông tin trên chứng thư chữ ký số được cấp là chính xác

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 theo quy định

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 chữ ký 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 chữ ký số

4.5.1. Sử dụng khóa bí mật và chứng thư chữ ký số

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. Sử dụng khoá công khai và chứng thư chữ ký số bởi các bên tin tưởng

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

a) Trạng thái chứng thư số, phạm vi sử dụng, giới hạn trách nhiệm và các thông tin trên chứng thư số của người ký

b) Chữ ký số phải được tạo bởi khóa bí mật tương ứng với khóa công khai trên chứng thư số của người ký

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

d) 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://www.misaca.vn/misaca1.crl hoặc dịch vụ kiểm tra trạng thái chứng thư số trực tuyến tại địa chỉ http://ocsp1.misaca.vn.

e) 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 chữ ký 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 chữ ký số được gia hạn được thực hiện như trường hợp cấp mới chứng thư số.

4.6.1. Các trường hợp được gia hạn chứng thư chữ ký số

Trước ngày hết hạn của chứng thư số công cộng, thuê bao 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 có thể yêu cầu gia hạn chứng thư chữ ký số

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

a) Đối với thuê bao là cá nhân: chính cá nhân đó mới có quyền đề nghị gia hạn chứng thư số.

b) 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 việc gia hạn chứng thư chữ ký số

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. Xác nhận đối với chứng thư chữ ký số được gia hạn

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 chứng thư chữ ký số được gia hạn đến các đối tượng khác

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

4.7. Thay đổi cặp 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. Các trường hợp được thay đổi cặp khoá

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 gửi yêu cầu thay đổi cặp khoá

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 cặp 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 được cập nhật sau khi thay đổi cặp khóa

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

4.7.7. Thông báo chứng thư chữ ký số được cập nhật sau khi thay đổi cặp khóa đến các đối tượng khác

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. Xác nhận đối với chứng thư chữ ký số được cập nhật

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

4.8.6. Công bố chứng thư số được cập nhật sau khi thay đổi thông tin

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 được phép 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 Khoa học và công nghệ). 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:

a) Khi thuê bao yêu cầu bằng văn bản và yêu cầu này đã được MISA-CA xác minh là chính xác.

b) Khi thông tin trong chứng thư số khác với thông tin của thuê bao đã được MISA thực hiện thẩm định với Khách hàng.

c) 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

d) Khi có yêu cầu của cơ quan tiến hành tố tụng, cơ quan công an hoặc Bộ Khoa học và công nghệ.

e) Khi Khách hàng vi phạm một trong các điều khoản của thỏa thuận/hợp đồng cung cấp dịch vụ giữa MISA-CA và Khách hàng.

f) Các trường hợp thu hồi chứng thư số khác đã được quy định trong thỏa thuận/hợp đồng cung cấp dịch vụ giữa MISA-CA và Khách hàng.

4.9.2. Đối tượng được phép yêu cầu thu hồi chứng thư số

a) Đối với thuê bao là cá nhân: chính cá nhân đó mới có quyền đề nghị yêu cầu thu hồi chứng thư số.

b) 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.

c) MISA-CA có thể thu hồi chứng thư số trong các trường hợp quy định tại Điều 4.9.1.

d) Cơ quan nhà nước có thẩm quyền (như cơ quan tố tụng, cơ quan công an hoặc Bộ Khoa học và công nghệ).

4.9.3. Quy trình, 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 hạn gia hạn yêu cầu thu hồi chứng thư chữ ký số

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

4.9.5. Thời gian phải xử lý yêu cầu thu hồi chứng thư chữ ký số

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 trạng thái thu hồi chứng thư chữ ký số đối với các bên tin tưởng

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 công bố danh sách thu hồi chứng thư chữ ký số (CRL)

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. Độ trễ công bố CRL

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

4.9.9. Kiểm tra trạng thái/thu hồi chứng thư chữ ký số trực tuyến

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

4.9.10. Yêu cầu kiểm tra trạng thái thu hồi chứng thư chữ ký số trực tuyến

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. Yêu cầu đặc biệt liên quan đến thay đổi cặp khóa

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 được phép tạm dừng, phục hồi chứng thư chữ ký số

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, phục hồi chứng thư chữ ký số

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 Khoa học và công nghệ).

4.9.15. Quy trình, thủ tục yêu cầu tạm dừng, phục hồi chứng thư chữ ký số

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, phục hồi chứng thư chữ ký số

Ngay sau khi kết thúc thẩm định yêu cầu.

4.10. Kiểm tra trạng thái chứng thư số

4.10.1. Các hình thức kiểm tra trạng thái chứng thư chữ ký số

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

4.10.2. Khả năng sẵn sàng của dịch vụ kiểm tra trạng thái chứng thư chữ ký số

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 khác

Không có quy định.

4.11. Chấm dứt dịch vụ

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

a) Thuê bao đã hết hạn mà không gia hạn

b) Thu hồi chứng thư số xảy ra mà không xin cấp một chứng thư số mới

4.12. Lưu trữ và phục hồi khóa

4.12.1. Chính sách và thực tiễn việc lưu trữ và phục hồi khóa

Không có quy định.

4.12.2. Chính sách và thực tiễn việc mã hóa và phục hồi 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

a) Khi vào TTDL thì nhân viên phải xuất trình giấy tờ cho bảo vệ tòa nhà TTDL như thẻ căn cước, hộ chiếu để làm thủ tục vào.

b) 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.

c) 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.

d) 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.

e) 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.

f) 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.

g) Tất cả mọi truy cập đều được ghi nhận.

5.1.3. Điều hòa và nguồn điện

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:

a) Sử dụng hệ thống UPS có khả năng duy trì nguồn điện tối thiểu 30 phút

b) 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

c) Có đầy đủ các hệ thống làm mát chuyên dụng để kiểm soát nhiệt độ và độ ẩm

5.1.4. Tiếp xúc với 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 ngừa và bảo vệ chống 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. Xử lý 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. Kiểm soát quy trình

5.2.1. Các vai trò 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:

a) Xác minh các thông tin trong hồ sơ cấp chứng thư số
b) 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
c) Chuyển giao, thu hồi chứng thư số
d) Quản lý thông tin thuê bao, thông tin yêu cầu từ thuê bao
e) Người được tin tưởng bao gồm nhưng không giới hạn các đối tượng sau:
f) Người đứng đầu hệ thống CA
g) Người vận hành, cấp chứng thư số
h) Người quản trị hệ thống
i) Người đảm bảo an toàn, an ninh hệ thống
j) Người kiểm toán hệ thống kỹ thuật
k) 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 cần thiết 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. Định danh và xác thực cho từng thành viên

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. Vai trò, trách nhiệm của từng thành viên

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

a) Xác minh thông tin trong hồ sơ đăng ký chứng thư số của thuê bao
b) 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
c) Chuyển giao chứng thư số cho thuê bao
d) Quản lý thông tin của thuê bao
e) Tư vấn, hỗ trợ khách hàng trong quá trình sử dụng

5.3. Kiểm soát nhân sự

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

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. Quy trình kiểm tra lý lịch

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:

a) Giấy xác nhận của địa phương về cá nhân, gia đình

b) Kiểm tra tham khảo đồng nghiệp

c) Sự xác nhận của mức độ đào tạo cao nhất đã đạt được

d) 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 cho cán bộ vận hành, quản lý hệ thống

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:

a) Các khái niệm PKI cơ bản

b) Trách nhiệm công việc

c) Các chính sách và thủ tục an ninh của hoạt động MISA-CA

d) Sử dụng và vận hành các thiết bị phần cứng và phần mềm

e) Xử lý các sự cố

f) 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 và trình tự 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. Các hình thức xử lý đối với hành động không được phép

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. Yêu cầu đối với nhà thầu 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. Cung cấp tài liệu cho nhân sự

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 quy trình ghi nhật ký hệ thống

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:

a) Các sự kiện:
   i. Tạo khóa CA,
   ii. Bật tắt các hệ thống và ứng dụng,
   iii. Thay đổi khóa CA,
   iv. Sự kiện có liên quan đến quản lý chu kỳ mã hoá,
   v. Quá Trình xử lý dữ liệu kích hoạt cho khóa bí mật của CA, các bản ghi truy cập vật lý,
   vi. Bảo trì và thay đổi cấu hình hệ thống,
   vii. Bản ghi huỷ bỏ các phương tiện chứa khóa, dữ liệu kích hoạt, hoặc thông tin thuê bao.
   viii. Việc sử dụng khóa của thuê bao
b) Các sự kiện về việc xác nhận chính thuê bao là người cung cấp hồ sơ và yêu cầu cấp chứng thư số
c) Các sự kiện về vòng đời của chứng thư (bao gồm cấp mới, gia hạn, thu hồi)
d) Sự kiện liên quan tới nhân viên tin cậy bao gồm:
   i. Hành động truy cập hay thoát ra;
   ii. Tạo và xóa bỏ mật khẩu hay thay đổi đặc quyền của người sử dụng.
e) Các thông tin khác theo quy định của RootCA.

5.4.2. Tần suất xử lý nhật ký hệ thống

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 hệ thống

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 nhật ký hệ thống

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. Quy trình sao lưu nhật ký hệ thống

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 hệ thống (nội bộ so với bên ngoài)

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 cho đối tượng gây ra sự kiện

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 bảo mật

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:

a) Thông tin đơn xin cấp chứng thư số

b) Các thông tin bổ sung của đơn xin cấp chứng thư số

c) Thông tin vòng đời chứng thư số như: thu hồi, đổi khóa, làm mới…

d) Và các thông tin khác theo quy định của RootCA

e) Các dữ liệu nhật ký trong phần 5.4

5.5.2. Thời hạn lưu trữ bản ghi

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 bản ghi

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. Quy trình sao lưu bản ghi

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

5.5.5. Yêu cầu về gắn dấu thời gian cho 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 thu thập bản ghi (nội bộ so với bên ngoài)

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

5.5.7. Quy trình truy cập và xác minh thông tin bản ghi

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 cặp khóa

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:

a) 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.

b) 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 sự cố, thảm họa và phục hồi

5.7.1. Quy trình xử lý sự cố và thảm họa

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. Sự cố về tài nguyên 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. Quy trình xử lý khóa bí mật bị xâm phạm

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.

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

a) Trạng thái thu hồi chứng thư số của MISA-CA sẽ được công bố bởi RootCA.

b) 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 phục hồi hoạt động sau thảm họa

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:

a) Ban hành chứng thư số

b) Thu hồi chứng thư số

c) 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.

5.8. Dừng hoạt động cung cấp dịch vụ

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 chứng 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:

a) 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;

b) 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;

c) 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;

d) 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;

e) 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;

f) 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:

a) Thu hồi các chứng thư số đang hoạt động thuộc CA đã chấm dứt;

b) 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;

c) 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. Đảm bảo an toàn an ninh về kỹ thuật

6.1. Tạo và phân phối cặp khóa

6.1.1. Cách thức tạo 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 23/2025/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. Chuyển giao khóa bí mật

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. Chuyển giao khóa công khai cho tổ chức phát hành chứng thư chữ ký số

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. Chuyển giao khóa công khai của tổ chức phát hành chứng thư chữ ký số cho bên tin tưởng

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 cho 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

Xem trong phần 7.1.2.

6.2. Kiểm soát và bảo vệ khóa bí mật, mô-đun mật mã

6.2.1. Tiêu chuẩn và kiểm soát đối với mô-đun mật mã

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. Kiểm soát đa bên đối với khóa bí mật (n out of m)

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. Chuyển giao 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. Dự phòng 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 hoặc ra khỏi mô-đun mật mã

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 trên mô-đun mật mã

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 Khoa học và công nghệ 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:

a) 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.

b) 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 thức vô hiệu hóa 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 thức 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 Khoa học và công nghệ ban hành, đảm bảo không thể phục hồi lại khóa đã huỷ bằng bất cứ hình thức nào.

6.2.11. Đánh giá mô-đun mật mã

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 vấn đề khác liên quan đến 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 hạn hoạt động của chứng thư số và thời hạn sử dụng cặp khóa

a) Thời gian hoạt động của chứng thư số do MISA-CA cấp tuân theo quy định của Bộ Khoa học và công nghệ, 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

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

c) 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. Kích hoạt dữ liệu

6.4.1. Khởi tạo 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 chứa 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 sẻ 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 máy tính

6.5.1. Các yêu cầu kỹ thuật cụ thể về an ninh 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. Định kỳ đánh giá an ninh hệ thống máy tính

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. Kiểm soát vòng đời kỹ thuật

6.6.1. Kiểm soát phát triển hệ thống

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.

6.6.2. Kiểm soát vòng đời hệ thống

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

6.7. Giám sát an ninh hệ thống mạng

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

a) Chính sách an ninh thông tin

b) 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

c) Hệ thống Firewall lớp ngoài (External Firewall): phân tách và quản lý truy cập giữa các lớp mạng nội bộ

d) Hệ thống Firewall tích hợp sẵn với hệ thống phát hiện và chống thâm nhập mạng IPS.

e) Hệ thống Web Application Firewall phòng chống tấn công ở mức chuyên sâu trong lớp ứng dụng Web.

f) Hệ thống Load Balancer: phân tải các yêu cầu truy cập vào hệ thống và nâng cao khả năng sẵn sàng của dịch vụ.

g) Hệ thống phòng chống Antivirus tập trung: Client/server, quản lý tập trung.

h) Hệ thống cập nhật bản vá cho các máy chủ/máy trạm.

i) 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. Dấu thời gian (Time-stamping)

MISA-CA không cung cấp dịch vụ này.

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

7.1. Đặc dạng của 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. 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 trường 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 thế 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. Định danh 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, hạn chế 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 quy chế chứng thực

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 trường mở rộng Policy Constraint

Không có quy định

7.1.8. Cú pháp và ngữ nghĩa trong quy chế chứng thực

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 cho trường mở rộng quan trọng Certificate Policies

Không có quy định

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

7.2.1. Số phiên bản của CRL

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

7.2.2. CRL và phần mở rộng đầu vào CRL

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

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

7.3.1. Số phiên bản của OCSP

Sử dụng phiên bản 1.

7.3.2. Phần mở rộng của OCSP

Không có quy định.

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

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 và các tình huống kiểm tra kỹ thuật

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. Danh tính và khả năng của đơn vị,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. Tính độc lập của bên đánh giá đối với tổ chức được đánh giá

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. 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:

a) 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

b) 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

c) 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

8.5. Công bố kết quả kiểm tra kỹ thuật

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.

8.6. Tần suất và các trường hợp đánh giá

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:

a) Môi trường hoạt động của Công ty

b) Hệ thống kỹ thuật cung cấp dịch vụ của Công ty

c) Đánh giá việc tuân thủ theo các chuẩn của Công ty

d) Quy trình quản lý, cung cấp và sử dụng chứng thư chữ ký số của Công ty

e) Các nội dung khác

9. CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC

9.1. Phí, giá

9.1.1. Phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư chữ ký số

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

9.1.2. Giá chứng thư số

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

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 hoặc thay đổi thông tin chứng thư chữ ký số.

9.1.3. Các loại chi phí 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.

9.1.4. 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.

9.2. Trách nhiệm tài chính

9.2.1. Phạm vi 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:

a) Lỗi do CA gây ra, bao gồm lỗi kỹ thuật khi phát hành chứng thư theo trách nhiệm của CA.
b) 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:

a) Các trường hợp sử dụng chứng thư không được đề cập đến trong Quy chế chứng thực này
b) Các trường hợp giả mạo chứng thư số

c) 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
d) 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. Phạm vi bảo hiểm hoặc bảo hành cho người dùng cuối

Không có quy định

9.3. Bảo mật các thông tin nghiệp vụ

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. Phạm vi thông tin nghiệp vụ cần được bảo 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:

a) 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
b) 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
c) 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
d) 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. Phạm vi thông tin nghiệp vụ cần được bảo mật

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

a) Thông tin trong chứng thư số của MISA-CA hay danh sách chứng thư số bị thu hồi

b) Thông tin trong các Quy chế chứng thực

c) Thông tin được tiết lộ không phải do lỗi của các thành viên trong MISA-CA

d) Thông tin đã bị cơ quan pháp luật thu thập từ các thành viên trong MISA-CA

e) Thông tin được công bố khi đã thông qua chủ sở hữu của nó.

9.3.3. Trách nhiệm bảo mật thông tin nghiệp vụ

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. Bảo vệ dữ liệu cá nhân

9.4.1. Biện pháp bảo vệ dữ liệu cá nhân

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. Phạm vi bảo vệ dữ liệu cá nhân

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. Những thông tin cá nhân ngoài phạm vi bảo vệ

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 dữ liệu cá nhân

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 dữ liệu cá nhân

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 theo yêu cầu của cơ quan quản lý

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

a) 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.

b) Quá trình công bố nhằm tuân thủ quy định của pháp luật.

9.4.7. Các tình huống cung cấp 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. Tuyên bố và cam kết

9.6.1. Tuyên bố và cam kết của tổ chức phát hành chứng thư chữ ký số

MISA-CA đảm bảo rằng:

a) Không thay đổi thông tin đăng ký chứng thư số được cung cấp bởi đối tượng đăng ký.

b) Không có lỗi trong quá trình duyệt và ban hành chứng thư số.

c) Chứng thư số do MISA-CA ban hành đáp ứng các yêu cầu trong quy chế này.

d) Cung cấp dịch vụ thu hồi và cho phép sử dụng địa chỉ lưu trữ phù hợp với quy chế chứng thực này.

e) Chịu trách nhiệm về việc quản lý và xác minh các điều kiện hoạt động của RA theo quy định của pháp luật.

9.6.2. Tuyên bố và cam kết của thuê bao

Thuê bao đảm bảo rằng:

a) 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)

b) Trường hợp tự tạo cặp khóa cho mình, thuê bao phải bảo đảm thiết bị tạo cặp khóa đáp ứng quy chuẩn kỹ thuật và tiêu chuẩn bắt buộc áp dụng.

c) Thiết bị của mình được bảo vệ và không cho người khác sử dụng

d) Kiểm soát và sử dụng khóa bí mật của mình một cách an toàn trong suốt thời gian chứng thư chữ ký số công cộng có hiệu lực và bị tạm dừng.

e) Thông báo trong thời gian 24 giờ cho tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng nếu phát hiện thấy dấu hiệu khóa bí mật của mình đã bị lộ, bị đánh cắp hoặc sử dụng trái phép để có các biện pháp xử lý.

f) Thuê bao là người nắm giữ hợp pháp khóa bí mật tương ứng với khóa công khai trên chứng thư chữ ký số công cộng đó và những thông tin trên chứng thư chữ ký số công cộng liên quan đến thuê bao là đúng sự thật, đồng thời phải thực hiện các nghĩa vụ xuất phát từ chứng thư chữ ký số công cộng đó.

g) Mọi thông tin cung cấp bởi thuê bao là đúng

h) 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

i) Không sử dụng chứng thư số được cấp thực hiện các chức năng của một CA

j) 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. Tuyên bố và cam kết của bên tin tưởng

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.

a) 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.

b) Thỏa thuận thuê bao có thể bao gồm thêm những điều khoản khác. Nội dung thỏa thuận thuê bao được trình bày trong phần phụ lục.

9.6.4. Tuyên bố và cam kết của 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 hành

Trong giới hạn cho phép của luật pháp, hợp đồng thuê bao và người nhận có thể bị MISA-CA từ chối bảo hành.

9.8. Giới hạn trách nhiệm

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. Bồi thường thiệt hại

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:

a) 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.

b) 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.

c) 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:

a) Không thực hiện những bắt buộc đối với người nhận và làm thiệt hại cho MISA-CA hoặc các bên liên quan.

b) 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. Hiệu lực của quy chế chứng thực

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. Chấm dứt hiệu lực

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. Ảnh hưởng của việc chấm dứt hiệu lực

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 và trao đổi thông tin với các bên tham gia

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. Bổ sung và sửa đổi

9.12.1. Quy trình 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 hạn 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 cần thay đổi OID (Object identifier - mã định danh đối tượng)

Các trường hợp OID cần phải thay đổi tuân theo quy định của Bộ Khoa học và công nghệ.

9.13. Thủ tục giải quyết khiếu nại

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 bên tin tưởng

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

9.14. Hệ thống căn cứ pháp lý

Tài liệu quy chế chứng thực được điều chỉnh bởi các văn bản quy phạm pháp luật, bao gồm:

- Luật Giao dịch điện tử ngày 22 tháng 6 năm 2023;

- Nghị định số 23/2025/NĐ-CP ngày 21 tháng 02 năm 2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ tin cậy.

9.15. Tuân thủ quy định pháp luật hiện hành

- Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

- Luật An ninh mạng ngày 12 tháng 6 năm 2018;

- Luật Dữ liệu ngày 30 tháng 11 năm 2024;

- Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

- Nghị định số 69/2024/NĐ-CP ngày 25 tháng 6 năm 2024 của Chính phủ quy định về định danh và xác thực điện tử;

- Thông tư số 13/2025/TT-BTC ngày 19 tháng 3 năm 2025 của Bộ trưởng Bộ Tài chính quy định mức thu, chế độ thu, nộp, quản lý và sử dụng phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư chữ ký số.

9.16. Các điều khoản chung

9.16.1. Thỏa thuận toàn bộ

Không có quy định

9.16.2. Chuyển nhượng

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

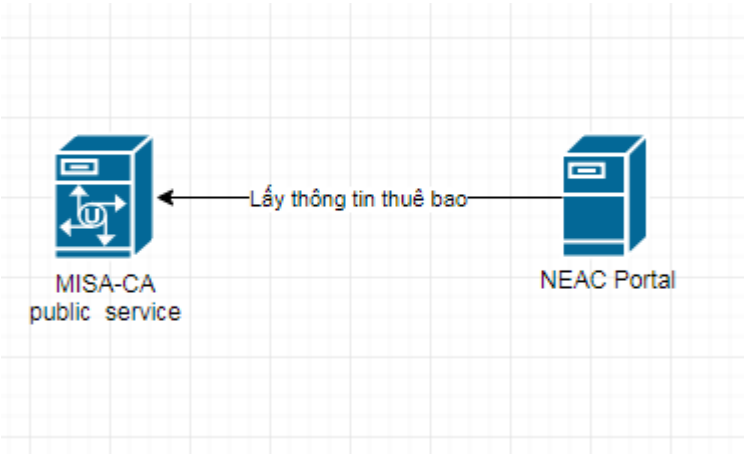
Trong phạm vi luật pháp cho phép, thỏa thuận của thuê bao và thỏa thuận bên liên quan bắt buộc phải tuân theo các điều khoản bảo vệ dịch vụ MISA-CA.

9.17. Các điều khoản khác

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:

a) 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.



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

ĐẠI DIỆN CÔNG TY CỔ PHẦN MISA
Tổng Giám đốc

Digitally signed by: MISA JOINT STOCK COMPANY
Date: 15/04/2026, 15:26:59

Lê Hồng Quang