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

Dự thảo TCVN - Giao thức tạo chữ ký số cho mô hình ký số từ xa

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 - Giao thức tạo chữ ký số cho mô hình ký số từ xa *(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

1. Chi tiết ý kiến tiếp thu, giải trình

STT	Nội dung góp ý	Ý kiến tiếp thu, giải trình

[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

		(NEAC / Ban soạn thảo TCVN)
I	**Các Bộ, Cơ quan ngang Bộ, cơ quan thuộc Chính phủ**	
1. Bộ Quốc phòng		
1	Đề nghị bổ sung yêu cầu về rủi ro phân tích cú pháp (Parsing vulnerabilities): "Các ứng dụng máy chủ (SSA) và SAM phải có cơ chế xác thực lược đồ (Schema validation) nghiêm ngặt và vô hiệu hóa xử lý thực thể bên ngoài khi phân tích cú pháp gói tin SAD". Lý do: Việc truyền SAD bằng định dạng XML/JSON tiềm ẩn nguy cơ bị tấn công tiêm nhiễm (Injection) hoặc tấn công thực thể bên ngoài (XXE - XML External Entity).	Tiếp thu ý kiến góp ý, bảo lưu; Giải trình lý do bảo lưu như sau: Không bổ sung vào dự thảo một yêu cầu riêng quy định SSA và SAM phải vô hiệu hóa thực thể XML bên ngoài, giới hạn kích thước dữ liệu hoặc áp dụng một cấu hình cụ thể cho bộ phân tích cú pháp. Các biện pháp này thuộc thiết kế, lập trình, cấu hình và vận hành an toàn của hệ thống triển khai. Dự thảo TCVN quy định thành phần, cấu trúc và ngữ nghĩa liên thông của giao thức theo ETSI TS 119 432; việc bổ sung yêu cầu triển khai riêng sẽ mở rộng phạm vi và có thể làm sai khác hồ sơ giao thức nguồn.
2	Đề nghị rà soát hiệu chỉnh lại các hình số 1, 2, 3 để đảm bảo tính chính xác và bổ sung nội dung xác thực và ủy quyền của tiêu chuẩn ETSI TS 119 432.	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo tại Mục 4.1, trang số 13 đến trang số 14; Mục 5.2 đến Mục 5.4, trang số 18 đến trang số 20; Hình 1, Hình 2 và Hình 3 là: "Mô-đun kích hoạt chữ ký số (SAM) trong vùng bảo vệ chống can thiệp vật lý chỉ cần thiết khi Dịch vụ tạo chữ ký số (SCS) tuân thủ cơ chế kích hoạt chữ ký số thuộc Mức bảo đảm kiểm soát duy nhất cấp 2 (SCAL2)."; Hình 1 thể hiện "Xác thực và cấp quyền cho chủ thể ký (M)"; Hình 2 có tên "Kiến trúc dịch vụ ký số từ xa với SCAL1"; Hình 3 có tên "Kiến trúc dịch vụ ký số từ xa với SCAL2" và thể hiện "Giao thức kích hoạt chữ ký số (SAP)" cùng "Mô-đun kích hoạt chữ ký số/Thiết bị tạo chữ ký số".

2. Bộ Công an		
1	Đề nghị hiệu chỉnh lại đối với thuật ngữ *"Cơ quan trạng thái chứng chỉ"* thành *"Cơ quan đóng dấu thời gian"* theo tài liệu ETSI đối với kiến trúc dịch vụ ký số từ xa. Tại SCAL1 chỉnh từ CSP viết tắt của thuật ngữ Certificate Status Authority, Thuật ngữ TSA viết tắt của "Time-Stamping Authority", tương tự ở mô tả kiến trúc dịch vụ ký số từ xa với SCAL2 trong dự thảo tiêu chuẩn dịch vụ tin cậy, đề nghị sửa *"giao thức ký số cho mô hình ký số từ xa"* thành *"Tổ chức cung cấp dịch vụ kiểm tra trạng thái chứng thư số trực tuyến"* và *"Tổ chức cung cấp dịch vụ cấp dấu thời gian"* .	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo tại Hình 2 thuộc Mục 5.3, trang số 19 và Hình 3 thuộc Mục 5.4, trang số 20 là: "CSA - Tổ chức cung cấp dịch vụ kiểm tra trạng thái chứng thư số trực tuyến" và "TSA - Tổ chức cung cấp dịch vụ cấp dấu thời gian".
3. Bộ Nội vụ		
1	Đề nghị bổ sung nội dung yêu cầu chữ ký số từ xa phải bảo đảm khả năng kiểm tra tính xác thực, tính toàn vẹn và giá trị chứng cứ của tài liệu trong suốt vòng đời lưu trữ, từ tạo lập, thu nộp, bảo quản, tổ chức sử dụng và chuyển giao giữa các hệ thống vì đối với tài liệu lưu trữ số, việc xác thực không chỉ phục vụ giao dịch tại thời điểm ký mà còn phải bảo đảm khả năng kiểm chứng sau nhiều năm, kể cả khi chứng thư số hết hạn, bị thu hồi hoặc thuật toán ký số thay đổi.	Tiếp thu ý kiến góp ý, bảo lưu; Giải trình lý do bảo lưu như sau: Yêu cầu kiểm tra, bảo quản và duy trì giá trị chứng cứ của tài liệu trong toàn bộ vòng đời lưu trữ thuộc phạm vi tiêu chuẩn về định dạng chữ ký, dữ liệu xác thực, dấu thời gian và dịch vụ bảo quản. Dự thảo này quy định giao thức tạo chữ ký số từ xa nên không bổ sung yêu cầu lưu trữ dài hạn.
2	Đề nghị cân nhắc bổ sung yêu cầu kiểm soát nghiệp vụ đối với trường hợp ký số hàng loạt vì trong hoạt động lưu trữ, có những trường hợp cần thực hiện ký số hàng loạt như ký xác thực tài liệu lưu trữ số hóa, bản sao tài liệu lưu trữ số, gói hồ sơ, tài liệu thu nộp hoặc các kết quả xử lý nghiệp vụ trên Hệ thống.	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo tại Mục 5.3, trang số 19 và Mục 7.11, trang số 32 đến trang số 33 là: "Khi việc xác thực chủ thể ký thành công, khóa ký tương ứng có thể được sử dụng cho các hoạt động ký số thay mặt cho chủ thể ký trong một khung thời gian nhất định và/hoặc một số lượng hoạt động ký số nhất định, từ đó cho phép quản lý các hoạt động ký số hàng loạt."; "Thành phần

		này có thể được sử dụng để khởi tạo và quản lý một chuỗi các chữ ký với số lượng đã thỏa thuận, được coi là một đơn vị công việc duy nhất (được gọi là giao dịch trong mục này) giữa khách hàng và SCS.”
3	Tại mục 7.24 - Thành phần thông báo kết quả hoạt động, đề nghị bổ sung danh mục mã trạng thái (status) và mã lỗi (error code) theo một bộ chuẩn thống nhất; quy định ý nghĩa của từng mã và trường hợp áp dụng.	Tiếp thu ý kiến góp ý, bảo lưu; Giải trình lý do bảo lưu như sau: Không bổ sung một danh mục mã trạng thái và mã lỗi riêng vì Mục 7.24 đã sử dụng cơ chế kết quả của OASIS DSS-v2.0 và mã lỗi của tiêu chuẩn CSC. Việc xây dựng thêm một bộ mã riêng có thể gây trùng lặp hoặc xung đột. Dự thảo tại Mục 7.24.2, trang số 53 quy định: “Các mã trạng thái và thông báo lỗi được định nghĩa trong mục 10.1 của tiêu chuẩn CSC phải được sử dụng nếu phù hợp.”
4	Tại mục 8. Các thông điệp tạo chữ ký từ xa, đề nghị bổ sung ví dụ minh họa đối với các thông điệp API (JSON/XML) cho các chức năng chính như khởi tạo yêu cầu ký, truy vấn trạng thái, nhận kết quả và xử lý lỗi, nhằm bảo đảm các tổ chức cung cấp dịch vụ và các hệ thống thông tin của cơ quan nhà nước có cơ sở triển khai thống nhất, liên thông và giảm chi phí tích hợp.	Tiếp thu ý kiến góp ý, bảo lưu; Giải trình lý do bảo lưu như sau: Không bổ sung các ví dụ API JSON/XML vào nội dung quy phạm của dự thảo. Các lược đồ tại Phụ lục A là cơ sở để xây dựng và kiểm thử thông điệp; ví dụ API phụ thuộc môi trường triển khai và có thể được công bố trong tài liệu hướng dẫn kỹ thuật riêng.
4. Bộ Công Thương		
1	Không có ý kiến	
5. Ngân hàng Nhà nước Việt Nam		
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	Tiếp thu ý kiến góp ý, bảo lưu; Giải trình lý do bảo lưu như sau: Dự thảo không cố định một thuật toán chữ ký duy nhất. Mục 7.13 sử dụng các tham số signaturePolicyID, signAlgo

	(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.	và signAlgoParams cùng định danh OID/URI nên có thể bổ sung hoặc thay thế thuật toán mà không thay đổi cấu trúc thông điệp. PQC và lộ trình chuyển đổi PQC chưa phải là nội dung của ETSI TS 119 432 V1.2.1 và cần được quy định tại tiêu chuẩn thuật toán hoặc lộ trình mật mã riêng. Vì vậy, không bổ sung điều khoản PQC riêng vào dự thảo này.
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, bảo lưu; Giải trình lý do bảo lưu như sau: JSON trong dự thảo là định dạng biểu diễn thông điệp giao thức, không đồng nghĩa chữ ký được tạo phải có định dạng JAdES. JAdES là một định dạng chữ ký độc lập thuộc ETSI EN 119 182-1:2021 nên được xem xét trong một tiêu chuẩn hoặc hồ sơ kỹ thuật riêng về định dạng chữ ký JSON.
3	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, bảo lưu; Giải trình lý do bảo lưu như sau: Dự thảo đã sử dụng requestID tại 7.3 để tương quan yêu cầu và phản hồi; thành phần tại 7.11 hỗ trợ quản lý một chuỗi chữ ký như một giao dịch. Việc tương quan nhật ký giữa các thành phần nội bộ của hệ thống có thể sử dụng requestID hoặc mã tương quan nội bộ khi triển khai.

6. Vụ Kinh tế số và Xã hội số - Bộ Khoa học và Công nghệ		
1	a) Do không có văn bản gốc ETSI TS 119 432 đối chiếu nên không thể xác định tính chính xác, tuy nhiên, đề nghị rà soát thuật ngữ cơ bản ("Điều kiện" thành "Mục kiện"). Xuyên suốt dự thảo, từ "điều kiện" (condition/qualified) đã bị dịch sai thành "mục kiện". Ví dụ: "mục kiện của Việt Nam", "chữ ký số đủ mục kiện" (Qualified Electronic Signature), "thiết bị tạo chữ ký số đủ mục kiện", "Mục kiện tùy chọn", "Mục kiện bắt buộc".	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo tại Bảng chữ viết tắt thuộc Mục 3.3, trang số 12 và các bảng quy định thành phần tại Mục 7, Mục 8, trang số 23 đến trang số 73 là: "QES - Qualified Electronic Signature - Chữ ký điện tử đủ điều kiện"; các lỗi "mục kiện", "mục chỉnh" đã được sửa và mức hiện diện được trình bày theo tính chất của từng thành phần.
2	Rất nhiều thẻ XML và tên thuộc tính kỹ thuật bị dịch một nửa sang tiếng Việt, khiến cấu trúc mã nguồn (XML Schema) trở nên vô nghĩa, khó hiểu: - Từ "Type" bị dịch thành "Loại" ngay trong tên biến: etsisig: Signature Loại thay vì SignatureType. - Thuộc tính ValidityPeriod bị biến dạng một cách khó hiểu thành Validi Loạiriod. - Thuộc tính CommitmentTypeIndication bị kẹp tiếng Việt vào giữa thành CommitmentLoạiIndication. - Thuộc tính RequestBaseType bị dịch thành dsb: RequestBaseLoại. - Từ "Parameters" bị dịch thành "Tham số" nhưng vẫn giữ đuôi số nhiều "s": etsisig: Signature Algorithm Tham số. - Các thành phần đầu vào/đầu ra chuẩn của OASIS bị dịch thẳng tên thẻ: etsisig: Các đầu vào tùy chọn (đáng lẽ phải là OptionalInputs), etsisig: Đầu ra Tùy chọn (đáng lẽ phải là OptionalOutputs).	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo tại Mục 7.6.3, trang số 28; Mục 7.13.3, trang số 35; Mục 7.14, trang số 36; Mục 7.16.3, trang số 40; Mục 8.3.1.3, trang số 63 và các phần tử liên quan trong Mục 7, Mục 8 là: "etsisig:SignatureType", "etsisig:ValidityPeriod", "CommitmentTypeIndication", "dsb:RequestBaseType", "SignatureAlgorithmParameters", "dss2:OptionalInputs" và "dss2:OptionalOutputs". Các tên phần tử, kiểu và thuộc tính kỹ thuật được giữ nguyên bằng tiếng Anh; phần mô tả tiếng Việt được trình bày tách biệt.

3	Trong các bảng cấu trúc JSON/XML, nhiều thuật ngữ chuyên ngành bị pha trộn nửa Anh nửa Việt không đồng nhất. Ví dụ: "Thuộc tính Signed Envelope", hoặc phần giải nghĩa điều kiện xuất hiện ghi "Mục kiện bắt buộc".	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo tại các bảng thành phần JSON/XML thuộc Mục 7 và Mục 8, trang số 23 đến trang số 73 là: tên phần tử, tên khóa và kiểu dữ liệu kỹ thuật được giữ nguyên bằng tiếng Anh; phần mô tả được trình bày bằng tiếng Việt; các mức hiện diện được thống nhất là "Bắt buộc", "Tùy chọn" và "Bắt buộc có điều kiện". Các cụm pha trộn như "Signature Loại", "Validi Loạiriod", "CommitmentLoạiIndication", "RequestBaseLoại", "Signature Algorithm Tham số", "Các đầu vào tùy chọn" và "Đầu ra Tùy chọn" trong tên định danh kỹ thuật đã được loại bỏ.
7. Vụ Pháp chế		
1	Không có ý kiến	
II. Các Tổ chức, doanh nghiệp		
1. Tập đoàn Viễn thông Quân đội (Viettel CA)		
1	1. Mô hình SCAL 1 và SCAL 2 gần như là giống nhau. Đề xuất: Sự khác biệt giữa mô hình SCAL và SCAL 2 nên được mô tả rõ hơn ở trong hình ảnh thay vì chỉ bổ sung chữ SAM ở mục "Ứng dụng ký số phía máy chủ"	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo tại Mục 4.4.1.2, trang số 17; Mục 5.3 và Hình 2, trang số 19; Mục 5.4 và Hình 3, trang số 19 đến trang số 20 là: đối với SCAL1, "Việc sử dụng khóa để ký của chủ thể ký được ủy quyền do SSASC thực thi thông qua quá trình xác thực chủ thể ký."; đối với SCAL2, "Việc sử dụng khóa để ký của chủ thể ký được ủy quyền do mô-đun kích hoạt chữ ký số thực thi thông qua

		dữ liệu kích hoạt chữ ký số do chủ thể ký cung cấp, sử dụng một giao thức kích hoạt chữ ký số, nhằm cho phép sử dụng khóa ký tương ứng để ký các tài liệu cụ thể.” Hình 2 thể hiện SCD trong SSASC; Hình 3 thể hiện SAM/SCD và “Giao thức kích hoạt chữ ký số (SAP)”.
2	Mô hình SCAL 1 không hợp lý. Đề xuất: Mô hình SCALI đang bao gồm cả thành phần tương tác của người ký đến ứng dụng máy chủ ký số để tạo SAD (Chỉ có ở SCAL 2)	Tiếp thu ý kiến góp ý; Nội dung tiếp thu được chỉnh sửa tại Hình 2, trang số 19
3	Bảng 26 dịch thiếu các mục cert/serialNumber. cert/subjectDN, multisign. Đề xuất Bổ sung dịch thuật	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo tại Bảng 26 trang 49
4	Tiêu chuẩn ETSI hỗ trợ nhiều mức Assurance Level trong khi tại Việt Nam chữ ký công cộng có giá trị pháp lý tương đương chữ ký tay và con dấu đồng thời chữ ký số từ xa đã quy định bắt buộc SCAL2. Nếu không quy định thống nhất mức bảo đảm sẽ có thể dẫn đến cách hiểu và triển khai không đồng nhất giữa các nhà cung cấp. Đề xuất: làm rõ các dịch vụ tin cậy khi áp dụng vào việt nam phải đáp ứng mực bảo đảm tương đương Qualified theo mô hình của ETSI, bảo đảm tính thống nhất trong triển khai và tránh áp dụng các mức bảo đảm thấp hơn	Tiếp thu ý kiến góp ý, bảo lưu; Giải trình lý do bảo lưu như sau: Dự thảo TCVN cần giữ cả SCAL1 và SCAL2 để phản ánh đầy đủ các mức bảo đảm mà giao thức hỗ trợ và bảo đảm khả năng tương thích. Yêu cầu đối với hệ thống ký số từ xa công cộng khi triển khai tại Việt Nam được xác định theo QCVN 137:2025/BKHCN và các quy định pháp luật có liên quan; việc áp dụng mức bảo đảm bắt buộc thuộc phạm vi quy chuẩn và điều kiện cung cấp dịch vụ, không nên loại bỏ SCAL1 hoặc sửa cấu trúc giao thức trong TCVN này.
2. Công ty Cổ phần Công nghệ EFY Việt Nam (EFY)		
1	Không có ý kiến	
3. Công ty Cổ phần Chữ ký số WinCA (WinCA)		

1	Trong Lời giới thiệu có nói “...bao gồm cả chữ ký số đủ mục kiện (Qualified Electronic Signature - QES)" Góp ý: cần giải thích rõ từ “mục kiện”, đó là khái niệm mới hay sai sót về câu chữ, chính tả. Tương tự với “mục chỉnh” trong Lời nói đầu. Đưa ra định nghĩa tiếng Việt với từ “Qualified", có thể dùng “Đủ điều kiện” hoặc “Đủ tiêu chuẩn”	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo tại Bảng chữ viết tắt thuộc Mục 3.3, trang số 12 là: “QES - Qualified Electronic Signature - Chữ ký điện tử đủ điều kiện” và “QSCD - Qualified electronic Signature Creation Device - Thiết bị tạo chữ ký điện tử đủ điều kiện”. Các lỗi “mục kiện” và “mục chỉnh” đã được loại bỏ khỏi dự thảo.
2	Không có điều khoản nào yêu cầu sử dụng HTTPS/TLS để bảo vệ kênh truyền. Góp ý: Bổ sung yêu cầu bắt buộc sử dụng TLS phiên bản tối thiểu (ví dụ TLS 1.2 trở lên) cho tất cả kết nối	Tiếp thu ý kiến góp ý, bảo lưu; Giải trình lý do bảo lưu như sau: Không bổ sung yêu cầu cố định TLS 1.2 vì việc cố định một phiên bản giao thức có thể nhanh chóng lạc hậu. Mục 7.7 quy định thành phần xác thực ứng dụng khách và xác định cơ chế xác thực cụ thể thuộc phạm vi triển khai của dịch vụ; các kết nối vẫn phải áp dụng cơ chế bảo vệ phù hợp với quy định an toàn hiện hành tại thời điểm triển khai.
3	Quy định yêu cầu xác thực chứng thư số p12	Tiếp thu ý kiến góp ý, bảo lưu; Giải trình lý do bảo lưu như sau: PKCS#12 (.p12/.pfx) là định dạng vùng chứa có thể lưu khóa bí mật, chứng thư chữ ký số và chuỗi chứng thư chữ ký số, không phải là một loại chứng thư hoặc giao thức xác thực. Dự thảo xác định thông tin xác thực chữ ký bằng credentialID đối với JSON; KeySelector được sử dụng trong hồ sơ truy xuất thông tin tại Mục 8.6. Vì vậy, không bổ sung yêu cầu xác thực chứng thư số p12.
4	Có thể bổ sung điều khoản mới về "Yêu cầu bảo mật kênh truyền"	Tiếp thu ý kiến góp ý, bảo lưu; Giải trình lý do bảo lưu như sau: Không bổ sung một điều khoản riêng về “Yêu cầu bảo mật kênh truyền” vì yêu cầu này thuộc kiến trúc, cấu hình và vận hành an toàn của hệ thống triển khai, không phải thành phần hoặc ngữ nghĩa của giao thức

4. Công ty Cổ phần VNPAY (VNPAY)		
1	Tại Hình 1: Các bước và thành phần dữ liệu của quy trình tạo chữ ký. Có mô tả "Bộ soạn thảo ĐTBS": nội dung này cần sửa thành "Bộ soạn thảo DTBS"	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo tại Hình 1 thuộc Mục 4.1, trang số 14 là: "Bộ soạn thảo DTBS". Dạng viết tắt "ĐTBS" đã được thay bằng "DTBS".
2	Tại Hình 1:Các bước và thành phần dữ liệu của quy trình tạo chữ ký. Có mô tả "Biểu diễn dữ liệu để ký (ĐTBSR)": nội dung này cần sửa thành "Biểu diễn dữ liệu để ký (DTBSR)"	Tiếp thu ý kiến góp ý. Nội dung tiếp thu được chỉnh sửa trong dự thảo tại Hình 1 thuộc Mục 4.1, trang số 14 là: "Thể hiện của dữ liệu cần ký (DTBSR)". Dạng viết tắt "ĐTBSR" đã được thay bằng "DTBSR".