BỘ KHOA HỌC VÀ CÔNG NGHỆ

TRUNG TÂM CHỨNG THỰC ĐIỆN TỬ QUỐC GIA

THUYẾT MINH

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ YÊU CẦU ĐỐI VỚI DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG

Hà Nội - 2025

MỤC LỤC

DANH SÁCH BẢNG BIỂU

DANH MỤC CÁC CHỮ VIẾT TẮT

Kí hiệu	Tiếng anh	Tiếng việt
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

1. Tên và mã hiệu quy chuẩn

Tên quy chuẩn: Quy chuẩn kỹ thuật quốc gia về yêu cầu đối với dịch vụ chứng thực chữ ký số công cộng.

Mã hiệu quy chuẩn: QCVN xxx:2025/BKHCN.

2. Đặt vấn đề

Trong bối cảnh Việt Nam đang đẩy mạnh chuyển đổi số quốc gia, các dịch vụ tin cậy đóng vai trò nền tảng, không thể thiếu để đảm bảo tính pháp lý, an toàn và thông suốt cho các giao dịch điện tử. Các dịch vụ như chữ ký điện tử, dấu thời gian, chứng thực thông điệp dữ liệu là những yếu tố cốt lõi, tạo dựng niềm tin và thúc đẩy sự phát triển của kinh tế số, chính phủ số và xã hội số.

Luật Giao dịch điện tử năm 2023 (Luật số 20/2023/QH15) đã được ban hành, tạo ra hành lang pháp lý quan trọng, công nhận giá trị pháp lý và quy định các yêu cầu đối với các dịch vụ này. Để hiện thực hóa các mục tiêu của Luật, việc đảm bảo các Nhà cung cấp dịch vụ tin cậy (Trust Service Providers - TSP) hoạt động một cách tin cậy, an toàn và tuân thủ pháp luật là yêu cầu tiên quyết. Điều này không chỉ củng cố niềm tin của người dùng mà còn là yếu tố then chốt để các giao dịch điện tử được công nhận và phát huy hiệu quả.

3. Tình hình cung cấp dịch vụ tin cậy tại Việt Nam

- Tổ chức cung cấp dịch vụ tin cậy: Tính đến tháng 7 năm 2025, đã có tổng cộng 25 Tổ chức cung cấp dịch vụ (CA công cộng) đã được cấp giấy phép cung cấp dịch vụ và đang hoạt động trên thị trường chữ ký số và dịch vụ chứng thực chữ ký số công cộng tại Việt Nam.

Chữ ký số được sử dụng chính trong các lĩnh vực kinh tế xã hội, bao gồm:

+ Khai, nộp thuế điện tử;

+ Khai báo bảo hiểm xã hội;

+ Hải quan điện tử;

+ Hóa đơn điện tử;

+ Giao dịch trong lĩnh vực chứng khoán, ngân hàng;

+ Thực hiện dịch vụ công trực tuyến và giao dịch thương mại điện tử;

+ Các giao dịch điện tử dân sự khác.

- Tính đến tháng 7 năm 2025, Các CA công cộng đã phát hành 5.132.523 (lấy theo báo cáo Quý 2) chứng thư chữ ký số công cộng đang hoạt động. Chữ ký số đã được sử dụng rộng rãi, phục vụ hiệu quả quá trình chuyển đổi số Quốc gia.

4. Sở cứ xây dựng các yêu cầu kỹ thuật

4.1. Tình hình tiêu chuẩn hóa của các tổ chức tiêu chuẩn hóa trên thế giới

4.1.1. Viện Tiêu chuẩn Viễn thông Châu Âu (ETSI)

Dịch vụ tin cậy (Trusted Services) là nền tảng quan trọng trong việc xây dựng môi trường giao dịch điện tử an toàn, bảo mật và có giá trị pháp lý trong Liên minh Châu Âu (EU). Các dịch vụ này được điều chỉnh bởi Quy chế eIDAS (Regulation (EU) No 910/2014), đặt ra khung pháp lý thống nhất cho định danh điện tử (eID) và dịch vụ tin cậy trên toàn EU.

Quy chế eIDAS có hiệu lực từ 1/7/2016, với mục tiêu:

- Tạo sự tin cậy trong giao dịch điện tử xuyên biên giới.
- Đảm bảo giá trị pháp lý của chữ ký điện tử, con dấu điện tử, dấu thời gian, và các dịch vụ tin cậy khác.
- Quy định tiêu chuẩn cho nhà cung cấp dịch vụ tin cậy đủ điều kiện.

Để triển khai eIDAS trong thực tế, EU đã giao cho ETSI (European Telecommunications Standards Institute) xây dựng hệ thống tiêu chuẩn kỹ thuật. Các tiêu chuẩn này quy định từ yêu cầu chung cho nhà cung cấp dịch vụ, yêu cầu kỹ thuật cho từng loại dịch vụ, định dạng dữ liệu, đến quy trình đánh giá sự phù hợp. Nhờ đó, các dịch vụ tin cậy giữa các quốc gia EU có thể liên thông, tương thích và được công nhận lẫn nhau.

Viện Tiêu chuẩn Viễn thông châu Âu (viết tắt ETSI) là một tổ chức tiêu chuẩn hóa phi lợi nhuận và độc lập trong công nghiệp viễn thông tại Châu Âu, với dự án rộng khắp trên thế giới. ETSI đã thành công trong việc tiêu chuẩn hóa thiết bị vô tuyến công suất thấp, thiết bị cự ly ngắn, hệ thống thông tin di động và hệ thống vô tuyến mặt đất TETRA.

ETSI được thành lập bởi CEPT vào năm 1988 và chính thức được công nhận bởi Ủy ban Châu Âu và ban thư ký EFTA. Trụ sở của viện đặt tại Sophia Antipolis (Pháp), ETSI là tổ chức chịu trách nhiệm chính thức cho việc tiêu chuẩn hóa về các công nghệ thông tin và truyền thông (ICT) tại Châu Âu. Những công nghệ này bao gồm viễn thông, phát thanh truyền hình và các lĩnh vực liên quan như truyền tải thông minh và điện tử y sinh. ETSI có 740 thành viên từ 62 quốc gia/đơn vị hành chính trong và ngoài Châu Âu, bao gồm các nhà sản xuất, các nhà vận hành khai thác mạng, các nhà quản lý, các nhà cung cấp dịch vụ, cơ quan nghiên cứu và người sử dụng trong thực tế ở mọi lĩnh vực then chốt trong ICT.

Mục tiêu của hệ thống tiêu chuẩn ETSI

- Đảm bảo an toàn và bảo mật cho các dịch vụ tin cậy.

- Tương thích kỹ thuật giữa các quốc gia EU.
- Hỗ trợ đánh giá sự phù hợp và chứng nhận theo eIDAS.
- Giảm chi phí triển khai nhờ dùng chung định dạng và quy trình.

Hệ thống tiêu chuẩn ETSI liên quan đến dịch vụ tin cậy chủ yếu nằm trong các nhóm:

Nhóm tiêu chuẩn về yêu cầu kiểm soát và chính sách vận hành cho TSP

- **EN 319 401** – Yêu cầu chung cho nhà cung cấp dịch vụ tin cậy Quy định quản trị, quản lý rủi ro, chính sách bảo mật, vận hành an toàn, quản lý nhân sự, xử lý sự cố.
- **EN 319 411-1** – Yêu cầu cho CA phát hành chứng thư không đủ điều kiện.
- **EN 319 411-2** – Yêu cầu cho CA phát hành chứng thư đủ điều kiện.
- **EN 319 412-x** – Định dạng và cấu trúc chứng thư số X.509. Gồm 5 phần, quy định từ thông tin bắt buộc đến các extension cho chứng thư đủ điều kiện.
- **EN 319 421** – Yêu cầu cho dịch vụ đóng dấu thời gian.
- **EN 319 422** – Yêu cầu cho dịch vụ bảo quản lâu dài chữ ký điện tử và dữ liệu.

Nhóm tiêu chuẩn về hướng dẫn kỹ thuật và đánh giá sự phù hợp

- **TS 119 403** – Quy trình đánh giá sự phù hợp cho dịch vụ tin cậy.
- **TS 119 102-x** – Chuẩn giao diện và dịch vụ chữ ký điện tử (DSS – Digital Signature Services).
- **TS 119 432** & **TS 119 442** – Giao thức và định dạng dữ liệu cho dịch vụ gửi/nhận dữ liệu bảo đảm (ERDS).
- **TS 119 511** – Yêu cầu kỹ thuật cho dịch vụ bảo quản lâu dài (LTA – Long Term Preservation).
- **TS 119 172** – Yêu cầu kỹ thuật cho bằng chứng điện tử (Evidence Record Syntax – ERS).

Cấu trúc phân tầng tiêu chuẩn ETSI

Hệ thống tiêu chuẩn của ETSI có thể chia thành 3 tầng:

1. **Tầng yêu cầu chung**: EN 319 401.

2. **Tầng yêu cầu theo loại dịch vụ**: EN 319 411, 421, 422.

3. **Tầng kỹ thuật & định dạng dữ liệu**: EN 319 412, TS 119 102, TS 119 432, TS 119 511.

Hệ thống tiêu chuẩn của ETSI đối với dịch vụ tin cậy là nền tảng kỹ thuật vững chắc giúp triển khai thành công khung pháp lý eIDAS. Bộ tiêu chuẩn này không chỉ đảm bảo an toàn, bảo mật và giá trị pháp lý của các giao dịch điện tử mà còn tạo điều kiện thuận lợi cho thương mại và dịch vụ công xuyên biên giới.

Đối với Việt Nam, việc nghiên cứu và áp dụng các tiêu chuẩn ETSI – đặc biệt là EN 319 401, EN 319 411-1, EN 319 421, EN 319 422 - có thể giúp nâng cao chất lượng và uy tín của dịch vụ tin cậy, đồng thời tạo tiền đề hội nhập với thị trường quốc tế.

4.1.2. Viện tiêu chuẩn quốc gia Hoa kỳ (NIST)

Trong bối cảnh số hóa mạnh mẽ, các giao dịch điện tử ngày càng đòi hỏi mức độ bảo mật và tin cậy cao. **NIST** (Viện Tiêu chuẩn và Công nghệ Hoa Kỳ) đóng vai trò trung tâm trong việc phát triển các tiêu chuẩn, hướng dẫn kỹ thuật và quy trình nhằm đảm bảo an toàn thông tin, nhận dạng số và dịch vụ tin cậy tại Hoa Kỳ.

Hệ thống tiêu chuẩn của NIST không mang tính ràng buộc pháp lý như luật, nhưng thường được các cơ quan chính phủ Hoa Kỳ bắt buộc áp dụng và được khu vực tư nhân sử dụng rộng rãi như một chuẩn mực kỹ thuật. Các tiêu chuẩn này hỗ trợ các tổ chức triển khai:

- Nhận dạng số (Digital Identity)
- Xác thực điện tử (Authentication)
- Quản lý khóa và chứng thư số
- Chữ ký điện tử và xác minh
- Bảo vệ tính toàn vẹn và bí mật dữ liệu
- Quản lý vòng đời thông tin nhạy cảm

Tại Hoa Kỳ, việc sử dụng các tiêu chuẩn NIST cho dịch vụ tin cậy gắn với một số đạo luật và chính sách:

- **E-Government Act 2002**: Yêu cầu các cơ quan liên bang triển khai xác thực điện tử an toàn.
- **Federal Information Security Modernization Act (FISMA)**: Bắt buộc áp dụng tiêu chuẩn bảo mật thông tin do NIST ban hành.
- **OMB Circular A-130**: Quy định quản lý thông tin liên bang, yêu cầu tuân thủ tiêu chuẩn NIST.

- **Electronic Signatures in Global and National Commerce Act (ESIGN Act)**: Công nhận giá trị pháp lý của chữ ký điện tử, kết hợp tiêu chuẩn kỹ thuật từ NIST.

Hệ thống tiêu chuẩn của NIST có thể chia thành 5 nhóm chính:

Nhóm tiêu chuẩn về nhận dạng và xác thực số

NIST SP 800-63 – Digital Identity Guidelines: Là bộ tiêu chuẩn nền tảng cho các hệ thống nhận dạng điện tử.

- Gồm 4 phần: **SP 800-63-3**: Tổng quan, khung đánh giá mức độ tin cậy định danh (Identity Assurance Level – IAL), xác thực (Authenticator Assurance Level – AAL) và ràng buộc thông tin (Federation Assurance Level – FAL); **SP 800-63A**: Yêu cầu kỹ thuật và quy trình định danh (Identity Proofing); **SP 800-63B**: Yêu cầu kỹ thuật cho cơ chế xác thực (mật khẩu, OTP, MFA, chứng thư số); **SP 800-63C**: Yêu cầu kỹ thuật cho liên kết định danh (Federation) giữa các hệ thống.

Nhóm tiêu chuẩn về hạ tầng khóa công khai (PKI) và chứng thư số

FIPS 201 – Personal Identity Verification (PIV): Tiêu chuẩn bắt buộc cho thẻ định danh nhân viên liên bang. Quy định định dạng thẻ thông minh, cơ chế lưu trữ chứng thư số, khóa mật mã, và thông tin sinh trắc.

NIST SP 800-32 – Introduction to Public Key Technology and the Federal PKI Infrastructure: Hướng dẫn triển khai hạ tầng PKI cho cơ quan chính phủ.

NIST SP 800-57 (Parts 1–3) – Key Management Guidelines: Quy định vòng đời khóa, độ dài khóa, thuật toán được chấp thuận, chính sách hủy bỏ khóa.

NIST SP 800-73 & SP 800-78: Chuẩn kỹ thuật cho PIV Card và thuật toán mật mã áp dụng.

Nhóm tiêu chuẩn về chữ ký số và thuật toán mật mã

- **FIPS 186-5 – Digital Signature Standard (DSS):** Xác định các thuật toán chữ ký số được chấp thuận, Quy định kích thước khóa, tham số an toàn:
  - DSA (Digital Signature Algorithm)
  - RSA
  - ECDSA (Elliptic Curve DSA)

NIST SP 800-131A: Yêu cầu về chuyển đổi sang thuật toán mật mã an toàn (ví dụ: loại bỏ SHA-1).

NIST SP 800-106, SP 800-107: Yêu cầu cho hàm băm và ứng dụng trong chữ ký số.

Nhóm tiêu chuẩn về bảo quản lâu dài và bằng chứng dữ liệu

NIST SP 800-102 – Recommendation for Digital Signature Timeliness: Hướng dẫn lưu giữ dấu thời gian kèm chữ ký số để bảo đảm giá trị chứng cứ lâu dài.

NIST SP 800-207 – Zero Trust Architecture: Mô hình bảo mật không tin cậy mặc định, hỗ trợ bảo vệ dữ liệu trong suốt vòng đời.

NIST SP 800-88 – Guidelines for Media Sanitization: Yêu cầu xóa, tiêu hủy dữ liệu an toàn khi kết thúc vòng đời.

Nhóm tiêu chuẩn về kiểm toán và đánh giá sự phù hợp

NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems: Bộ kiểm soát an toàn thông tin áp dụng cho hệ thống xử lý dữ liệu nhạy cảm; Tiêu chuẩn này liên quan trực tiếp đến yêu cầu bảo mật của dịch vụ tin cậy.

NIST SP 800-115 – Technical Guide to Information Security Testing and Assessment: Hướng dẫn kiểm tra bảo mật, đánh giá tính tuân thủ.

Tiêu chuẩn cho Modun mật mã

FIPS PUB 140-2 (Federal Information Processing Standard Publication 140-2) là tiêu chuẩn liên bang của Hoa Kỳ do NIST ban hành, quy định yêu cầu bảo mật cho mô-đun mật mã (cryptographic modules) được sử dụng để bảo vệ thông tin nhạy cảm nhưng không thuộc phân loại mật (Sensitive But Unclassified - SBU).

FIPS 140-2 áp dụng cho:

- **Phần mềm, phần cứng, firmware** có chức năng mật mã (encryption, decryption, key management, digital signature…).
- Các **mô-đun mật mã** trong: Hệ thống PKI, HSM (Hardware Security Module); VPN, firewall, thiết bị mạng; Ứng dụng chữ ký điện tử, xác thực mạnh; Dịch vụ tin cậy như Timestamping, e-Seal, Long-term Preservation

- **FIPS 140-3** được ban hành vào năm 2019 để thay thế FIPS 140-2, dựa trên chuẩn quốc tế **ISO/IEC 19790:2012**. Tuy nhiên, FIPS 140-2 vẫn đang được công nhận cho các mô-đun đã chứng nhận trước đó, trong giai đoạn chuyển tiếp.

Trong bối cảnh **dịch vụ tin cậy** như chữ ký điện tử, con dấu điện tử, timestamping, việc sử dụng mô-đun mật mã đạt chứng nhận FIPS 140-2 (thường ở Level 3 trở lên) mang lại:

- Đảm bảo an toàn khóa bí mật.
- Ngăn ngừa xâm nhập vật lý vào HSM.

- Tuân thủ yêu cầu bảo mật liên bang Hoa Kỳ và được quốc tế công nhận.
- Tăng uy tín khi cung cấp dịch vụ tin cậy xuyên biên giới.

FIPS PUB 140-2 là tiêu chuẩn cốt lõi cho bảo mật mô-đun mật mã tại Hoa Kỳ, được công nhận rộng rãi trên toàn cầu. Mặc dù đã có FIPS 140-3, nhưng 140-2 vẫn đóng vai trò quan trọng trong nhiều hệ thống bảo mật và dịch vụ tin cậy hiện hành. Việc áp dụng mô-đun đạt chuẩn này giúp tổ chức đáp ứng yêu cầu pháp lý, bảo mật và xây dựng niềm tin cho người dùng.

4.1.3. Các tổ chức tiêu chuẩn khác

Hệ thống tiêu chuẩn PKCS (Public-Key Cryptography Standards) là một tập hợp các đặc tả kỹ thuật do RSA Laboratories phát triển từ cuối những năm 1980 và đầu 1990, nhằm chuẩn hóa việc sử dụng mật mã khóa công khai trong phần mềm và phần cứng. Đây là một trong những nền tảng quan trọng cho nhiều giao thức bảo mật và tiêu chuẩn quốc tế hiện nay.

- PKCS được công bố lần đầu năm 1991 bởi RSA Laboratories.
- Mục tiêu: tạo ra các đặc tả kỹ thuật cho các hàm, cấu trúc dữ liệu, định dạng và giao thức liên quan đến mật mã khóa công khai.
- Ứng dụng: được dùng rộng rãi trong các giải pháp chữ ký số, chứng thư số, xác thực, bảo mật dữ liệu, và các giao thức như TLS/SSL, S/MIME, IPsec.
- Nhiều tiêu chuẩn PKCS đã được IETF, ISO/IEC và OASIS tiếp nhận hoặc kế thừa.

Trong dịch vụ tin cậy (theo định nghĩa của eIDAS hoặc các hệ thống tương tự), PKCS đóng vai trò:

- PKCS #1, #7, #10, #12: Là nền tảng cho chữ ký số, chứng thư số, mã hóa dữ liệu.
- PKCS #11: Kết nối an toàn với thiết bị phần cứng như HSM (Hardware Security Module), smartcard, token.
- PKCS #12: Quản lý và phân phối chứng thư số bảo mật.
- PKCS #5: Bảo vệ dữ liệu bằng mật khẩu khi lưu trữ hoặc truyền tải.
- PKCS #15: Quản lý thông tin chứng thực trên thẻ công dân điện tử, thẻ nhân viên, thiết bị OTP.
- Nhiều PKCS ban đầu chỉ là đặc tả riêng của RSA, nhưng sau đó đã được:
  - IETF chuẩn hóa (ví dụ PKCS #7 → RFC 5652).
  - ISO/IEC tích hợp (PKCS #1 vào ISO/IEC 9796, 14888…).

- OASIS tiếp nhận (PKCS #11 hiện do OASIS duy trì).

• Điều này giúp PKCS trở thành bộ tiêu chuẩn nền tảng, đảm bảo khả năng tương thích giữa các hệ thống.

Hệ thống tiêu chuẩn PKCS là một tập hợp các quy tắc kỹ thuật then chốt trong mật mã khóa công khai, đặt nền móng cho các giao thức bảo mật hiện đại. Trong lĩnh vực dịch vụ tin cậy, PKCS không chỉ đảm bảo an toàn cho khóa và chứng thư số, mà còn giúp chuẩn hóa quy trình giao tiếp giữa các hệ thống và thiết bị bảo mật, tạo ra môi trường tin cậy xuyên suốt từ người dùng đến nhà cung cấp dịch vụ.

4.2. Tình hình áp dụng tiêu chuẩn một số nước trên thế giới

4.2.1. Liên minh Châu Âu

• **ETSI** không ban hành luật, mà xây dựng tiêu chuẩn kỹ thuật để các QTSP và cơ quan đánh giá sự phù hợp áp dụng khi triển khai eIDAS.

• Khi một nhà cung cấp dịch vụ đáp ứng tiêu chuẩn ETSI và được tổ chức đánh giá chứng nhận, dịch vụ sẽ được công nhận đủ điều kiện trong toàn EU.

• Các tiêu chuẩn ETSI được thiết kế để hỗ trợ trực tiếp các điều khoản trong eIDAS, ví dụ:

- Điều 24 eIDAS → EN 319 411-2 (yêu cầu cho CA đủ điều kiện)
- Điều 34 eIDAS → EN 319 421 (yêu cầu cho dịch vụ đóng dấu thời gian đủ điều kiện)
- Điều 34(1) và 40 → EN 319 422 (bảo quản lâu dài)

Việc áp dụng hệ thống tiêu chuẩn giúp tăng cường

1. Đồng bộ và liên thông giữa các quốc gia EU.
2. Giảm rủi ro pháp lý nhờ tuân thủ khung tiêu chuẩn đã được chấp nhận.
3. Tăng tính minh bạch và tin cậy đối với người dùng cuối.
4. Hỗ trợ chứng nhận và giám sát cho cơ quan quản lý.
5. Thúc đẩy giao dịch điện tử xuyên biên giới.

4.2.2. Các tiểu Vương quốc Ả rập Thống nhất - UAE

UAE vận hành khung pháp lý của riêng mình về **dịch vụ tin cậy**

• **Federal Decree-Law No. 46 of 2021** – khung pháp luật chính của UAE về giao dịch điện tử và dịch vụ tin cậy.

• **Cabinet Decision No. 28 of 2023** – triển khai chi tiết yêu cầu cấp giấy phép, phân loại "qualified" và "approved" trust services, và thiết lập **UAE Trust List**.

Có thể thấy UAE mô phỏng một số nguyên tắc thiết kế tương đồng với eIDAS.

- UAE đã thiết kế một số thành phần rất giống EU - phân loại chữ ký theo mức độ, danh sách nhà cung cấp đáng tin, và yêu cầu bảo mật kỹ thuật; viện dẫn áp dụng một số tiêu chuẩn của ETSI.

- Mối tương đồng này cho thấy một xu hướng quốc tế hóa quan điểm về an toàn kỹ thuật, độ tin cậy và giá trị pháp lý của dịch vụ tin cậy.

4.2.3. Hàn Quốc

Hàn Quốc đã xây dựng một hệ thống pháp lý và kỹ thuật chặt chẽ cho dịch vụ tin cậy - kết hợp hạ tầng PKI quốc gia (GPKI/NPKI), CPS chi tiết, danh sách tin cậy và chính sách mở cửa cạnh tranh cho nhà cung cấp tư nhân.

Hàn Quốc không xây dựng tiêu chuẩn kỹ thuật mà ban hành dưới hình thức Yêu cầu kỹ thuật cho dịch vụ tin cậy, chính là các tiêu chí đảm bảo tính bảo mật**,** tính toàn vẹn**,** tính xác thực**,** khả năng kiểm toán **và** tính sẵn sàng của dịch vụ (PKI, CA, TSA, ERDS, timestamping, long-term preservation…). Ở Hàn Quốc, hạ tầng GPKI/NPKI + các CA thương mại áp dụng bộ yêu cầu tương tự: CPS/CP đầy đủ, bảo quản khóa an toàn, xác minh định danh chặt chẽ, hỗ trợ cơ chế xác thực và xác minh trạng thái chứng thư. Cụ thể

Xác minh định danh (Identity Proofing)

• **Mức độ xác minh theo rủi ro**: phân tầng IAL/AAL (tương tự NIST SP 800-63).

• **Yêu cầu bằng chứng định danh**: giấy tờ chính thức (thẻ căn cước, hộ chiếu), xác minh trực tiếp qua hệ thống chính phủ (DB matching), video/KYC khi remote.

• **Ghi nhận hồ sơ**: lưu trữ bản sao/ghi chép quy trình xác minh, dấu thời gian, nhân viên thực hiện - để phục vụ kiểm toán.

Vòng đời chứng thư (Certificate Lifecycle)

• **Chuẩn định dạng**: X.509 v3 cho chứng thư; CSR theo PKCS#10; đóng gói ký theo CMS/PKCS#7 (hoặc RFC tương đương).

• **Policy & CPS**: mọi CA/TSP phải có CP/CPS chi tiết (mô tả issuance, revoke, key management, audit).

- **Chu kỳ/tuổi thọ key**: RSA ≥ 2048-bit tối thiểu; khuyến nghị ≥ 3072 cho tương lai. ECC: P-256/P-384 (curve secp256r1/secp384r1). Hash: SHA-256 trở lên.

- **Key usage & extensions**: cấu hình keyUsage, extendedKeyUsage, basicConstraints, CRL/OCSP URLs, AuthorityInfoAccess, Certificate Policies.

- **Revocation**: hỗ trợ **OCSP** (real-time) và **CRL**; OCSP responder phải có SLA / khả năng chịu tải; OCSP stapling có thể được yêu cầu cho ứng dụng web.

Quản lý khóa (Key Management) & HSM

- **Tạo khoá**: key pair cho CA và key mật quan trọng phải được tạo trong HSM (không tạo bằng phần mềm trên máy chủ phổ thông).

- **HSM**: dùng HSM đạt chuẩn (FIPS 140-2/140-3 Level 2/3, ưu tiên Level 3 cho CA gốc và CA cấp cao).

- **Quy trình khóa (key ceremony)**: văn bản hóa, có nhiều người tham gia (multi-party), ghi nhật ký, ký biên bản.

- **Sao lưu khóa**: lưu trữ khóa bí mật dạng được mã hóa & phân mảnh (ví dụ Shamir secret sharing) trong môi trường an toàn; chính sách phục hồi thảm họa.

- **Chính sách escrow / backup**: nếu có escrow, phải ghi rõ điều kiện giải mã, kiểm soát truy cập.

Bảo mật vận hành (Operational Security)

- **Phân quyền & tách vai trò**: Separation of duties — quản trị HSM, quản trị CA, operator triển khai, auditor là các vai trò khác nhau.

- **Môi trường vận hành**: OS hardened, cập nhật patch, whitelist/disable unnecessary services.

- **Mã hóa kênh quản trị**: quản trị qua mạng phải sử dụng TLS 1.2+/mutual TLS.

- **Giám sát & logging**: ghi nhật ký chi tiết các hoạt động CA/HSM/OCSP/TSA (log tamper-evident), đồng bộ thời gian (NTP/PTP) với nguồn thời gian đáng tin cậy; giữ log đủ lâu (chính sách retention rõ ràng).

- **Kiểm thử an ninh**: pentest định kỳ, vulnerability scanning, code review cho phần mềm liên quan.

Bảo mật vật lý

- **Data center & phòng HSM**: kiên cố, kiểm soát truy cập sinh trắc, camera, báo động.

- **Niêm phong & phát hiện mở**: seals tamper-evident cho thiết bị vật lý.

• **Lưu trữ offline**: root CA offline, subordinate CA online/online-offline hybrid theo thiết kế.

4.3. Tình hình tiêu chuẩn hóa về dịch vụ tin cậy tại Việt Nam

4.3.1. Hiện trạng xây dựng và áp dụng quy chuẩn

Hiện nay đã có 28 Tiêu chuẩn quốc gia liên quan đến kỹ thuật mật mã, 11 TCVN liên quan đến chữ ký số.

Bộ Thông tin và Truyền thông (trước đây): Thực hiện nhiệm vụ được giao tại Luật Giao dịch điện tử 2005, Bộ Thông tin và Truyền thông đã ban hành Thông tư số 06/2015/TT-BTTTT và Thông tư số 16/2019/TT-BTTTT quy định tiêu chuẩn áp dụng cho chữ ký số và dịch vụ chứng thực chữ ký số. Đây là 2 thông tư quan trọng làm căn cứ để các Doanh nghiệp xây dựng đề án, thiết lập hệ thống và vận hành trong quá trình cung cấp dịch vụ của mình.

- Ban Cơ yếu CP: Ban cơ yếu Chính phủ chủ yếu tập trung vào xây dựng các tiêu chuẩn liên quan đến mật mã và thiết bị phần cứng sử dụng trong hoạt động mật mã dân sự. Ban cơ yếu cũng ban hành Thông tư quy định danh mục tiêu chuẩn áp dụng cho Modun mật mã trong định danh và xác thực điện tử.

4.4. Lựa chọn tài liệu tham chiếu

Căn cứ vào các nội dung nghiên cứu nêu trên, có thể rút ra các nhận xét như sau:

Các dịch vụ tin cậy đang được triển khai tại Việt Nam đã tuân thủ hệ thống các tiêu chuẩn do Bộ Thông tin và Truyền thông quy định. Hệ thống tiêu chuẩn này chủ yếu dựa trên các tiêu chuẩn quốc tế phổ biến của EU, Hoa kỳ.

Cách thức rà soát, đề xuất tiêu chuẩn:

- Xác định mô hình dịch vụ và các yêu cầu đối với dịch vụ tin cậy;

- Rà soát các quy định của Thông tư 06/2015/TT-BTTTT và 16/2019/TT-BTTTT;

- Nghiên cứu hệ thống tiêu chuẩn đối với dịch vụ tin cậy của các tổ chức tiêu chuẩn hóa (ISO, ETSI, …);

- Đề xuất tiêu chuẩn tham chiếu áp dụng cho dịch vụ tin cậy trên cơ sở mục tiêu quản lý, các yêu cầu của dịch vụ tin cậy tại Việt Nam;

Nguyên tắc lựa chọn tài liệu tham chiếu

Nguyên tắc 1: Phù hợp với quy định của Luật Giao dịch điện tử 2023, Luật tiêu chuẩn và quy chuẩn kỹ thuật;

Nguyên tắc 2: Lựa chọn các tiêu chuẩn quốc tế được sử dụng phổ biến, được nhiều nước áp dụng; ưu tiên sử dụng các tiêu chuẩn Việt Nam tương đương đã được công bố;

Nguyên tắc 3: Phù hợp với điều kiện thực tế triển khai dịch vụ tin cậy tại Việt Nam; rà soát kế thừa các quy định tại Thông tư số 06/2015/TT-BTTTT và Thông tư 16/2019/TT-BTTTT.

Các tiêu chuẩn của ETSI quy định chi tiết về các yêu cầu kỹ thuật, yêu cầu kiểm soát và vận hành trong quá trình cung cấp dịch vụ.

Do vậy nhóm biên soạn đề xuất rà soát xây dựng Quy chuẩn kỹ thuật quốc gia về yêu cầu đối với dịch vụ chứng thực chữ ký số công cộng trên cơ sở tham chiếu các tiêu chuẩn của RSA, NIST, ETSI bao gồm:

- Tiêu chuẩn #PKCS (RSA Cryptography Standard), IETF

- Tiêu chuẩn FIPS PUB 140-2, 140-3 (Security Requirements for Cryptographic Modules)

Tiêu chuẩn 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)

5. Giải thích nội dung QCVN

5.1. Cách thức xây dựng

Cách thức xây dựng dự thảo quy chuẩn tuân thủ các bước theo quy định, bao gồm các nội dung:

- Tổ chức nghiên cứu, xây dựng dự thảo quy chuẩn;

- Lấy ý kiến góp ý của các cơ quan, tổ chức, cá nhân có liên quan và lấy ý kiến trên cổng thông tin điện tử của Chính phủ, của Bộ Khoa học và Công nghệ;

- Tổ chức các hội nghị, hội thảo, lấy ý kiến của chuyên gia và các tổ chức, cá nhân có liên quan;

- Gửi thông báo cho Văn phòng TBT

- Tổ chức thẩm tra và thực hiện các thủ tục ban hành quy chuẩn.

5.2. Về hình thức trình bày

Dự thảo quy chuẩn được trình bày theo đúng hướng dẫn về việc trình bày và thể hiện nội dung quy chuẩn quy định tại Phụ lục V của Thông tư số 26/2019/TT-BKHCN ngày 25 tháng 12 năm 2019 của Bộ trưởng Bộ Khoa học và Công nghệ.

5.3. Tên Dự thảo Quy chuẩn

Để đảm bảo sự rõ ràng trong quá trình áp dụng quy chuẩn, nhóm chủ trì biên soạn đề xuất tên Quy chuẩn là: **QCVN xxx:2025/BTTTT - Quy chuẩn kỹ thuật quốc gia về yêu cầu đối với dịch vụ chứng thực chữ ký số công cộng.**

5.4. Nội dung dự thảo quy chuẩn

Quy chuẩn này quy định các yêu cầu đối với dịch vụ chứng thực chữ ký số công cộng, bao gồm:

- Yêu cầu kỹ thuật đối với mật mã và chữ ký số;
- Yêu cầu kỹ thuật đối với thông tin, dữ liệu;
- Yêu cầu kỹ thuật đối với chứng thư chữ ký số;
- Yêu cầu kỹ thuật đối với HSM và thiết bị mật mã, lưu khóa;
- Yêu cầu đối với mô hình ký số từ xa;
- Yêu cầu đối với mô hình ký số trên thiết bị di động;
- Yêu cầu về quy trình kiểm soát và vận hành đối với tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.

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 tại Việt Nam.

Bố cục quy chuẩn gồm các phần như sau:

QUY ĐỊNH CHUNG

- Phạm vi điều chỉnh
- Đối tượng áp dụng
- Tài liệu viện dẫn
- Giải thích từ ngữ
- Ký hiệu
- Chữ viết tắt

QUY ĐỊNH KỸ THUẬT

QUY ĐỊNH VỀ QUẢN LÝ

TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

TỔ CHỨC THỰC HIỆN

CÁC PHỤ LỤC

6. Bảng tham chiếu nội dung QCVN với các tài liệu tham chiếu

Bảng 1. Bảng tham chiếu tài liệu tham khảo

QCVN xxx:2025/BKHCN	Tài liệu tham khảo	Sửa đổi, bổ sung
1. Quy định chung		
1.1. Phạm vi điều chỉnh		Tự xây dựng
1.2. Đối tượng áp dụng		Tự xây dựng
1.3. Tài liệu viện dẫn		Tự xây dựng
1.4. Giải thích từ ngữ		Tự xây dựng
1.5. Ký hiệu		Tự xây dựng
1.6. Chữ viết tắt		Tự xây dựng
2. Quy định kỹ thuật		
2.1. Yêu cầu về kỹ thuật		
2.1.1. Yêu cầu về kỹ thuật mật mã	#PKCS1; ANSI X9.62-2005; TCVN 7816:2007; FIPS PUB 197; FIPS PUB 180-4; FIPS PUB 202;	Chấp thuận nguyên vẹn
2.1.2. Yêu cầu về thông tin, dữ liệu	RFC 5280; PKCS #7 (RFC 2630); PKCS #8 (RFC 5208); PKCS #10 (RFC 2986); PKCS #11; PKCS #12	Chấp thuận nguyên vẹn
2.1.3. Yêu cầu đối với chứng thư chữ ký số	RFC 3647; RFC 4523; RFC 4510; RFC 4511; RFC 4512; RFC 4513; RFC 2585; RFC 6960	Chấp thuận nguyên vẹn
2.1.4. Yêu cầu bảo mật cho HSM và thẻ mật mã	FIPS PUB 140-2; FIPS PUB 140-3; EN 419 221-5:2018	Chấp thuận nguyên vẹn
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	ETSI EN 319 411-1	Chấp thuận nguyên vẹn
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	ETSI TS 119 432; EN 419241-1:2018; EN 419241-2:2019	Chấp nhận nguyên vẹn

QCVN xxx:2025/BKHCN	Tài liệu tham khảo	Sửa đổi, bổ sung
2.3.2. Yêu cầu về quy trình kiểm soát và vận hành	ETSI EN 319 411-1	Chấp thuận nguyên vẹn
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	ETSI TR 102 203; ETSI TS 102 204; ETSI TR 102 206; ETSI TS 102 207	Chấp nhận nguyên vẹn
2.4.2. Yêu cầu đối với thẻ SIM	FIPS PUB 140-2; FIPS PUB 140-3; TCVN 8709 (ISO/IEC 15408)	Chấp nhận nguyên vẹn
2.4.3. Yêu cầu về quy trình kiểm soát và vận hành	ETSI EN 319 411-1	Chấp thuận nguyên vẹn
4. Quy định quản lý		Tự xây dựng
5. Trách nhiệm của tổ chức, cá nhân		Tự xây dựng
6. Tổ chức thực hiện		Tự xây dựng

7. Khuyến nghị áp dụng QCVN

Luật Giao dịch điện tử năm 2023 (Luật số 20/2023/QH15) đã được ban hành, tạo ra hành lang pháp lý quan trọng, công nhận giá trị pháp lý và quy định các yêu cầu đối với các dịch vụ này. Để hiện thực hóa các mục tiêu của Luật, việc đảm bảo các Nhà cung cấp dịch vụ tin cậy (Trust Service Providers - TSP) hoạt động một cách tin cậy, an toàn và tuân thủ pháp luật là yêu cầu tiên quyết. Điều này không chỉ củng cố niềm tin của người dùng mà còn là yếu tố then chốt để các giao dịch điện tử được công nhận và phát huy hiệu quả.

Quy chuẩn kỹ thuật quốc gia về yêu cầu đối với dịch vụ chứng thực chữ ký số công cộng sẽ được áp dụng trong việc xây dựng đề án và triển khai hệ thống cung cấp dịch vụ; làm căn cứ thực hiện kiểm toán kỹ thuật trong quá trình hoạt động cung cấp dịch vụ của các tổ chức cung cấp dịch vụ.

Việc xây dựng dự thảo quy chuẩn đã thực hiện đầy đủ các bước theo quy định bao gồm: xây dựng dự thảo quy chuẩn, tổ chức hội thảo với các đơn vị trong Bộ, các doanh nghiệp, đăng tải xin ý kiến rộng rãi trên cổng thông tin điện tử của Bộ và của Chính phủ.

Kiến nghị Bộ Khoa học và Công nghệ sớm ban hành quy chuẩn để phục vụ công tác quản lý, làm cơ sở để các Doanh nghiệp triển khai cung cấp dịch vụ tin cậy, thúc đẩy quá trình chuyển đổi số ở nước ta.