

Số: /2025/TT-BKHCN

Hà Nội, ngày tháng năm 2025

THÔNG TƯ
Quy định kiểm toán kỹ thuật

Căn cứ Luật Giao dịch điện tử ngày 22 tháng 06 năm 2023;

Căn cứ Luật Chất lượng sản phẩm, hàng hóa ngày 21 tháng 11 năm 2007;

Căn cứ Nghị định số 23/2025/NĐ-CP ngày 21 tháng 02 năm 2025 của Chính phủ quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký điện tử và dịch vụ tin cậy;

Căn cứ Nghị định số 132/2008/NĐ-CP ngày 31 tháng 12 năm 2008 của Chính phủ quy định chi tiết thi hành một số điều của Luật Chất lượng sản phẩm, hàng hóa; Nghị định số 74/2018/NĐ-CP ngày 15 tháng 5 năm 2018 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 132/2008/NĐ-CP ngày 31 tháng 12 năm 2008 của Chính phủ quy định chi tiết thi hành một số điều Luật Chất lượng sản phẩm, hàng hóa;

Căn cứ Nghị định số 55/2025/NĐ-CP ngày 02 tháng 3 năm 2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Khoa học và Công nghệ;

Theo đề nghị Giám đốc Trung tâm Chứng thực điện tử quốc gia;

Bộ trưởng Bộ Khoa học và Công nghệ ban hành Thông tư quy định về kiểm toán kỹ thuật

Điều 1. Phạm vi điều chỉnh

Thông tư này quy định chi tiết về hoạt động kiểm toán kỹ thuật quy định tại Điều 27 Nghị định số 23/2025/NĐ-CP ngày 21/02/2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ tin cậy.

Điều 2. Đối tượng áp dụng

Thông tư này áp dụng đối với:

1) Tổ chức cung cấp dịch vụ tin cậy;

- 2) Cơ quan, tổ chức tạo lập chữ ký điện tử chuyên dùng bảo đảm an toàn;
- 3) Tổ chức kiểm toán kỹ thuật;
- 4) Tổ chức, cá nhân liên quan đến hoạt động kiểm toán kỹ thuật.

Điều 3. Giải thích từ ngữ

Trong Thông tư này, các từ ngữ dưới đây được hiểu như sau:

1. Kiểm toán kỹ thuật là hoạt động đánh giá kỹ thuật độc lập, khách quan đối với hệ thống thông tin, quy trình cung cấp dịch vụ tin cậy nhằm xác định việc đáp ứng tiêu chuẩn kỹ thuật bắt buộc áp dụng, quy chuẩn kỹ thuật, yêu cầu kỹ thuật theo quy định của pháp luật về giao dịch điện tử và các văn bản pháp luật có liên quan;

2. Tổ chức kiểm toán kỹ thuật là tổ chức đánh giá sự phù hợp được Bộ Khoa học và Công nghệ chỉ định theo quy định tại Nghị định số 132/2008/NĐ-CP ngày 31/12/2008 của Chính phủ quy định chi tiết thi hành một số điều của Luật Chất lượng sản phẩm, hàng hoá, được sửa đổi, bổ sung tại Nghị định số 74/2018/NĐ-CP ngày 15/05/2018 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 132/2008/NĐ-CP ngày 31/12/2008 của Chính phủ quy định chi tiết thi hành một số điều Luật chất lượng sản phẩm, hàng hóa và Nghị định số 154/2018/NĐ-CP ngày 09/11/2018 của Chính phủ sửa đổi, bổ sung, bãi bỏ một số quy định về điều kiện đầu tư, kinh doanh trong lĩnh vực quản lý nhà nước của Bộ Khoa học và Công nghệ và một số quy định về kiểm tra chuyên ngành, có đủ năng lực thực hiện hoạt động đánh giá kỹ thuật đối với tổ chức cung cấp dịch vụ tin cậy theo quy định tại Thông tư này; ¹

3. Tổ chức được kiểm toán kỹ thuật bao gồm:

- a) Tổ chức cung cấp dịch vụ tin cậy;
- b) Cơ quan, tổ chức tạo lập chữ ký điện tử chuyên dùng bảo đảm an toàn.

Điều 4. Nội dung kiểm toán kỹ thuật

¹ Viện Tiêu chuẩn Viễn thông Châu Âu ban hành ETSI EN 319 403 quy định các yêu cầu về năng lực, hoạt động và tính khách quan của các tổ chức đánh giá và chứng nhận sự phù hợp của nhà cung cấp dịch vụ tin cậy và các dịch vụ tin cậy mà họ cung cấp theo các tiêu chí xác định. ETSI EN 319 403 được xây dựng dựa trên các yêu cầu của ISO/IEC 17065 và các yêu cầu riêng cho đánh giá dịch vụ tin cậy

- Nội dung kiểm toán kỹ thuật đánh giá sự phù hợp bao gồm (1) hệ thống kỹ thuật, (2) quy trình quản lý được quy định tại Khoản 3, Khoản 4, Khoản 5 Điều 18 Nghị định số 23/2025/NĐ-CP ngày 21/02/2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ tin cậy.

- Yêu cầu cụ thể về các tiêu chí kiểm toán kỹ thuật đánh giá sự phù hợp được quy định tại Phụ lục 01 kèm theo thông tư này.

Điều 5. Chu kỳ kiểm toán kỹ thuật

1. Kiểm toán kỹ thuật được thực hiện định kỳ 2 năm/lần;²

2. Trong thời gian tối đa 01 (một) năm kể từ ngày được cấp chứng thư số lần đầu, Tổ chức cung cấp dịch vụ tin cậy phải hoàn thành kiểm toán kỹ thuật lần đầu theo quy định tại Thông tư này.

Điều 6. Quy trình kiểm toán kỹ thuật

Kiểm toán kỹ thuật được thực hiện theo 02 (hai) giai đoạn:

1. Giai đoạn 1 - Đánh giá Tài liệu: Tổ chức kiểm toán kỹ thuật đánh giá tài liệu của tổ chức được kiểm toán kỹ thuật về sự phù hợp với các yêu cầu được quy định.

2. Giai đoạn 2 - Đánh giá thực tế: Tổ chức kiểm toán kỹ thuật đánh giá việc quản lý, tổ chức, quy trình, tài liệu, cơ sở vật chất và cơ sở hạ tầng tại trụ sở của tổ chức được kiểm toán kỹ thuật về sự phù hợp với các yêu cầu được quy định.

Điều 7. Báo cáo kiểm toán kỹ thuật

Báo cáo kiểm toán kỹ thuật phải bao gồm các thông tin sau:

1. Thông tin chung về cuộc kiểm toán kỹ thuật:

a) Mô tả chi tiết về quá trình đánh giá kỹ thuật.

b) Tiêu chuẩn, chuẩn mực và/hoặc các yêu cầu pháp lý mà cuộc kiểm toán kỹ thuật được thực hiện dựa trên đó.

2. Đánh giá rủi ro bảo mật thông tin: Phân tích về việc đánh giá phân tích rủi ro bảo mật thông tin của Tổ chức được kiểm toán kỹ thuật.

3. Thời gian kiểm toán kỹ thuật:

a) Tổng thời gian đã sử dụng cho cuộc kiểm toán kỹ thuật.

² Theo quy định tại Điều 31 của NĐ 23/2025/NĐ-CP

b) Chi tiết về thời gian dành cho việc xem xét tài liệu, đánh giá phân tích rủi ro, kiểm toán kỹ thuật tại chỗ và lập báo cáo kiểm toán kỹ thuật.

4. Phương pháp kiểm toán kỹ thuật:

a) Các câu hỏi kiểm toán kỹ thuật đã được thực hiện, lý do lựa chọn.

b) Quy trình kiểm tra/kiểm thử (Test procedure).

5. Các thông tin phục vụ việc ra quyết định chứng nhận, bao gồm:

a) Các lĩnh vực được kiểm toán kỹ thuật, bao gồm các yêu cầu chứng nhận và các địa điểm đã được kiểm toán kỹ thuật, các bằng chứng quan trọng đã thu thập;

b) Các đánh giá được đưa ra, cả tích cực và tiêu cực;

c) Thông tin chi tiết về bất kỳ sự không phù hợp nào được xác định, được hỗ trợ bởi bằng chứng khách quan (nếu có) và một tham chiếu duy nhất đến yêu cầu không được đáp ứng;

d) Nhận xét về sự phù hợp của Tổ chức được kiểm toán kỹ thuật với các tiêu chí mà cuộc kiểm toán kỹ thuật đã được thực hiện, cùng với một tuyên bố rõ ràng về sự phù hợp hoặc không phù hợp.

đ) Các bảng câu hỏi, danh sách kiểm tra, đánh giá, nhật ký hoặc ghi chú của chuyên gia đánh giá đã hoàn thành.

e) Thông tin về các mẫu được đánh giá trong quá trình đánh giá kỹ thuật phải được đưa vào báo cáo kiểm toán kỹ thuật hoặc trong các tài liệu chứng nhận khác.

Điều 8. Chỉ định tổ chức kiểm toán kỹ thuật

1. Tổ chức kiểm toán kỹ thuật được Bộ Khoa học và Công nghệ đánh giá và chỉ định khi đáp ứng các điều kiện tại Nghị định số 74/2018/NĐ-CP ngày 15/05/2018 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 132/2008/NĐ-CP ngày 31/12/2008 của Chính phủ quy định chi tiết thi hành một số điều Luật chất lượng sản phẩm, hàng hóa được sửa đổi, bổ sung tại Nghị định số 154/2018/NĐ-CP ngày 09/11/2018 của Chính phủ sửa đổi, bổ sung, bãi bỏ một số quy định về điều kiện đầu tư, kinh doanh trong lĩnh vực quản lý nhà nước của Bộ Khoa học và Công nghệ và một số quy định về kiểm tra chuyên ngành;

Danh sách tổ chức kiểm toán kỹ thuật được Bộ Khoa học và Công nghệ chỉ định được đăng tải trên Trang thông tin điện tử của Bộ Khoa học và Công nghệ;

2. Hồ sơ đăng ký chỉ định tổ chức kiểm toán kỹ thuật thực hiện theo quy định tại Nghị định số 74/2018/NĐ-CP ngày 15/05/2018 của Chính phủ sửa đổi, bổ

sung một số điều của Nghị định số 132/2008/NĐ-CP ngày 31/12/2008 của Chính phủ quy định chi tiết thi hành một số điều Luật chất lượng sản phẩm, hàng hóa được sửa đổi, bổ sung tại Nghị định số 154/2018/NĐ-CP ngày 09/11/2018 của Chính phủ sửa đổi, bổ sung, bãi bỏ một số quy định về điều kiện đầu tư, kinh doanh trong lĩnh vực quản lý nhà nước của Bộ Khoa học và Công nghệ và một số quy định về kiểm tra chuyên ngành;

3. Trình tự, thủ tục chỉ định tổ chức kiểm toán kỹ thuật thực hiện theo quy định tại Nghị định số 74/2018/NĐ-CP ngày 15/05/2018 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 132/2008/NĐ-CP ngày 31/12/2008 của Chính phủ quy định chi tiết thi hành một số điều Luật chất lượng sản phẩm, hàng hóa được sửa đổi, bổ sung tại Nghị định số 154/2018/NĐ-CP ngày 09/11/2018 của Chính phủ sửa đổi, bổ sung, bãi bỏ một số quy định về điều kiện đầu tư, kinh doanh trong lĩnh vực quản lý nhà nước của Bộ Khoa học và Công nghệ và một số quy định về kiểm tra chuyên ngành.

Điều 9. Điều kiện đối với chuyên gia đánh giá

1. Trình độ học vấn: Tốt nghiệp đại học trở lên về công nghệ thông tin hoặc gần đào tạo về công nghệ thông tin hoặc trong các ngành liên quan (an toàn thông tin, luật về công nghệ, quản lý chất lượng...) và có kinh nghiệm tối thiểu 02 năm tương ứng với ngành được đào tạo.

2. Kinh nghiệm thực tế: Tối thiểu 3–5 năm kinh nghiệm làm việc trong lĩnh vực kỹ thuật liên quan: Hệ thống công nghệ thông tin, bảo mật mạng, dịch vụ tin cậy, hạ tầng khóa công khai, chữ ký điện tử.

3. Kinh nghiệm đánh giá: Ít nhất 2–3 năm kinh nghiệm thực tế trong công tác đánh giá sự phù hợp, kiểm toán hệ thống kỹ thuật.

4. Chứng chỉ chuyên môn (ưu tiên): Chứng chỉ kiểm toán hoặc đánh giá chất lượng như: ISO 27001 Lead Auditor, ISO 20000, ISO/IEC 17065 Assessor, CISA (Certified Information Systems Auditor).

Điều 10. Trách nhiệm của Tổ chức kiểm toán kỹ thuật

1. Thực hiện quyền và nghĩa vụ theo quy định tại Luật Chất lượng sản phẩm, hàng hóa và văn bản pháp luật liên quan. Trường hợp vi phạm, tùy theo tính chất, mức độ sẽ bị xem xét, xử lý theo quy định của pháp luật;

2. Định kỳ vào ngày 15 tháng 12 hằng năm hoặc đột xuất khi có yêu cầu, báo cáo kết quả hoạt động đánh giá sự phù hợp đã được chỉ định theo quy định tại Mẫu số 11 Phụ lục ban hành kèm theo Nghị định số 74/2018/NĐ-CP ngày 15/5/2018

của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 132/2008/NĐ-CP ngày 31/12/2008 của Chính phủ quy định chi tiết thi hành một số điều Luật Chất lượng sản phẩm, hàng hóa cho Bộ Khoa học và Công nghệ để tổng hợp;

3. Thông báo cho cơ quan chỉ định về mọi thay đổi có ảnh hưởng tới năng lực hoạt động thử nghiệm, giám định, kiểm định, chứng nhận đã được chỉ định trong thời hạn 15 ngày, kể từ ngày có sự thay đổi.

Điều 11. Trách nhiệm của Tổ chức được kiểm toán kỹ thuật

1. Thực hiện kiểm toán kỹ thuật định kỳ 02 năm; (theo quy định tại Khoản 2, Điều 31, Nghị định số 23/2025/NĐ-CP ngày 21/02/2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ tin cậy);

2. Chịu trách nhiệm trước pháp luật về tính trung thực, chính xác, hợp pháp của các thông tin, hồ sơ, tài liệu và bằng chứng cung cấp trong quá trình kiểm toán kỹ thuật;

3. Trong thời gian tối đa 05 (năm) ngày kể từ ngày nhận được kết quả kiểm toán kỹ thuật, tổ chức được kiểm toán phải gửi báo cáo kết quả kiểm toán kỹ thuật đến Trung tâm Chứng thực điện tử quốc gia để phục vụ mục đích quản lý và giám sát.

Điều 12. Trách nhiệm của cơ quan quản lý

1. Trách nhiệm của Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia

- Chủ trì, tham mưu để Bộ Khoa học và Công nghệ chỉ định tổ chức kiểm toán kỹ thuật theo quy định của Thông tư này.

- Quản lý hoạt động của các tổ chức kiểm toán kỹ thuật được chỉ định.

- Thanh tra, kiểm tra hoạt động đánh giá sự phù hợp của các tổ chức kiểm toán kỹ thuật được chỉ định theo quy định của pháp luật.

- Phối hợp với các đơn vị liên quan trong việc rà soát, cập nhật, hoàn thiện hệ thống tiêu chuẩn quốc gia, quy chuẩn kỹ thuật bắt buộc áp dụng phục vụ hoạt động kiểm toán kỹ thuật và đánh giá sự phù hợp trong lĩnh vực chữ ký điện tử, chứng thư điện tử và dịch vụ tin cậy.

- Tổ chức đào tạo, bồi dưỡng chuyên môn, nghiệp vụ cho đội ngũ chuyên gia kiểm toán kỹ thuật.

2. Trách nhiệm của Trung tâm Chứng thực điện tử quốc gia:

- Phối hợp với Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia trong hoạt động chỉ định và quản lý các tổ chức kiểm toán kỹ thuật theo quy định pháp luật.

- Làm đầu mối tiếp nhận báo cáo kiểm toán kỹ thuật từ các tổ chức được kiểm toán kỹ thuật;

- Tổng hợp, phân tích, đánh giá các tài liệu, kết quả liên quan đến kiểm toán kỹ thuật để hỗ trợ quản lý nhà nước đối với hoạt động cung cấp dịch vụ tin cậy và chữ ký điện tử chuyên dùng bảo đảm an toàn.

Điều 13. Tổ chức thực hiện và Hiệu lực thi hành

1. Thông tư có hiệu lực thi hành từ ngày ... tháng năm 2025./.

2. Trong thời hạn 3 (ba) năm kể từ ngày thông tư này có hiệu lực, các tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng đã được cấp phép theo Nghị định số 130/2018/NĐ-CP ngày 29/9/2018 của Chính phủ quy định chi tiết thi hành luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số phải lập kế hoạch và hoàn thành việc kiểm toán kỹ thuật lần đầu.

3. Trong quá trình tổ chức thực hiện, nếu có khó khăn, vướng mắc, tổ chức, cá nhân có liên quan cần phản ánh về Bộ Khoa học và Công nghệ (Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia và Trung tâm Chứng thực điện tử quốc gia) để kịp thời giải quyết.

Nơi nhận:

- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc TW;
- Sở KHCN các tỉnh, thành phố trực thuộc TW;
- Cục Kiểm tra văn bản QPPL (Bộ Tư pháp);
- Công báo, Cổng thông tin điện tử Chính phủ;
- Bộ KHCN: Bộ trưởng và các Thứ trưởng, các cơ quan, đơn vị thuộc Bộ;
- Cổng thông tin điện tử Bộ;
- Lưu: VT, NEAC (20b).

BỘ TRƯỞNG

Nguyễn Mạnh Hùng

Phụ lục 1**TIÊU CHÍ KIỂM TOÁN KỸ THUẬT**

(Ban hành kèm theo Thông tư số.....ngày..... tháng..... năm.....của Bộ trưởng Bộ Khoa học và Công nghệ)

1. Tiêu chí chung**a) Chính sách và Thực hành:**

- Tuyên bố Thực hành
- Điều khoản và Điều kiện
- Chính sách An ninh Thông tin

b) Quản lý và Vận hành:

- Tổ chức nội bộ (Độ tin cậy của tổ chức, Phân tách trách nhiệm)
- Nguồn nhân lực (Tuyển dụng, Đào tạo, Mô tả công việc, Xung đột lợi ích)
- Quản lý tài sản (Yêu cầu chung, Kiểm kê, Phân loại, Xử lý phương tiện)
- Kiểm soát truy cập
- Kiểm soát mật mã
- An ninh vật lý và môi trường
- An ninh vận hành
- An ninh mạng
- Quản lý sự cố
- Thu thập bằng chứng
- Quản lý tính liên tục trong kinh doanh
- Chấm dứt hoạt động của Tổ chức được kiểm toán và kế hoạch chấm dứt

2. Tiêu chí riêng đối với dịch vụ chứng thực chữ ký số**a) Quản lý vòng đời khoá**

- Tạo khoá
- Sao lưu và khôi phục khoá
- Phân phối khoá công khai
- Quản lý, Lưu trữ khoá, Huỷ khoá

- Thu hồi và cấp lại khoá
- Quản lý vòng đời thiết bị lưu trữ khoá
- Vận chuyển khoá/ Di chuyển khoá

b) Quản lý vòng đời chứng thư chữ ký số

- Đăng ký thuê bao
- Gia hạn chứng thư chữ ký số
- Cấp/Cấp lại chứng thư chữ ký số
- Phân phối chứng thư chữ ký số
- Tạm ngừng, Thu hồi chứng thư chữ ký số
- Xác thực chứng thư chữ ký số: CRL, OCSP
- Thông tin về chứng thư chữ ký

3. Tiêu chí riêng đối với dịch vụ cấp dấu thời gian

a) Thời gian

- Nguồn thời gian
- Độ chính xác thời gian
- Giám sát đồng bộ thời gian

b) Khoá

- Bảo vệ khoá
- Quản lý khoá TSA

c) Dấu thời gian

- Giao thức ký
- Dấu thời gian duy nhất
- Toàn vẹn dấu thời gian
- Định dạng và quy trình cấp dấu thời gian

4. Tiêu chí riêng đối với dịch vụ chứng thực thông điệp dữ liệu

a) Bảng chứng gửi nhận thông điệp

- Tạo và lưu bảng chứng gửi
- Tạo và lưu bảng chứng nhận

- Đảm bảo toàn vẹn bằng chứng
- Chuẩn định dạng và giao thức
- Xác thực danh tính người gửi, người nhận

b) Truy xuất và lưu trữ dữ liệu

- Truy xuất thông điệp và bằng chứng
- Lưu trữ an toàn và duy trì dài hạn giá trị bằng chứng