BỘ KHOA HỌC VÀ CÔNG NGHỆ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 51 /2025/TT-BKHCN	*Hà Nội, ngày 31 tháng 12 năm 2025*

THÔNG TƯ

Ban hành "Quy chuẩn kỹ thuật quốc gia về yêu cầu đối với dịch vụ cấp dấu thời gian"

Căn cứ Luật Giao dịch điện tử số 20/2023/QH15;

Căn cứ Luật Tiêu chuẩn và quy chuẩn kỹ thuật số 68/2006/QH11, được sửa đổi, bổ sung bởi Luật số 35/2018/QH14 và Luật số 70/2025/QH15;

Căn cứ 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;

Căn cứ Nghị định số 127/2007/NĐ-CP ngày 01 tháng 8 năm 2007 của Chính phủ quy định chi tiết thi hành một số điều của Luật Tiêu chuẩn và quy chuẩn kỹ thuật được sửa đổi, bổ sung bởi Nghị định số 78/2018/NĐ-CP;

Căn cứ Nghị định số 55/2025/NĐ-CP ngày 02 tháng 3 năm 2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Khoa học và Công nghệ;

Theo đề nghị của Giám đốc Trung tâm Chứng thực điện tử quốc gia;

Bộ trưởng Bộ Khoa học và Công nghệ ban hành Thông tư ban hành "Quy chuẩn kỹ thuật quốc gia về yêu cầu đối với dịch vụ cấp dấu thời gian".

Điều 1. Ban hành kèm theo Thông tư này Quy chuẩn kỹ thuật quốc gia về yêu cầu đối với dịch vụ cấp dấu thời gian (QCVN 138:2025/BKHCN).

Điều 2. Lộ trình áp dụng

Trừ trường hợp tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng lựa chọn áp dụng quy định của Luật Giao dịch điện tử số 20/2023/QH15, các tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng đang hoạt động hợp pháp có trách nhiệm rà soát, nâng cấp hệ thống thông tin và đội ngũ nhân lực quản lý và kỹ thuật đáp ứng quy định tại QCVN 138:2025/BKHCN trước ngày 10 tháng 4 năm 2027.

Điều 3. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày 01 tháng 7 năm 2026.

2. Các quy định dưới đây hết hiệu lực thi hành kể từ ngày Thông tư này có hiệu lực thi hành:

a) Thông tư số 06/2015/TT-BTTTT ngày 23 tháng 3 năm 2015 của Bộ trưởng Bộ Thông tin và Truyền thông quy định danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số;

b) Thông tư số 16/2019/TT-BTTTT ngày 05 tháng 12 năm 2019 của Bộ trưởng Bộ Thông tin và Truyền thông 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.

Điều 4. Điều khoản chuyển tiếp

Hồ sơ đề nghị cấp Giấy phép cung cấp dịch vụ cấp dấu thời gian đã nộp cho cơ quan nhà nước có thẩm quyền nhưng đến ngày Thông tư này có hiệu lực thi hành chưa được cấp giấy phép thì được tiếp tục áp dụng quy định của Thông tư số 06/2015/TT-BTTTT và Thông tư số 16/2019/TT-BTTTT.

Điều 5. Tổ chức thực hiện

1. Giám đốc Trung tâm Chứng thực điện tử quốc gia có trách nhiệm tổ chức hướng dẫn triển khai thực hiện Thông tư này.

2. Các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này.

3. Trong quá trình thực hiện, nếu phát sinh vướng mắc, cơ quan, tổ chức, cá nhân kịp thời phản ánh bằng văn bản về Bộ Khoa học và Công nghệ (Trung tâm Chứng thực điện tử quốc gia) để nghiên cứu sửa đổi, bổ sung cho phù hợp./.

Nơi nhận:
- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc TW;
- Sở KHCN các tỉnh, thành phố trực thuộc TW;
- Cục Kiểm tra văn bản và Quản lý xử lý vi phạm hành chính (Bộ Tư pháp);
- Công báo, Cổng thông tin điện tử Chính phủ;
- Bộ KHCN: Bộ trưởng và các Thứ trưởng, các cơ quan, đơn vị thuộc Bộ;
- Cổng thông tin điện tử Bộ;
- Lưu: VT, NEAC.

BỘ TRƯỞNG

Nguyễn Mạnh Hùng

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

QCVN 138:2025/BKHCN

QUY CHUẨN KỸ THUẬT QUỐC GIA
VỀ YÊU CẦU ĐỐI VỚI DỊCH VỤ CẤP DẤU THỜI GIAN

NATIONAL TECHNICAL REGULATION ON REQUIREMENTS FOR TIME-STAMPING SERVICES

HÀ NỘI – 2025

Mục lục

Lời nói đầu

QCVN 138:2025/BKHCN do Trung tâm Chứng thực điện tử Quốc gia biên soạn, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ trưởng Bộ Khoa học và Công nghệ ban hành kèm theo Thông tư số ..../2025/TT-BKHCN ngày ... tháng .... năm 2025.

QUY CHUẨN KỸ THUẬT QUỐC GIA
VỀ YÊU CẦU ĐỐI VỚI DỊCH VỤ CẤP DẤU THỜI GIAN

NATIONAL TECHNICAL REGULATION ON REQUIREMENTS FOR TIME-STAMPING SERVICES

1. QUY ĐỊNH CHUNG

1.1. Phạm vi điều chỉnh

Quy chuẩn này quy định các yêu cầu kỹ thuật về dịch vụ cấp dấu thời gian, yêu cầu về quy trình vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ cấp dấu thời gian.

1.2. Đối tượng áp dụng

Quy chuẩn này được áp dụng cho Tổ chức cung cấp dịch vụ cấp dấu thời gian, các tổ chức, cá nhân có liên quan đến cung cấp dịch vụ cấp dấu thời gian tại Việt Nam.

Quy chuẩn này không áp dụng cho Tổ chức cung cấp dịch vụ cấp dấu thời gian chuyên dùng công vụ.

1.3. Tài liệu viện dẫn

[1] PKCS #1 (RFC 3447): "RSA Cryptography Standard"

[2] ANSI X9.62-2005: "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)"

[3] TCVN 7816:2007: "Công nghệ thông tin - Kỹ thuật mật mã thuật toán mã dữ liệu AES"

[4] FIPS PUB 197: "Advanced Encryption Standard"

[5] FIPS PUB 180-4: "Secure Hash Standard"

[6] FIPS PUB 202: "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions"

[7] RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"

[8] PKCS #7 (RFC 2630): "Cryptographic Message Syntax Standard"

[9] PKCS #8 (RFC 5208): "Private-Key Information Syntax Standard"

[10] PKCS #10 (RFC 2986): "Certification Request Syntax Standard"

[11] PKCS #11: "Cryptographic Token Interface Standard"

[12] PKCS #12: "Personal Information Exchange Syntax Standard"

[13] RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework"

[14] RFC 4523: "Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates"

[15] RFC 4510: "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map"

[16] RFC 4511: "Lightweight Directory Access Protocol (LDAP): The Protocol"

[17] RFC 4512: "Lightweight Directory Access Protocol (LDAP): Directory Information Models"

[18] RFC 4513: "Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms"

[19] RFC 2585: "Internet X.509 Public Key Infrastructure - Operational Protocols: FTP and HTTP"

[20] RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP"

[21] FIPS PUB 140-2: "Security Requirements for Cryptographic Modules"

[22] FIPS PUB 140-3: "Security Requirements for Cryptographic Modules"

[23] EN 419221-5:2018: "Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services"

[24] RFC 3161: "Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)"

[25] RFC 5816: "ESSCertIDv2 Update for RFC 3161"

[26] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping Protocol and Time-stamp Token Profiles"

[27] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Issuing Time-Stamps"

1.4. Giải thích từ ngữ

1.4.1. Dịch vụ cấp dấu thời gian: Dịch vụ do tổ chức cung cấp dịch vụ tin cậy thực hiện nhằm cấp dấu thời gian điện tử cho thông điệp dữ liệu, chứng minh thông điệp dữ liệu đã tồn tại tại một thời điểm xác định và kể từ thời điểm đó chưa bị thay đổi.

1.4.2. Dấu thời gian (Time-stamp token): Thông điệp dữ liệu được ký số bởi tổ chức cung cấp dịch vụ cấp dấu thời gian, chứa giá trị băm của thông điệp dữ liệu gốc, thời điểm chính xác và các thông tin cần thiết khác nhằm chứng minh sự tồn tại và tính toàn vẹn của thông điệp dữ liệu tại thời điểm đó.

1.4.3. Thời điểm cấp dấu thời gian: Thời điểm chính xác được ghi nhận trong dấu thời gian, được lấy từ nguồn thời gian đáng tin cậy và được bảo vệ bằng chữ ký số của tổ chức cung cấp dịch vụ cấp dấu thời gian.

1.4.4. Thiết bị bảo mật phần cứng: Thiết bị phần cứng chuyên dụng (Hardware Security Module) dùng để tạo, lưu trữ và quản lý khóa bí mật của tổ chức cung cấp dịch vụ tin cậy, bao gồm tổ chức cung cấp dịch vụ cấp dấu thời gian, đáp ứng các yêu cầu bảo mật cao.

1.4.5. Khóa bí mật của tổ chức cung cấp dịch vụ cấp dấu thời gian: Khóa bí mật trong cặp khóa bất đối xứng thuộc quyền kiểm soát duy nhất của tổ chức cung cấp dịch vụ cấp dấu thời gian, được sử dụng để tạo chữ ký số lên dấu thời gian.

1.4.6. Nguồn thời gian đáng tin cậy: Nguồn cung cấp thời gian chính xác, có khả năng truy xuất và đồng bộ với thời gian quốc gia hoặc nguồn thời gian chuẩn quốc tế, được bảo vệ chống can thiệp.

1.4.7. Kiểm toán kỹ thuật: Hoạt động đánh giá độc lập, khách quan đối với hệ thống thông tin, quy trình cung cấp dịch vụ nhằm xác định việc đáp ứng tiêu chuẩn kỹ thuật bắt buộc áp dụng, quy chuẩn kỹ thuật, yêu cầu kỹ thuật của chữ ký điện tử bảo đảm an toàn, chứng thư chữ ký điện tử bảo đảm an toàn, chữ ký số, chứng thư chữ ký số và dịch vụ tin cậy. Trong đó, tiêu chuẩn kỹ thuật bắt buộc áp dụng khi được viện dẫn trong quy chuẩn kỹ thuật hoặc văn bản quy phạm pháp luật.

1.4.8. Tổ chức kiểm toán kỹ thuật: Tổ chức chứng nhận được chỉ định theo quy định của pháp luật về tiêu chuẩn, quy chuẩn kỹ thuật, chất lượng sản phẩm, hàng hóa.

1.5. Chữ viết tắt

CA	Certification Authority	Tổ chức chứng thực
CP	Certificate Policy	Chính sách chứng thư
CPS	Certification Practice Statement	Quy chế chứng thực
CRL	Certificate Revocation List	Danh sách chứng thư bị thu hồi
DN	Distinguished Name	Tên phân biệt (trong định danh X.509)

EAL	Evaluation Assurance Level	Cấp độ đảm bảo đánh giá (trong đánh giá an toàn thông tin ISO/IEC 15408)
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số đường cong Elliptic
ETSI	European Telecommunications Standards Institute	Viện Tiêu chuẩn Viễn thông Châu Âu
FIPS	Federal Information Processing Standards	Bộ tiêu chuẩn xử lý thông tin liên bang Hoa Kỳ
HSM	Hardware Security Module	Thiết bị bảo mật phần cứng (thiết bị lưu và xử lý khóa bí mật)
IETF	Internet Engineering Task Force	Nhóm công tác kỹ thuật Internet
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission	Tổ chức Tiêu chuẩn hóa Quốc tế / Ủy ban Kỹ thuật điện quốc tế
LDAP	Lightweight Directory Access Protocol	Giao thức truy cập thư mục nhẹ
OCSP	Online Certificate Status Protocol	Giao thức kiểm tra trạng thái chứng thư trực tuyến
PKCS	Public-Key Cryptography Standards	Bộ tiêu chuẩn mật mã khóa công khai
PKI	Public Key Infrastructure	Hạ tầng khóa công khai
RA	Registration Authority	Tổ chức đăng ký
RFC	Request for Comments	Tài liệu tiêu chuẩn kỹ thuật do IETF ban hành
RSA	Rivest–Shamir–Adleman	Thuật toán mật mã khóa công khai
SHA	Secure Hash Algorithm	Thuật toán băm an toàn
TSP	Trust Service Provider	Tổ chức cung cấp dịch vụ tin cậy
UTC	Coordinated Universal Time	Giờ Phối hợp Quốc tế
X.509	ITU-T Recommendation X.509	Khung chuẩn cho chứng thư số trong hệ thống PKI

2. QUY ĐỊNH KỸ THUẬT

2.1. Yêu cầu kỹ thuật

2.1.1. Yêu cầu về mật mã và chữ ký số

Sử dụng các kỹ thuật mật mã theo quy định tại Bảng 1:

Bảng 1 - Yêu cầu về kỹ thuật mật mã

Loại Yêu cầu	Tiêu chuẩn tham chiếu		Quy định áp dụng
	Ký hiệu	Tên tiêu chuẩn	
Mật mã phi đối xứng và chữ ký số	PKCS #1 (RFC 3447)	RSA Cryptography Standard	- Áp dụng một trong hai tiêu chuẩn. - Đối với tiêu chuẩn RSA: + Tối thiểu phiên bản 2.1; + Áp dụng lược đồ RSAES-OAEP để mã hoá và RSASSA-PSS để ký. + Độ dài khóa tối thiểu là 2048 bit - Đối với tiêu chuẩn ECDSA: độ dài khóa tối thiểu là 256 bit
	ANSI X9.62-2005	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)	
Mật mã đối xứng	TCVN 7816:2007	Công nghệ thông tin - Kỹ thuật mật mã thuật toán mã dữ liệu AES	Áp dụng một trong hai tiêu chuẩn
	FIPS PUB 197	Advanced Encryption Standard	
Yêu cầu cho hàm băm	FIPS PUB 180-4	Secure Hash Standard	Áp dụng một trong các hàm băm sau: SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256,

			SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256
	FIPS PUB 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions	

2.1.2. Yêu cầu về thông tin, dữ liệu

Định dạng thông tin, dữ liệu đáp ứng các quy định tại Bảng 2

Bảng 2 - Yêu cầu về thông tin dữ liệu

Loại Yêu cầu	Tiêu chuẩn tham chiếu		Quy định áp dụng
	Ký hiệu	Tiêu chuẩn tham chiếu	
Định dạng chứng thư chữ ký số và danh sách thu hồi chứng thư chữ ký số	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	
Cú pháp thông điệp mật mã	PKCS #7 (RFC 2630)	Cryptographic Message Syntax Standard	Phiên bản 1.5
Cú pháp thông tin khóa riêng	PKCS #8 (RFC 5208)	Private-Key Information Syntax Standard	Phiên bản 1.2
Cú pháp yêu cầu chứng thực	PKCS #10 (RFC 2986)	Certification Request Syntax Standard	Phiên bản 1.7
Giao diện giao tiếp với các thẻ mật mã	PKCS #11	Cryptographic token interface standard	Phiên bản 2.20
Cú pháp trao đổi thông tin cá nhân	PKCS #12	Personal Information Exchange Syntax Standard	Phiên bản 1.0

2.1.3. Yêu cầu đối với chứng thư chữ ký số

Chứng thư chữ ký số đáp ứng các quy định tại Bảng 3

Bảng 3 - Yêu cầu đối với chứng thư chữ ký số

Loại Yêu cầu	Tiêu chuẩn tham chiếu		Quy định áp dụng
	Ký hiệu	Tên tiêu chuẩn	
Chính sách chứng thư chữ ký số	RFC 3647	Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework	
Lược đồ Giao thức truy nhập thư mục	RFC 4523	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates	
Giao thức truy nhập thư mục	RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map	Áp dụng bộ bốn tiêu chuẩn
	RFC 4511	Lightweight Directory Access Protocol (LDAP): The Protocol	
	RFC 4512	Lightweight Directory Access Protocol (LDAP): Directory Information Models	
	RFC 4513	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms	

Giao thức truyền, nhận chứng thư chữ ký số và danh sách chứng thư chữ ký số bị thu hồi	RFC 2585	Internet X.509 Public Key Infrastructure - Operational Protocols: FTP and HTTP	Áp dụng một hoặc cả hai giao thức FTP và HTTP
Giao thức cho kiểm tra trạng thái chứng thư chữ ký số trực tuyến	RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	

2.1.4. Yêu cầu đối với HSM và thiết bị mật mã, lưu khóa

Thiết bị HSM và thiết bị mật mã, lưu khóa phải đáp ứng các quy định tại Bảng 4:

Bảng 4 - Yêu cầu đối với thiết bị HSM và thẻ mật mã

Loại Yêu cầu	Tiêu chuẩn tham chiếu		Quy định áp dụng
	Ký hiệu	Tên tiêu chuẩn	
Thiết bị HSM, thiết bị mật mã, lưu khóa	FIPS PUB 140-2 (tối thiểu mức 3)	Security Requirements for Cryptographic Modules	Áp dụng một trong ba tiêu chuẩn.
	FIPS PUB 140-3 (tối thiểu mức 3)	Security Requirements for Cryptographic Modules	
	EN 419221-5:2018	Protection Profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services	

2.1.5. Yêu cầu đối với dịch vụ cấp dấu thời gian

Dịch vụ cấp dấu thời gian phải đáp ứng các yêu cầu quy định tại bảng 5:

Bảng 5 - Yêu cầu đối với dịch vụ cấp dấu thời gian

Loại Yêu cầu	Tiêu chuẩn tham chiếu		Quy định áp dụng
	Ký hiệu	Tên tiêu chuẩn	
Giao thức cấp dấu thời gian	RFC 3161	Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)	Áp dụng bộ tiêu chuẩn: RFC 3161, RFC 5816. Hoặc Tiêu chuẩn ETSI EN 319 422 phiên bản V1.1.1.
	RFC 5816	ESSCertIDv2 Update for RFC 3161	
	ETSI EN 319 422	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles	

2.2. Yêu cầu về quy trình vận hành và kiểm soát

Tổ chức cung cấp dịch vụ cấp dấu thời gian phải triển khai các biện pháp bảo đảm quy trình vận hành và kiểm soát cung cấp dịch vụ tuân thủ tiêu chuẩn ETSI EN 319 421 (áp dụng phiên bản V1.2.1).

3. QUY ĐỊNH VỀ QUẢN LÝ

3.1. Phương thức đánh giá sự phù hợp đối với các yêu cầu tại mục 2.2 của Quy chuẩn thực hiện theo phương thức 6 (đánh giá hệ thống quản lý) theo quy định tại Thông tư 28/2012/TT-BKHCN ngày 12 tháng 12 năm 2012 quy định về công bố hợp chuẩn, công bố hợp quy và phương thức đánh giá sự phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật và Thông tư 19/2025/TT-BKHCN ngày 06 tháng 10 năm 2025 quy định kiểm toán kỹ thuật với chữ ký điện tử dịch vụ tin cậy.

3.2. Tổ chức cung cấp dịch vụ cấp dấu thời gian thuộc phạm vi điều chỉnh tại mục 1.1 thực hiện công bố hợp quy theo quy định và chịu sự kiểm tra của các cơ quan quản lý nhà nước theo các quy định tại Thông tư 28/2012/TT-BKHCN ngày 12 tháng 12 năm 2012 quy định về công bố hợp chuẩn, công bố hợp quy và phương thức đánh giá sự phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật; Thông tư 19/2025/TT-BKHCN ngày 06/10/2025 quy định kiểm toán kỹ thuật đối với chữ ký điện tử và dịch vụ tin cậy và các quy định hiện hành.

3.3. Phương tiện, thiết bị đo: tuân thủ các quy định hiện hành của pháp luật về đo lường.

4. TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

4.1. Trách nhiệm của Tổ chức đánh giá sự phù hợp

4.1.1. Thực hiện đánh giá sự phù hợp theo đúng quy định của Quy chuẩn này và thực hiện các nghĩa vụ báo cáo kết quả hoạt động đánh giá chứng nhận hợp quy đến Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia theo các quy định hiện hành.

4.1.2. Lưu trữ hồ sơ chứng nhận theo quy định tại Thông tư số 03/2025/TT-BKHCN ngày 15/5/2025 của Bộ trưởng Bộ Khoa học và Công nghệ quy định thời hạn lưu trữ hồ sơ, tài liệu ngành Khoa học và Công nghệ.

4.2. Trách nhiệm của Tổ chức cung cấp dịch vụ cấp dấu thời gian

4.2.1. Tuân thủ các quy định trong quy chuẩn kỹ thuật này.

4.2.2. Lưu trữ hồ sơ chứng nhận theo quy định tại Thông tư số 03/2025/TT-BKHCN ngày 15/5/2025 của Bộ trưởng Bộ Khoa học và Công nghệ quy định thời hạn lưu trữ hồ sơ, tài liệu ngành Khoa học và Công nghệ.

5. TỔ CHỨC THỰC HIỆN

5.1. Trung tâm Chứng thực điện tử Quốc gia tổ chức triển khai hướng dẫn và quản lý theo quy định của Quy chuẩn kỹ thuật này.

Căn cứ vào quy định quản lý, Trung tâm Chứng thực điện tử Quốc gia có trách nhiệm đề xuất, kiến nghị Bộ Khoa học và Công nghệ sửa đổi, bổ sung nội dung Quy chuẩn kỹ thuật này.

5.2. Trong trường hợp các quy định pháp luật, văn bản quy phạm pháp luật viện dẫn tại Quy chuẩn kỹ thuật này có sửa đổi, bổ sung hoặc được thay thế thì thực hiện theo quy định tại văn bản mới. Trong trường hợp các tiêu chuẩn được viện dẫn trong Quy chuẩn này có sự thay đổi, bổ sung, thay thế thì thực hiện theo hướng dẫn của Bộ Khoa học và Công nghệ.