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 CẤP DẤU THỜI GIAN

NATIONAL TECHNICAL REGULATION ON REQUIREMENTS FOR TIME-STAMPING 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 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 đối với dịch vụ cấp dấu thời gian, 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 cấp dấu thời gian.

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 cấp dấu thời gian 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;

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

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

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

FIPS PUB 197: "Advanced Encryption Standard"

FIPS PUB 180-4: "Secure Hash Standard"

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

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

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

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

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

PKCS #11: "Cryptographic Token Interface Standard"

PKCS #12: "Personal Information Exchange Syntax Standard"

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

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

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

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"

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

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

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

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

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

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

RFC 5816: "ESSCertIDv2 Update for RFC 3161"

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

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

1.5. 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 về mật mã và chữ ký số

Chữ ký số phải đáp ứng các tiêu chuẩn sau:

<table>
<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 rowspan="2">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 rowspan="2">Áp dụng một trong hai tiêu chuẩn</td></tr>
<tr><td>FIPS PUB 197</td><td>Advanced Encryption Standard</td></tr>
<tr><td>Yêu cầu cho hàm băm</td><td>FIPS PUB 180-4</td><td>Secure Hash Standard</td><td>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</td></tr>
</table>

	FIPS PUB 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions	

2.1.2. Yêu cầu về thông tin, dữ liệu

Thông tin, dữ liệu về chứng thư chữ ký số phải đáp ứng các tiêu chuẩn sau:

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 chính sách cho chứng thư chữ ký số

Chính sách quản lý đối với chứng thư chữ ký số phải đáp ứng tiêu chuẩn sau:

Chính sách chứng thư chữ ký số	RFC 3647	Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework	

2.1.4. Yêu cầu về giao thức lưu trữ và truy xuất chứng thư chữ ký số

Giao thức lưu trữ và truy xuất chứng thư chữ ký số phải đáp ứng các tiêu chuẩn sau:

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	

2.1.5. Yêu cầu về kiểm tra trạng thái chứng thư chữ ký số

Kiểm tra trạng thái chứng thư chữ ký số phải đáp ứng các tiêu chuẩn sau:

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	

2.1.6. Yêu cầu về bảo mật cho HSM quản lý khóa bí mật của tổ chức cung cấp dịch vụ cấp dấu thời gian

Bảo mật cho HSM quản lý khóa bí mật của tổ chức cung cấp dịch vụ cấp dấu thời gian phải đáp ứng tiêu chuẩn sau đây:

Yêu cầu đối với phần cứng HSM	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	- Áp dụng một trong ba tiêu chuẩn. - Đối với các tiêu chuẩn FIPS PUB 140-2/ FIPS PUB 140-3: Yêu cầu tối thiểu mức 3 (level 3)
	FIPS PUB 140-3	Security Requirements for Cryptographic Modules	
	EN 419221-5:2018	Protection Profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services	

2.1.7. Yêu cầu về dịch vụ cấp dấu thời gian

Dịch vụ cấp dấu thời gian phải đáp ứng các tiêu chuẩn sau:

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	
Yêu cầu chính sách cho tổ chức cung cấp dịch vụ dịch vụ cấp dấu thời gian	ETSI EN 319 421	Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps	Phiên bản V1.2.1

2.2. Yêu cầu về vận hành và kiểm soát

Tổ chức cung cấp dịch vụ cấp dấu thời gian phải triển khai các biện pháp bảo đảm kiểm soát và quy trình vận hành cung cấp dịch vụ tuân thủ tiêu chuẩn ETSI EN 319 421-1.

3. QUY ĐỊNH VỀ QUẢN LÝ

3.1. Dịch vụ cấp dấu thời gian thuộc phạm vi điều chỉnh tại mục 1.1 phải tuân thủ các quy định kỹ thuật 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 cấp dấu thời gian 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.