TRUNG TÂM CHỨNG THỰC ĐIỆN TỬ QUỐC GIA

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

BẢN TỔNG HỢP, TIẾP THU, GIẢI TRÌNH Ý KIẾN CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN ĐỐI VỚI DỰ THẢO TCVN GIAO DỊCH ĐIỆN TỬ - YÊU CẦU CHUNG VỀ KỸ THUẬT ĐỐI VỚI PHẦN MỀM KÝ SỐ, PHẦN MỀM KIỂM TRA CHỮ KÝ SỐ

Ngày 29/5/2026, Trung tâm Chứng thực điện tử quốc gia đã tiến hành xin ý kiến đối với dự thảo TCVN Giao dịch điện tử - Yêu cầu chung về kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số *(sau đây gọi tắt là Dự thảo TCVN)*.

Phòng Hạ tầng và Phát triển dịch vụ đã tổng hợp, tiếp thu, giải trình ý kiến đóng góp đối với Dự thảo TCVN, cụ thể như sau:

I. TỔNG SỐ Ý KIẾN NHẬN ĐƯỢC

Trung tâm Chứng thực điện tử quốc gia nhận được ý kiến đóng góp của các cơ quan, tổ chức sau:

- **05** Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ[1];

- **02** đơn vị thuộc Bộ KH&CN[2];

- **04** CA công cộng[3].

II. NỘI DUNG GÓP Ý CỤ THỂ

STT	Nội dung góp ý	Giải trình việc tiếp thu
I	**Các Bộ, Cơ quan ngang Bộ, cơ quan thuộc Chính phủ**	
1	**Bộ Quốc phòng**	
1.1	Đề nghị tại các mục 5.1.3, 5.1.5.1, nghiên cứu, chỉnh sửa, khuyến cáo sử dụng tiêu chuẩn ETSI 119 312 V2.1.1 (2026-06) (Lý do: phiên bản ETSI TS 119 312 V1.4.3 áp dụng tại Dự thảo chưa phù hợp. Phiên bản V2.1.1 có những khuyến cáo về sử dụng hàm băm trong bối cảnh hậu lượng	Tiếp thu ý kiến góp ý. NEAC đã chỉnh lý nội dung, khuyến nghị sử dụng tiêu chuẩn ETSI 119 312

[1] Bộ Quốc phòng, Bộ Công an, Bộ Nội vụ, Bộ Công thương, Ngân hàng nhà nước Việt Nam
[2] Vụ Pháp chế, Vụ Kinh tế & Xã hội số
[3] EFY-CA, Viettel-CA, VNPAY-CA, WINCA

	tử, khuyến cáo sử dụng hàm băm đối với chữ ký số lai (sử dụng cả khóa mật mã cổ điển và mật mã kháng lượng tử) cũng như ký số phục vụ lưu trữ lâu dài);	V2.1.1 thay cho phiên bản ETSI TS 119 312 V1.4.3 tại mục 5.1.3 và mục 5.1.5.1 của Dự thảo.
1.2	Nghiên cứu, bổ sung các thuật toán ký số kháng lượng tử như ML DSA, SLH-DSA, LMS và XMSS;	Tiếp thu ý kiến góp ý. NEAC sẽ nghiên cứu, đánh giá sự phù hợp của các thuật toán ký số kháng lượng tử (như ML-DSA, SLH-DSA, LMS, XMSS) trên cơ sở tiêu chuẩn, khuyến nghị quốc tế, mức độ hoàn thiện của công nghệ và khả năng đáp ứng của hạ tầng kỹ thuật để xem xét bổ sung vào Dự thảo khi đủ điều kiện.
1.3	Tại mục 5.1.4.1, nghiên cứu, chỉnh sửa khuyến cáo sử dụng giao thức HTTP/2 (Lý do: giao thức HTTP/1.1 áp dụng tại dự thảo hiện đang được đề xuất thay thế bởi giao thức HTTP/2).	Tiếp thu ý kiến góp ý. NEAC đã chỉnh lý nội dung, khuyến nghị sử dụng giao thức HTTP/2 thay cho giao thức HTTP/1 tại mục 5.1.4.1, của Dự thảo.
2	**Bộ Công an**	
2.1	Tại dự thảo Giao dịch điện tử - yêu cầu về phần mềm ký số, phần mềm kiểm tra chữ ký số, kiểm tra lại Mục 7, 8, 9, dự thảo đề cập đến nội dung Quy chuẩn kỹ thuật, đề nghị bỏ 03 mục này.	Tiếp thu ý kiến góp ý. NEAC đã rà soát, điều chỉnh Dự thảo theo hướng không quy định các nội dung về quy chuẩn kỹ thuật tại Mục 7, Mục 8 và Mục 9.
2.2	Tại dự thảo Yêu cầu về phần mềm ký số, phần mềm kiểm tra chữ ký số: (1) Sửa đổi viện dẫn 4.1.2.2 tại mục 5.1.5.2 thành mục 5.1.2.2; viện dẫn 4.1.1 tại mục 5.1.5.3 thành mục 5.1.1; (2) Sửa đổi viện dẫn 5.1 tại mục 6 thành 6.1, mục 5.1.1 tại mục 6.1.2.2 thành 6.1.1, mục 4.1.2.2 tại mục 6.1.3 thành mục 5.1.2.2	Tiếp thu ý kiến góp ý. NEAC đã rà soát, chỉnh sửa các viện dẫn tại các mục được góp ý, bảo đảm

		tính chính xác và thống nhất của dự thảo
3	**Bộ Nội vụ**	
3.1	Xem xét bổ sung vào yêu cầu phần mềm ký số phải hỗ trợ định dạng ký số lâu dài (như áp dụng đóng dấu thời gian) để bảo đảm hồ sơ lưu trữ vĩnh viễn không bị mất giá trị pháp lý khi chứng thư số hết hạn.	NEAC không bổ sung nội dung theo góp ý và xin được giải trình làm rõ như sau: Theo quy định tại điểm c khoản 1 Điều 19 Luật Giao dịch điện tử số 20/2023/QH15, trường hợp pháp luật yêu cầu chỉ ra thời gian liên quan đến chứng thư điện tử thì chứng thư điện tử phải có dấu thời gian. Như vậy, việc gắn dấu thời gian không phải là yêu cầu bắt buộc đối với mọi thông điệp dữ liệu mà phụ thuộc vào quy định của pháp luật chuyên ngành. Bên cạnh đó, Dự thảo quy định các yêu cầu kỹ thuật chung đối với phần mềm ký số và phần mềm kiểm tra chữ ký số, không quy định về giá trị pháp lý của thông điệp dữ liệu hoặc các trường hợp bắt buộc áp dụng dấu thời gian. Việc áp dụng dấu thời gian nhằm bảo đảm giá trị pháp lý của hồ sơ điện tử trong từng lĩnh vực phải thực hiện theo quy định của pháp luật chuyên ngành.

3.2	Tiêu chuẩn cần yêu cầu phần mềm kiểm tra chữ ký số có công cụ trực quan để cán bộ văn thư căn chỉnh, đặt vị trí con dấu, chữ ký mô phỏng đúng theo quy định về thể thức văn bản hành chính (không bị đè chữ, lệch trang).	Tiếp thu ý kiến góp ý. NEAC đã bổ sung các yêu cầu về giao diện đối với phần mềm ký số trong Dự thảo, làm cơ sở để phần mềm hỗ trợ người sử dụng trong việc hiển thị, bố trí và thao tác với chữ ký số, hình ảnh chữ ký và con dấu trên văn bản điện tử. Cụ thể tại các mục: 5.2.4, 5.2.5.
4	**Bộ Công thương**	
4.1	Không có ý kiến bổ sung	Ghi nhận ý kiến. Không có nội dung cần tiếp thu, chỉnh lý.
5	**Ngân hàng nhà nước Việt Nam**	
5.1	1. Chưa đề cập mật mã kháng lượng tử (PQC) Các dự thảo chưa đề cập đến mật mã kháng lượng tử Post-Quantum Cryptography (PQC). Năm 2024, NIST đã chính thức công bố FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) và FIPS 205 (SLH-DSA) – các thuật toán mật mã kháng lượng tử đầu tiên được chuẩn hóa ở cấp độ quốc gia. Đề nghị xem xét, cân nhắc bổ sung vào 04 dự thảo một điều khoản chung về "tính linh hoạt mật mã" (crypto agility), yêu cầu tất cả hệ thống ký số phải được thiết kế để có thể thay thế thuật toán mà không cần thiết kế lại toàn bộ, đồng thời tham chiếu đến lộ trình chuyển đổi PQC quốc gia.	Tiếp thu ý kiến góp ý. NEAC sẽ nghiên cứu, đánh giá tác động của việc áp dụng mật mã kháng lượng tử và các yêu cầu về tính linh hoạt mật mã (crypto agility) trên cơ sở các tiêu chuẩn, khuyến nghị quốc tế và điều kiện triển khai thực tế tại Việt Nam, để xem xét bổ sung trong dự thảo khi đủ điều kiện về công nghệ, tiêu chuẩn kỹ thuật và hạ tầng.

5.2	2. Thiếu nhất quán về JAdES Cả dự thảo TCVN 5 và dự thảo TCVN 8 đều xử lý JSON như một định dạng dữ liệu/giao thức, nhưng không quy định định dạng chữ ký số JAdES (ETSI EN 119 182-1:2021) tương ứng. Điều này tạo ra sự không nhất quán trong bộ tiêu chuẩn: JSON được thừa nhận ở cấp giao thức (Dự thảo TCVN 5) và cấp định dạng dữ liệu (Dự thảo TCVN 8), nhưng lại không có định dạng chữ ký số JSON tương ứng. Đề nghị xem xét, cân nhắc bổ sung JAdES vào Dự thảo TCVN 5 và Dự thảo TCVN 8.	Tiếp thu ý kiến góp ý. NEAC đã bổ sung nội dung về tiêu chuẩn JAdES tại mục 5.1.1 của Dự thảo, nhằm bảo đảm tính thống nhất giữa định dạng dữ liệu JSON và định dạng chữ ký số tương ứng.
5.3	3. Thiếu hướng dẫn cho môi trường cloud và kiến trúc hiện đại Toàn bộ dự thảo TCVN ngầm giả định môi trường triển khai on-premise truyền thống. Trong khi đó, thực tế triển khai của các tổ chức lớn ngày càng có xu hướng chuyển sang điện toán đám mây với kiến trúc vi dịch vụ (microservices), container (Kubernetes/Docker) và dịch vụ HSM đám mây. Các dự thảo TCVN chưa định hướng cho các môi trường này dẫn đến việc triển khai đám mây không tuân thủ tiêu chuẩn. Đề nghị xem xét bổ sung vào dự thảo TCVN 6 và dự thảo TCVN 7 hướng dẫn về các yêu cầu bảo mật bổ sung khi triển khai TW4S và SAM/QSCD trong môi trường điện toán đám mây.	Tiếp thu ý kiến góp ý. NEAC đã rà soát, bổ sung các nội dung liên quan đến yêu cầu triển khai trong môi trường điện toán đám mây và các yêu cầu bảo mật tương ứng trong Dự thảo, phù hợp với phạm vi điều chỉnh của từng tiêu chuẩn.
5.4	4. Chưa có audit trail xuyên suốt end-to-end Mỗi dự thảo quy định yêu cầu kiểm toán (audit log) cho từng thành phần riêng lẻ: SSASC, SAM, phần mềm ký số... Tuy nhiên, không có yêu cầu nào về việc liên kết và tương quan (correlate) các log từ các thành phần khác nhau để có thể truy vết hoàn chỉnh một giao dịch ký từ đầu đến cuối (SIC → SCASC → SSASC → SAM → CM). Trong trường hợp xảy ra tranh chấp pháp lý hoặc điều tra sự cố, chuỗi bằng chứng không liên tục có thể làm giảm giá trị chứng cứ của hệ thống ký số. Đề nghị xem xét bổ sung yêu cầu mỗi giao dịch ký phải được gắn một mã định danh duy nhất (transaction ID) xuyên suốt tất cả các thành phần, đảm bảo khả năng truy vết toàn bộ chuỗi xử lý.	Tiếp thu ý kiến góp ý. NEAC sẽ nghiên cứu, đánh giá tác động của việc bổ sung các yêu cầu về audit trail và khả năng truy vết xuyên suốt đối với giao dịch ký số trên cơ sở bảo đảm tính khả thi, yêu cầu kỹ thuật và phạm vi điều chỉnh của các dự thảo.
5.5	5. Các ý kiến khác - Sửa lỗi tham chiếu nội bộ trong dự thảo TCVN 8 ("Mục 4.1.x" thành "Mục 5.1.x"); Xem xét, cân nhắc đưa yêu cầu TLS lên tối thiểu TLS 1.3; cập nhật RFC 3447 thành RFC 8017; cân nhắc bổ sung điều khoản cấm sử dụng SHA-1; pin phiên bản CSC API.	Tiếp thu ý kiến góp ý. NEAC đã rà soát, cập nhật và chỉnh sửa các nội dung được góp ý trong Dự thảo bao gồm các lỗi tham chiếu, cập

		nhật tiêu chuẩn và tài liệu viện dẫn, đồng thời bổ sung, điều chỉnh các yêu cầu kỹ thuật phù hợp.
II	**Đơn vị thuộc Bộ Khoa học và Công nghệ**	
6	**Vụ Pháp chế**	
6.1	Điều 23 Luật Tiêu chuẩn và Quy chuẩn kỹ thuật quy định: "Tiêu chuẩn được áp dụng trên nguyên tắc tự nguyện", tuy nhiên các dự thảo TCVN đang sử dụng nhiều từ "phải" trong các nội dung dẫn chiếu, áp dụng các tiêu chuẩn quốc tế; đồng thời quy định quản lý, trách nhiệm của tổ chức, cá nhân; tổ chức phải thực hiện;.... Đề nghị cơ quan chủ trì rà soát và chỉnh lý để đảm bảo không đặt ra nghĩa vụ pháp lý hay làm cho TCVN trở thành văn bản bắt buộc áp dụng. - TCVN "Yêu cầu về phần mềm ký số, phần mềm kiểm tra chữ ký số": đề nghị cân nhắc bỏ viện dẫn văn bản quy phạm trong toàn bộ dự thảo TCVN, (vd:Thông tư số 15/2025/TT-BKHCN). Lý do: thông tư là văn bản quy phạm pháp luật có tính bắt buộc áp dụng, việc viện dẫn thông tư trong TCVN có thể khiến TCVN thành văn bản bắt buộc áp dụng/hướng dẫn thi hành thông tư, đề nghị đơn vị chủ trì cân nhắc.	Tiếp thu ý kiến góp ý. NEAC đã rà soát, chỉnh lý Dự thảo theo hướng bảo đảm phù hợp với nguyên tắc áp dụng tự nguyện của tiêu chuẩn quy định tại Luật Tiêu chuẩn và Quy chuẩn kỹ thuật; đồng thời rà soát, điều chỉnh các nội dung viện dẫn và cách diễn đạt để tránh làm phát sinh cách hiểu TCVN là văn bản quy định nghĩa vụ pháp lý hoặc có tính bắt buộc áp dụng.
7	**Vụ Kinh tế và Xã hội số**	
7.1	a) Mâu thuẫn cơ bản về thể thức pháp lý (Tiêu chuẩn vs. Quy chuẩn): - Tài liệu có tiêu đề là "TIÊU CHUẨN QUỐC GIA TCVN xxxx:2026". - Tuy nhiên, ở phần cuối (Mục 8 và Mục 9), tài liệu lại yêu cầu các cá nhân, tổ chức phải "thực hiện theo các quy định trong Quy chuẩn kỹ thuật này".	Tiếp thu ý kiến góp ý. NEAC đã chỉnh sửa các nội dung sử dụng chưa thống nhất giữa "tiêu chuẩn" và "quy chuẩn kỹ thuật" trong Dự thảo bảo đảm thống nhất về thuật ngữ và thể thức trình bày.

7.2	b) Lỗi biên tập và tham chiếu chéo lộn xộn: - Dự thảo chứa rất nhiều lỗi đánh số mục bị sai lệch hoàn toàn so với cấu trúc thực tế của nó. Ví dụ: Đầu Mục 5 yêu cầu phần mềm ký số đáp ứng chức năng nêu ở "mục 4.1". Tuy nhiên, các yêu cầu này thực tế nằm ở Mục 5.1. - Mục 5.1.5.2 yêu cầu tuân thủ điều kiện nêu tại "mục 4.1.2.2", nhưng đúng ra phải là 5.1.2.2. - Mục 5.1.5.3 yêu cầu tuân thủ định dạng tại "mục 4.1.1", nhưng đúng ra phải là 5.1.1. - Mục 6 yêu cầu đáp ứng chức năng ở "mục 5.1", nhưng thực tế cấu trúc yêu cầu của nó nằm ở Mục 6.1. Các tiểu mục 6.1.2.2 và 6.1.3 cũng tham chiếu ngược sai về các mục 5.1.1 và 4.1.2.2.	Tiếp thu ý kiến góp ý. NEAC đã rà soát tổng thể và chỉnh sửa các lỗi về đánh số, tham chiếu chéo và viện dẫn nội bộ trong Dự thảo bảo đảm các nội dung được dẫn chiếu thống nhất, chính xác và phù hợp với cấu trúc của Dự thảo.
7.3	c) Về tiêu chuẩn quốc tế và an toàn thông tin: Văn bản quy định yêu cầu sử dụng chuẩn bảo mật đường truyền tối thiểu là TLS 1.2. Mặc dù TLS 1.2 vẫn đang được chấp nhận rộng rãi, tuy nhiên đối với các hệ thống yêu cầu độ bảo mật cao tính tới thời điểm năm 2026, các chuẩn quốc tế (như NIST hay IETF) đều đang khuyến nghị hoặc bắt buộc chuyển dịch sang TLS 1.3 để vá các điểm yếu của bản cũ. Nhìn chung các chuẩn kỹ thuật khác (RSA >= 2048, ECDSA >= 256) được liệt kê trong văn bản vẫn tuân thủ tương đối tốt các khuyến nghị quốc tế hiện hành.	Tiếp thu ý kiến góp ý. NEAC đã rà soát, cập nhật các yêu cầu kỹ thuật về bảo mật đường truyền tại Mục 5.1.4.1 của Dự thảo, bảo đảm phù hợp với các tiêu chuẩn, khuyến nghị quốc tế hiện hành và yêu cầu an toàn thông tin trong quá trình triển khai.
III	**Các tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng**	
8	**EFY-CA**	
8.1	- Mục 5.1: Tham chiếu nội dung mục 4.1.	Tiếp thu ý kiến góp ý.

	Ý kiến của EFY: Tham chiếu nội dung chưa đúng. - Mục 5.1.5.2, 5.1.5.3, 6, 6.1.2.2, 6.1.3: Tham chiếu nội dung tại Mục 4.x. Ý kiến của EFY: Tham chiếu nội dung chưa đúng. - Mục 5.2.3: các thông báo bằng chữ hoặc ký hiệu cho chủ thể ký biết việc ký số vào thông điệp dữ liệu thành công hay không thành công phải được thể hiện bằng tiếng Việt. Ý kiến của EFY: Đề xuất thể hiện thông báo bằng tiếng Việt (bắt buộc) hoặc ngôn ngữ khác (nếu hỗ trợ). - Điểm c, mục 6.2.2: thông tin về đơn vị quản lý chứng thư chữ ký số. Ý kiến của EFY: Đề xuất "Thông tin về đơn vị quản lý chứng thư chữ ký số (nếu có)" do có thể phát sinh trường hợp như chứng thư chữ ký số cá nhân thì không có đơn vị quản lý chứng thư chữ ký số.	NEAC đã chỉnh sửa các lỗi tham chiếu trong Dự thảo, đồng thời rà soát, bổ sung và hoàn thiện một số quy định về ngôn ngữ hiển thị thông báo và thông tin về đơn vị quản lý chứng thư chữ ký số để bảo đảm tính thống nhất và phù hợp với thực tế triển khai.
9	**VNPAY-CA**	
9.1	Góp ý 1: Tại mục 5.1 có mô tả "Phần mềm ký số phải đáp ứng tối thiểu các chức năng được nêu ở mục 4.1. Yêu cầu về chức năng": Nhóm soạn thảo cần hiệu chỉnh lại đầu mục tham chiếu.	Tiếp thu ý kiến góp ý. NEAC đã rà soát, chỉnh sửa nội dung tham chiếu trong Dự thảo, bảo đảm thống nhất với cấu trúc và nội dung của Dự thảo.
9.2	Góp ý 2: Tại mục 5.1.5.2 có mô tả "… đảm bảo tuân thủ các điều kiện được nêu tại mục 4.1.2.2. Xác thực thông tin chứng thư chữ ký số của chủ thể ký": Nhóm soạn thảo cần hiệu chỉnh lại đầu mục tham chiếu.	Tiếp thu ý kiến góp ý. NEAC đã rà soát, chỉnh sửa nội dung tham chiếu trong Dự thảo, bảo đảm thống nhất với cấu trúc và nội dung của Dự thảo.

9.3	Góp ý 3: Tại mục 5.1.5.3 có mô tả "…tuân thủ theo đúng các định dạng được nêu tại mục 4.1.1. Chuyển đổi định dạng thông điệp dữ liệu": Nhóm soạn thảo cần hiệu chỉnh lại đầu mục tham chiếu.	Tiếp thu ý kiến góp ý. NEAC đã rà soát, chỉnh sửa nội dung tham chiếu trong Dự thảo, bảo đảm thống nhất với cấu trúc và nội dung của Dự thảo.
9.4	Góp ý 4: Tại mục 6.1.3 có mô tả "… phải thỏa mãn các quy định tại Mục 4.1.2.2. Xác thực thông tin chứng thư chữ ký số của chủ thể ký": Nhóm soạn thảo cần hiệu chỉnh lại đầu mục tham chiếu.	Tiếp thu ý kiến góp ý. NEAC đã rà soát, chỉnh sửa nội dung tham chiếu trong Dự thảo, bảo đảm thống nhất với cấu trúc và nội dung của Dự thảo.
10	**WINCA**	
10.1	5.1. Yêu cầu về giao diện - Góp ý: cần có quy định hiển thị toàn bộ nội dung tài liệu ký trước khi ký, đảm bảo đáp ứng yêu cầu What You See Is What You Sign (WYSIWYS). - Phần mềm ký số phải đảm bảo rằng người ký thực hiện ký là chỉ ký tài liệu mà người ký đã nhìn thấy và chấp thuận dữ liệu được ký. Tránh trường hợp ký ngầm thêm 1 hoặc nhiều tài liệu nào khác mà người ký không được biết.	Tiếp thu ý kiến góp ý. NEAC đã bổ sung, hoàn thiện các yêu cầu về giao diện đối với phần mềm ký số tại mục 5.2.3 của Dự thảo. Theo đó, giao diện phần mềm ký số bảo đảm yêu cầu hiển thị toàn bộ nội dung tài liệu ký trước khi ký, đáp ứng sự chấp thuận của chủ thể ký về mặt nội dung thông điệp dữ liệu.
10.2	5.2. Trên thị trường có quá nhiều phần mềm ký số của nhà nước và tư nhân. - Góp ý: cần có chính sách/quy định quản lý hoặc đánh giá/lôi kéo các phần mềm ký số/kiểm tra chữ ký số đạt chuẩn và khuyến nghị sử dụng.	Tiếp thu ý kiến góp ý. Nội dung về đánh giá, kiểm tra, khuyến nghị sử dụng hoặc xây dựng phần mềm ký số, phần mềm kiểm tra chữ ký số dùng

	- Cần xây dựng/phát hành 1 phần mềm chung đáp ứng tiêu chuẩn TCVN, làm cơ sở cho các đơn vị/cơ quan/tổ chức phát triển phần mềm ký số thực hiện tích hợp và mang lại trải nghiệm thống nhất cho người dùng cuối.	chung không thuộc phạm vi điều chỉnh của Dự thảo. Tuy nhiên, NEAC sẽ nghiên cứu việc xây dựng các tài liệu, báo cáo đánh giá đối với phần mềm ký số và phần mềm kiểm tra chữ ký số để các cơ quan, tổ chức, doanh nghiệp tham khảo trong quá trình triển khai.
11	**Viettel-CA**	
11.1	Không có ý kiến bổ sung	Ghi nhận ý kiến. Không có nội dung cần tiếp thu, chỉnh lý.