TCVN

TIÊU CHUẨN QUỐC GIA

TCVN XXX:2026

Xuất bản lần 1

GIAO DỊCH ĐIỆN TỬ - GIAO THỨC CẤP DẤU THỜI GIAN CHO DỊCH VỤ TIN CẬY

Electronic Transactions - Trust Services - Time-Stamping Protocol (TSP)

HÀ NỘI - 2026

Mục lục

Lời nói đầu

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

Lời giới thiệu

Xây dựng lòng tin trong môi trường giao dịch điện tử trực tuyến là yếu tố then chốt đối với sự phát triển bền vững của kinh tế số và xã hội số. Việc thiếu lòng tin, đặc biệt xuất phát từ những lo ngại về bảo mật thông tin, đây là một trong những rào cản lớn khiến cơ quan, tổ chức và người dân còn e dè khi thực hiện các giao dịch điện tử trên môi trường mạng.

Các tổ chức cung cấp dịch vụ tin cậy, đặc biệt là tổ chức cung cấp dịch vụ cấp dấu thời gian (Time-Stamping Authority - TSA), đóng vai trò bảo đảm độ tin cậy về thời gian trong giao dịch điện tử thông qua việc phát hành dấu thời gian điện tử, giúp chứng minh sự tồn tại của thông điệp dữ liệu tại một thời điểm xác định.

Tiêu chuẩn này quy định cấu hình cho giao thức cấp dấu thời gian (time-stamping protocol) và mã thông báo cấp dấu thời gian (time-stamp token), nhằm bảo đảm khả năng tương thích, tính thống nhất và độ tin cậy trong quá trình yêu cầu, phản hồi, xác minh, phát hành và truyền nhận dấu thời gian điện tử.

Tiêu chuẩn xác định các yêu cầu kỹ thuật tối thiểu mà máy khách cấp dấu thời gian và máy chủ cấp dấu thời gian phải tuân thủ, bao gồm định dạng bản tin yêu cầu, định dạng bản tin phản hồi, các trường dữ liệu bắt buộc hoặc khuyến nghị, thuật toán mật mã, chứng thư chữ ký số dấu thời gian và giao thức truyền tải được áp dụng.

Việc áp dụng tiêu chuẩn này góp phần hoàn thiện hệ thống tiêu chuẩn kỹ thuật áp dụng đối với lĩnh vực chữ ký số, dịch vụ tin cậy, phục vụ công tác quản lý nhà nước thống nhất, minh bạch, tiệm cận thông lệ quốc tế, đồng thời phù hợp với thực tế triển khai tại Việt Nam.

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

Giao dịch điện tử - Giao thức cấp dấu thời gian cho dịch vụ tin cậy

Electronic transactions - Trust Services - Time-Stamping Protocol (TSP)

1. Phạm vi áp dụng

Tiêu chuẩn này quy định cấu hình cho giao thức cấp dấu thời gian (time-stamping protocol) và mã thông báo cấp dấu thời gian (time-stamp token).

Tiêu chuẩn này quy định những gì mà một máy khách cấp dấu thời gian (time-stamping client) cần hỗ trợ và những gì mà một máy chủ cấp dấu thời gian (time-stamping server) cần hỗ trợ.

Các yêu cầu trong tiêu chuẩn này tập trung vào các yêu cầu kỹ thuật đối với máy khách và máy chủ cấp dấu thời gian, hồ sơ chứng thư chữ ký số của TSA, giao thức truyền tải, mã định danh đối tượng, các thuật toán mật mã và các yêu cầu bổ sung đối với dấu thời gian điện tử, nhằm bảo đảm dịch vụ cấp dấu thời gian được cung cấp một cách bảo mật, tin cậy, ổn định và phù hợp với các quy định hiện hành.

Tiêu chuẩn áp dụng đối với:

- Tổ chức cung cấp dịch vụ cấp dấu thời gian.

- Cơ quan, tổ chức, cá nhân lựa chọn sử dụng thuật toán khóa không đối xứng để thiết lập hệ thống cấp dấu thời gian.

Tiêu chuẩn này không quy định phương pháp đánh giá sự phù hợp, không quy định yêu cầu đối với tổ chức đánh giá sự phù hợp hoặc tổ chức đánh giá độc lập, cũng như không quy định chi tiết về hồ sơ, bằng chứng hoặc thông tin cần cung cấp phục vụ hoạt động đánh giá. Các nội dung này được quy định trong các tiêu chuẩn, quy chuẩn hoặc văn bản pháp luật có liên quan.

2. Tài liệu viện dẫn

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

TCVN 14617:2026, *Công nghệ thông tin - Dịch vụ tin cậy - Yêu cầu đối với chữ ký số và chứng thư chữ ký số;*

TCVN XXX:2026, *Giao dịch điện tử - Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp 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 *(Chữ ký điện tử và cơ sở hạ tầng (ESI); Yêu cầu về chính sách và bảo mật đối với các Tổ chức cung cấp dịch vụ tin cậy (TSP) cấp dấu thời gian);*

ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons *(Chữ ký điện tử và cơ sở hạ tầng (ESI); Hồ sơ chứng thư; Phần 3: Hồ sơ chứng thư cấp cho pháp nhân);*

ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites *(Chữ ký điện tử và Hạ tầng: Các bộ thuật toán mật mã);*

IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) *(Giao thức dấu thời gian (TSP) của cơ sở hạ tầng khóa công khai Internet X.509);*

IETF RFC 5816 ESSCertIDv2 Update for RFC 3161 *(Bản cập nhật ESSCertIDv2 cho RFC 3161);*

IETF RFC 7230 Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing *(Giao thức truyền tải siêu văn bản (HTTP/1.1): Cú pháp Thông điệp và Định tuyến)*;

IETF RFC 7235 Hypertext Transfer Protocol (HTTP/1.1): Authentication *(Giao thức Truyền tải Siêu văn bản (HTTP/1.1): Xác thực (tạm dịch)*;

IETF RFC 2818 HTTP Over TLS *(HTTP trên TLS);*

IETF RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile *(Hạ tầng khóa công khai Internet X.509: Hồ sơ chứng thư đủ điều kiện);*

IETF RFC 6838 Media Type Specifications and Registration Procedures *(Đặc tả loại phương tiện và thủ tục đăng ký)*.

3. Thuật ngữ và chữ viết tắt

3.1. Thuật ngữ và định nghĩa

3.1.1

Dấu thời gian (time-stamp)

Dấu thời gian là dữ liệu điện tử gắn với thông điệp dữ liệu cho phép xác định thời gian của thông điệp dữ liệu đó tồn tại ở một thời điểm cụ thể.

3.1.2

Dịch vụ cấp dấu thời gian (TimeStamping service)

Do tổ chức cung cấp dịch vụ tin cậy cung cấp, gắn thông tin về thời gian vào thông điệp dữ liệu.

3.1.3

Mã thông báo cấp dấu thời gian (time-stamp token)

Đối tượng dữ liệu được quy định trong IETF RFC 3161, đại diện cho một dấu thời gian.

3.1.4

Tổ chức cung cấp dịch vụ tin cậy (Trust Service Provider)

TSP

Tổ chức cung cấp một hoặc nhiều dịch vụ tin cậy.

3.1.5

Tổ chức cung cấp dịch vụ cấp dấu thời gian (Time-Stamping Authority)

TSA

Tổ chức cung cấp dịch vụ tin cậy cung cấp dịch vụ cấp dấu thời gian.

3.1.6

Chữ ký số (Digital signature)

Chữ ký điện tử sử dụng thuật toán khóa không đối xứng, gồm khóa bí mật và khóa công khai, trong đó khóa bí mật được dùng để ký số và khóa công khai được dùng để kiểm tra chữ ký số. Chữ ký số bảo đảm tính xác thực, tính toàn vẹn và tính chống chối bỏ nhưng không bảo đảm tính bí mật của thông điệp dữ liệu.

CHÚ THÍCH: Chữ ký số có giá trị pháp lý tương đương với chữ ký của cá nhân đó trên văn bản giấy.

[NGUỒN: Điều 3, Luật số 20/2023/QH15]

3.1.7

Chứng thư chữ ký số (Digital signature certificate)

Chứng thư chữ ký số là một dạng chứng thư chữ ký điện tử do Tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp nhằm cung cấp thông tin về khóa công khai của một cá nhân, tổ chức từ đó xác nhận cá nhân, tổ chức là chủ thể ký thông qua việc sử dụng khóa bí mật tương ứng.

CHÚ THÍCH: "Chủ thể ký" là 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.

[NGUỒN: Điều 3, Thông tư số 15/2025/BKHCN]

3.2. Chữ viết tắt

ASN	Abstract Syntax Notation	Ký hiệu cú pháp trừu tượng
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số dựa trên đường cong elliptic
EU	Europe	Châu Âu
ETSI	European Telecommunications Standards Institute	Viện Tiêu chuẩn Viễn thông Châu Âu
HTTP	HyperText Transfer Protocol	Giao thức Truyền tải siêu văn bản
HTTPS	Hypertext Transfer Protocol over TLS	Giao thức truyền tải siêu văn bản qua TLS

TSA	Time-Stamping Authority	Tổ chức cung cấp dịch vụ cấp dấu thời gian
TST	Time-Stamp Token	Mã thông báo dấu thời gian
TS	Technical Specification	Đặc tả kỹ thuật (ký hiệu tài liệu ETSI TS)
SHA	Secure Hash Algorithm	Thuật toán băm an toàn
RSA	Rivest–Shamir–Adleman	Thuật toán mã hóa khóa công khai
EdDSA	Edwards-Curve Digital Signature Algorithm	Thuật toán chữ ký số trên đường cong Edwards
XMSS	eXtended Merkle Signature Scheme	Lược đồ chữ ký Merkle mở rộng
LMS	Leighton-Micali Signature	Lược đồ chữ ký Leighton-Micali
PQC	Post-Quantum Cryptography	Mật mã hậu lượng tử
DSA	Digital Signature Algorithm	Thuật toán chữ ký số
SLH	Stateless Hash-based (as in SLH-DSA, FIPS 205)	Thuật toán chữ ký số dựa trên hàm băm không trạng thái
IETF	Internet Engineering Task Force	Lực lượng chuyên trách về kỹ thuật internet
RFC	Request for Comments	Chuỗi tài liệu tiêu chuẩn của IETF
OID	Object Identifier	Định danh đối tượng
PKI	Public Key Infrastructure	Hạ tầng khóa công khai
CMS	Cryptographic Message Syntax	Cú pháp thông điệp mật mã
NTP	Network Time Protocol	Giao thức đồng bộ thời gian mạng

4. Yêu cầu đối với máy khách cấp dấu thời gian

4.1. Yêu cầu kỹ thuật đối với định dạng bản tin yêu cầu

4.1.1. Định dạng bản tin yêu cầu

Máy khách cấp dấu thời gian phải hỗ trợ bản tin yêu cầu cấp dấu thời gian theo quy định tại mục 2.4.1 của IETF RFC 3161, với các sửa đổi được quy định trong các yêu cầu dưới đây:

4.1.2. Các trường dữ liệu cần được hỗ trợ

Các trường sau trong yêu cầu cấp dấu thời gian nên được hỗ trợ:

+ reqPolicy: trường tùy chọn chỉ ra chính sách của TSA được áp dụng khi cấp mã thông báo dấu thời gian, nếu trường reqPolicy chứa mã định danh chính sách (OID) mà TSA không hỗ trợ, TSA phải trả về bản tin phản hồi với trạng thái lỗi (PKIFailureInfo) có giá trị unacceptedPolicy;

+ nonce: số ngẫu nhiên mà máy khách chỉ tạo ra một lần duy nhất, nó cho phép máy khách xác minh tính kịp thời của bản tin phản hồi, bản tin phản hồi phải bao gồm cùng giá trị nonce; nếu không, bản tin phản hồi phải bị từ chối;

+ certReq: nếu trường certReq được đặt giá trị true, TSA phải đính kèm chứng thư chữ ký số tương ứng với mã định danh ESSCertID trong thuộc tính SigningCertificate của bản tin phản hồi, tại trường certificates của cấu trúc SignedData trong bản tin phản hồi đó. Trường certificates cũng có thể chứa nội dung các chứng thư chữ ký số khác.

CHÚ THÍCH 1: Mô tả trên làm rõ các trường mà máy chủ cấp dấu thời gian cần hỗ trợ để tiếp nhận và xử lý bản tin yêu cầu cấp dấu thời gian.

CHÚ THÍCH 2: Quy định chi tiết về sử dụng ESSCertIDv2 (theo IETF RFC 5816) trong bản tin phản hồi được nêu tại mục 5.2.2.

4.1.3. Các thuật toán hàm băm sử dụng

Các thuật toán hàm băm được sử dụng để băm mã thông báo dấu thời gian được quy định tại mục 5.1.3 của TCVN 14617:2026.

Bảng 1 - Các thuật toán hàm băm được sử dụng để băm mã thông báo dấu thời gian

Mã thông báo dấu thời gian	Mã thông báo dấu thời gian yêu cầu
Hàm băm	phải hỗ trợ SHA-256; nên hỗ trợ SHA-384, SHA-512 hoặc SHA3-256, SHA3-512.

4.2 Yêu cầu kỹ thuật đối với định dạng bản tin trả lời

4.2.1 Yêu cầu cốt lõi

Máy khách yêu cầu cấp dấu thời gian phải hỗ trợ định dạng bản tin phản hồi cấp dấu thời gian (Time-Stamp Response) được quy định tại mục 2.4.2 của IETF RFC 3161, cùng với các sửa đổi, bổ sung được quy định tại các yêu cầu dưới đây:

4.2.2. Các trường cần được hỗ trợ

Các yêu cầu sau được áp dụng đối với bản tin phản hồi:

+ trường accuracy (độ chính xác về thời gian) phải được hỗ trợ; và

+ trường nonce (số ngẫu nhiên) nên được hỗ trợ.

Tổ chức cung cấp dịch vụ cấp dấu thời gian (TSA) không cần hỗ trợ việc sắp xếp thứ tự, do đó các máy khách không nên phụ thuộc vào việc sắp xếp thứ tự của các dấu thời gian.

Nếu trường nonce có mặt trong yêu cầu, trường nonce phải có mặt trong phản hồi với cùng giá trị.

4.2.3. Các thuật toán cần hỗ trợ

Các thuật toán ký của mã thông báo dấu thời gian được quy định tại mục 5.1.1 của TCVN 14617:2026 cùng với các thuật toán tại bảng 2 của tiêu chuẩn này.

Bảng 2 – Các thuật toán ký của mã thông báo dấu thời gian

Mã thông báo dấu thời gian	Mã thông báo dấu thời gian yêu cầu
Thuật toán ký	phải hỗ trợ RSA, ECDSA; nên hỗ trợ DSA, EdDSA.

4.2.4. Độ dài khóa cần được hỗ trợ

Độ dài khóa ký cho thuật toán nên được lựa chọn hỗ trợ theo khuyến nghị tại mục 8.4 của ETSI TS 119 312.

Bảng 3 - Độ dài khoá của các thuật toán theo thời gian

Thuật toán	Tham số	1 năm	3 năm	5 năm
RSA	Độ dài khóa	≥ 2 048	≥ 2 048	≥ 4 096
DSA	pLen	2048	2048	4096
EC-DSA/ EC-SDSA-opt	pLen=qLen	256, 384 hoặc 512	256, 384 hoặc 512	256, 384 hoặc 512

Bảng 4 - Bộ thuật toán cho khả năng chống chịu của thuật toán theo thời gian

Tên bộ thuật toán	1 năm	3 năm	5 năm
sha256-with-rsa	≥ 2 048	≥ 2 048	không khuyến nghị cho hệ thống mới
sha384-with-rsa	≥ 2 048	≥ 2 048	không khuyến nghị cho hệ thống mới
sha512-with-rsa	≥ 2 048	≥ 2 048	không khuyến nghị cho hệ thống mới
rsa-pss with mgf1SHA-256Identifier	≥ 2 048	≥ 2 048	≥ 4 096
rsa-pss with mgf1SHA-384Identifier	≥ 2 048	≥ 2 048	≥ 4 096
rsa-pss with mgf1SHA-512Identifier	≥ 2 048	≥ 2 048	≥ 4 096
rsa-pss with mgf1SHA3-	≥ 2 048	≥ 2 048	≥ 4 096

Identifier			
sha256-with-dsa	2 048	2 048	3 072
sha512-with-dsa	2 048	2 048	3 072
sha224-with-ecdsa	không khuyến nghị cho hệ thống mới	không khuyến nghị cho hệ thống mới	không khuyến nghị cho hệ thống mới
sha2-with-ecsdsa	khuyến nghị	khuyến nghị	khuyến nghị
sha2-with-ecdsa	khuyến nghị	khuyến nghị	khuyến nghị
sha3-with-ecdsa	khuyến nghị	khuyến nghị	khuyến nghị
sha3-with-ecsdsa	khuyến nghị	khuyến nghị	khuyến nghị

CHÚ THÍCH 1: Các khuyến nghị về bộ mật mã được quy định trong ETSI TS 119 312 có thể được thay thế bằng các khuyến nghị quốc gia.

5. Yêu cầu đối với một máy chủ cấp dấu thời gian

5.1. Yêu cầu kỹ thuật đối với định dạng bản tin yêu cầu

5.1.1. Yêu cầu cốt lõi

Máy chủ cấp dấu thời gian phải hỗ trợ tiếp nhận và xử lý định dạng bản tin yêu cầu cấp dấu thời gian được quy định tại mục 2.4.1 của RFC 3161, cùng với các sửa đổi, bổ sung được quy định tại các yêu cầu dưới đây:

5.1.2. Các trường cần được hỗ trợ

Máy chủ cấp dấu thời gian phải áp dụng các yêu cầu sau đối với bản tin yêu cầu:

+ trường reqPolicy phải được hỗ trợ;

+ trường nonce phải được hỗ trợ;

+ trường certReq phải được hỗ trợ.

CHÚ THÍCH 1: Mô tả chi tiết các trường được thể hiện tại mục 4.1.2 của tiêu chuẩn này.

5.1.3. Các thuật toán cần hỗ trợ

Các thuật toán hàm băm áp dụng cho dữ liệu cấp dấu thời gian cần tuân thủ các quy định tại mục 5.1.3 của TCVN 14617:2026.

Bảng 5 - Các thuật toán hàm băm áp dụng cho mã thông báo dấu thời gian

Mã thông báo dấu thời gian	Mã thông báo dấu thời gian phát hành	Mã thông báo dấu thời gian xác minh

Hàm băm	phải hỗ trợ SHA-256; nên hỗ trợ SHA-384, SHA-512 hoặc SHA3-256, SHA3-512.	phải hỗ trợ SHA-256; phải hỗ trợ SHA-384, SHA-512 hoặc SHA3-256, SHA3-512.

5.2. Yêu cầu kỹ thuật đối với định dạng bản tin phản hồi

5.2.1. Yêu cầu cốt lõi

Máy chủ cấp dấu thời gian phải hỗ trợ tạo lập định dạng bản tin phản hồi cấp dấu thời gian được quy định tại mục 2.4.2 của RFC 3161, cùng với các sửa đổi, bổ sung được quy định tại các yêu cầu dưới đây:

5.2.2. Các trường dữ liệu cần hỗ trợ

Các quy định tại mục 2.4.2 của RFC 3161, quá trình tạo bản tin phản hồi phải áp dụng các yêu cầu bổ sung sau:

+ Trường policy phải có mặt như một mã định danh cho chính sách dấu thời gian và phải chứa định danh đối tượng (OID) của chính sách áp dụng cho TSA quy định tại Điều 10 của tiêu chuẩn này;

+ Trường genTime phải có mặt và đại diện cho thời gian với độ chính xác cần thiết để hỗ trợ mức độ chính xác đã được khai báo;

+ Trường accuracy phải có mặt và bắt buộc hỗ trợ độ sai lệch thời gian tối đa là một (01) giây so với nguồn thời gian theo quy định của pháp luật về nguồn thời gian chuẩn quốc gia;

+ Trường ordering không được có mặt hoặc phải được đặt giá trị thành false;

+ Không có phần mở rộng (extension) nào được đánh dấu là quan trọng (critical).

Yêu cầu sau áp dụng cho nội dung của cấu trúc SignedData (dữ liệu đã ký) trong đó cấu trúc TSTInfo được đóng gói:

+ Mã định danh chứng thư chữ ký số của tổ chức cung cấp dịch vụ cấp dấu thời gian (sử dụng ESSCertID theo chuẩn RFC 3161 hoặc ESSCertIDv2 theo chuẩn RFC 5816) phải được bao gồm dưới dạng thuộc tính signerInfo bên trong thuộc tính SigningCertificate hoặc SigningCertificateV2.

5.2.3. Các thuật toán cần được sử dụng

Các thuật toán hàm băm được sử dụng để băm thông tin cần được cấp dấu thời gian và các thuật toán ký mã thông báo cấp dấu thời gian nên là các thuật toán được quy định tại mục 5.1.1 của TCVN 14617:2026 cùng với các thuật toán tại bảng 6 của tiêu chuẩn này.

Bảng 6 - Các thuật toán ký mã thông báo cấp dấu thời gian

Mã thông báo dấu thời gian	**Mã thông báo dấu thời gian phát hành**	**Mã thông báo dấu thời gian xác minh**

Thuật toán ký	phải hỗ trợ RSA, ECDSA; nên hỗ trợ EdDSA, SLH-DSA, XMSS hoặc LMS (PQC).	phải hỗ trợ RSA, ECDSA; nên hỗ trợ DSA, EdDSA, SLH-DSA, XMSS, LMS.

CHÚ THÍCH 1: Các quy định về thuật toán hàm băm áp dụng cho mã thông báo dấu thời gian được quy định tại mục 5.1.3 của tiêu chuẩn này.

CHÚ THÍCH 2: Việc bổ sung các thuật toán mật mã hậu lượng tử nhằm hỗ trợ khả năng chuyển đổi và tăng khả năng chống chịu của thuật toán theo thời gian, không thay thế ngay các thuật toán đang được khuyến nghị áp dụng tại tiêu chuẩn này.

6. Hồ sơ chứng thư chữ ký số của TSA

6.1. Yêu cầu chung

Chứng thư chữ ký số của tổ chức cung cấp dịch vụ cấp dấu thời gian; cơ quan, tổ chức, cá nhân lựa chọn sử dụng thuật toán khóa không đối xứng để thiết lập hệ thống cấp dấu thời gian phải đáp ứng các yêu cầu quy định tại TCVN 14617:2026, cùng với các sửa đổi, bổ sung được quy định tại các yêu cầu dưới đây:

6.2. Yêu cầu đối với tên chủ thể

Thuộc tính countryName phải xác định quốc gia nơi tổ chức cung cấp dịch vụ cấp dấu thời gian được thành lập.

Thuộc tính organizationName phải chứa tên đăng ký hoạt động hợp pháp và đầy đủ của tổ chức cung cấp dịch vụ cấp dấu thời gian. Tên này nên khớp với tên đăng ký kinh doanh chính thức của tổ chức cung cấp dịch vụ cấp dấu thời gian.

Thuộc tính commonName đóng vai trò là một mã định danh cho TSA. Trong phạm vi quản lý của tổ chức cung cấp dịch vụ cấp dấu thời gian, thuộc tính commonName phải được định danh duy nhất một TSA cụ thể được sử dụng.

6.3. Yêu cầu về độ dài khóa

Độ dài khóa cho thuật toán chữ ký được chọn của chứng thư chữ ký số của tổ chức cung cấp dịch vụ cấp dấu thời gian nên là độ dài được khuyến nghị trong Điều 8.4 của ETSI TS 119 312.

CHÚ THÍCH 1: Các khuyến nghị về độ dài khóa cho thuật toán chữ ký được nêu tại bảng 3 và bảng 4 của tiêu chuẩn này.

CHÚ THÍCH 2: Các khuyến nghị về bộ mật mã được quy định trong ETSI TS 119 312 có thể được thay thế bằng các khuyến nghị quốc gia.

6.4. Yêu cầu về mục đích sử dụng khóa

Phần mở rộng mục đích sử dụng khóa (Extended Key Usage) của chứng thư chữ ký số TSA bắt buộc phải được thiết lập theo đúng quy định tại IETF RFC 3161 Điều 2.3.

Phần mở rộng về thời hạn sử dụng khóa bí mật (Private Key Usage Period) của chứng thư chữ ký số TSA nên được sử dụng nhằm giới hạn thời gian hiệu lực của khóa ký dấu thời gian của TSA.

6.5. Yêu cầu về thuật toán

Khóa công khai và chứng thư chữ ký số của TSA nên sử dụng các thuật toán được quy định tại mục 5.1.1 của TCVN 14617:2026 cùng với các thuật toán quy định tại bảng 5 của tiêu chuẩn này.

Bảng 5 - Khoá công khai và chứng thư chữ ký số của TSA

Chứng thư chữ ký số của TSA	Bên phát hành chứng thư chữ ký số TSA	Bên sử dụng chứng thư chữ ký số TSA
Khóa công khai	Khuyến nghị hỗ trợ EdDSA; nên hỗ trợ SLH-DSA, XMSS hoặc LMS (PQC)	phải hỗ trợ DSA, EdDSA; nên hỗ trợ SLH-DSA, XMSS, LMS

7. Hồ sơ cho các giao thức truyền tải cần được hỗ trợ

Máy khách yêu cầu cấp dấu thời gian và máy chủ cấp dấu thời gian phải hỗ trợ việc truyền tải bản tin cấp dấu thời gian qua giao thức HTTP (IETF RFC 7230 đến RFC 7235) hoặc HTTPS (IETF RFC 2818) theo quy định tại Điều 3.4 của IETF RFC 3161.

Khuyến nghị ưu tiên sử dụng giao thức bảo mật HTTPS (RFC 2818) thay thế cho giao thức HTTP (từ RFC 7230 đến RFC 7235) nhằm đảm bảo an toàn, tính toàn vẹn và bảo mật cho dữ liệu trong quá trình truyền tải bản tin.

8. Mã định danh đối tượng của các thuật toán mật mã

Mã định danh đối tượng (OID) đối với các thuật toán hàm băm và thuật toán ký được khuyến nghị áp dụng phải tuân thủ các quy định tại Điều 11 của tiêu chuẩn ETSI TS 119 312.

9. Các yêu cầu bổ sung đối với dấu thời gian điện tử

9.1. Các yêu cầu bổ sung

Mã thông báo cấp dấu thời gian bắt buộc phải chứa phần mở rộng qcStatements bên trong trường extension, cú pháp của phần mở rộng này phải tuân thủ quy định theo IETF RFC 3739 tại mục 3.2.6.

Khi phần mở rộng qcStatements được sử dụng, phần mở rộng này phải chứa một cấu trúc tuyên bố esi4-qtstStatement-1 theo định nghĩa và các khai báo ASN.1 như sau:

+ id-etsi-tsts là một mã định danh đối tượng (OBJECT IDENTIFIER).

+ id-etsi-tsts-EuQCompliance là một mã định danh đối tượng được xác định từ mã id-etsi-tsts.

+ esi4-qtsstStatement-1 là một cấu trúc QC-STATEMENT được định danh bởi mã id-etsi-tsts-EuQCompliance.

Phần mở rộng qcStatements không được phép thiết lập/đánh dấu là quan trọng (critical).

CHÚ THÍCH 1: Các yêu cầu tại Điều này áp dụng cho tổ chức cung cấp dịch vụ cấp dấu thời gian. Đối với các cơ quan, tổ chức, cá nhân thiết lập hệ thống cấp dấu thời gian lựa chọn áp dụng.

CHÚ THÍCH 2: Việc tích hợp khai báo các tuyên bố này mang ý nghĩa tổ chức cung cấp dịch vụ cấp dấu thời gian chính thức tuyên bố mã thông báo cấp dấu thời gian được phát hành như một dấu thời gian điện tử.

10. Cấu trúc của trường policy

Khi mã thông báo cấp dấu thời gian được phát hành bởi tổ chức cung cấp dịch vụ cấp dấu thời gian tuân thủ theo TCVN XXX:2026 về Giao dịch điện tử - Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ cấp dấu thời gian, thì trường *policy* bên trong cấu trúc *TSTInfo* bắt buộc phải bao gồm một trong các thông tin sau:

- Mã định danh được quy định tại mục 5.2.1 của TCVN XXX:2026 về Giao dịch điện tử - Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ cấp dấu thời gian; hoặc
- Mã định danh riêng của tổ chức cung cấp dịch vụ cấp dấu thời gian quy định tại mục 5.2.2 của TCVN XXXX:2026 về Giao dịch điện tử - Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ cấp dấu thời gian.

11. Kiểu định dạng nội dung của tệp hoặc dữ liệu và phần mở rộng tệp của mã thông báo cấp dấu thời gian

Các giá trị về loại phương tiện và định dạng phần mở rộng tệp được sử dụng để nhận diện mã thông báo cấp dấu thời gian phải tuân thủ theo quy định tại IETF RFC 6838.

Thư mục tài liệu tham khảo

[1] Luật Giao dịch điện tử năm 2023;

[2] Nghị định số 23/2025/NĐ-CP ngày 21 tháng 02 năm 2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ tin cậy;

[3] Thông tư số 51/2025/TT-BKHCN ngày 31 tháng 12 năm 2025 của Bộ Khoa học và Công nghệ ban hành "Quy chuẩn kỹ thuật quốc gia về yêu cầu đối với dịch vụ cấp dấu thời gian";

[4] ETSI EN 319 422 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles;

[5] TCVN 14617:2026 Công nghệ thông tin - Dịch vụ tin cậy - Yêu cầu đối với chữ ký số và chứng thư chữ ký số;

[6] TCVN XXX:2026 Giao dịch điện tử - Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ cấp dấu thời gian.