BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CHỨNG THỰC ĐIỆN TỬ QUỐC GIA

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

BẢNG TỔNG HỢP, TIẾP THU, GIẢI TRÌNH Ý KIẾN CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN VÀ ĐỐI TƯỢNG CHỊU SỰ TÁC ĐỘNG TRỰC TIẾP ĐỐI VỚI DỰ THẢO TIÊU CHUẨN VIỆT NAM GIAO DỊCH ĐIỆN TỬ - GIAO THỨC CẤP DẤU THỜI GIAN CHO DỊCH VỤ TIN CẬY

Ngày 03/7/2026, Trung tâm Chứng thực điện tử quốc gia đã tiến hành xin ý kiến đối với dự thảo TCVN Giao dịch điện tử - Giao thức cấp dấu thời gian cho dịch vụ tin cậy (sau đây gọi tắt là Dự thảo TCVN).

Chi nhánh Hồ Chí Minh 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:

- 02 Bộ ngành ;
- 01 đơn vị thuộc Bộ KH&CN;
- 01 đơn vị CA công cộng.

STT	Nhóm vấn đề, điều, khoản	Chủ thể góp ý	Nội dung góp ý	Nội dung tiếp thu, giải trình
A	**CÁC Ý KIẾN NHẤT TRÍ**			
I	**Các Bộ, cơ quan ngang Bộ**			
II	**Các đơn vị trong Bộ**			
III	**Các Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng**			
IV	**UBND/Sở KH&CN các tỉnh, thành phố trực thuộc Trung ương**			
B	**CÁC Ý KIẾN GÓP Ý**			
I	**Cổng thông tin điện tử của Chính phủ**			
1.	Bộ Tài Chính			
2.	Bộ Nội Vụ			
II	**Cổng thông tin điện tử của Bộ**			
1.	Vụ KTS&XHS			
III.	**Các Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng**			
1.	Tổng Công ty Viễn thông Viettel – Viettel-CA			
	CÁC Ý KIẾN GÓP Ý ĐỐI VỚI DỰ THẢO THÔNG TƯ TCVN			
I	**Các Bộ, Cơ quan ngang Bộ, cơ quan trực thuộc Chính phủ**			
		Bộ Tài Chính	Dự thảo đang khuyến nghị ưu tiên sử dụng giao thức bảo mật HTTPS (RFC 2818) thay thế cho HTTP thông thường, đề nghị cơ quan soạn thảo điều chỉnh thành yêu cầu bắt buộc sử dụng giao thức bảo mật HTTPS thay thế cho HTTP để bảo	Tiếp thu ý kiến góp ý, bảo lưu nội dung hiện tại; Giải trình lý do bảo lưu như sau: Tại Mục 7 của dự thảo TCVN quy định: "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

			đảm tính an toàn, toàn vẹn và bảo mật dữ liệu trong quá trình truyền tải bản tin trên môi trường mạng.	RFC 7230 đến RFC 7235) hoặc HTTPS (IETF RFC 2818)". Đồng thời, dự thảo đã ghi rõ: "Khuyến nghị ưu tiên sử dụng giao thức bảo mật HTTPS (RFC 2818) thay thế cho giao thức HTTP". Lý do bảo lưu: - Đây là TCVN (tiêu chuẩn quốc gia) mang tính khuyến nghị, không phải QCVN (quy chuẩn quốc gia) mang tính bắt buộc. Việc quy định bắt buộc sử dụng HTTPS thuộc phạm vi quy chuẩn kỹ thuật; - Tiêu chuẩn gốc IETF RFC 3161 (Mục 3.4) và ETSI EN 319 422 đều quy định hỗ trợ cả HTTP và HTTPS, với HTTPS là khuyến nghị ưu tiên; - Trong thực tế triển khai, một số môi trường mạng nội bộ (intranet) có thể sử dụng HTTP với các biện pháp bảo mật khác (VPN, mạng riêng) mà không nhất thiết phải sử dụng HTTPS; - Việc bắt buộc HTTPS trong tiêu chuẩn có thể tạo rào cản không cần thiết cho một số trường hợp triển khai hợp lệ. Yêu cầu bắt buộc về bảo mật giao thức nên được quy định tại văn bản quy phạm pháp luật hoặc quy chuẩn kỹ thuật có liên quan.
			Quy chuẩn độ dài khóa RSA (Mục 4.2.4 & Mục 6.3): Bảng khuyến	Tiếp thu ý kiến góp ý. Nội dung tiếp thu đã được chỉnh sửa trong dự thảo

			nghị độ dài khóa áp dụng mức ≥ 1900 bits cho thuật toán RSA, đang thấp hơn mức tối thiểu 2048 bits được quy định tại Quy chuẩn kỹ thuật bắt buộc QCVN 138:2025/BKHCN. Trong thực tế triển khai hạ tầng PKI và thiết bị phần cứng (HSM), độ dài khóa RSA thường được cấu hình theo lũy thừa 2 (như 2048, 3072, 4096 bits). Do đó cơ quan soạn thảo nên điều chỉnh hoặc bổ sung chú thích quy đổi mức tối thiểu lên ≥ 2048 bits để phù hợp với thực tế triển khai thiết bị an toàn bảo mật.	TCVN. Ban biên soạn đã chỉnh sửa toàn bộ các bảng khuyến nghị độ dài khóa RSA trong dự thảo TCVN từ ≥ 1900 bits thành ≥ 2048 bits, cụ thể: - Bảng 3 Độ dài khoá của các thuật toán theo thời gian (Mục 4.2.4): Khuyến nghị độ dài khóa RSA ≥ 2048 bits; - Bảng 4 Bộ thuật toán cho khả năng chống chịu của thuật toán theo thời gian (Mục 4.2.4): Khuyến nghị các bộ thuật toán ≥ 2048 bits; - Mục 6.3: Bảng khuyến nghị độ dài khóa cho chứng thư chữ ký số TSA ≥ 2048 bits.
			Tại dự thảo sử dụng khái niệm TSA (Tổ chức cung cấp dịch vụ cấp dấu thời gian) để thay thế cho 02 khái niệm TSU (Time-Stamping Unit) và TSA (Time-Stamping Authority) trong tiêu chuẩn gốc ETSI EN 319 422. Đề nghị đơn vị soạn thảo bổ sung ghi chú giải thích lý do gộp hai khái niệm này thành một, để đơn vị đối chiếu với bản tiêu chuẩn gốc không bị nhầm lẫn.	Tiếp thu ý kiến góp ý, bảo lưu nội dung hiện tại; Giải trình lý do bảo lưu như sau: Ban biên soạn đã bổ sung ghi chú giải thích trong phần "Lời nói đầu" và tại Mục 3.1.5 (Thuật ngữ và định nghĩa) về lý do gộp hai khái niệm TSU (Time-Stamping Unit) và TSA (Time-Stamping Authority) thành một khái niệm TSA duy nhất. Lý do gộp: - Theo quy định tại Nghị định 23 tại Điều 4 Khoản 1 quy định chứng thư chữ ký số gốc của tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia là

				chứng thư do chính tổ chức này tự cấp cho mình. Khoản 2 tiếp tục quy định chứng thư chữ ký số của tổ chức cung cấp dịch vụ tin cậy do tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia cấp, trong đó nêu rõ có "chứng thư chữ ký số cho dịch vụ cấp dấu thời gian".- Mô hình quốc tế theo ETSI EN 319 422 áp dụng mô hình 3 cấp, trong đó TSA là tổ chức quản lý và TSU là đơn vị vận hành hệ thống cấp dấu thời gian nằm dưới quyền quản lý của TSA; - Mô hình quốc tế theo ETSI EN 319 422 áp dụng mô hình 3 cấp, trong đó TSA là tổ chức quản lý và TSU là đơn vị vận hành hệ thống cấp dấu thời gian nằm dưới quyền quản lý của TSA; - Mô hình triển khai dịch vụ cấp dấu thời gian tại Việt Nam chỉ có 2 cấp, trong đó TSA vừa là tổ chức cung cấp dịch vụ vừa trực tiếp vận hành thiết bị cấp dấu thời gian. TSA đóng vai trò thực thể đầu cuối, cung cấp dịch vụ trực tiếp qua tài khoản thuê bao; - Việc gộp khái niệm giúp đơn giản hóa và phù hợp với mô hình cung cấp dịch vụ tại Việt Nam, tránh gây nhầm lẫn khi không tồn tại cấp TSU riêng biệt trong thực tế triển khai.
			Đồng bộ thời gian chuẩn (Mục 5.2.2): Trường accuracy bắt buộc hỗ trợ độ sai lệch thời gian tối đa là	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo

			1 giây so với nguồn thời gian chuẩn. Do đó, cần bổ sung quy định rõ nguồn thời gian chuẩn phải được đồng bộ theo Chuẩn giờ quốc gia (UTC-VN) do cơ quan thẩm quyền quốc gia về đo lường/thời gian quản lý.	TCVN như sau: - 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; Lý do: Nguồn thời gian theo quy định của pháp luật về nguồn thời gian chuẩn quốc gia (quy định tại điểm a khoản 5 điều 18 Nghị định 23/NĐ-CP quy định chữ ký điện tử và dịch vụ tin cậy)
			Tại Mục 9 để phân định rõ các yêu cầu áp dụng bắt buộc tại Việt Nam và các yêu cầu nhằm phục vụ tương thích quốc tế. Đề nghị đơn vị soạn thảo nghiên cứu chuyển các yêu cầu liên quan đến Quy định (EU) số 910/2014 từ tính chất bắt buộc sang tùy chọn tham khảo, chỉ áp dụng khi có nhu cầu tương thích hoặc cung cấp dịch vụ theo khung pháp lý của EU.	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo TCVN như sau: Dự thảo đổi phạm vi từ yêu cầu có điều kiện đối với "qualified electronic time-stamp" của EU thành "các yêu cầu bổ sung đối với dấu thời gian điện tử", đồng thời quy định bắt buộc qcStatements đối với tổ chức cung cấp dịch vụ cấp dấu thời gian. Các khai báo ASN.1 của Phụ lục B được đưa trực tiếp vào Điều 9. Bổ sung Chú thích 1 để xác định phạm vi bắt buộc đối với tổ chức cung cấp dịch vụ cấp dấu thời gian và lựa chọn áp dụng đối với hệ thống khác; bổ sung Chú thích 2 để giải thích ý nghĩa của việc tích hợp tuyên bố. Đây là thay đổi phạm vi và

				mức độ bắt buộc so với ETSI EN 319 422, không phải chuyển tương đương.
		Bộ Nội Vụ	Tại Mục 5.2.2 quy định 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 chuẩn. Đề nghị làm rõ "nguồn thời gian chuẩn" được sử dụng làm căn cứ đối chiếu, kiểm tra; nghiên cứu quy định theo hướng sử dụng Giờ chuẩn quốc gia Việt Nam hoặc nguồn thời gian được cơ quan có thẩm quyền công nhận. Lý do: Dự thảo quy định độ sai lệch thời gian tối đa là 01 giây nhưng chưa xác định cụ thể nguồn thời gian chuẩn làm căn cứ đối chiếu. Việc xác định rõ nguồn thời gian chuẩn sẽ bảo đảm tính thống nhất, khách quan và khả năng kiểm tra, đánh giá, nghiệm thu khi áp dụng tiêu chuẩn.	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo TCVN như sau: - 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; Lý do: Nguồn thời gian theo quy định của pháp luật về nguồn thời gian chuẩn quốc gia (quy định tại điểm a khoản 5 điều 18 Nghị định 23/NĐ-CP quy định chữ ký điện tử và dịch vụ tin cậy)
II	**Các đơn vị trong Bộ**			
		Vụ KTS&XHS	Theo chuẩn quốc tế, tổ chức cung cấp dịch vụ (TSA) có thể áp dụng chứng thư cho thể nhân (ETSI EN 319 412-	Tiếp thu ý kiến góp ý, bảo lưu; Giải trình lý do bảo lưu như sau: - Theo quy định tại Nghị định 23 tại Điều

			2) hoặc pháp nhân (ETSI EN 319 412-3). Tuy nhiên, Mục 6.1 của tài liệu chỉ yêu cầu chứng thư chữ ký số của TSA đáp ứng tiêu chuẩn ETSI EN 319 412-3 (hồ sơ chứng thư cấp cho pháp nhân) tạo ra sự chưa thống nhất so với Mục 2 (Tài liệu viện dẫn) liệt kê cả tiêu chuẩn ETSI EN 319 412-2 (hồ sơ chứng thư cấp cho thể nhân) làm mất đi tính nguyên bản của ETSI EN 319 422.	4 Khoản 1 quy định chứng thư chữ ký số gốc của tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia là chứng thư do chính tổ chức này tự cấp cho mình. Khoản 2 tiếp tục quy định chứng thư chữ ký số của tổ chức cung cấp dịch vụ tin cậy do tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia cấp, trong đó nêu rõ có "chứng thư chữ ký số cho dịch vụ cấp dấu thời gian".- Mô hình quốc tế theo ETSI EN 319 422 áp dụng mô hình 3 cấp, trong đó TSA là tổ chức quản lý và TSU là đơn vị vận hành hệ thống cấp dấu thời gian nằm dưới quyền quản lý của TSA; - Mô hình triển khai dịch vụ cấp dấu thời gian tại Việt Nam chỉ có 2 cấp, trong đó TSA vừa là tổ chức cung cấp dịch vụ vừa trực tiếp vận hành thiết bị cấp dấu thời gian. TSA đóng vai trò thực thể đầu cuối, cung cấp dịch vụ trực tiếp qua tài khoản thuê bao; - Việc gộp khái niệm giúp đơn giản hóa và phù hợp với mô hình cung cấp dịch vụ tại Việt Nam, tránh gây nhầm lẫn khi không tồn tại cấp TSU riêng biệt trong thực tế triển khai.
			Tại Mục 4.1.3 và Mục 5.1.3 định dạng cho "bản tin yêu cầu" (Request message format) nhưng lại đưa "Thuật toán ký" vào bảng. Về mặt kỹ thuật theo chuẩn RFC 3161, bản tin yêu cầu cấp dấu thời gian (TimeStampReq) từ máy khách gửi	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo tại nội dung bảng mục 4.1.3 và bảng 5.1.3 đã bỏ nội dung về "Thuật toán ký" cho "Mã thông báo dấu thời gian".

			lên máy chủ chỉ chứa mã băm (hash) của dữ liệu, không hề mang thuật toán chữ ký. Việc áp đặt máy khách phải hỗ trợ thuật toán ký (RSA, DSA...) cho bản tin yêu cầu là sai lệch kiến trúc giao thức. Thuật toán ký chỉ xuất hiện ở bước tạo lập bản tin phản hồi (của Server) và bước xác minh (của Client).	
			Tại Mục 4.2.3 "Yêu cầu kỹ thuật đối với định dạng bản tin trả lời" (Response). Tuy nhiên, bảng liệt kê thuật toán bên dưới lại ghi sai tiêu đề cột thành "Mã thông báo dấu thời gian yêu cầu".	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo tại nội dung mục 4.2.3 sửa tên bảng thành "Bảng 2 - khuyến nghị các thuật toán ký của mã thông báo dấu thời gian".
			Tại Mục 5.1.3 "Yêu cầu kỹ thuật đối với định dạng bản tin yêu cầu" (dành cho máy chủ xử lý). Tuy nhiên, các cột trong bảng lại phân chia thành "Mã thông báo dấu thời gian phát hành" và "Mã thông báo dấu thời gian xác minh". Thao tác phát hành và xác minh diễn ra ở bản tin trả lời (Response), không nằm trong bản tin yêu cầu.	Tiếp thu ý kiến góp ý, bảo lưu nội dung hiện tại; Giải trình lý do bảo lưu như sau: Tại Bảng 5 (Mục 5.1.3) của dự thảo TCVN, các cột "Mã thông báo dấu thời gian phát hành" và "Mã thông báo dấu thời gian xác minh" phản ánh đúng quy định tại Mục A.8 của tiêu chuẩn ETSI TS 119 312 về yêu cầu thuật toán cho máy chủ cấp dấu thời gian (TSA). Lý do bảo lưu:

				- Theo ETSI TS 119 312, máy chủ TSA có hai vai trò khác nhau: phát hành (issuance) và xác minh (verification). Mỗi vai trò có yêu cầu thuật toán khác nhau; - Khi phát hành dấu thời gian: máy chủ phải hỗ trợ SHA-256, nên hỗ trợ SHA-384, SHA-512; - Khi xác minh dấu thời gian: máy chủ phải hỗ trợ cả SHA-256, SHA-384 và SHA-512 (yêu cầu nghiêm ngặt hơn vì cần đọc được mọi dấu thời gian đã phát hành trước đó); - Đây là phân biệt theo vai trò của máy chủ (phát hành và xác minh), không phải theo loại bản tin (yêu cầu hay phản hồi). Cấu trúc này hoàn toàn phù hợp với tiêu chuẩn gốc ETSI EN 319 422; - So sánh: Bảng 1 (Mục 4.1.3) dành cho máy khách chỉ có 1 cột "yêu cầu" vì máy khách chỉ gửi yêu cầu, trong khi Bảng 5 (Mục 5.1.3) dành cho máy chủ cần 2 cột vì máy chủ vừa phát hành vừa xác minh dấu thời gian.
			Tại Mục 4.2.4 và Mục 6.3 "Bảng	Tiếp thu ý kiến góp ý. Nội dung tiếp

			khuyến nghị độ dài khoá của các thuật toán theo thời gian" đưa ra khuyến nghị độ dài khóa cho thuật toán RSA là >= 1900 bits hiện nay không còn phù hợp để ứng dụng trong thực tế và cũng không vượt qua được các yêu cầu an toàn của Việt Nam hiện hành (ví dụ: QCVN 139:2025/BKHCN thường yêu cầu khóa RSA tối thiểu 2048 bits)	thu được chỉnh sửa trong dự thảo tại nội dung liên quan về độ dài khoá Ban biên soạn đã chỉnh sửa các thuật toán liên quan đền RSA từ >= 1900 sửa thành “>=2048” mục 4.2.4 sửa tên bảng thành “Bảng 3 - Độ dài khoá của các thuật toán theo thời gian”, “Bảng 4 – Bộ thuật toán cho khả năng chống chịu của thuật toán theo thời gian”
			"Dấu thời gian điện tử đủ điều kiện" (Qualified electronic time-stamp) để chỉ các dấu thời gian tuân thủ quy định EU 910/2014. Mặc dù đây là cách dịch sát nghĩa, nhưng trong bối cảnh pháp lý Việt Nam, cần làm rõ liệu "đủ điều kiện" ở đây có đồng nhất hoàn toàn với các quy định pháp luật về chữ ký số/dịch vụ tin cậy của Việt Nam hay không.	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo TCVN như sau: Dự thảo đổi phạm vi từ yêu cầu có điều kiện đối với “qualified electronic time-stamp” của EU thành “các yêu cầu bổ sung đối với dấu thời gian điện tử”, đồng thời quy định bắt buộc qcStatements đối với tổ chức cung cấp dịch vụ cấp dấu thời gian. Các khai báo ASN.1 của Phụ lục B được đưa trực tiếp vào Điều 9. Bổ sung Chú thích 1 để xác định phạm vi bắt buộc đối với tổ chức cung cấp dịch vụ cấp dấu thời gian và lựa chọn áp dụng đối với hệ thống khác; bổ sung Chú thích 2 để giải thích ý nghĩa của việc tích hợp tuyên bố. Đây là thay đổi phạm vi và mức độ bắt buộc so với ETSI EN 319 422, không phải chuyển tương đương.

			"Cũ/kế thừa" (Legacy) trong các bảng khuyến nghị độ dài khóa, từ "Legacy" được dịch là "cũ/kế thừa". Về mặt kỹ thuật, thuật ngữ này trong tiêu chuẩn gốc ám chỉ các thuật toán không còn được khuyến khích sử dụng cho các hệ thống mới do độ an toàn thấp. Việc dịch là "cũ/kế thừa" có thể gây hiểu lầm cho người vận hành rằng chúng vẫn được chấp nhận như một phương án thay thế hợp lệ, trong khi thực tế là nên loại bỏ	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo TCVN. Ban biên soạn nhận thấy ý kiến góp ý là xác đáng. Thuật ngữ "Legacy" trong tiêu chuẩn gốc ETSI TS 119 312 ám chỉ các thuật toán đã lỗi thời, không còn được khuyến nghị cho hệ thống mới do độ an toàn không đảm bảo. Việc dịch là "cũ/kế thừa" có thể gây hiểu nhầm rằng các thuật toán này vẫn được chấp nhận sử dụng. Ban biên soạn đã chỉnh sửa thuật ngữ "cũ/kế thừa" thành "không khuyến nghị cho hệ thống mới" tại Bảng 4 (Mục 4.2.4) để phản ánh đúng bản chất kỹ thuật của thuật ngữ gốc, tránh gây nhầm lẫn cho người vận hành hệ thống.
			Tiêu chuẩn đưa vào các thuật toán hậu lượng tử (PQC) như SLH-DSA, XMSS, LMS là điểm "điều chỉnh, sửa đổi, bổ sung" so với bản gốc ETSI EN 319 422 (tập trung vào RSA/ECDSA). Đề nghị cân nhắc việc ghi chú rõ trong phần "Lời nói đầu" để người áp dụng	Tiếp thu ý kiến góp ý, bảo lưu việc bổ sung nội dung tại phần “Lời nói đầu”. Lý do bảo lưu: Lời nói đầu chỉ thể hiện thông tin về cơ sở xây dựng, tổ chức biên soạn và thủ tục công bố tiêu chuẩn, không phải phần quy định hoặc thuyết minh các yêu cầu kỹ thuật. Việc bổ sung mục tiêu cập nhật thuật toán

			tránh nhầm lẫn với bản gốc quốc tế	RSA và các thuật toán mật mã hậu lượng tử tại Lời nói đầu là chưa phù hợp với chức năng của phần này. Ban biên soạn giữ nguyên Lời nói đầu và làm rõ tại chú thích 3 của mục 5.2.3 Các thuật toán cần được sử dụng "CHÚ THÍCH: Việc bổ sung các thuật toán mật mã hậu lượng tử nhằm hỗ trợ khả năng chuyển đổi và tăng khả năng chống chịu mật mã trong dài hạn, không thay thế ngay các thuật toán đang được khuyến nghị áp dụng tại tiêu chuẩn này."
			Đề nghị rà soát, đảm bảo các thuật ngữ kỹ thuật trong tiêu chuẩn này không xung đột với các văn bản pháp luật về giao dịch điện tử hiện hành khi thay thế/cập nhật các khái niệm của ETSI.	Tiếp thu ý kiến góp ý. Ban biên soạn đã rà soát toàn bộ dự thảo TCVN. Các thuật ngữ kỹ thuật chính trong tiêu chuẩn đã được đối chiếu và đảm bảo thống nhất với các văn bản pháp luật về giao dịch điện tử hiện hành, cụ thể: - "Dấu thời gian" (time-stamp): phù hợp với định nghĩa tại khoản 18 Điều 3 Luật Giao dịch điện tử 2023; - "Dịch vụ cấp dấu thời gian" (Time-Stamping service): phù hợp với khoản 2 Điều 29 Luật Giao dịch điện tử 2023; - "Tổ chức cung cấp dịch vụ tin cậy"

				(TSP): phù hợp với khoản 1 Điều 29 Luật Giao dịch điện tử 2023; - "Tổ chức cung cấp dịch vụ cấp dấu thời gian" (TSA): phù hợp với Nghị định 23/NĐ-CP quy định chữ ký điện tử và dịch vụ tin cậy. Ban biên soạn xác nhận các thuật ngữ kỹ thuật trong dự thảo TCVN không xung đột với các văn bản pháp luật về giao dịch điện tử hiện hành.
III	**UBND/Sở KH&CN**			
IV	**Các Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng**			
		Viettel Telecom	Chưa làm rõ các nội dung được điều chỉnh so với tiêu chuẩn ETSI/Châu Âu.	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo TCVN. Ban biên soạn giữ nguyên Lời nói đầu và làm rõ tại chú thích 3 của mục 5.2.3 Các thuật toán cần được sử dụng "CHÚ THÍCH: Việc bổ sung các thuật toán mật mã hậu lượng tử nhằm hỗ trợ khả năng chuyển đổi và tăng khả năng chống chịu mật mã trong dài hạn, không thay thế ngay các thuật toán đang được khuyến nghị áp dụng tại tiêu chuẩn này.". Các điểm điều chỉnh chính bao gồm: 1) Gộp khái niệm TSU và TSA thành TSA phù hợp với mô hình 2 cấp tại Việt Nam; 2) Bổ sung các thuật toán hậu lượng tử (PQC): SLH-DSA, XMSS, LMS;

				3) Điều chỉnh độ dài khóa RSA tối thiểu từ ≥ 1900 bits lên ≥ 2048 bits theo QCVN 138:2025/BKHCN; 4) Điều chỉnh yêu cầu về chứng thư chữ ký số TSA (Mục 6.1) chỉ viện dẫn ETSI EN 319 412-3 (pháp nhân) phù hợp với thực tế Việt Nam; 5) Bổ sung nội dung phù hợp với Luật Giao dịch điện tử 2023 và Nghị định 23/NĐ-CP.
			Tại Mục 5.2.2 Quy định về ESSCertID/ESSCertIDv2 chỉ xuất hiện tại Mục 5.2.2 (đối với bản tin phản hồi), trong khi Mục 4.1.2 vẫn chỉ mô tả trường certReq với ESSCertID và Signing Certificate, chưa thống nhất với nội dung tại Mục 5.2.2.	Tiếp thu ý kiến góp ý, bảo lưu nội dung hiện tại; Giải trình lý do bảo lưu như sau: Tại Mục 4.1.2 của dự thảo TCVN quy định các trường dữ liệu cần được hỗ trợ trong bản tin yêu cầu (Request) từ phía máy khách, trong đó mô tả trường certReq với ESSCertID và Signing Certificate. Đây là nội dung phù hợp vì: - Mục 4.1.2 mô tả yêu cầu từ phía MÁY KHÁCH: trường certReq chỉ là tùy chọn cho phép máy khách yêu cầu TSA đính kèm chứng thư chữ ký số trong phản hồi. Tại bước này, máy khách chỉ cần biết về ESSCertID để có thể xác minh chứng thư sau khi nhận phản hồi; - Mục 5.2.2 mô tả yêu cầu từ phía MÁY CHỦ khi tạo bản tin phản hồi (Response): tại bước này, máy chủ PHẢI bao gồm ESSCertID hoặc ESSCertIDv2 trong thuộc tính SigningCertificate hoặc SigningCertificateV2, theo RFC 5816; - Sự khác biệt giữa hai mục phản ánh đúng vai trò khác nhau của máy khách và máy chủ trong giao thức RFC 3161. Tuy nhiên,

				Ban biên soạn sẽ bổ sung chú thích tại Mục 4.1.2 để tham chiếu đến Mục 5.2.2 về quy định ESSCertIDv2, giúp người đọc dễ đối chiếu.
			Tại Mục 4.1.2 chỉ mô tả ý nghĩa của trường reqPolicy nhưng chưa quy định cách TSA xử lý khi nhận được một OID chính sách không được hỗ trợ.	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo TCVN. Ban biên soạn đã bổ sung tại Mục 4.1.2 và Mục 5.1.2 quy định về cách TSA xử lý khi nhận được một OID chính sách (reqPolicy) không được hỗ trợ. Cụ thể, bổ sung nội dung: "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 theo quy định tại IETF RFC 3161 Mục 2.4.2." Nội dung bổ sung này phù hợp với quy định tại IETF RFC 3161 về xử lý lỗi trong giao thức cấp dấu thời gian, giúp đảm bảo tính rõ ràng và đầy đủ của tiêu chuẩn.