TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN xxxx:2026

Xuất bản lần 1

GIAO DỊCH ĐIỆN TỬ - YÊU CẦU CHUNG VỀ KỸ THUẬT ĐỐI VỚI PHẦN MỀM KÝ SỐ, PHẦN MỀM KIỂM TRA CHỮ KÝ SỐ

Electronic transactions - Technical Requirements for signature creation and signature verification applications

HÀ NỘI - 2026

Mục lục

Lời nói đầu

TCVN XXXX:2026 được xây dựng trên cơ sở tham khảo các Tiêu chuẩn quốc tế về ký số và kiểm tra chữ ký số, có điều chỉnh, sửa đổi, bổ sung để phù hợp với điều kiện của Việt Nam.

TCVN XXXX:2026 do Trung tâm Chứng thực điện tử Quốc gia biên soạn, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

T I Ê U C H U Ẩ N Q U Ố C G I A **TCVN xxxx:2026**

Giao dịch điện tử - Yêu cầu chung về kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số

Electronic Transactions - Technical Requirements for signature creation and signature verification applications

1 Phạm vi áp dụng

Tài liệu này các yêu cầu chức năng và giao diện đối với phần mềm ký số, phần mềm kiểm tra chữ ký số.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây là cần thiết để áp dụng tiêu chuẩn này. Đối với tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất (bao gồm cả phiên bản sửa đổi, bổ sung).

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

ETSI EN 319 122: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures (Part 1: Building blocks and CAdES baseline signatures)

ETSI EN 319 132: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures (Part 1: Building blocks and XAdES baseline signatures)

ETSI EN 319 142: Electronic Signatures and Infrastructures (ESI); PAdES digital signatures (thường chia Part 1 & 2: Building blocks và Additional profiles)

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

ETSI TS 119 612: Electronic Signatures and Trust Infrastructures (ESI); Trusted Lists

FIPS PUB 197: Advanced Encryption Standard (AES)

ISO 14533: Processes, data elements and documents in commerce, industry and administration - Long term signature profiles

ISO 32000: Document management - Portable document format (PDF)

NIST SP 800-57 Part 1: Recommendation for Key Management: Part 1 – General

NIST SP 800-89: Recommendation for Obtaining Assurances for Digital Signature Applications

NIST SP 800-107: Recommendation for Applications Using Approved Hash Algorithms

RFC 3447: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1

RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2

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

RFC 6234: US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)

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

RFC 8259: The JavaScript Object Notation (JSON) Data Interchange Format

RFC 9110: HTTP Semantics

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

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa sau:

3.1

Phần mềm ký số

Chương trình độc lập hoặc một thành phần (module) phần mềm hoặc giải pháp có chức năng ký số vào thông điệp dữ liệu.

3.2

Phần mềm kiểm tra chữ ký số

Chương trình độc lập hoặc một thành phần (module) phần mềm hoặc giải pháp có chức năng kiểm tra tính hợp lệ của chữ ký số trên thông điệp dữ liệu đã ký.

3.3

Thông điệp dữ liệu

Thông tin được tạo ra, được gửi, được nhận, được lưu trữ bằng phương tiện điện tử.

3.4

Cặp khóa không đối xứng

Khóa công khai và khóa bí mật tương ứng.

3.5

Khóa bí mật

Thành phần của cặp khóa không đối xứng được sử dụng để ký thông điệp dữ liệu.

3.6

Khóa công khai

Thành phần của cặp khóa không đối xứng được sử dụng để xác thực chữ ký số trên thông điệp dữ liệu.

3.7

Hàm băm

Thuật toán chuyển đổi thông điệp dữ liệu đầu vào thành một chuỗi có độ dài cố định.

3.8

Mã băm

Kết quả đầu ra của hàm băm.

3.9

Chủ thể ký

Cá nhân hoặc tổ chức sở hữu chứng thư chữ ký số và sử dụng khóa bí mật tương ứng để thực hiện ký số trên thông điệp dữ liệu.

3.10

Chứng thư chữ ký số

Thông điệp dữ liệu nhằm xác nhận cơ quan, tổ chức, cá nhân được chứng thực là người ký chữ ký số.

3.11

Đường dẫn tin cậy

Danh sách có thứ tự các chứng thư chữ ký số, bao gồm chứng thư chữ ký số của thuê bao, chứng thư chữ ký số của các Tổ chức cung cấp dịch vụ chứng thực chữ ký số và chứng thư chữ ký số gốc tin cậy nhằm xác minh nguồn gốc của chứng thư chữ ký số.

3.12

Danh sách tin cậy

Tập hợp chứng thư chữ ký số nước ngoài được công nhận tại Việt Nam.

4 Ký hiệu và chữ viết tắt

Chữ viết tắt	Nghĩa tiếng Anh	Nghĩa tiếng Việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa nâng cao
ANSI	American National Standards Institute	Viện Tiêu chuẩn quốc gia Hoa Kỳ
CRL	Certificate Revocation List	Danh sách chứng thư chữ ký số bị thu hồi
CMS	Cryptographic Message Syntax	Cú pháp thông điệp mật mã

ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán Chữ ký Số Đường cong Elliptic
ES-OAEP	RSA Encryption Scheme - Optimal Asymmetric Encryption Padding	Lược đồ Mã hóa RSA - OAEP
ETSI TS	European Telecommunications Standards Institute - Technical Specification	Viện Tiêu chuẩn Viễn thông Châu Âu - Đặc tả Kỹ thuật
FIPS PUB	Federal Information Processing Standards Publication	Tài liệu Tiêu chuẩn xử lý thông tin Liên bang
HKDF	HMAC-based Key Derivation Function	Hàm dẫn xuất khóa dựa trên HMAC
HMAC	Hash-based Message Authentication Code	Mã xác thực thông điệp dữ liệu dựa trên hàm băm
HTTP	HyperText Transfer Protocol	Giao thức truyền siêu văn bản
ISO	International Organization for Standardization	Tổ chức tiêu chuẩn quốc tế
JSON	JavaScript Object Notation	Ký hiệu đối tượng JavaScript
NIST SP	National Institute of Standards and Technology - Special Publication	Viện Tiêu chuẩn và Công nghệ Hoa Kỳ - Ấn phẩm đặc biệt
OCSP	Online Certificate Status Protocol	Giao thức kiểm tra trạng thái chứng thư chữ ký số trực tuyến
PDF	Portable Document Format	Định dạng tài liệu di động
RFC	Request for Comments	Yêu cầu bình luận (Tiêu chuẩn IETF)
RSA	Rivest-Shamir-Adleman	Thuật toán RSA
SHA	Secure Hash Algorithm	Thuật toán hàm băm an toàn
SSA-PSS	Signature Scheme with Appendix - Probabilistic Signature Scheme	Lược đồ chữ ký phụ lục - Lược đồ chữ ký xác suất
TCVN	Tiêu chuẩn Việt Nam	Tiêu chuẩn Việt Nam
TLS	Transport Layer Security	Bảo mật tầng giao vận
XML	eXtensible Markup Language	Ngôn ngữ đánh dấu mở rộng

5 Phần mềm ký số

5.1 Yêu cầu về chức năng

Phần mềm ký số đáp ứng tối thiểu các chức năng được nêu ở mục 5.1. Yêu cầu về chức năng.

5.1.1. Chuyển đổi định dạng thông điệp dữ liệu

Thông điệp dữ liệu ký số được chuyển thành một trong các định dạng theo yêu cầu tại Bảng 1:

Tên loại	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Phiên bản áp dụng
Định dạng tài liệu di động	ETSI EN 319 142-1	Electronic Signatures and Infrastructures (ESI);	Áp dụng một trong hai bộ tiêu chuẩn:

PDF (Portable Document Format)		PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures	ETSI EN 319 142-1, Phiên bản V1.2.1; ETSI EN 319 142-2, Phiên bản V1.1.1 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	
Định dạng ngôn ngữ đánh dấu mở rộng XML (eXtensible Markup Language)	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
Định dạng ký hiệu đối tượng JavaScript (JSON)	RFC 8259	The JavaScript Object Notation (JSON) Data Interchange Format	
	ETSI TS 119 182-1	Electronic Signatures and Trust Infrastructures (ESI); JAdES digital signatures; Part 1:	Phiên bản V1.2.1

		Building blocks and JAdES baseline signatures	
Định dạng thông điệp mã hóa CMS (Cryptographic Message Syntax)	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

5.1.2. Xác thực thông tin của chủ thể ký

Trước khi thực hiện ký số, phần mềm ký số thực hiện xác thực thông tin chủ thể ký thông qua các tác vụ sau:d

5.1.2.1. Xác thực danh tính chủ thể ký

Việc xác thực danh tính chủ thể ký tuân thủ quy định về định danh điện tử và các khuyến nghị được mô tả tại NIST SP 800-89.

5.1.2.2. Xác thực thông tin chứng thư chữ ký số của chủ thể ký

Chứng thư chữ ký số của chủ thể ký tuân thủ các yêu cầu sau:

a) Định dạng chứng thư chữ ký số tuân thủ theo X.509 được mô tả tại RFC 5280;

b) Thời điểm thực hiện ký số nằm trong khoảng thời hạn có hiệu lực của chứng thư chữ ký số của chủ thể ký;

c) Thông tin về thời hạn có hiệu lực chứng thư chữ ký số của chủ thể ký tuân thủ RFC 6960 (dành cho OCSP) và RFC 5280 (dành cho CRL);

d) Chứng thư chữ ký số có hiệu lực (không bị tạm dừng hoặc thu hồi) tại thời điểm thực hiện ký số;

e) Chứng thư chữ ký số của chủ thể ký được tin cậy, thể hiện bằng một trong những điều sau:

- Đường dẫn tin cậy trong chứng thư chữ ký số của chủ thể ký liên kết đến chứng thư chữ ký số của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia (tham khảo RFC 5280);

HOẶC

- Chứng thư chữ ký số của chủ thể ký có trong Danh sách tin cậy chứng thư chữ ký điện tử nước ngoài được công nhận tại Việt Nam (định dạng Danh sách tin cậy tuân thủ ETSI 119 612).

5.1.2.3. Xác thực việc sở hữu khóa của chủ thể ký

Việc sở hữu khóa của chủ thể ký được xác thực thông qua các phương thức bảo đảm được mô tả tại tài liệu NIST SP 800-89.

5.1.3. Xử lý thông điệp dữ liệu được ký số

Việc thực hiện xử lý thông điệp dữ liệu ký số thông qua hàm băm theo yêu cầu tại Bảng 2:

Tên loại	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Phiên bản áp dụng
Yêu cầu về hàm băm	RFC 6234	US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)	
	NIST SP 800-107 Revision 1	Recommendation for Obtaining Assurances for Digital Signature Applications	
	ETSI TS 119 312	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites	Phiên bản V2.1.1
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	
Mật mã phi đối xứng và chữ ký số	PKCS #1 (RFC 8017)	PKCS #1: RSA Cryptography Specifications Version 2.2	- 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 hóa 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)	

5.1.4. Xử lý yêu cầu ký số

Việc xử lý yêu cầu ký số được thực hiện thông qua việc kết nối đến hệ thống hoặc thiết bị lưu trữ khóa bí mật và được đảm bảo bởi các tác vụ sau:

5.1.4.1. Bảo mật giao thức đường truyền

Giao thức kết nối giữa phần mềm ký số và thiết bị lưu trữ khóa bí mật được bảo đảm an toàn, tuân theo yêu cầu tại Bảng 3:

Tên loại	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Phiên bản áp dụng
Giao thức đường truyền	RFC 9110	HTTP Semantics	Áp dụng HTTP/2
	RFC 9113	HTTP/2	
Giao thức bảo mật tầng giao vận	RFC 9846	The Transport Layer Security (TLS) Protocol Version 1.3	Áp dụng tối thiểu TLS 1.3

5.1.4.2. Quản lý khóa

Việc quản lý khóa của chủ thể ký đảm bảo tuân thủ tiêu chuẩn NIST SP 800-57 Part 1 Rev 5 về quản lý khóa.

5.1.5. Xử lý kết quả ký số

Sau khi kết nối đến hệ thống hoặc thiết bị lưu trữ khóa bí mật, phần mềm ký số nhận được kết quả của tác vụ ký số kể cả trong trường hợp giao dịch ký số thất bại.

Trường hợp giao dịch ký số thành công, phần mềm ký số tiến hành gắn kết quả ký số vào thông điệp dữ liệu và đảm bảo tính đúng đắn của các thông tin sau:

5.1.5.1. Kiểm tra thuật toán sử dụng để ký số

Phần mềm ký số triển khai các biện pháp kỹ thuật để tiến hành kiểm tra tính hợp lệ của khóa công khai và các tham số miền liên quan để đảm bảo tính hợp lệ của thuật toán đã được sử dụng để ký số.

Việc kiểm tra được thực hiện theo yêu cầu tại Bảng 4:

Tên loại	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Phiên bản áp dụng
Thuật toán sử dụng để ký số	ETSI TS 119 312	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites	Phiên bản V2.1.1
	NIST SP 800-57 Part 1 Revision 5	Recommendation for Key Management: Part 1 – General	
	NIST SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications	
	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and	

		Certificate Revocation List (CRL) Profile	

5.1.5.2. Kiểm tra thông tin chứng thư chữ ký số

Việc kiểm tra thông tin chứng thư chữ ký số có trong kết quả giá trị chữ ký số đảm bảo tuân thủ các điều kiện được nêu tại mục 5.1.2.2. Xác thực thông tin chứng thư chữ ký số của chủ thể ký.

5.1.5.3. Gắn kết quả ký số vào thông điệp dữ liệu

Việc gắn kết quả ký số vào thông điệp dữ liệu đảm bảo thông điệp dữ liệu tuân thủ theo đúng các định dạng được nêu tại mục 5.1.1. Chuyển đổi định dạng thông điệp dữ liệu.

5.2. Yêu cầu về giao diện

Về giao diện, phần mềm ký số bảo đảm các yêu cầu sau:

5.2.1. Thông tin của các tổ chức cung cấp dịch vụ tin cậy để đảm bảo quyền tự do lựa chọn nhà cung cấp của chủ thể ký được hiển thị đầy đủ, rõ ràng;

5.2.2. Thông tin của các tổ chức cung cấp dịch vụ tin cậy hỗ trợ chức năng ký số của các tổ chức cung cấp dịch vụ tương ứng;

5.2.3. Hiển thị toàn bộ nội dung tài liệu ký trước khi ký, đảm bảo đáp ứng sự chấp thuận của chủ thể ký về mặt nội dung thông điệp dữ liệu;

5.2.4. Hiển thị trực quan giao diện ký số hỗ trợ việc căn chỉnh, đặt vị trí con dấu, chữ ký mô phỏng đảm bảo đúng theo các quy định về thể thức văn bản;

5.2.5. Các thông báo bằng chữ hoặc ký hiệu cho chủ thể ký biết việc ký số vào thông điệp dữ liệu thành công hay không thành công được thể hiện bằng Tiếng Việt và ngôn ngữ khác (nếu có hỗ trợ);

5.2.6. Tính năng tải về tài liệu đã ký được triển khai cùng phần mềm ký số.

6. Phần mềm kiểm tra chữ ký số

Phần mềm kiểm tra chữ ký số đáp ứng tối thiểu các chức năng được nêu ở mục 6.1. Yêu cầu về chức năng.

6.1. Yêu cầu về chức năng

6.1.1. Trích xuất thông tin từ thông điệp dữ liệu đã ký

Phần mềm kiểm tra chữ ký số thực hiện được việc trích xuất tối thiểu các thông tin sau từ thông điệp dữ liệu đã ký:

a) Chứng thư chữ ký số trên thông điệp dữ liệu đã ký;

b) Mã băm của thông điệp dữ liệu đã ký được giải mã từ chữ ký số sử dụng khóa công khai trên chứng thư chữ ký số của thông điệp dữ liệu đã ký;

c) Mã băm của thông điệp dữ liệu đang kiểm tra.

6.1.2. Xác thực thông tin về mã băm

Phần mềm kiểm tra chữ ký số kiểm tra thông tin về mã băm để đảm bảo tính toàn vẹn, tính xác thực và tính chống chối bỏ của thông điệp dữ liệu.

6.1.2.1. Kiểm tra yêu cầu về mã băm

Mã băm trong thông điệp dữ liệu đã ký thỏa mãn các yêu cầu tại Bảng 2.

6.1.2.2. Kiểm tra tính trùng khớp của mã băm

Các mã băm tại điểm b) và điểm c) tại Mục 6.1.1. trùng khớp.

6.1.3. Xác thực thông tin chứng thư chữ ký số

Thông tin chứng thư chữ ký số trong thông điệp dữ liệu đã ký thỏa mãn các yêu cầu tại Mục 5.1.2.2. Xác thực thông tin chứng thư chữ ký số của chủ thể ký.

6.2. Yêu cầu về giao diện

Về giao diện, phần mềm kiểm tra chữ ký số bảo đảm các yêu cầu sau:

6.2.1. Hiển thị thông báo về tính hợp lệ của chữ ký số;

6.2.2. Hiển thị các thông tin về chữ ký số và chứng thư chữ ký số trên thông điệp dữ liệu đã ký, với tối thiểu các trường thông tin sau:

a) Thông tin về cơ quan, tổ chức tạo lập, cấp, phát hành chứng thư chữ ký số;

b) Thông tin về chủ thể ký;

c) Thông tin về đơn vị quản lý chứng thư chữ ký số (nếu có);

d) Thông tin về thời điểm ký số hoặc dấu thời gian (nếu có);

e) Thông báo về tính toàn vẹn của thông điệp dữ liệu đã ký;

f) Thông tin về tính hợp lệ của chứng thư chữ ký số tại thời điểm ký;

g) Thông tin về thời hạn có hiệu lực của chứng thư chữ ký số.

Thư mục tài liệu tham khảo

TCVN xxxx:2026 được xây dựng dựa trên cơ sở tham khảo Thông tư 15/2025/TT-BKHCN ngày 15/8/2025 của Bộ Khoa học và Công nghệ.