DỰ THẢO

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

QCVN xxx: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 xxx:2025/BKHCN do Trung tâm Chứng thực điện tử Quốc gia biên soạn, Bộ Khoa học và Công nghệ thẩm định và ban hành kèm theo Thông tư số ..../2025/TT-BTTTT 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 đối với dịch vụ chứng thực thông điệp dữ liệu, bao gồm yêu cầu kỹ thuật về chữ ký số, chứng thư chữ ký số, yêu cầu về 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.

1.3. Tài liệu viện dẫn

TCVN xxx:2025 - Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung đối với Tổ chức cung cấp dịch vụ tin cậy;

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

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

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

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

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

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

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

IETF RFC 5322: "Internet Message Format"

ETSI EN 319 531: “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers”

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”

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IETF RFC 4998: "Evidence Record Syntax (ERS)"

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

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

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

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

1.4. Giải thích từ ngữ

1.5. Chữ viết tắt

CA	Certification Authority	Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng
RA	Registration Authority	Tổ chức đăng ký
TSP	Trust Service Provider	Tổ chức cung cấp dịch vụ tin cậy
CP	Certificate Policy	Chính sách chứng thư
CPS	Certification Practice Statement	Quy chế chứng thực
PKI	Public Key Infrastructure	Hạ tầng khóa công khai
HSM	Hardware Security Module	Thiết bị bảo mật phần cứng (thiết bị lưu và xử lý khóa bí mật)
CRL	Certificate Revocation List	Danh sách chứng thư bị thu hồi
OCSP	Online Certificate Status Protocol	Giao thức kiểm tra trạng thái chứng thư trực tuyến
LDAP	Lightweight Directory Access Protocol	Giao thức truy cập thư mục nhẹ
EAL	Evaluation Assurance Level	Cấp độ đảm bảo đánh giá (trong đánh giá an toàn thông tin ISO/IEC 15408)
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission	Tổ chức tiêu chuẩn hóa quốc tế / Ủy ban kỹ thuật điện quốc tế
ETSI	European Telecommunications Standards Institute	Viện Tiêu chuẩn Viễn thông Châu Âu
RFC	Request for Comments	Tài liệu tiêu chuẩn kỹ thuật do IETF ban hành
IETF	Internet Engineering Task Force	Nhóm công tác kỹ thuật Internet

FIPS	Federal Information Processing Standards	Bộ tiêu chuẩn xử lý thông tin liên bang Hoa Kỳ
SHA	Secure Hash Algorithm	Thuật toán băm an toàn
RSA	Rivest-Shamir-Adleman	Thuật toán mật mã khóa công khai
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số dựa trên đường cong elliptic
PKCS	Public-Key Cryptography Standards	Bộ tiêu chuẩn mật mã khóa công khai (do RSA Labs phát triển)
X.509	ITU-T Recommendation X.509	Khung chuẩn cho chứng thư số trong hệ thống PKI
DN	Distinguished Name	Tên phân biệt (trong định danh X.509)
UTC	Coordinated Universal Time	Giờ Phối hợp Quốc tế

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

<table>
<tr><th rowspan="2">Loại Yêu cầu</th><th colspan="2">Tiêu chuẩn tham chiếu</th><th rowspan="2">Quy định áp dụng</th></tr>
<tr><th>Ký hiệu</th><th>Tên tiêu chuẩn</th></tr>
<tr><td rowspan="2">Mật mã phi đối xứng và chữ ký số</td><td>PKCS #1
(RFC 3447)</td><td>RSA Cryptography Standard</td><td rowspan="2">- 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</td></tr>
<tr><td>ANSI X9.62-2005</td><td>Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)</td></tr>
<tr><td>Mật mã đối xứng</td><td>TCVN 7816:2007</td><td>Công nghệ thông tin - Kỹ thuật mật mã - thuật toán mã dữ liệu AES</td><td>Áp dụng một trong hai tiêu chuẩn</td></tr>
</table>

	FIPS PUB 197	Advanced Encryption Standard	
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 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	Security Requirements for Cryptographic Modules	- Áp dụng một trong ba tiêu chuẩn. - Đối với tiêu chuẩn FIPS PUB 140-2 và FIPS PUB 140-3: Yêu cầu tối thiểu mức 3 (level 3) - Đối với tiêu chuẩn EN 419 221-5:2018: Yêu cầu tối thiểu EAL mức 4 (level 4)
	FIPS PUB 140-3	Security Requirements for Cryptographic Modules	
	EN 419 221-5:2018	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 kĩ 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:	Phiên bản V1.1.1

		Evidence and identification bindings	
Dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm cho thư điện tử	ETSI EN 319 532: Part 1	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1: Framework and Architecture	Phiên bản V1.1.1
	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 V 1.3.1
	ETSI EN 319 532: Part 4	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 4: Interoperability Profiles	Phiên bản V 1.3.1

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: ETSI TS 101 533-1 phiên bản V1.3.1; 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 readable signature policy documents	Phiên bản V1.1.1
	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); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures	Áp dụng một trong hai bộ tiêu chuẩn: ETSI EN 319 142-1 ETSI EN 319 142-2 Hoặc ISO 14533-3:2017 ISO 32000-1:2008 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 kiểm soát và vận hành

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 kiểm soát và vận hành 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 kiểm soát và vận hành 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 kiểm soát và vận hành cung cấp dịch vụ đáp ứng các quy định của tiêu chuẩn ETSI TS 119 511.

3. QUY ĐỊNH VỀ QUẢN LÝ

3.1. Dịch vụ chứng thực thông điệp dữ liệu thuộc phạm vi điều chỉnh tại mục 1.1 phải tuân thủ các quy định trong quy chuẩn kỹ thuật này;

3.2. Phương thức chứng nhận sự phù hợp thực hiện phương thức 6 (đánh giá hệ thống quản lý) theo quy định tại Thông tư 28/2012/TT-BKHCN và Thông tư quy định hoạt động kiểm toán kỹ thuật đối với dịch vụ tin cậy;

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

Tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu phải thực hiện kiểm toán kỹ thuật theo quy định tại **Mục 3.2 của** Quy chuẩn kỹ thuật này và chịu sự kiểm tra của các cơ quan quản lý nhà nước theo các quy định hiện hành.

5. TỔ CHỨC THỰC HIỆN

5.1. Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia, 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, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia, 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.