| BỘ KHOA HỌC VÀ CÔNG NGHỆ | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM<br>Độc lập - Tự do - Hạnh phúc |
|---|---|
| Số: 53 /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 chứng thực thông điệp dữ liệu"**

*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 chứng thực thông điệp dữ liệu".*

**Điều 1.** Ban hành kèm theo Thông tư này Quy chuẩn kỹ thuật quốc gia về yêu cầu đối với dịch vụ chứng thực thông điệp dữ liệu (QCVN 139:2025/BKHCN).

**Điều 2. Hiệu lực thi hành**

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

**Điều 3. 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 139:2025/BKHCN**

# QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ YÊU CẦU ĐỐI VỚI DỊCH VỤ CHỨNG THỰC THÔNG ĐIỆP DỮ LIỆU

***NATIONAL TECHNICAL REGULATION ON REQUIREMENTS FOR ELECTRONIC REGISTERED DELIVERY SERVICES***

**HÀ NỘI – 2025**

## Mục lục

## Lời nói đầu

QCVN 139:2025/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 CHỨNG THỰC THÔNG ĐIỆP DỮ LIỆU

## *NATIONAL TECHNICAL REGULATION ON REQUIREMENTS FOR ELECTRONIC REGISTERED DELIVERY SERVICES*

## 1. QUY ĐỊNH CHUNG

### 1.1. Phạm vi điều chỉnh

Quy chuẩn này quy định các yêu cầu kỹ thuật về dịch vụ chứng thực thông điệp dữ liệu, yêu cầu về quy trình vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu.

### 1.2. Đối tượng áp dụng

Quy chuẩn này được áp dụng cho các tổ chức, cá nhân có liên quan đến cung cấp dịch vụ chứng thực thông điệp dữ liệu tại Việt Nam.

Quy chuẩn này không áp dụng cho Tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu chuyên dùng công vụ.

### 1.3. Tài liệu viện dẫn


[1] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"

[2] ETSI EN 319 102-1: " Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation"

[3] ISO 29115: "Information technology -- Security techniques -- Entity authentication assurance framework"

[4] NIST SP 800-63B: "Digital Identity Guidelines Authentication and Lifecycle Management"

[5] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers"

[6] ETSI EN 319 532-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats"

[7] IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies"

[8] IETF RFC 5322: "Internet Message Format"

[9] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers"

[10] ETSI TS 119 511: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques"

[11] ISO/IEC 15408 (parts 1 to 3): "Information technology -- Security techniques -- Evaluation criteria for IT security"

[12] ISO/IEC 19790: "Information technology -- Security techniques -- Security requirements for cryptographic modules"

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

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

[15] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations"

[16] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites"

[17] ETSI TS 119 122-3: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES"

[18] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC Baseline containers"

[19] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements"

[20] ETSI TS 119 512: "Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services"

[21] ISO/IEC 21320-1 (2015): "Information technology -- Document Container File -- Part 1: Core"

[22] ISO 14641-1:2018: "Electronic archiving -- Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation"

[23] ISO 14721:2012: "Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model"

[24] ISO 16363:2011: "Space data and information transfer systems -- Audit and certification of trustworthy digital repositories"

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

[26] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax"

[27] IETF RFC 4998: "Evidence Record Syntax (ERS)"

[28] IETF RFC 5280 (2008): Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"

[29] IETF RFC 5816 (2010): "ESSCertIDv2 Update for RFC 3161"

[30] IETF RFC 6283 (2011): "Extensible Markup Language Evidence Record Syntax (XMLERS)"

[31] IETF RFC 6960 (2013): "Online Certificate Status Protocol - OCSP"

### 1.4. Giải thích từ ngữ

**1.4.1. Dịch vụ chứng thực thông điệp dữ liệu:** Dịch vụ do tổ chức cung cấp dịch vụ tin cậy thực hiện nhằm chứng minh việc gửi, nhận, thời điểm gửi, nhận, tính toàn vẹn và nguồn gốc của thông điệp dữ liệu giữa người gửi và người nhận.

**1.4.2. Thông điệp dữ liệu:** Thông tin được tạo ra, gửi đi, nhận hoặc lưu trữ bằng phương tiện điện tử.

**1.4.3. Dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm:** Dịch vụ chứng thực thông điệp dữ liệu cung cấp bằng chứng về việc gửi, việc nhận, thời điểm gửi, thời điểm nhận và danh tính của người gửi, người nhận.

**1.4.4. Dịch vụ gửi, nhận thư điện tử:** Dịch vụ chứng thực thông điệp dữ liệu chuyên biệt dành cho thư điện tử, cung cấp bằng chứng về việc gửi, việc nhận và tính toàn vẹn của thư điện tử cùng các phần đính kèm.

**1.4.5. Dịch vụ lưu trữ và xác nhận tính toàn vẹn của thông điệp dữ liệu:** Dịch vụ lưu trữ thông điệp dữ liệu kèm theo các bằng chứng liên quan và cung cấp khả năng xác minh lại tính toàn vẹn của thông điệp dữ liệu đó trong suốt thời hạn lưu trữ.

**1.4.6. Ký số trên thông điệp dữ liệu để lưu trữ dài hạn:** Việc áp dụng chữ ký số và/hoặc dấu thời gian lên thông điệp dữ liệu và các bằng chứng liên quan nhằm duy trì giá trị pháp lý và khả năng xác minh được trong thời gian dài, kể cả khi thuật toán hoặc chứng thư số hết hiệu lực.

**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 đối với kỹ thuật 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.<br>- Đối với tiêu chuẩn RSA:<br>+ Tối thiểu phiên bản 2.1;<br>+ Áp dụng lược đồ RSAES-OAEP để mã hoá và RSASSA-PSS để ký.<br>+ Độ dài khóa tối thiểu là 2048 bit<br>- 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 | |
| Hàm băm | FIPS PUB 180-4 | Secure Hash Standard | Áp dụng một trong các hàm băm sau:<br>SHA-256,<br>SHA-384,<br>SHA-512,<br>SHA-512/224, |
| | FIPS PUB 202 | SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions | |

| | | | |
|---|---|---|---|
| | | | SHA-512/256,<br>SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256 |

### 2.1.2. Yêu cầu đối với 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 | Tên tiêu chuẩn | |
| 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<br>(tối thiểu EAL mức 4) | Protection Profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services | |

### 2.2. Yêu cầu đối với dịch vụ chứng thực thông điệp dữ liệu

#### 2.2.1. Yêu cầu kỹ thuật đối với dịch vụ chứng thực thông điệp dữ liệu

Dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu quy định tại Bảng 5:

**Bảng 5 - Yêu cầu đối với dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm**

| Loại Yêu cầu | Tiêu chuẩn tham chiếu | | Quy định áp dụng |
|---|---|---|---|
| | Ký hiệu | Tên tiêu chuẩn | |
| Dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm | ETSI EN 319 522: Part 1 | Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture | Phiên bản V1.2.1 |
| | ETSI EN 319 522: Part 2 | Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents | Phiên bản V1.2.1 |
| | ETSI EN 319 522: Part 3 | Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats | Phiên bản V1.2.1 |
| | ETSI EN 319 522: Part 4-1 | Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: Message delivery bindings | Phiên bản V1.2.1 |
| | ETSI EN 319 522: Part 4-2 | Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: Evidence and identification bindings | Phiên bản V1.1.1 |
| Dịch vụ gửi, nhận thông điệp dữ liệu | ETSI EN 319 532: Part 1 | Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; | Phiên bản V1.1.1 |

| | | | |
|---|---|---|---|
| bảo đảm cho thư điện tử | | Part 1: Framework and Architecture | |
| | ETSI EN 319 532: Part 2 | Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 2: Semantic contents | Phiên bản V1.1.1 |
| | ETSI EN 319 532: Part 3 | Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats | Phiên bản V1.3.1 |
| | ETSI EN 319 532: Part 4 | Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 4: Interoperability Profiles | Phiên bản V1.3.1 |

Việc Ký số trên thông điệp dữ liệu để lưu trữ dài hạn phải đáp ứng các yêu cầu quy định tại Bảng 6:

**Bảng 6 - Yêu cầu về ký số trên thông điệp dữ liệu để lưu trữ dài hạn**

| Loại Yêu cầu | Tiêu chuẩn tham chiếu | | Quy định áp dụng |
|---|---|---|---|
| | Ký hiệu | Tên tiêu chuẩn | |
| Giao thức dịch vụ tin cậy bảo quản dữ liệu dài hạn | ETSI TS 119 512 | Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services | Phiên bản V1.1.1 |
| Bảo mật hệ thống bảo quản dữ liệu | ETSI TS 101 533-1 | Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management | Áp dụng cả ba tiêu chuẩn:<br>ETSI TS 101 533-1 phiên bản V1.3.1;<br>RFC 4998 và RFC 6283 |
| | RFC 4998 | Data Preservation Systems Security; | |
| | RFC 6283 | Part 1: Requirements for Implementation and Management | |
| Chính sách về chữ ký số và chữ ký điện tử | ETSI TS 119 172: Part 1 | Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human | Phiên bản V1.1.1 |

| | | | |
|---|---|---|---|
| | | readable signature policy documents | |
| | ETSI TS 119 172: Part 2 | Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 2: XML format for signature policies | Phiên bản V1.1.1 |
| | ETSI TS 119 172: Part 3 | Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 3: ASN.1 format for signature policies | Phiên bản V1.1.1 |
| | ETSI TS 119 172: Part 4 | Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists | Phiên bản V1.1.1 |
| Tạo và xác thực chữ ký số AdES | ETSI EN 319 102-1 | Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation | Phiên bản V1.4.1 |
| | ETSI TS 119 102-2 | Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report | Phiên bản V1.4.1 |
| Chữ ký số cho CMS | ETSI EN 319 122-1 | Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures | Phiên bản V1.3.1 |
| | ETSI EN 319 122-2 | Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures | Phiên bản V1.1.1 |
| | ETSI TS 119 122-3 | Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES | Phiên bản V1.1.1 |

| | | | |
|---|---|---|---|
| Chữ ký số cho PDF | ETSI EN 319 142-1 | Electronic Signatures and Infrastructures (ESI);<br>PAdES digital signatures;<br>Part 1: Building blocks and PAdES baseline signatures | Áp dụng một trong hai bộ tiêu chuẩn:<br>ETSI EN 319 142-1<br>ETSI EN 319 142-2<br>Hoặc<br>ISO 14533-3:2017<br>ISO 32000-1:2008<br>ISO 32000-2:2020 |
| | ETSI EN 319 142-2 | Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles | |
| | ISO 32000-1:2008 | Document management - Portable document format - Part 1: PDF 1.7 | |
| | ISO 14533-3:2017 | Processes, data elements and documents in commerce, industry and administration — Long-term signature formats — Part 3: Long-term signature profiles for PDF Advanced Electronic Signatures (PAdES) | |
| | ISO 32000-2:2020 | Document management - Portable document format – Part 2: PDF 2.0 | |
| Chữ ký số cho XML | ETSI EN 319 132-1 | Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures | Phiên bản V1.2.1 |
| | ETSI EN 319 132-2 | Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures | Phiên bản V1.1.1 |

**2.2.2. Yêu cầu đối với quy trình vận hành và kiểm soát**

2.2.2.1. Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải triển khai các biện pháp bảo đảm quy trình vận hành và kiểm soát cung cấp dịch vụ đáp ứng các quy định của tiêu chuẩn ETSI EN 319 521.

2.2.2.2. Tổ chức cung cấp dịch vụ gửi, nhận thư điện tử phải triển khai các biện pháp bảo đảm quy trình vận hành và kiểm soát cung cấp dịch vụ đáp ứng các quy định của tiêu chuẩn ETSI EN 319 531.

2.2.2.3. Tổ chức cung cấp dịch vụ lưu trữ và xác nhận tính toàn vẹn của thông điệp dữ liệu phải triển khai các biện pháp bảo đảm quy trình vận hành và kiểm soát cung cấp dịch vụ đáp ứng các quy định của tiêu chuẩn ETSI TS 119 511.

## 3. QUY ĐỊNH VỀ QUẢN LÝ

**3.1.** Phương thức đánh giá sự phù hợp đối với các yêu cầu tại mục 2.2.2 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 đối với chữ ký điện tử và dịch vụ tin cậy và các quy định hiện hành.

**3.2.** Tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu 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 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 chứng thực thông điệp dữ liệu

**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.