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 TIẾP THU, GIẢI TRÌNH Ý KIẾN GÓP Ý

TCVN Giao dịch điện tử - Yêu cầu về Giao diện dịch vụ Web cho mô hình ký số trên thiết bị di động (Mobile PKI)

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 - Yêu cầu về Giao diện dịch vụ Web cho mô hình ký số trên thiết bị di động (Mobile PKI) *(sau đây gọi tắt là Dự thảo TCVN)*.

Chi nhánh Đà Nẵng 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 liên quan[1].
- **01** đơn vị thuộc Bộ KH&CN[2];
- **02** CA công cộng[3].

[1] Bộ Tài chính, Bộ Nội vụ
[2] Vụ Kinh tế & Xã hội số
[3] Viettel-CA, VNPAY-CA

II. NỘI DUNG GÓP Ý CỤ THỂ

1. Chi tiết ý kiến tiếp thu, giải trình

STT	Nội dung góp ý	Ý kiến tiếp thu, giải trình (NEAC / Ban soạn thảo TCVN)
1. Vụ Kinh tế số và Xã hội số - Bộ Khoa học và Công nghệ		
1	Dự thảo viện dẫn trực tiếp tài liệu "ETSI TS 102 204 V1.1.4 (2003-08)", không phù hợp với sự phát triển của công nghệ di động hiện tại (2026).	**Tiếp thu một phần:** Đã bổ sung chú thích tại Điều 2 làm rõ: ETSI TS 102 204 V1.1.4 được sử dụng làm nền tảng kỹ thuật để bảo đảm khả năng liên thông với các hệ thống MSSP/CA hiện đang triển khai tại Việt Nam theo mô hình này. Các yêu cầu cụ thể về mật mã, giao thức truyền tải và mô hình thiết bị đã được rà soát, cập nhật phù hợp với công nghệ hiện hành (mục 3.1.10, 4.1.1, Điều 9, 10.5). Tiêu chuẩn sẽ được xem xét sửa đổi định kỳ theo sự phát triển công nghệ và các đặc tả kế thừa. Việc thay thế hoàn toàn tài liệu viện dẫn gốc sẽ làm thay đổi toàn bộ cấu trúc kỹ thuật của tiêu chuẩn, cần thực hiện trong chu kỳ soát xét toàn diện tiếp theo.
2	Dự thảo bắt buộc (PHẢI) triển khai dịch vụ dựa trên SOAP 1.2, WSDL 1.1 và định dạng thông điệp XML; kiến trúc RESTful API/JSON đã thay thế gần như hoàn toàn SOAP/XML trong môi trường tích hợp di động và Web hiện đại, gây khó khăn, tốn kém cho các tổ chức muốn tích hợp (AP).	**Tiếp thu một phần:** Đã bổ sung chú thích tại Điều 9: tổ chức cung cấp dịch vụ có thể triển khai bổ sung hồ sơ ràng buộc RESTful API/JSON tương đương về ngữ nghĩa với các kiểu thông điệp MSS quy định tại Điều 7, song song với hồ sơ SOAP 1.2. Hồ sơ SOAP 1.2/HTTP tiếp tục là yêu cầu bắt buộc tối thiểu trong phiên bản này nhằm bảo đảm khả năng liên thông với các hệ thống CA hiện đang vận hành. Đặc tả chi tiết cho hồ sơ ràng buộc RESTful API sẽ được xây dựng trong lần soát xét tiếp theo của tiêu chuẩn.
3	Mục 10.5 liệt kê tập hợp thuật toán mã hóa cho	**Tiếp thu:** Đã loại bỏ hoàn toàn 2 bộ thuật toán

	phép sử dụng là TLS_RSA_WITH_3DES_EDE_CBC_SHA và TLS_RSA_WITH_AES_128_CBC_SHA. Thuật toán 3DES đã bị cấm sử dụng trên toàn cầu do có lỗ hổng bảo mật nghiêm trọng; việc đưa vào tiêu chuẩn quốc gia về chữ ký số là không phù hợp về an ninh mạng. Đề nghị cập nhật bộ thuật toán hiện đại (AES-GCM, TLS 1.3).	TLS_RSA_WITH_3DES_EDE_CBC_SHA và TLS_RSA_WITH_AES_128_CBC_SHA (trao đổi khóa RSA tĩnh, không hỗ trợ PFS). Thay thế bằng các bộ thuật toán hiện đại hỗ trợ Perfect Forward Secrecy: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (TLS 1.2) và TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384 (TLS 1.3). Bổ sung yêu cầu bắt buộc sử dụng tối thiểu TLS 1.2, khuyến nghị TLS 1.3, và bắt buộc vô hiệu hóa các phiên bản TLS/SSL cũ (SSL 3.0, TLS 1.0, TLS 1.1).
4	Luật Giao dịch điện tử 2023 phân loại rõ chữ ký điện tử theo các mức độ an toàn (chữ ký điện tử chuyên dùng, chữ ký số...); tuy nhiên mục 3.1.5 định nghĩa "Chữ ký trên thiết bị di động" quá chung chung, thiếu các yếu tố kỹ thuật ràng buộc (khóa bí mật, chứng thư số, hàm băm) để được công nhận giá trị pháp lý là "Chữ ký số" theo pháp luật Việt Nam.	**Tiếp thu một phần:** Định nghĩa 3.1.5 là thuật ngữ kỹ thuật tổng quát, kế thừa từ khung MSS quốc tế (ETSI), mô tả phương thức sử dụng thiết bị di động để xác nhận ý định giao dịch, không phải là thuật ngữ pháp lý. Đã bổ sung chú thích sau định nghĩa, làm rõ ranh giới giữa chữ ký trên thiết bị di động (thuật ngữ kỹ thuật) và chữ ký số (thuật ngữ pháp lý theo Luật GDĐT 2023), đồng thời dẫn chiếu điều kiện công nhận giá trị pháp lý tại Luật GDĐT 2023, Nghị định 23/2025/NĐ-CP và TCVN Khung bảo mật cho mô hình ký số trên thiết bị di động (đang được xây dựng song song).
5	Trong định nghĩa 3.1.9 và 3.1.11, dự thảo sử dụng từ "công dân"; giao dịch điện tử và chữ ký số phục vụ cho cả tổ chức, doanh nghiệp và người nước ngoài (Người dùng cuối/Chủ thể ký). Việc chỉ dùng từ "công dân" là hẹp hơn phạm vi điều chỉnh của Luật Giao dịch điện tử.	**Tiếp thu:** Đã thay thuật ngữ công dân bằng người dùng cuối tại định nghĩa 3.1.9 (Yêu cầu chữ ký), 3.1.11 (Chuyển vùng giao dịch) và bảng chữ viết tắt MSISDN (mục 3.2) để bảo đảm phạm vi áp dụng phù hợp với đối tượng điều chỉnh của Luật Giao dịch điện tử 2023.
6	Trong mục 3.1.10 (Thẻ SIM) và mục 4.1.1 (thẻ	**Tiếp thu một phần:** Đã bổ sung chú thích tại 3.1.10 khẳng định Thẻ

	thông minh tích hợp, có hoặc không có thẻ thông minh), dự thảo cho thấy tư duy thiết kế mang nặng hơi hướng mô hình SIM PKI cũ (cần sự can thiệp của MNO). Xu hướng hiện nay là Remote Signing (Cloud PKI) qua ứng dụng di động, bảo vệ bằng sinh trắc học/Secure Enclave, không phụ thuộc SIM. Dự thảo chưa làm rõ tương thích với các giao thức ký số từ xa hiện đại (chuẩn CSC).	SIM (SIM-Card) là một trong các phương án triển khai MSCD. Phù hợp với nguyên tắc trung lập công nghệ nêu tại 5.1, các phương án khác như phần cứng bảo mật tích hợp trong chip thiết bị hoặc giải pháp ký số từ xa dựa trên HSM phía máy chủ cũng được chấp nhận là MSCD hợp lệ, miễn là đáp ứng đầy đủ các yêu cầu bảo mật quy định tại Điều 6.4. Việc tái cấu trúc toàn bộ kiến trúc kỹ thuật của tài liệu theo mô hình Remote Signing làm nền tảng chính sẽ được xem xét trong lần soát xét toàn diện tiếp theo.
7	Tài liệu đề cập thiết bị di động như một "cây bút điện tử" và mô hình ký số qua SIM/thẻ thông minh. Dự thảo cần mở rộng, cập nhật để tương thích với các mô hình xác thực mới dựa trên Cloud PKI (Remote Signing) đang phổ biến hơn việc phụ thuộc vào thẻ SIM hoặc thiết bị phần cứng cồng kềnh.	**Tiếp thu một phần:** Đã bổ sung chú thích tại mục 4.1.2 làm rõ hình ảnh "công cụ ký"/"cây bút điện tử" mang tính khái niệm, minh họa vai trò của thiết bị di động, không hàm ý giới hạn công nghệ triển khai; dẫn chiếu các mô hình thay thế (SIM, phần tử an toàn nhúng, Remote Signing/Cloud PKI) đã được bổ sung tại 3.1.10 và 4.1.1.
2. Viettel-CA		
1	Dự thảo quy định giao thức SOAP/XML cho toàn bộ API giao tiếp giữa các thành phần. SOAP là giao thức lỗi thời, nặng về cấu trúc XML, khó tích hợp hệ thống hiện đại; các nhà CA hiện tại đang dùng SOAP nên quy định vẫn có cơ sở thực tế nhưng sẽ tạo rào cản cho nhà cung cấp mới. Đề xuất bổ sung hỗ trợ giao thức REST song song với SOAP, về lâu dài định hướng REST là giao thức ưu tiên, SOAP giữ lại	**Tiếp thu một phần:** Nội dung tương đồng với góp ý của Vụ Kinh tế số và Xã hội số (mục 2). Đã bổ sung chú thích tại Điều 9 cho phép triển khai bổ sung hồ sơ ràng buộc RESTful API/JSON song song với SOAP 1.2; SOAP 1.2/HTTP tiếp tục là hồ sơ bắt buộc tối thiểu trong phiên bản này để bảo đảm liên thông với các hệ thống CA hiện hành, đúng như nhận định của Viettel-CA. Đặc tả REST chi tiết sẽ được xây dựng trong lần soát xét tiếp theo, định hướng REST là giao thức được khuyến khích áp dụng cho các triển khai mới.

	để tương thích ngược.	
2	Dự thảo ghi mật khẩu của AP (AP_PWD) là trường bắt buộc trong thông điệp trừu tượng để định danh AP khi sử dụng API. Việc truyền mật khẩu là hành động không bảo đảm về ATTT do dữ liệu có thể bị lấy cắp và bị tấn công dựa trên dữ liệu đó. Đề xuất sử dụng JWT token, hoặc mã hóa dữ liệu dạng MAC dùng cặp khóa AP được cấp, MSSP kiểm tra lại bằng public key tương ứng.	**Tiếp thu:** Đã sửa mục 7.1 (Kiểu thông điệp trừu tượng): thuộc tính "Bắt buộc" của AP_PWD chuyển từ "Có" thành "Có điều kiện" - chỉ bắt buộc sử dụng khi kênh truyền chỉ áp dụng xác thực máy chủ một chiều qua TLS. Bổ sung quy định: trường hợp áp dụng xác thực TLS hai chiều (mutual TLS) bằng chứng thư số X.509v3 của AP, hoặc áp dụng cơ chế ký/xác thực thông điệp bằng MAC/token dựa trên cặp khóa được cấp cho AP, MSSP có thể không yêu cầu truyền AP_PWD dạng bản rõ; khuyến nghị các tổ chức triển khai mới ưu tiên áp dụng các phương án này. Nội dung sửa đổi cũng bảo đảm nhất quán với mục 10.2.3 vốn đã quy định mật khẩu AP chỉ áp dụng "trong trường hợp chỉ sử dụng xác thực máy chủ qua TLS".
3	Mục 7.1: Dự thảo yêu cầu kiểm tra trạng thái chứng thư chữ ký số người dùng có hợp lệ trước khi ký nhưng không ghi thông tin chứng thư chữ ký số đang ký, không có cơ chế truyền thông tin chứng thư chữ ký số khi người dùng ký. Thực tế người dùng có thể có nhiều chứng thư chữ ký số (còn hiệu lực/đã thu hồi); trên SIM, CA có thể bất đồng bộ với hệ thống nên chứng thư chữ ký số hết hạn/bị thu hồi có thể chưa được xóa khỏi SIM. Đề xuất: việc kiểm tra trạng thái chứng thư chữ ký số cần đi kèm việc truyền thông tin chứng thư chữ ký số đang dùng để ký qua API.	**Tiếp thu:** Đã bổ sung chú thích tại mục 8.3.3 (KeyReferenceType): trường hợp người dùng cuối sở hữu nhiều chứng thư chữ ký số, RP/AP nên chỉ định KeyReference tương ứng với chứng thư chữ ký số đang có hiệu lực dùng để ký, thông qua CertificateURL hoặc HashOfUsersPublicKey. MSSP PHẢI kiểm tra trạng thái hiệu lực của chứng thư chữ ký số được tham chiếu tại thời điểm xử lý yêu cầu ký và trả về mã trạng thái tương ứng (mã 501 - REVOKED_CERTIFICATE tại Phụ lục B) nếu chứng thư chữ ký số không còn hiệu lực, khắc phục tình huống dữ liệu chứng thư chữ ký số trên thiết bị người dùng chưa đồng bộ kịp thời với hệ thống MSSP/CA.
4	Dự thảo đề cập nhiều mã lỗi được định nghĩa chi tiết, mã lỗi rõ ràng (ví dụ mã 500). Thực tế các	**Tiếp thu một phần:** Giữ nguyên danh mục mã trạng thái/mã lỗi tại Phụ lục A và Phụ lục B (kế thừa từ khung MSS quốc tế) do đây là cơ sở cần

	đơn vị cung cấp có bộ mã lỗi riêng, thường tránh mã lỗi tương đồng với HTTP code để tránh nhầm lẫn; dự thảo ghi nhiều mã 500 nhưng chưa đầy đủ toàn bộ mã lỗi cần định nghĩa. Đề xuất loại bỏ định nghĩa mã lỗi chi tiết, cho phép nhà cung cấp tự định nghĩa, bảo đảm cover các trường hợp TC đề ra.	thiết để bảo đảm khả năng liên thông giữa các hệ thống và phục vụ xây dựng bộ kiểm thử tuân thủ (conformance testing) của tiêu chuẩn. Đã bổ sung chú thích ngay đầu Phụ lục B làm rõ: các giá trị mã trạng thái là mã con đặc thù ứng dụng, được truyền trong nội dung thông điệp SOAP Body/Fault (tầng ứng dụng), hoàn toàn độc lập với mã trạng thái HTTP ở tầng vận chuyển nên không phát sinh nhầm lẫn kỹ thuật khi được phân tích đúng ngữ cảnh; đồng thời cho phép tổ chức cung cấp dịch vụ bổ sung mã trạng thái/mã lỗi riêng ngoài danh mục quy định để phục vụ nhu cầu vận hành nội bộ, với điều kiện bảo đảm đầy đủ các mã bắt buộc của tiêu chuẩn.
5	Đề xuất chuyển yêu cầu áp dụng mã hóa kênh truyền OTA (như chuẩn 3GPP TS 03.48 hoặc tương đương) thành quy định bắt buộc đối với bộ giao tiếp giữa MSSP và MSCD; đồng thời cần làm rõ ranh giới trách nhiệm bảo mật giữa Tổ chức cung cấp dịch vụ (CA) và Nhà mạng viễn thông (MNO).	**Bảo lưu:** Nội dung góp ý liên quan đến kênh giao tiếp nội bộ giữa MSSP và MSCD (qua giao diện OTA của SIM) không thuộc phạm vi điều chỉnh của TCVN Giao dịch điện tử - Yêu cầu về giao diện dịch vụ Web cho mô hình ký số trên thiết bị di động (tiêu chuẩn này chỉ quy định giao diện dịch vụ Web giữa AP và MSSP theo mô hình ETSI TS 102 204). Yêu cầu về mã hóa kênh OTA và ranh giới trách nhiệm bảo mật giữa CA và MNO thuộc phạm vi điều chỉnh của TCVN "Giao dịch điện tử - Yêu cầu về khung bảo mật cho mô hình ký số trên thiết bị di động (Mobile PKI)" (ETSI TR 102 206).
3. VNPAY-CA		
1	Tại mục 4.2 - Khai báo lược đồ XML: lệch phiên bản của namespace trong mô tả và trong khai báo XML (http://uri.etsi.org/TS102204/v1.2.1# và v1.1.2#).	**Tiếp thu:** Đã rà soát toàn bộ tài liệu và đồng bộ thống nhất định danh namespace XML về http://uri.etsi.org/TS102204/v1.1.2# tại tất cả các vị trí liên quan: mục 4.2 (đoạn mô tả định danh chuẩn XML và khai báo targetNamespace/xmlns:mss trong ví dụ XML Schema) và Điều 6 (khai báo xmlns:mss trong ví dụ WSDL).

4. Bộ Tài chính (Công văn số 12905/BTC-CNTT ngày 20/8/2026)		
1	(Mục 2.7.a Công văn 12905/BTC-CNTT) Tại mục 7.2 về các tham số yêu cầu ký số, đề nghị đơn vị dự thảo nghiên cứu bổ sung giao thức và cấu trúc thông điệp hỗ trợ ký theo lô (batch signing). Điều này đặc biệt quan trọng đối với các đơn vị phải xử lý lượng chứng từ thu/chi lớn trong một thao tác, giúp tối ưu hóa đường truyền và trải nghiệm người dùng di động.	**Tiếp thu một phần:** Đã bổ sung chú thích ngay trước Điều 7.3: đối với các đơn vị có nhu cầu xử lý đồng thời khối lượng lớn chứng từ thu/chi (ngân hàng, tổ chức tài chính), tổ chức cung cấp dịch vụ có thể triển khai bổ sung cơ chế ký theo lô bằng cách đóng gói nhiều yêu cầu SigREQ độc lập trong một phiên giao dịch nghiệp vụ ở tầng ứng dụng (AP), với điều kiện mỗi giao dịch ký thành phần vẫn tuân thủ đầy đủ cấu trúc thông điệp SigREQ/SigRESP quy định tại Điều 7. Việc chuẩn hóa một giao thức và cấu trúc thông điệp ký theo lô riêng ở tầng giao diện Web (kèm cơ chế tối ưu số lượt round-trip) là một thay đổi cấu trúc kỹ thuật đáng kể, cần được nghiên cứu, đánh giá tác động đầy đủ và sẽ được bổ sung trong lần soát xét tiếp theo của tiêu chuẩn.
2	(Mục 2.7.b) Tại mục 10.5 về các giao thức bảo mật kênh truyền đang "bắt buộc một danh sách các tập hợp thuật toán mã hóa có thể sử dụng", trong đó liệt kê cụ thể hai bộ mã hóa TLS_RSA_WITH_3DES_EDE_CBC_SHA và TLS_RSA_WITH_AES_128_CBC_SHA. Tại QCVN 137:2025/BKHCN không khuyến nghị sử dụng 3DES và SHA-1 vì các thuật toán này không còn an toàn. Đề nghị rà soát, điều chỉnh tập hợp thuật toán mã hóa có thể sử dụng.	**Đã tiếp thu:** Nội dung này đã được tiếp thu và chỉnh sửa từ vòng góp ý trước (góp ý của Vụ Kinh tế số và Xã hội số - Bộ Khoa học và Công nghệ, mục 3 tại Mục I của Bảng này): mục 10.5 của Dự thảo TCVN hiện hành (phiên bản đã gửi kèm hồ sơ xin ý kiến) đã loại bỏ hoàn toàn hai bộ thuật toán TLS_RSA_WITH_3DES_EDE_CBC_SHA và TLS_RSA_WITH_AES_128_CBC_SHA, thay thế bằng các bộ thuật toán hỗ trợ Perfect Forward Secrecy (TLS_ECDHE_RSA_WITH_AES_128/256_GCM_SHA cho TLS 1.2, TLS_AES_128/256_GCM_SHA cho TLS 1.3), đồng thời bổ sung yêu cầu bắt buộc tối thiểu TLS 1.2 và vô hiệu hóa các phiên bản TLS/SSL cũ. Không phát sinh nội dung cần chỉnh sửa thêm.
3	(Mục 2.7.c) Các ràng buộc kết nối hiện đang chỉ quy định giao thức SOAP và định dạng XML. Đề nghị bổ sung thêm chuẩn kết nối RESTful	**Tiếp thu:** Nội dung này đã được bổ sung chú thích tại Điều 9 từ vòng góp ý trước (góp ý tương tự của Vụ Kinh tế số và Xã hội số và Viettel-CA). Theo góp ý cụ thể hơn của Bộ Tài chính về cơ chế ký JWS/JWT,

	API và định dạng JSON (kèm cơ chế ký JWS/JWT) như một giải pháp kết nối song song nhằm phù hợp với xu hướng công nghệ hiện đại, giúp các hệ thống thông tin, ứng dụng (AP) dễ dàng tích hợp.	đã cập nhật chú thích tại Điều 9 nêu rõ: tổ chức cung cấp dịch vụ có thể triển khai bổ sung hồ sơ ràng buộc RESTful API/JSON tương đương ngữ nghĩa với các kiểu thông điệp MSS quy định tại Điều 7, kèm theo cơ chế ký/xác thực thông điệp bằng JSON Web Signature (JWS) hoặc JSON Web Token (JWT), song song với hồ sơ SOAP 1.2 (tiếp tục là hồ sơ bắt buộc tối thiểu để bảo đảm liên thông với hệ thống hiện hành). Đặc tả chi tiết (cấu trúc thông điệp JSON và cơ chế ký JWS/JWT) sẽ được xây dựng trong lần soát xét tiếp theo.
4	(Mục 2.7.d) Cần rà soát và chuẩn hóa thuật ngữ để tuân thủ Luật Giao dịch điện tử 2023 và Nghị định số 23/2025/NĐ-CP. Về thuật ngữ người dùng/công dân: Dự thảo có sử dụng các từ "người dùng", "người dùng cuối", "công dân". Đề nghị chuẩn hóa thành "Chủ thể ký" hoặc "Thuê bao" để phù hợp theo Luật Giao dịch điện tử 2023.	**Tiếp thu một phần:** Đã rà soát và khắc phục 3 vị trí còn sót thuật ngữ "công dân" tại mục 4.1.2 (thay bằng "người dùng cuối"), bảo đảm nhất quán với các sửa đổi tại 3.1.9, 3.1.11 và bảng MSISDN đã thực hiện ở vòng góp ý trước. Đồng thời, đã bổ sung chú thích ngay sau định nghĩa 3.1.4 (Người dùng cuối) làm rõ mối quan hệ tương đương thuật ngữ: "người dùng cuối" là thuật ngữ kỹ thuật kế thừa từ khung MSS quốc tế (ETSI) chỉ vai trò sở hữu/sử dụng thiết bị di động trong giao thức; khi thực hiện hành vi ký, thuật ngữ pháp lý tương ứng theo Luật GDĐT 2023 là "chủ thể ký" (đã được định nghĩa tại 3.1.3); trường hợp là thuê bao đăng ký dịch vụ với nhà mạng/MSSP, có thể gọi là "thuê bao" theo pháp luật viễn thông. Không thực hiện thay thế toàn bộ (khoảng 40 vị trí) thuật ngữ "người dùng cuối" thành "Chủ thể ký"/"Thuê bao" trong toàn văn bản vì đây là thuật ngữ kỹ thuật ở tầng giao thức MSS, được sử dụng nhất quán cùng các vai trò kỹ thuật khác (AP, RP, MSSP) xuyên suốt Điều 7-10; việc thay thế toàn bộ có nguy cơ làm giảm độ chính xác kỹ thuật tại các ngữ cảnh không liên quan trực tiếp đến hành vi ký (ví dụ: đăng ký thuê bao, nhận thông báo, cấp biên lai).
5	(Mục 2.7.d) Về Bên tin cậy (Relying Party - RP) và Bên cung cấp ứng dụng (AP): Cần làm rõ mối	**Tiếp thu:** Đã bổ sung chú thích ngay sau bảng chữ viết tắt (mục 3.2), trước Điều 4, làm rõ: AP và RP là các vai trò kỹ thuật trong giao thức

	quan hệ pháp lý giữa AP, RP và Tổ chức cung cấp dịch vụ chứng thực chữ ký số (CA/MSSP). Trong pháp luật Việt Nam, dịch vụ ký số phải do Tổ chức cung cấp dịch vụ chứng thực chữ ký số (công cộng hoặc chuyên dùng) đảm nhiệm.	MSS, không phải chủ thể pháp lý được cấp phép cung cấp dịch vụ chứng thực chữ ký số; trong đa số giao dịch AP và RP là cùng một chủ thể; AP/RP không được tự thực hiện chức năng ký số, xác thực chữ ký số hoặc cấp dấu thời gian nếu không phải là Tổ chức cung cấp dịch vụ chứng thực chữ ký số (CA) theo Luật GDĐT 2023; MSSP phải là, hoặc phải hoạt động dưới sự ủy quyền/hợp tác kỹ thuật của, một CA được cấp phép hợp pháp theo Luật GDĐT 2023 và Nghị định 23/2025/NĐ-CP.
6	(Mục 2.7.d) Về "Chữ ký trên thiết bị di động": Dự thảo định nghĩa thuật ngữ này tại mục 3.1.5. Cần làm rõ đây là một dạng thể hiện của Chữ ký số sử dụng phương tiện tạo chữ ký số nằm trên SIM/eSIM hoặc ứng dụng xác thực di động an toàn, tuân thủ các quy định về mức độ an toàn của thiết bị tạo chữ ký số theo Nghị định 23/2025/NĐ-CP.	**Tiếp thu:** Đã bổ sung nội dung vào chú thích hiện có tại 3.1.5 (đã được bổ sung một phần từ vòng góp ý trước): làm rõ về bản chất, chữ ký trên thiết bị di động là một dạng thể hiện của chữ ký số, trong đó phương tiện tạo chữ ký số (khóa bí mật) được lưu trữ và bảo vệ trên SIM/eSIM tích hợp hoặc trên ứng dụng xác thực di động an toàn (ứng dụng ký số từ xa/Cloud PKI - dẫn chiếu 3.1.10, 4.1.1); phương tiện tạo chữ ký số này phải tuân thủ các quy định về mức độ an toàn của phương tiện tạo chữ ký số theo Nghị định 23/2025/NĐ-CP.
5. Bộ Nội vụ (Công văn góp ý đối với 08 dự thảo TCVN thuộc lĩnh vực dịch vụ tin cậy đợt 2)		
1	(Mục 2.6) Tại các Mục 7.1, 7.2, 7.6 và 7.7 (trang 25 đến trang 32), có một số lỗi chính tả và khoảng trắng không phù hợp trong tên tham số, như: "AP_Tran sID"; "SingatureProfileCo mp arison"; "EncryptedDat a"; yêu cầu rà soát, chỉnh sửa thêm một số trường hợp tương tự. Đề nghị rà soát, chuẩn hóa tên các tham số, loại bỏ khoảng trắng không phù hợp và sửa các lỗi chính tả, do tên tham số trong các thông điệp trao đổi cần bảo đảm tính chính xác và thống nhất nhằm	**Tiếp thu:** Đã rà soát toàn bộ định danh XML Schema (thuộc tính xs:attribute/xs:element) và toàn bộ mã trạng thái/mã lỗi tại Phụ lục A, Phụ lục B của dự thảo để đối chiếu lỗi chính tả và khoảng trắng không phù hợp trong tên tham số. Kết quả: "AP_TransID" và "EncryptedData" trong bản dự thảo hiện hành đã đúng chính tả, không cần chỉnh sửa thêm. Đã sửa lỗi thực tế phát hiện tại mục 7.2: "SingatureProfileComp arison"/"SingatureProfileComparisonType" (vừa thiếu chữ "n" vừa thừa khoảng trắng) thành "SignatureProfileComparison"/"SignatureProfileComparisonType". Qua rà soát mở rộng theo đúng tinh thần góp ý, đã phát hiện và sửa thêm 03

	tránh phát sinh lỗi trong quá trình liên thông, trao đổi dữ liệu giữa các hệ thống AP và MSSP, đặc biệt đối với các thông điệp được cấu trúc và trao đổi dưới dạng XML.	trường hợp tương tự tại Phụ lục A, Phụ lục B: “INTERNAL_ERROR ETSI” → “INTERNAL_ERROR” (mã 900, thừa từ); “REVOKED_ CERTIFICATE” → “REVOKED_CERTIFICATE” (mã 501, thừa khoảng trắng); “OUSTANDING_TRANSACTION” → “OUTSTANDING_TRANSACTION” (mã 504, thiếu chữ “T”). Đã đối chiếu toàn bộ 80 định danh XML Schema và toàn bộ mã trạng thái/mã lỗi trong tài liệu, xác nhận không còn trường hợp tương tự.