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 CHỮ KÝ SỐ CÔNG CỘNG

NATIONAL TECHNICAL REGULATION ON REQUIREMENTS FOR PUBLIC DIGITAL SIGNATURE AUTHENTICATION 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 CHỮ KÝ SỐ CÔNG CỘNG

NATIONAL TECHNICAL REGULATION ON REQUIREMENTS FOR PUBLIC DIGITAL SIGNATURE AUTHENTICATION 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 chữ ký số công cộng, bao gồm:

- Dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số trên các phương tiện lưu khóa bí mật bằng thiết bị phần cứng;

- Dịch vụ chứng thực chữ ký số công cộng theo mô hình từ xa;

- Dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số trên thiết bị di động.

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 chữ ký số công cộng.

1.3. Tài liệu viện dẫn

IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
IETF RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
ISO/IEC 15408	Information security, cybersecurity and privacy protection - Evaluation criteria for IT security (parts 1 to 3)
ISO/IEC 9594-8 /Recommendation ITU-T X.509	Information technology - Open systems interconnection - Part 8: The Directory: Public-key and attribute certificate frameworks".
FIPS PUB 140-2	Security Requirements for Cryptographic Modules
FIPS PUB 202	SHA-3 Standard - Permutation-Based Hash and Extendable - Output Functions
FIPS PUB 180-4	Secure Hash Standard
FIPS PUB 197	Advanced Encryption Standard
EN 419 221-5:2018	Protection Profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services requirements
EN 419 221-1:2018	Trustworthy Systems Supporting Server Signing - Part 1: General system security requirements
EN 419 221-2:2019	Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing

ETSI EN 319 401	Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 411-1	Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI TS 119 431-1	Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev
ETSI TS 119 432	Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation
ETSI TR 102 203	Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements
ETSI TS 102 204	Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface
ETSI TR 102 206	Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework
ETSI TS 102 207	Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services
TCVN 8709 (ISO/IEC 15408)	Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn công nghệ thông tin (Common Criteria for Information Technology Security Evaluation)
TCVN 7816:2007	Công nghệ thông tin - Kỹ thuật mật mã - thuật toán mã dữ liệu AES

1.4. Giải thích từ ngữ

Định nghĩa các mô hình ký số

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 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	PKCS #1 (RFC 3447)	RSA Cryptography Standard	- Áp dụng một trong hai tiêu chuẩn.

xứng và chữ ký số	ANSI X9.62-2005	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)	- 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
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: 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	RFC 2585	Internet X.509 Public Key Infrastructure - Operational Protocols: FTP and HTTP	Áp dụng một hoặc cả hai giao thức FTP và HTTP

thư chữ ký số bị thu hồi			
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 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, và 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	
Token và Smart card	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	Yêu cầu tối thiểu mức 2 (level 2)
	FIPS PUB 140-3	Security Requirements for Cryptographic Modules	

2.2. Yêu cầu đối với mô hình ký số trên các phương tiện lưu khóa bí mật bằng thiết bị phần cứng

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

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số trên các phương tiện lưu khóa bí mật bằng thiết bị phần cứng 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 319 411-1 (áp dụng phiên bản V1.4.1).

2.3. Yêu cầu đối với mô hình ký số từ xa

2.3.1. Yêu cầu đối với hệ thống quản lý khóa bí mật, chứng thư chữ ký số và tạo chữ ký số của khách hàng

Hệ thống quản lý khóa bí mật, chứng thư chữ ký số và tạo chữ ký số của khách hàng đáp ứng các quy định tại Bảng 5

Bảng 5 - 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	
Giao thức tạo chữ ký số	ETSI TS 119 432	Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation	Phiên bản V1.2.1
Ứng dụng ký trên máy chủ ký số	EN 419241-1:2018	Trustworthy Systems Supporting Server Signing - Part 1: General system security requirements	
Yêu cầu cho mô đun ký số	EN 419241-2:2019	Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing	

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

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa 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 119 431-1 (áp dụng phiên bản V1.1.1) và ETSI TS 119 431-2 (áp dụng phiên bản V1.1.1).

2.4. Yêu cầu đối với mô hình ký số trên thiết bị di động

2.4.1. Yêu cầu đối với chức năng và giao diện

Chức năng và giao diện của Hệ thống ký số trên thiết bị di động đáp ứng các yêu cầu quy định tại Bảng 6

Bảng 6 - Yêu cầu đối với chức năng và giao diện

Loại Yêu cầu	Tiêu chuẩn tham chiếu		Quy định áp dụng
	Ký hiệu	Tên tiêu chuẩn	
Yêu cầu về chức năng, nghiệp vụ	ETSI TR 102 203	Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements	Phiên bản V1.1.1
Giao diện dịch vụ Web	ETSI TS 102 204	Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface	Phiên bản V1.1.4

Khung bảo mật	ETSI TR 102 206	Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework	Phiên bản V1.1.3
Thông số kỹ thuật chuyển vùng	ETSI TS 102 207	Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services	Phiên bản V1.1.3

2.4.2. Yêu cầu đối với thẻ SIM

Thẻ SIM phải đáp ứng các yêu cầu tại Bảng 7:

Bảng 7 - Yêu cầu đối với thẻ SIM

Loại Yêu cầu	Tiêu chuẩn tham chiếu		Quy định áp dụng
	Ký hiệu	Tên tiêu chuẩn	
Thẻ SIM	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 2 (level 2) - Đối với tiêu chuẩn TCVN 8709: Yêu cầu tối thiểu EAL mức 4 (level 4)
	FIPS PUB 140-3	Security Requirements for Cryptographic Modules	
	TCVN 8709 (ISO/IEC 15408)	Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn công nghệ thông tin (Common Criteria for Information Technology Security Evaluation)	

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

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số trên thiết bị di động 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 319 411-1 (áp dụng phiên bản V1.4.1).

3. QUY ĐỊNH VỀ QUẢN LÝ

3.1. Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng 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 đối với các yêu cầu tại mục 2.2.1, mục 2.3.2, mục 2.4.3 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 và quy định về 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 chữ ký số 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