TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN XXXX:2026

Xuất bản lần 1

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

Electronic Transactions – General requirements for operation and controls for time-stamping service providers

HÀ NỘI - 2026

Mục lục

Lời nói đầu

TCVN XXXX:2026 được xây dựng trên cơ sở tham khảo Tiêu chuẩn quốc tế ETSI TS 319 421 của Viện Tiêu chuẩn Viễn thông Châu Âu (ETSI), 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.

Lời giới thiệu

Trong bối cảnh chuyển đổi số, các giao dịch điện tử, hoạt động quản lý nhà nước, giao dịch dân sự, thương mại và cung cấp dịch vụ công ngày càng phụ thuộc vào việc xác định chính xác thời điểm phát sinh, gửi, nhận và xử lý thông tin điện tử. Dấu thời gian đóng vai trò quan trọng trong việc gắn kết thông tin về thời gian với thông điệp dữ liệu, qua đó hỗ trợ việc xác lập, bảo vệ và chứng minh giá trị pháp lý của thông điệp dữ liệu trong môi trường điện tử.

Theo quy định của pháp luật về giao dịch điện tử, dấu thời gian có thể được sử dụng để chứng minh thời điểm tồn tại của thông điệp dữ liệu, chữ ký số hoặc các dữ liệu điện tử khác. Việc bảo đảm tính chính xác, độ tin cậy và khả năng kiểm tra của dấu thời gian là yếu tố then chốt nhằm duy trì giá trị pháp lý, giá trị chứng cứ và mức độ tin cậy của các giao dịch điện tử trong suốt vòng đời sử dụng.

Tuy nhiên, hoạt động cấp dấu thời gian có thể chịu tác động của nhiều yếu tố rủi ro, bao gồm sự sai lệch của nguồn thời gian, sự cố kỹ thuật, thay đổi công nghệ, lỗ hổng an toàn thông tin hoặc các hạn chế trong quản lý và vận hành hệ thống. Do đó, TSA cần thiết lập và duy trì các chính sách, quy trình quản lý, biện pháp kỹ thuật và cơ chế kiểm soát phù hợp nhằm bảo đảm dịch vụ được cung cấp một cách liên tục, chính xác và tin cậy.

Tiêu chuẩn này quy định các yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ cấp dấu thời gian, không phụ thuộc vào lĩnh vực ứng dụng hay loại hình thông điệp dữ liệu cụ thể. Tiêu chuẩn được xây dựng nhằm tạo cơ sở cho việc triển khai, quản lý, giám sát và đánh giá sự phù hợp của các tổ chức cung cấp dịch vụ, qua đó góp phần tăng cường lòng tin của bên thứ ba và xã hội đối với việc sử dụng dấu thời gian trong môi trường điện tử.

Giao dịch điển tử - Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ cấp dấu thời gian

Electronic Transactions – General requirements for operation and controls for time-stamping service providers

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ cấp dấu thời gian

Các thông số kỹ thuật khác sẽ được điều chỉnh và mở rộng các yêu cầu này khi áp dụng cho các loại hình dịch vụ tin cậy cụ thể.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên 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 14618:2026, Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về đối với tổ chức cung cấp dịch vụ tin cậy

Recommendation ITU-R TF.460-6 (2002), *Standard-frequency and time-signal emissions (Phát xạ tần số chuẩn và tín hiệu thời gian).*

ISO/IEC 15408 (all parts), *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security (An toàn thông tin, an ninh mạng và bảo vệ quyền riêng tư — Tiêu chí đánh giá an toàn công nghệ thông tin)*

ISO/IEC 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules (Công nghệ thông tin — Kỹ thuật an toàn — Yêu cầu an toàn đối với mô-đun mật mã).*

TCVN 14618:2026, *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (Chữ ký điện tử và hạ tầng tin cậy (ESI) — Yêu cầu chung về chính sách đối với tổ chức cung cấp dịch vụ tin cậy).*

ETSI EN 319 411-1, *Electronic Signatures and Infrastructures (ESI) — Policy and security requirements for Trust Service Providers issuing certificates (Chữ ký điện tử và hạ tầng tin cậy (ESI) — Yêu cầu về chính sách và an toàn đối với tổ chức cung cấp dịch vụ tin cậy cấp chứng thư chữ ký số).*

ETSI EN 319 422, *Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles (Chữ ký điện tử và hạ tầng tin cậy (ESI) — Giao thức cấp dấu thời gian và hồ sơ thẻ dấu thời gian).*

ETSI EN 319 122-1, *Electronic Signatures and Infrastructures (ESI) — CAdES digital signatures — Part 1: Building blocks and CAdES baseline signatures (Chữ ký điện tử và hạ tầng tin cậy (ESI) — Chữ ký số CAdES — Phần 1: Các khối cấu thành và chữ ký CAdES cơ sở).*

FIPS PUB 140-2 (2002), *Security Requirements for Cryptographic Modules (Yêu cầu an toàn đối với mô-đun mật mã).*

FIPS PUB 140-3 (2019), *Security Requirements for Cryptographic Modules (Yêu cầu an toàn đối với mô-đun mật mã).*

3 Thuật ngữ, định nghĩa và chữ viết tắt

3.1 Thuật ngữ và định nghĩa

Trong tiêu chuẩn này, các thuật ngữ được nêu trong TCVN 14618:2026 và các thuật ngữ sau đây được áp dụng:

3.1.1

Bên thứ ba (Relying party)

Bên nhận, sử dụng, ứng dụng dấu thời gian.

3.1.2

Thuê bao (Subscriber)

Cá nhân hoặc tổ chức được cấp dấu thời gian và bị ràng buộc bởi các nghĩa vụ của thuê bao.

3.1.3

Thông điệp dữ liệu

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

3.1.4

Dấu thời gian (TimeStamp)

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.

Nguồn: Tài liệu tham khảo số [1]

3.1.5

Chính sách dấu thời gian (TimeStamp policy)

Tập hợp các quy tắc được định danh, xác định phạm vi áp dụng của dấu thời gian đối với một cộng đồng cụ thể và/hoặc một lớp ứng dụng có các yêu cầu an toàn chung.

3.1.6

Tổ chức cấp dấu thời gian (TimeStamping Authority - TSA)

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

3.1.7

Dịch vụ cấp dấu thời gian (TimeStamping service)

Dịch vụ tin cậy cung cấp dịch vụ cấp dấu thời gian, gắn thông tin về thời gian vào thông điệp dữ liệu.

Nguồn: Tài liệu tham khảo số [1]

3.1.8

Dịch vụ tin cậy (trust service)

Dịch vụ tin cậy bao gồm:

a) Dịch vụ cấp dấu thời gian;

b) Dịch vụ chứng thực thông điệp dữ liệu;

c) Dịch vụ chứng thực chữ ký số công cộng.

Nguồn: Tài liệu tham khảo số [1]

3.1.11

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

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

3.1.10

Quy chế chứng thực TSA (CP/CPS)

Tài liệu mô tả các thực hành mà TSA áp dụng khi phát hành dấu thời gian.

CHÚ THÍCH: Đây là một loại bản tuyên bố thực hành dịch vụ tin cậy theo định nghĩa tại TCVN 14618:2026.

3.2 Chữ viết tắt

Trong tài liệu này, các chữ viết tắt được nêu trong TCVN 14618:2026 và các chữ viết tắt sau đây được áp dụng:

Chữ viết tắt	Tiếng Anh	Nghĩa tiếng Việt
CA	Certification Authority	Tổ chức cung cấp dịch vụ chứng thực chữ ký số
CP/CPS	Certificate Policy/ Certificate Practice Statement	Quy chế chứng thực
TSA	Time-Stamping Authority	Tổ chức cung cấp dịch vụ cấp dấu thời gian
TSP	Trust Service Provider	Tổ chức cung cấp dịch vụ tin cậy
UTC	Coordinated Universal Time	Giờ Phối hợp Quốc tế

4 Tổng quan

4.1. Các thông tin về yêu cầu chính sách chung

Tài liệu này viện dẫn TCVN 14618:2026 cho các yêu cầu chính sách chung áp dụng cho các loại dịch vụ của tổ chức cung cấp dịch vụ tin cậy.

Các yêu cầu chính sách này dựa trên việc sử dụng mật mã khóa công khai, chứng thư khóa công khai và các nguồn thời gian tin cậy.

Thuê bao và các bên liên quan được khuyến nghị tham khảo CP/CPS của TSA để biết thêm chi tiết cụ thể về cách mà chính sách cấp dấu thời gian được triển khai thực tế (ví dụ: các giao thức được sử dụng trong việc cung cấp dịch vụ này).

4.2. Dịch vụ cấp dấu thời gian

Dịch vụ cấp dấu thời gian được chia thành các thành phần dịch vụ sau:

a) Tạo dấu thời gian: Thành phần này tạo ra các dấu thời gian.

b) Quản lý cấp dấu thời gian: Thành phần này giám sát và kiểm soát hoạt động của dịch vụ cấp dấu thời gian nhằm đảm bảo rằng dịch vụ được cung cấp theo đúng các quy định và thông số kỹ thuật do TSA xác định.

VÍ DỤ: Quản lý cấp dấu thời gian bảo đảm rằng đồng hồ được sử dụng để cấp dấu thời gian được đồng bộ chính xác với UTC.

Việc chia thành phần dịch vụ nhằm làm rõ các yêu cầu đối với cụ thể đối dịch vụ cấp dấu thời gian.

4.3 Tổ chức cung cấp dịch vụ cấp dấu thời gian (TSA)

TSA là tổ chức cung cấp dịch vụ tin cậy (TSP) cung cấp dịch vụ cấp dấu thời gian.

TSA có thể sử dụng các bên khác để cung cấp một số phần phục vụ cung cấp dịch vụ cấp dấu thời gian nhưng TSA luôn duy trì trách nhiệm tổng thể và bảo đảm rằng các yêu cầu chính sách được xác định trong tài liệu này được đáp ứng.

4.4 Thuê bao

Thuê bao sử dụng dịch vụ cấp dấu thời gian bao gồm: Tổ chức và cá nhân.

Trường hợp thuê bao là tổ chức, tổ chức này có thể bao gồm nhiều người sử dụng cuối hoặc một cá nhân người sử dụng cuối. Các nghĩa vụ áp dụng đối với tổ chức đó cũng sẽ áp dụng đối với các người sử dụng cuối. Trong mọi trường hợp, tổ chức sẽ chịu trách nhiệm nếu các nghĩa vụ của người sử dụng cuối không được thực hiện đúng, và do đó tổ chức có trách nhiệm truyền đạt thông tin đầy đủ, phù hợp đến các người sử dụng cuối của mình.

Trường hợp thuê bao là cá nhân, cá nhân đó sẽ chịu trách nhiệm trực tiếp nếu không thực hiện đúng các nghĩa vụ của mình.

5 Giới thiệu về chính sách dấu thời gian và các yêu cầu chung

5.1 Yêu cầu chung

Các yêu cầu chính sách được quy định trong tài liệu này dưới dạng chính sách dấu thời gian. Tài liệu này quy định một chính sách dấu thời gian, cụ thể là Chính sách dấu thời gian theo thông lệ tốt nhất

(Best practices Time-Stamp Policy – BTSP) dành cho các TSA phát hành dấu thời gian được hỗ trợ bởi chứng thư chữ ký số chứa khóa công khai, với độ chính xác thời gian từ 1 giây trở lên.

5.1.1 TSA có thể xây dựng chính sách riêng của mình nhằm mở rộng hoặc tăng cường chính sách được quy định trong tài liệu này.

5.1.2 Trường hợp TSA xây dựng chính sách riêng thì chính sách đó phải bao gồm hoặc quy định chặt chẽ hơn các yêu cầu được xác định trong tài liệu này.

5.1.3 Trường hợp TSA cung cấp độ chính xác tốt hơn 1 giây thì độ chính xác đó phải được nêu trong tuyên bố công bố của TSA (xem điều 6.3) và trong từng dấu thời gian được phát hành với độ chính xác tốt hơn 1 giây.

5.2 Tên và định danh chính sách

Định danh của chính sách dấu thời gian được quy định trong tài liệu này như sau:

BTSP: Chính sách dấu thời gian theo thông lệ tốt nhất (best practices policy for time-stamp).

Thông qua việc đưa định danh đối tượng này vào dấu thời gian, TSA tuyên bố sự phù hợp với chính sách dấu thời gian tương ứng.

5.2.1 TSA phải bao gồm định danh của chính sách dấu thời gian được hỗ trợ trong tuyên bố công bố TSA cung cấp cho thuê bao và bên thứ ba nhằm thể hiện tuyên bố phù hợp của mình.

5.2.2 Trường hợp TSA sử dụng định danh riêng cho chính sách dấu thời gian của mình thì TSA phải chỉ rõ trong tài liệu chính sách và trong CP/CPS TSA về định danh chính sách cấp dấu thời gian được hỗ trợ (tức BTSP).

5.3 Cộng đồng người sử dụng và phạm vi áp dụng

5.3.1 Chính sách dấu thời gian theo thông lệ tốt nhất

Chính sách này nhằm đáp ứng các yêu cầu đối với dấu thời gian phục vụ duy trì hiệu lực dài hạn (ví dụ như quy định trong ETSI EN 319 122-1), đồng thời cũng có thể áp dụng chung cho các trường hợp sử dụng khác có yêu cầu về mức độ bảo đảm tương đương.

5.3.1.1 Chính sách này có thể được áp dụng cho dịch vụ cấp dấu thời gian cho công cộng hoặc dịch vụ cấp dấu thời gian sử dụng trong một cộng đồng khép kín.

6 Chính sách và quy chế chứng thực

6.1 Đánh giá rủi ro

6.1.1 Áp dụng các yêu cầu tại điều 5 của TCVN 14618:2026.

6.2 Quy chế chứng thực – CP/CPS

6.2.1 Áp dụng các yêu cầu tại điều 6.1 của TCVN 14618:2026.

6.2.2 CP/CPS phải bổ sung thêm các yêu cầu đặc thù cho TSA, bao gồm các yêu cầu cụ thể sau:

a) Ít nhất một thuật toán băm được sử dụng để thể hiện dữ liệu cần ký số;

b) Độ chính xác của thời gian trong dấu thời gian so với UTC;

c) Những giới hạn, hạn chế trong sử dụng dịch vụ cấp dấu thời gian;

d) Nghĩa vụ của thuê bao theo quy định tại khoản 6.5.2 (nếu có);

e) Nghĩa vụ của bên thứ ba theo quy định tại khoản 6.6;

f) Thông tin về cách xác minh dấu thời gian để bên thứ ba dựa vào và thực hiện (xem điều 6.6) và thông tin về bất kỳ vấn đề nào có thể có liên quan đến thời điểm hết hiệu lực.

g) Đáp ứng yêu cầu đối với dịch vụ cấp dấu thời gian theo quy định pháp luật quốc gia.

6.2.3 TSA nên mô tả trong CP/CPS về tính sẵn sàng của dịch vụ.

VÍ DỤ: Thời gian trung bình dự kiến giữa các lần gián đoạn của dịch vụ cấp dấu thời gian, thời gian trung bình dự kiến để khôi phục sau khi xảy ra gián đoạn và các biện pháp được thiết lập cho khôi phục sau thảm họa, bao gồm cả các dịch vụ sao lưu.

6.2.4 CP/CPS của TSA có thể được cung cấp như một phần của thỏa thuận với thuê bao/bên thứ ba.

6.3 Điều khoản và điều kiện

6.3.1 Áp dụng các quy định tại điều 6.2 của TCVN 14618:2026.

6.4 Chính sách bảo mật thông tin

6.4.1 Áp dụng các quy định tại điều 6.3 của TCVN 14618:2026.

6.5 Nghĩa vụ của TSA

6.5.1 Tổng quan chung

6.5.1.1 TSA phải thực hiện mọi nghĩa vụ được ghi rõ trong dấu thời gian (ví dụ: thuộc tính mở rộng trong định dạng dấu) dù là được thể hiện trực tiếp hoặc được dẫn chiếu từ tài liệu khác.

6.5.2 Nghĩa vụ của TSA đối với thuê bao

Tài liệu này không đặt ra bất kỳ nghĩa vụ cụ thể nào đối với thuê bao, ngoài các yêu cầu riêng của TSA đã được nêu trong điều khoản và điều kiện của TSA.

6.6. Thông tin cung cấp cho bên thứ ba

6.6.1 Các điều khoản và điều kiện được cung cấp cho bên thứ ba (xem Điều 6.3) phải bao gồm nghĩa vụ của bên thứ ba khi xem xét một dấu thời gian, phải thực hiện các nội dung sau:

a) Xác minh rằng dấu thời gian đã được ký số hợp lệ; khóa bí mật được sử dụng để ký dấu thời gian không bị xâm phạm cho đến thời điểm thực hiện việc xác minh.

b) Xem xét mọi giới hạn, hạn chế về việc sử dụng dấu thời gian được nêu trong chính sách dấu thời gian;

c) Xem xét các quy định khác (nếu có) trong các thỏa thuận hoặc tại các tài liệu liên quan khác.

7 Vận hành và quản lý TSA

7.1 Giới thiệu

Các yêu cầu chính sách quy định trong tiêu chuẩn này không nhằm đặt ra bất kỳ hạn chế nào đối với việc xác định giá hoặc thu phí dịch vụ của TSA.

Các yêu cầu trong tiêu chuẩn này được xây dựng theo cách tiếp cận dựa trên mục tiêu an toàn, trong đó trước hết xác định các mục tiêu an toàn cần đạt được. Để tạo lập mức độ tin cậy phù hợp, tiêu chuẩn này quy định các yêu cầu cụ thể về biện pháp kiểm soát nhằm đáp ứng các mục tiêu an toàn đó.

Trên cơ sở các điều khoản và mức chất lượng dịch vụ đã được thỏa thuận với thuê bao, việc cấp dấu thời gian đáp ứng một yêu cầu cụ thể là thuộc quyền quyết định của TSA.

7.2. Tổ chức nội bộ

7.2.1 Áp dụng các quy định tại điều 6.1 của tiêu chuẩn TCVN 14618:2026.

Ngoài ra, TSA phải đáp ứng các yêu cầu cụ thể sau:

7.2.2 TSA phải là pháp nhân được thành lập theo quy định của pháp luật quốc gia.

7.2.3 TSA phải xây dựng, duy trì và áp dụng hệ thống quản lý chất lượng và quản lý an toàn thông tin phù hợp với ~~phạm vi, tính chất và quy mô~~ dịch vụ cấp dấu thời gian.

7.2.4 TSA phải bố trí đủ số lượng nhân sự có trình độ chuyên môn, được đào tạo phù hợp, có kiến thức kỹ thuật và kinh nghiệm thực tế cần thiết để thực hiện các hoạt động liên quan đến loại hình, phạm vi và khối lượng công việc phục vụ cung cấp dịch vụ cấp dấu thời gian.

7.3 Nguồn nhân lực

7.3.1 Áp dụng các yêu cầu được nêu trong điều 7.2 của TCVN 14618:2026.

7.4 Quản lý tài sản

7.4.1 Áp dụng các yêu cầu được nêu trong điều 7.3 của TCVN 14618:2026.

7.5 Kiểm soát truy cập

7.5.1 Áp dụng các yêu cầu được nêu trong điều 7.4 của TCVN 14618:2026.

7.6. Kiểm soát mật mã

7.6.1 Quy định chung

7.6.1.1 Áp dụng các yêu cầu được nêu trong điều 7.5 của TCVN 14618:2026.

7.6.2. Tạo khóa

Việc tạo khoá bí mật của TSA phải tuân thủ các yêu cầu sau:

7.6.2.1 Việc tạo khoá bí mật của TSA phải được thực hiện trong môi trường an toàn (xem điều 7.8) bởi nhân sự đảm nhiệm vai trò tin cậy (xem điều 7.3) và áp dụng ít nhất cơ chế kiểm soát kép (khi thực hiện sẽ có người giám sát, kiểm soát bên cạnh).

7.6.2.2 Nhân sự được ủy quyền thực hiện tạo khoá phải được giới hạn trong phạm vi những người thực sự cần thiết theo CP/CPS của TSA.

7.6.2.3 Việc tạo khóa ký số của TSA phải được thực hiện trong một thiết bị mật mã an toàn, thiết bị này phải đáp ứng một trong các yêu cầu sau:

a) (Khuyến nghị) Là hệ thống đáng tin cậy, được đánh giá và bảo đảm ở mức EAL 4 trở lên theo ISO/IEC 15408, hoặc theo các tiêu chí đánh giá an toàn CNTT quốc gia hoặc quốc tế tương đương. Việc đánh giá này phải dựa trên mục tiêu an toàn hoặc hồ sơ bảo vệ đáp ứng các yêu cầu của tài liệu này, trên cơ sở phân tích rủi ro và có xét đến các biện pháp an toàn vật lý và các biện pháp phi kỹ thuật khác; hoặc

b) Đáp ứng các yêu cầu quy định tại ISO/IEC 19790, FIPS PUB 140-2 mức 3 hoặc FIPS PUB 140-3 mức 3.

7.6.2.4 Thuật toán tạo khóa, độ dài khóa bí mật và thuật toán chữ ký số được sử dụng để ký số dấu thời gian nên tuân theo quy định tại TCVN 14617:2026.

7.6.2.5 Khóa ký số không nên được nhập vào nhiều thiết bị mật mã khác nhau.

7.6.2.6 Trường hợp cùng một khóa tồn tại trong nhiều thiết bị mật mã khác nhau, các khóa này phải được liên kết với cùng một chứng thư chữ ký số công khai trên tất cả các thiết bị mật mã đó.

7.6.2.7 Tại mỗi thời điểm, một TSA chỉ được phép có một khóa bí mật ký số dấu thời gian đang hoạt động.

7.6.3 Bảo vệ khoá bí mật của TSA

7.6.3.1 Tính toàn vẹn và tính bảo mật của khóa bí mật TSA phải được duy trì, tối thiểu đáp ứng các yêu cầu cụ thể sau:

7.6.3.1.1 Khóa ký bí mật của TSA phải được lưu giữ và sử dụng trong một mô-đun mật mã an toàn, mô-đun này phải đáp ứng một trong các yêu cầu sau:

a) (Khuyến nghị) Là hệ thống đáng tin cậy, được đánh giá và bảo đảm ở mức EAL 4 trở lên theo ISO/IEC 15408, hoặc theo các tiêu chí đánh giá an toàn CNTT quốc gia hoặc quốc tế tương đương. Việc đánh giá này phải dựa trên mục tiêu an toàn hoặc hồ sơ bảo vệ đáp ứng các yêu cầu của tài liệu này, trên cơ sở phân tích rủi ro và có xét đến các biện pháp an toàn vật lý và các biện pháp phi kỹ thuật khác; hoặc

b) Đáp ứng các yêu cầu quy định tại ISO/IEC 19790, FIPS PUB 140-2 mức 3 hoặc FIPS PUB 140-3 mức 3.

7.6.3.1.2 Trường hợp khóa bí mật của TSA được sao lưu, việc sao chép, lưu trữ và khôi phục chỉ được thực hiện bởi nhân sự đảm nhiệm vai trò tin cậy, áp dụng tối thiểu cơ chế kiểm soát kép, trong môi trường được bảo vệ vật lý (xem điều 7.8).

7.6.3.1.3 Nhân sự được ủy quyền thực hiện chức năng sao lưu phải được giới hạn trong phạm vi những người thực sự cần thiết theo CP/CPS của TSA.

7.6.3.1.4 Mọi bản sao lưu của khóa ký bí mật TSA phải được mô-đun mật mã an toàn bảo vệ nhằm bảo đảm tính toàn vẹn và tính bảo mật trước khi được lưu trữ bên ngoài mô-đun đó.

7.6.4 Chứng thư chữ ký số

7.6.4.1 TSA phải bảo đảm tính toàn vẹn và tính xác thực của khoá thực hiện xác thực chữ ký số (khóa công khai), tối thiểu đáp ứng các yêu cầu cụ thể sau:

7.6.4.1.1 Khóa công khai dùng để xác thực chữ ký số phải được cung cấp cho bên thứ ba thông qua chứng thư chữ ký số chứa khóa công khai.

7.6.4.1.2 Chứng thư chữ ký số chứa khóa công khai dùng để xác thực chữ ký số của TSA nên được cấp bởi tổ chức chứng thực hoạt động phù hợp với ETSI 319 411-1.

7.6.4.1.3 TSA không được phép cấp dấu thời gian trước khi chứng thư chữ ký số chứa khóa công khai dùng để xác thực chữ ký số được nạp vào thiết bị mật mã an toàn của TSA.

7.6.4.2 Khi nhận được chứng thư chữ ký số chứa khóa công khai dùng để xác minh chữ ký số, TSA nên thực hiện việc kiểm tra để bảo đảm rằng chứng thư chữ ký số này đã được ký số hợp lệ, bao gồm việc xác minh chuỗi chứng thư đến một tổ chức chứng thực tin cậy.

7.6.5 Tạo lại khóa

7.6.5.1 Thời hạn hiệu lực của chứng thư chữ ký số của TSA không được dài hơn khoảng thời gian mà thuật toán và độ dài khóa được lựa chọn còn được công nhận là phù hợp với mục đích sử dụng (xem 7.6.2.5).

7.6.6 Quản lý vòng đời của phần cứng mật mã ký số

7.6.6.1 Phần cứng mật mã ký số không được bị can thiệp, sửa đổi trong quá trình vận chuyển.

7.6.6.2 Phần cứng mật mã ký số không được bị can thiệp, sửa đổi trong quá trình lưu giữ và bảo quản.

7.6.6.3 Việc cài đặt, kích hoạt và sao chép khóa bí mật vào phần cứng mật mã ký số chỉ được thực hiện bởi nhân sự đảm nhiệm vai trò tin cậy, áp dụng tối thiểu cơ chế kiểm soát kép, trong môi trường được bảo vệ vật lý (xem điều 7.8).

7.6.6.4 Khóa bí mật dùng để ký số được lưu trữ trong mô-đun mật mã an toàn phải được xóa bỏ không thể khôi phục khi thiết bị ngừng sử dụng.

7.6.7 Kết thúc vòng đời khóa

7.6.7.1 TSA phải xác định ngày hết hiệu lực đối với các khóa của TSA.

7.6.7.2 Ngày hết hiệu lực của các khóa TSA không được muộn hơn thời điểm kết thúc hiệu lực của chứng thư chữ ký số khóa công khai tương ứng.

7.6.7.3 Ngày hết hiệu lực của các khóa TSA nên xét đến vòng đời khóa được xác định trong mục “độ dài khóa khuyến nghị theo thời gian” của TCVN 14617:2026.

7.6.7.4 Nhằm bảo đảm khả năng xác thực tính hợp lệ của dấu thời gian trong một khoảng thời gian đủ dài, thời hạn hiệu lực của khóa ký số nên được rút ngắn.

VÍ DỤ: Khóa công khai có thời hạn hiệu lực là 4 năm, trong khi khóa bí mật được rút ngắn thời hạn hiệu lực xuống còn 1 năm, việc này giảm thời gian sử dụng khoá bí mật qua đó giảm khả năng khoá bí mật bị xâm phạm.

7.6.7.5 Ngày hết hiệu lực của các khóa có thể được xác định tại thời điểm khởi tạo mô-đun mật mã an toàn, hoặc thông qua việc thiết lập thời hạn sử dụng khóa bí mật trong chứng thư chữ ký số khóa công khai.

7.6.7.6 Khóa ký bí mật dùng để ký số không được sử dụng sau khi kết thúc thời hạn hiệu lực của khóa đó.

Cụ thể:

7.6.7.6.1 Các quy trình vận hành hoặc kỹ thuật phải được thiết lập để bảo đảm rằng khóa mới được đưa vào sử dụng khi khóa cũ của TSA hết hiệu lực.

7.6.7.6.2 Khóa ký bí mật dùng để ký số, hoặc bất kỳ phần nào của khóa, bao gồm mọi bản sao, phải được tiêu hủy theo cách không thể khôi phục lại.

7.7 Dấu thời gian

7.7.1 Cấp dấu thời gian

7.7.1.1 Dấu thời gian phải phù hợp với hồ sơ dấu thời gian được quy định tại ETSI EN 319 422.

7.7.1.2 Dấu thời gian phải được cấp một cách an toàn.

7.7.1.3 Dấu thời gian phải bao gồm giá trị thời gian chính xác.

Cụ thể:

7.7.1.3.1 Giá trị thời gian sử dụng trong dấu thời gian phải có khả năng truy xuất nguồn gốc tới nguồn thời gian theo quy định của pháp luật về nguồn thời gian chuẩn quốc gia;

7.7.1.3.2 Trường hợp độ chính xác được xác định và thể hiện trong dấu thời gian, thời gian được bao gồm trong dấu thời gian phải được đồng bộ theo độ chính xác đó.

7.7.1.3.3 Trường hợp đồng hồ của TSA được phát hiện là không đáp ứng độ chính xác đã công bố (xem 7.7.1.3.1 và 7.7.1.3.2) thì không được phép cấp dấu thời gian.

7.7.1.3.4 Dấu thời gian phải được ký số bằng khóa được tạo ra riêng biệt và chỉ sử dụng cho mục đích này.

7.7.1.3.5 Hệ thống tạo dấu thời gian phải từ chối mọi yêu cầu cấp dấu thời gian khi thời hạn hiệu lực của khóa bí mật dùng để ký số đã kết thúc.

7.8 An toàn vật lý và môi trường

7.8.1 Áp dụng các yêu cầu được quy định tại điều 7.6 của TCVN 14618:2026.

Ngoài ra, các yêu cầu dưới đây được áp dụng:

7.8.2 Các biện pháp kiểm soát truy cập phải được áp dụng đối với mô-đun mật mã nhằm đáp ứng các yêu cầu về an toàn của mô-đun mật mã an toàn được quy định tại điều 7.6, và áp dụng các biện pháp kiểm soát bổ sung sau đây áp dụng đối với quản lý cấp dấu thời gian:

7.8.2.1 Các bộ phận quản lý cấp dấu thời gian phải được vận hành trong môi trường bảo đảm bảo vệ cả về mặt vật lý và logic, nhằm ngăn ngừa việc dịch vụ bị xâm phạm do truy cập trái phép vào hệ thống hoặc dữ liệu.

7.8.2.2 Mọi lần ra vào khu vực được bảo vệ vật lý phải được sự giám sát độc lập.

7.8.2.3 Người không được phép truy cập phải được hộ tống bởi người được ủy quyền trong suốt thời gian ở trong khu vực an toàn.

7.8.2.4 Mọi lượt ra vào khu vực được bảo vệ vật lý phải được ghi nhật ký.

7.8.2.5 Việc bảo vệ vật lý phải được thực hiện thông qua việc thiết lập các vành đai an toàn được xác định rõ ràng, tức là các rào cản vật lý, xung quanh khu vực quản lý cấp dấu thời gian.

7.8.2.6 Mọi khu vực cơ sở được sử dụng chung với các tổ chức khác phải nằm ngoài vành đai an toàn này.

7.8.2.7 Các biện pháp an toàn vật lý và môi trường phải bảo vệ cơ sở hạ tầng nơi đặt tài nguyên hệ thống, các tài nguyên hệ thống và các cơ sở được sử dụng để hỗ trợ vận hành các tài nguyên đó.

7.8.2.8 Những biện pháp kiểm soát an toàn vật lý và môi trường của TSA đối với các hệ thống liên quan đến quản lý cấp dấu thời gian tối thiểu phải bao gồm kiểm soát truy cập vật lý, bảo vệ trước thiên tai, an

toàn phòng cháy chữa cháy, xử lý sự cố của các hạ tầng hỗ trợ như điện và viễn thông, sập kết cấu công trình, rò rỉ hệ thống cấp thoát nước, bảo vệ chống trộm cắp và đột nhập trái phép, cũng như khôi phục sau thảm họa.

7.8.2.9 Các biện pháp kiểm soát phải được áp dụng để ngăn chặn việc thiết bị, thông tin, phương tiện lưu trữ và phần mềm liên quan đến dịch vụ cấp dấu thời gian bị mang ra khỏi cơ sở khi chưa được phép.

7.8.3 Các chức năng khác có thể được hỗ trợ trong cùng khu vực an toàn, với điều kiện việc truy cập được giới hạn đối với nhân sự được ủy quyền.

7.9 An toàn vận hành

7.9.1 Áp dụng các yêu cầu được quy định tại điều 7.7 của TCVN 14618:2026 .

Ngoài ra, các yêu cầu dưới đây được áp dụng:

7.9.2 Nhu cầu về năng lực hệ thống phải được giám sát và việc dự báo nhu cầu năng lực trong tương lai phải được thực hiện nhằm bảo đảm đủ năng lực xử lý và dung lượng lưu trữ cho hoạt động cung cấp dịch vụ.

7.10 An toàn mạng

7.10.1 Áp dụng các yêu cầu được quy định tại điều 7.8 của TCVN 14618:2026 .

Ngoài ra, các yêu cầu dưới đây được áp dụng:

7.10.2 TSA phải duy trì và bảo vệ toàn bộ các hệ thống trong vùng an toàn.

7.10.3 TSA phải cấu hình tất cả các hệ thống bằng cách loại bỏ hoặc vô hiệu hóa mọi tài khoản, ứng dụng, dịch vụ, giao thức và cổng không còn sử dụng trong hoạt động của TSA.

7.10.4 Chỉ nhân sự đảm nhiệm vai trò tin cậy mới được phép truy cập các vùng an toàn và vùng an toàn cao.

7.11 Quản lý sự cố

7.11.1 Áp dụng các yêu cầu được quy định tại điều 7.9 của TCVN 14618:2026.

7.12 Thu thập bằng chứng

7.12.1 Áp dụng các yêu cầu được quy định tại điều 7.10 của TCVN 14618:2026.

Ngoài ra, các yêu cầu dưới đây được áp dụng:

Quản lý khoá:

7.12.2 Các bản ghi liên quan đến mọi sự kiện trong suốt vòng đời của khóa phải được ghi nhật ký.

7.12.3 Các bản ghi liên quan đến mọi sự kiện trong suốt vòng đời của chứng thư chữ ký số (nếu áp dụng) phải được ghi nhật ký.

Đồng bộ thời gian

7.12.4 Các bản ghi liên quan đến mọi sự kiện đồng bộ đồng hồ của TSA với nguồn thời gian theo quy định của pháp luật về nguồn thời gian chuẩn quốc gia phải được ghi nhật ký.

7.12.5 Các bản ghi phải bao gồm thông tin về việc hiệu chuẩn hoặc đồng bộ đồng hồ định kỳ được sử dụng trong dịch vụ cấp dấu thời gian.

7.12.6 Các bản ghi liên quan đến mọi sự kiện phát hiện việc mất đồng bộ thời gian phải được ghi nhật ký.

7.13 Quản lý tính liên tục trong hoạt động của TSA

7.13.1 Áp dụng các yêu cầu được quy định tại điều 7.11 của TCVN 14618:2026 .

Ngoài ra, các yêu cầu dưới đây được áp dụng:

7.13.2 Kế hoạch khôi phục sau thảm họa của TSA phải bao quát các trường hợp khóa bí mật dùng để ký số bị xâm phạm hoặc nghi ngờ bị xâm phạm, hoặc đồng hồ bị mất hiệu chuẩn, có thể đã ảnh hưởng đến các dấu thời gian đã được cấp.

7.13.3 Trong trường hợp xảy ra xâm phạm, nghi ngờ xâm phạm hoặc mất hiệu chuẩn trong quá trình cấp dấu thời gian, TSA phải cung cấp cho tất cả thuê bao và bên thứ ba mô tả về sự cố đã xảy ra.

7.13.4 Trong trường hợp hoạt động bị xâm phạm (ví dụ: khóa bị xâm phạm), nghi ngờ bị xâm phạm hoặc mất hiệu chuẩn, TSA không được tiếp tục cấp dấu thời gian cho đến khi đã thực hiện các biện pháp khắc phục để phục hồi sau sự cố.

7.13.5 Trong trường hợp xảy ra xâm phạm nghiêm trọng đối với hoạt động của TSA hoặc mất hiệu chuẩn, TSA phải cung cấp cho tất cả thuê bao và bên thứ ba các thông tin có thể được sử dụng để xác định những dấu thời gian có khả năng đã bị ảnh hưởng, trừ trường hợp việc cung cấp thông tin này xâm phạm quyền riêng tư của người sử dụng TSA hoặc làm ảnh hưởng đến an toàn của dịch vụ TSA.

CHÚ THÍCH: Trong trường hợp khóa bí mật bị xâm phạm, dấu vết kiểm toán của tất cả các dấu thời gian do TSA tạo ra có thể được sử dụng để phân biệt giữa các dấu thời gian hợp lệ và các dấu thời gian bị làm giả hoặc lùi thời gian. Việc sử dụng hai dấu thời gian từ hai TSA khác nhau cũng có thể là một biện pháp để xử lý vấn đề này.

7.14 Chấm dứt hoạt động của TSA và kế hoạch chấm dứt

7.14.1 Áp dụng các yêu cầu được quy định tại điều 7.12 của TCVN 14618:2026 .

Ngoài ra, các yêu cầu dưới đây được áp dụng:

7.14.2 Khi TSA chấm dứt việc cung cấp dịch vụ, TSA phải thu hồi tất cả các chứng thư chữ ký số của TSA chưa hết hiệu lực.

7.15 Tuân thủ pháp luật

7.15.1 Áp dụng các yêu cầu được quy định tại điều 7.13 của TCVN 14618:2026.

Thư mục tài liệu tham khảo

[1] Luật số 20/2023/QH15 ngày 22 tháng 6 năm 2023 của Quốc hội về giao dịch điện tử.

[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 trưởng 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 319 421 V1.3.1 (2025-05), Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

[5] ETSI EN 319 122-1, Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures.

[6] IETF RFC 3161 (August 2001), Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

[7] IETF RFC 5816 (March 2010), ESSCertIDv2 Update for RFC 3161.

[8] BIPM Circular T.

[9] ETSI TS 119 312, Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites.

[10] ETSI EN 319 403-1 V2.3.1 (2020-06), Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.

[11] EN 419231, Protection profile for trustworthy systems supporting time stamping.

[12] EN 419221-5:2018, Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services.

[13] IETF RFC 5280 (May 2008), Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

[14] ISO/IEC 18014-2:2021, Information security - Time-stamping services - Part 2: Mechanisms producing independent tokens.