

**PHÂN LOẠI CHỮ KÝ ĐIỆN TỬ: SO SÁNH TIẾP CẬN
PHÁP LÝ CỦA HOA KỲ, LIÊN MINH CHÂU ÂU VÀ VIỆT NAM**

CAO THỊ THUỶ NHƯ*

Ngày nhận bài: 05/09/2025

Ngày phản biện: 17/09/2025

Ngày đăng bài: 25/12/2025

Tóm tắt:

Trong bối cảnh chữ ký điện tử ngày càng được sử dụng phổ biến, việc phân loại chữ ký điện tử với tiêu chí phù hợp sẽ giúp xác định mức độ tin cậy, yêu cầu kỹ thuật và giá trị pháp lý tương ứng của từng loại chữ ký. Các hệ thống pháp luật trên thế giới đang áp dụng những cách tiếp cận phân loại chữ ký điện tử khác nhau, với sự khác biệt đáng kể về tiêu chí và định hướng lập pháp. Bài viết phân tích xu hướng, tiêu chí và mục đích của việc phân loại chữ ký điện tử; đối sánh với pháp luật Hoa Kỳ và Liên minh châu Âu (EU), qua đó đề xuất một số kiến nghị nhằm hoàn thiện khung pháp lý về chữ ký điện tử tại Việt Nam theo hướng nhất quán, phù hợp thực tiễn và hài hòa với xu thế quốc tế.

Từ khóa:

Giao dịch điện tử, chữ ký điện tử,

Abstract:

In the context of the growing use of electronic signatures, their classification based on appropriate criteria helps determine the level of reliability, technical requirements, and corresponding legal validity of each type of signature. Legal systems around the world adopt different approaches to classifying electronic signatures, with significant variations in criteria and legislative orientation. This article analyzes the trends, criteria, and purposes of such classifications; compares the approaches of U.S. and European Union (EU) law; and, on that basis, proposes recommendations to improve Vietnam's legal framework on electronic signatures in a consistent manner, aligned with practical needs and harmonized with international trends.

Keywords:

Electronic transactions, electronic

* TS., Trường Đại học Kinh tế - Luật, Đại học Quốc gia thành phố Hồ Chí Minh; Email: nhuctt@uel.edu.vn

chữ ký số, phân loại chữ ký điện tử signatures, digital signature
classification of electronic signatures

1. Đặt vấn đề

Trong bối cảnh chuyển đổi số, chữ ký điện tử (viết tắt CKĐT) ngày càng đóng vai trò quan trọng trong việc đảm bảo tính an toàn, tin cậy của giao dịch điện tử, thậm chí được xem là yếu tố trung tâm của khung pháp lý về kinh tế số¹. Để CKĐT phát huy hiệu quả vai trò nêu trên, việc xây dựng khung pháp lý phù hợp là cần thiết, trong đó bao hàm nội dung xác định hình thức và phân loại CKĐT.

Nhằm phân tích và đối sánh quy định về phân loại CKĐT trong ba hệ thống pháp luật Châu Âu, Hoa Kỳ và Việt Nam, bài viết trình bày lần lượt quy định của từng quốc gia/khu vực, sau đó so sánh điểm tương đồng, khác biệt về khái niệm, tiêu chí phân loại và giá trị pháp lý của các loại CKĐT, từ đó đưa ra đánh giá cùng một số gợi mở cho Việt Nam.

Để đạt mục tiêu trên, bài viết chủ yếu sử dụng hai phương pháp: (i) Phân tích, tổng hợp nhằm làm rõ các vấn đề lý luận, pháp lý và thực tiễn liên quan đến chủ đề; (ii) So sánh để chỉ ra điểm tương đồng, khác biệt giữa ba hệ thống pháp luật, làm cơ sở cho đánh giá và đề xuất.

Bài viết gồm ba nội dung chính. Trước hết, khái quát về CKĐT và phân loại CKĐT nhằm làm rõ một số vấn đề lý luận liên quan. Tiếp theo, phân tích quy định về phân loại CKĐT trong pháp luật Châu Âu, Hoa Kỳ và Việt Nam. Cuối cùng, so sánh ba hệ thống pháp luật, đánh giá và đưa ra gợi ý cho Việt Nam từ quan điểm tác giả.

2. Xu hướng, tiêu chí và mục đích phân loại chữ ký điện tử

Chữ ký điện tử (electronic signature), một cách chung nhất, là dữ liệu điện tử gắn liền hoặc kết hợp logic với thông điệp dữ liệu, với chức năng xác nhận danh tính người ký và thể hiện sự chấp thuận của họ². Dù mọi CKĐT đều thực hiện chức năng này, nhưng CKĐT vẫn được phân loại theo các tiêu chí bổ sung, tùy cách tiếp cận pháp lý của từng quốc gia.

¹ Harbhajan S. Kehal Varinder P. Singh (2005), *Digital Economy: Impacts, Influences and Challenges*, IGI Global, Chapter VI, p. 98-135.

² Luật mẫu của UNCITRAL về chữ ký điện tử: UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, Article 2(a).

2.1 Xu hướng tiếp cận phân loại chữ ký điện tử

Dưới góc độ pháp lý, việc phân loại CKĐT thường được tiếp cận theo hai xu hướng chính: tối thiểu (permissive) và chặt chẽ (prescriptive).

(i) Xu hướng tiếp cận tối thiểu (permissive): Các quốc gia theo xu hướng này thường không đặt nặng yếu tố công nghệ trong việc tạo lập CKĐT, và công nhận mọi hình thức dữ liệu điện tử đều có giá trị pháp lý như nhau với rất ít ngoại lệ, miễn là thể hiện được ý chí của người ký. Theo đó, pháp luật không can thiệp sâu vào việc phân loại CKĐT. Việc lựa chọn loại chữ ký và mức độ an toàn sẽ do các bên giao dịch quyết định và tự chịu rủi ro³.

(ii) Xu hướng tiếp cận chặt chẽ (prescriptive): Các quốc gia theo xu hướng này thường quy định rõ các loại CKĐT trong khung pháp lý, dựa trên tiêu chí kỹ thuật và mức độ an toàn. Với từng loại chữ ký, giá trị pháp lý được xác định tương ứng. Các loại chữ ký “mạnh” được chấp nhận rộng rãi, thậm chí bắt buộc trong một số giao dịch; và ngược lại⁴.

Hai xu hướng tiếp cận trên hoàn toàn đối lập, nhưng không thể khẳng định xu hướng nào ưu việt hơn, vì còn phụ thuộc vào điều kiện kinh tế - xã hội của từng quốc gia. Xu hướng tối thiểu (*permissive*) dễ áp dụng nhưng tiềm ẩn rủi ro trong việc chứng minh tính xác thực của chữ ký. Ngược lại, xu hướng chặt chẽ (*prescriptive*) có thể khắc phục hạn chế đó, song lại làm tăng chi phí và phức tạp hóa giao dịch.

Ngoài ra, một cách tiếp cận khác được xem là dung hòa, thường gọi là tiếp cận hai cấp (*two-tier*). Một mặt, pháp luật công nhận mọi dạng dữ liệu điện tử đều là CKĐT (theo *permissive*). Mặt khác, pháp luật vẫn phân tầng CKĐT, trao giá trị pháp lý cao hơn cho loại chữ ký đáp ứng yêu cầu kỹ thuật cao (theo *prescriptive*). Đây cũng là cách tiếp cận được UNCITRAL khuyến nghị trong Luật mẫu về chữ ký điện tử 2001⁵.

2.2 Tiêu chí phân loại và mục đích phân loại chữ ký điện tử

Các quốc gia theo xu hướng tiếp cận chặt chẽ (*prescriptive*), tùy theo mục

³ Emsigner, *The Legal Landscape of eSignatures: Understanding Global Regulations*, truy cập tại <https://blogs.emsigner.com/the-legal-landscape-of-esignatures-understanding-global-regulations>, truy cập ngày 19/8/2025.

⁴ emSigner, tldd số 3.

⁵ Adobe, *A global overview of electric signatures*, truy cập tại https://www.adobe.com/content/dam/dx-dc/pdf/ue/dc_esignatures_global_overview_ue.pdf, truy cập ngày 19/8/2025.

tiêu quản lý và định hướng phát triển CKĐT của mình, sẽ đặt ra những tiêu chí cụ thể để phân loại CKĐT. Khảo sát thực tiễn lập pháp cho thấy có hai tiêu chí phổ biến sau:

Tiêu chí thứ nhất: yêu cầu kỹ thuật đối với CKĐT.

Với tiêu chí này, nhà làm luật đưa ra các yêu cầu kỹ thuật nhằm phân chia cấp độ CKĐT. Ở cấp độ càng cao, CKĐT càng phải đáp ứng những tiêu chuẩn kỹ thuật nghiêm ngặt và được chứng thực bởi tổ chức cung cấp dịch vụ tin cậy, nhằm đảm bảo tính xác thực, toàn vẹn và không thể phủ nhận. Việc phân loại này cho phép pháp luật xác lập giá trị pháp lý tương ứng cho từng loại CKĐT, đồng thời giúp các bên nhận diện rõ rủi ro và lựa chọn loại chữ ký phù hợp với tính chất và giá trị giao dịch.

Tiêu chí thứ hai: phạm vi sử dụng CKĐT.

Theo tiêu chí này, nhà làm luật giới hạn phạm vi sử dụng từng loại CKĐT để phù hợp với đặc thù giao dịch của từng nhóm đối tượng (công chức, người dân và doanh nghiệp). Cách phân loại này giúp đưa ra yêu cầu kỹ thuật, cấp phép và quản lý phù hợp, giảm rủi ro và tối ưu hiệu quả giao dịch⁶. Nói cách khác, không phải mọi giao dịch đều cần CKĐT có mức độ bảo mật cao, nên việc khoanh vùng phạm vi sử dụng và áp dụng yêu cầu kỹ thuật tương ứng sẽ giúp phân bổ chi phí và hạ tầng hợp lý hơn.

Tóm lại, việc phân loại CKĐT phản ánh xu hướng tiếp cận chặt chẽ của các quốc gia trong xây dựng khung pháp lý về CKĐT. Mỗi tiêu chí phân loại hướng đến mục tiêu quản lý riêng: tiêu chí kỹ thuật nhằm xác lập thứ bậc giá trị pháp lý dựa trên mức độ tin cậy và bảo mật, trong khi tiêu chí về phạm vi sử dụng bảo đảm sự phù hợp với nhu cầu thực tiễn và tính chất của từng loại giao dịch.

3. Phân loại chữ ký điện tử theo pháp luật Hoa Kỳ, Liên minh châu Âu và Việt Nam

3.1 Phân loại chữ ký điện tử theo pháp luật Hoa Kỳ

Tại Hoa Kỳ, CKĐT được điều chỉnh chủ yếu bởi hai văn bản: Đạo luật Chữ ký Điện tử trong Thương mại Toàn cầu và Quốc gia (Electronic Signatures in Global and National Commerce Act - E-SIGN) năm 2000 do Quốc hội thông

⁶ Báo Đại biểu nhân dân, *Phân loại chữ ký điện tử theo phạm vi sử dụng*, truy cập tại <https://daibieunhandan.vn/phan-loai-chu-ky-dien-tu-theo-pham-vi-su-dung-post330751.html>, truy cập ngày 19/8/2025.

qua, tạo cơ sở pháp lý chung ở cấp liên bang; và Đạo luật Giao dịch Điện tử thống nhất (Uniform Electronic Transactions Act - UETA) năm 1999 do Ủy ban Luật thống nhất (ULC) ban hành để các tiểu bang tự nguyện nội luật hóa.

Hoa Kỳ tiếp cận theo hướng tối thiểu (permissive). Cả Đạo luật Chữ ký Điện tử trong Thương mại Toàn cầu và Quốc gia và Đạo luật Giao dịch Điện tử thống nhất đều không phân loại CKĐT theo tiêu chí nào. Thay vào đó, pháp luật chỉ đưa ra định nghĩa chung về CKĐT⁷, trong đó chấp nhận mọi hình thức dữ liệu điện tử đều là CKĐT, bao gồm chữ ký scan, nhấn nút “đồng ý”, xác thực qua email, mã PIN... Pháp luật Hoa Kỳ cũng không yêu cầu CKĐT phải được bảo đảm bởi chứng thư hay sử dụng phương tiện kỹ thuật cụ thể⁸. Mọi công nghệ đều được chấp nhận, miễn đáp ứng yêu cầu cơ bản: gắn với thông điệp dữ liệu và thể hiện sự chấp thuận của người ký.

Đồng thời, Đạo luật Chữ ký Điện tử trong Thương mại Toàn cầu và Quốc gia và Đạo luật Giao dịch Điện tử thống nhất cũng không đưa ra định nghĩa chính thức về chữ ký số như một dạng đặc biệt của CKĐT. UETA khẳng định đây không phải là đạo luật về chữ ký số, mà chỉ được thiết kế để hỗ trợ và bổ sung cho luật tiểu bang nếu tiểu bang có luật riêng về chữ ký số⁹. Dù sử dụng công nghệ mã hóa khóa công khai, chữ ký số cũng chỉ được xem là một hình thức CKĐT, tương tự việc nhập tên vào cuối email. Trong cả hai trường hợp, yếu tố quyết định tính hợp pháp không phải là công nghệ mà là ý định xác nhận nội dung văn bản của người ký¹⁰.

Trên tinh thần không phân loại và không ưu tiên loại CKĐT nào, mọi CKĐT đều không bị phủ nhận giá trị pháp lý theo pháp luật Hoa Kỳ. Một chữ ký không thể bị từ chối hiệu lực chỉ vì được thể hiện dưới dạng điện tử. Nếu pháp luật yêu cầu chữ ký, thì mọi CKĐT đều đáp ứng yêu cầu đó¹¹. Quy định này nhằm xóa bỏ việc phương tiện điện tử bị coi là lý do duy nhất để phủ nhận hiệu lực của hồ sơ, chữ ký hay hợp đồng¹².

CKĐT cũng được chấp nhận làm chứng cứ tại tòa như chữ ký tay. Đạo luật

⁷ E-Sign (Definitions), UETA (Section 2 (8)).

⁸ UETA (Section 2, Comment 7).

⁹ UETA (Prefatory note).

¹⁰ UETA (Section 2, Comment 7).

¹¹ E-SIGN (Introduction), UETA (Section 7 (a)(d)).

¹² UETA (Section 7, Comment 1).

Giao dịch Điện tử thống nhất khẳng định rằng trong tố tụng, bằng chứng về chữ ký không thể bị loại trừ chỉ vì chúng ở dạng điện tử¹³. Quy định này nhằm ngăn chặn việc từ chối công nhận CKĐT chỉ vì hình thức thể hiện. Tuy nhiên, các bên vẫn phải chứng minh tính xác thực của CKĐT để được chấp nhận¹⁴.

3.2 Phân loại chữ ký điện tử pháp luật của Liên minh châu Âu

Ở châu Âu, khung pháp lý về CKĐT được điều chỉnh bởi Quy định về nhận dạng điện tử và dịch vụ tin cậy cho giao dịch điện tử (eIDAS). Được ban hành lần đầu năm 2014, eIDAS thay thế Chỉ thị 1999/93/EC vốn chỉ tập trung vào CKĐT và không mang tính bắt buộc. Với eIDAS 2014, EU lần đầu tiên thiết lập một hệ thống pháp lý thống nhất cho nhận dạng điện tử và các dịch vụ tin cậy, sau đó được sửa đổi năm 2024 để triển khai Ví danh tính số châu Âu (EUDI Wallet) và nâng cao mức độ bảo mật, tương thích của CKĐT.

EU tiếp cận hài hòa giữa hai xu hướng tối thiểu và chặt chẽ. Theo đó, eIDAS công nhận mọi hình thức xác nhận bằng phương tiện điện tử là CKĐT thông qua định nghĩa CKĐT¹⁵ - tương tự cách tiếp cận trong E-SIGN và UETA của Hoa Kỳ. Tuy nhiên, khác với pháp luật Hoa Kỳ, eIDAS lại phân CKĐT thành hai loại dựa trên tiêu chí kỹ thuật, bao gồm:

(1) Chữ ký điện tử nâng cao (AdES – Advanced Electronic Signature):

AdES là CKĐT đáp ứng các yêu cầu sau: (i) liên kết duy nhất với người ký; (ii) cho phép xác định danh tính người ký; (iii) được tạo bằng dữ liệu tạo chữ ký mà người ký có thể kiểm soát duy nhất với mức độ tin cậy cao; (iv) gắn với dữ liệu được ký theo cách bảo đảm mọi thay đổi đều bị phát hiện¹⁶. Các yêu cầu trên cho thấy AdES được thiết kế để đảm bảo mức độ an toàn và tin cậy cao hơn những hình thức xác nhận điện tử đơn giản.

(2) Chữ ký điện tử đủ điều kiện (QES – Qualified Electronic Signature)

QES là CKĐT nâng cao (AdES) được tạo ra bằng thiết bị tạo chữ ký đủ điều kiện và được bảo đảm bởi chứng thư CKĐT đủ điều kiện¹⁷. Điều này có nghĩa rằng QES bản thân nó phải đáp ứng tiêu chuẩn của AdES, sau đó đáp ứng thêm hai điều kiện:

¹³ UETA (Section 13).

¹⁴ UETA (Section 13, Comment).

¹⁵ eIDAS 2014, Article 3(10).

¹⁶ eIDAS 2014, Article 3(11), Article 26.

¹⁷ eIDAS 2014, Article 3(12).

Thứ nhất, được tạo ra bằng thiết bị tạo chữ ký đủ điều kiện.

Thiết bị tạo chữ ký phải đáp ứng các yêu cầu bảo mật cao, bao gồm: (1) Đảm bảo dữ liệu tạo chữ ký được bảo mật, chỉ sử dụng một lần, không thể bị suy luận hay giả mạo, và chỉ người ký mới có quyền kiểm soát, sử dụng; (2) Không được phép thay đổi dữ liệu cần ký hoặc ngăn cản việc hiển thị đầy đủ dữ liệu cho người ký trước khi thực hiện ký¹⁸.

Thứ hai, được bảo đảm bởi chứng thư CKĐT đủ điều kiện.

Nội dung của chứng thư CKĐT đủ điều kiện phải bao gồm các thông tin: dấu hiệu nhận dạng đây là chứng thư đủ điều kiện; danh tính người ký; thông tin về nhà cung cấp dịch vụ tin cậy; thời hạn hiệu lực; dữ liệu xác thực chữ ký; mã định danh của chứng thư; chữ ký/ con dấu số của nhà cung cấp; địa chỉ để kiểm tra trạng thái hiệu lực của chứng thư¹⁹.

Như vậy, so với AdES, QES có yêu cầu kỹ thuật nghiêm ngặt hơn. Trong khi AdES chỉ cần đảm bảo liên kết duy nhất với người ký và khả năng phát hiện thay đổi sau khi ký, thì QES bổ sung lớp bảo mật từ phân cứng và chứng thực của bên thứ ba – yêu cầu giúp QES trở thành loại CKĐT tiêu chuẩn cao nhất ở châu Âu.

Ngoài hai loại CKĐT trên, một số quan điểm cho rằng EU còn thừa nhận CKĐT thông thường (Simple Electronic Signature – SES), được xem là cấp độ thấp nhất trong hệ thống CKĐT²⁰. Tuy nhiên, SES không phải là thuật ngữ chính thức trong eIDAS và cũng không được định nghĩa hay quy định riêng. Do đó, dưới góc nhìn của bài viết, SES dùng để chỉ phần còn lại của CKĐT (các hình thức xác nhận điện tử đơn giản ngoài AdES và QES) – một thuật ngữ phổ biến nhưng không chính thức.

Về giá trị pháp lý, mọi loại CKĐT đều không thể bị từ chối hiệu lực hoặc giá trị chứng cứ chỉ vì ở dạng điện tử hay không đạt chuẩn QES, nhằm bảo đảm công bằng và thúc đẩy công nhận giao dịch điện tử trong toàn EU²¹. Dù vậy, eIDAS chỉ công nhận giá trị tương đương chữ ký tay đối với QES²². Đặc biệt, QES được cấp tại một quốc gia thành viên EU sẽ được công nhận hợp lệ tại tất cả các quốc

¹⁸ eIDAS 2014, Annex II; eIDAS 2024, bãi bỏ yêu cầu 3, 4 trong Annex II của eIDAS 2014.

¹⁹ eIDAS 2014, Annex I; eIDAS 2024, sửa đổi nội dung (i) trong Annex I của eIDAS 2014.

²⁰ Trần Thị Bảo Ánh, Nguyễn Khánh Linh (2024), *Chữ ký điện tử và chữ ký số trong giao dịch điện tử - Thực tiễn và giải pháp hoàn thiện pháp luật*, Kỷ yếu Hội thảo Giao dịch điện tử và giải quyết các tranh chấp về giao dịch điện tử, Học viện Tòa án, Hà Nội, tr. 108-128.

²¹ eIDAS 2014, Article 25.1.

²² eIDAS 2014, Article 25.2.

gia thành viên khác²³, bảo đảm tính tương thích và tin cậy xuyên biên giới trong không gian số Châu Âu.

3.3 Phân loại chữ ký điện tử theo pháp luật Việt Nam

Ở Việt Nam, CKĐT được điều chỉnh bởi Luật Giao dịch điện tử năm 2023 và Nghị định 23/2025/NĐ-CP. So với Luật Giao dịch điện tử năm 2005 và Nghị định 130/2018/NĐ-CP trước đây, khung pháp lý hiện tại phản ánh sự thay đổi đáng kể trong tư duy lập pháp.

Theo Luật Giao dịch điện tử năm 2023, CKĐT là chữ ký được tạo lập dưới dạng dữ liệu điện tử gắn liền hoặc kết hợp một cách logic với thông điệp dữ liệu để xác nhận chủ thể ký và sự chấp thuận của họ đối với thông điệp dữ liệu. Trong khi đó, chữ ký số là CKĐT sử dụng thuật toán khóa không đối xứng, gồm khóa bí mật (dùng để ký số) và khóa công khai (dùng để kiểm tra chữ ký số), nhằm bảo đảm tính xác thực, tính toàn vẹn và tính chống chối bỏ nhưng không bảo đảm tính bí mật của thông điệp dữ liệu²⁴. Như vậy, có thể thấy, CKĐT là khái niệm rộng, còn chữ ký số là khái niệm hẹp hơn, với các yêu cầu kỹ thuật chặt chẽ hơn.

Không có tài liệu chính thức nào khẳng định việc Việt Nam theo xu hướng tiếp cận tối thiểu, chặt chẽ hay dung hòa. Tuy nhiên, dưới góc nhìn của mình, bài viết cho rằng Việt Nam theo xu hướng tiếp cận chặt chẽ. Với khái niệm CKĐT là “chữ ký”, Luật đã loại bỏ những hình thức xác nhận đơn giản (FIDO, OTP, SMS, chữ ký scan...) ra khỏi diện CKĐT²⁵. Đây chính là điểm khác biệt giữa pháp luật Việt Nam với pháp luật Hoa Kỳ và EU, đồng thời thể hiện sự thay đổi trong cách tiếp cận so với chính Luật Giao dịch điện tử năm 2005²⁶. Sự thay đổi này xuất phát từ lập luận rằng các hình thức xác nhận đơn giản tuy thể hiện sự chấp thuận của chủ thể ký, nhưng lại thiếu tính chống chối bỏ như CKĐT²⁷.

Trên tinh thần đó, CKĐT được phân thành ba loại dựa trên tiêu chí phạm vi sử dụng - tức CKĐT được sử dụng vào mục đích gì và bởi chủ thể nào:

²³ eIDAS 2014, Article 25.3; eIDAS 2024, Article 1(22) inserting Article 24a into eIDAS 2014.

²⁴ Điều 3.11, 3.12 Luật Giao dịch điện tử năm 2023.

²⁵ Điều 3.11, 22.4 Luật Giao dịch điện tử năm 2023.

²⁶ Điều 21.1 Luật Giao dịch điện tử năm 2005.

²⁷ NEAC, *OTP không phải là chữ ký điện tử*, truy cập tại <https://neac.gov.vn/vi/tin-tuc-su-kien/detail/otp-khong-phai-la-chu-ky-dien-tu-577.htm>, truy cập ngày 19/8/2025.

(1) CKĐT chuyên dùng: là CKĐT do cơ quan, tổ chức tự tạo lập²⁸ mà không sử dụng dịch vụ của các nhà cung cấp dịch vụ chứng thực chữ ký số công cộng. Dù vậy, CKĐT chuyên dùng vẫn phải đáp ứng đủ các yêu cầu về (i) xác thực danh tính và sự chấp thuận của người ký; (ii) gắn với thông điệp dữ liệu; (iii) thuộc sự kiểm soát của người ký; và (iv) có thể kiểm tra hiệu lực²⁹. Dù đáp ứng các yêu cầu cơ bản của một CKĐT³⁰, nhưng do tiêu chuẩn thấp hơn chữ ký số³¹ nên phạm vi sử dụng CKĐT chuyên dùng bị giới hạn trong (i) hoạt động nội bộ của cơ quan, tổ chức; (ii) hoạt động chuyên ngành hoặc lĩnh vực có liên kết; (iii) đại diện cơ quan, tổ chức trong giao dịch với chủ thể khác³².

(2) Chữ ký số công cộng: là chữ ký số được sử dụng trong hoạt động công cộng³³. Do là chữ ký số (cấp độ cao của CKĐT), chữ ký số công cộng phải đáp ứng các yêu cầu kỹ thuật cao hơn so với CKĐT chuyên dùng: (i) khả năng phát hiện thay đổi thông điệp dữ liệu sau khi ký; (ii) được bảo đảm bởi chứng thư chữ ký số; (iii) phương tiện tạo chữ ký phải an toàn, sử dụng duy nhất và đảm bảo tính toàn vẹn của dữ liệu ký³⁴. Với các yêu cầu kỹ thuật như vậy, chữ ký số công cộng phải được cung cấp bởi tổ chức chứng thực chữ ký số công cộng được cấp phép³⁵.

(3) Chữ ký số chuyên dùng công vụ: là chữ ký số được sử dụng trong hoạt động công vụ, bởi chủ thể đặc biệt là cán bộ, công chức³⁶. Do vẫn mang bản chất là chữ ký số, chữ ký số chuyên dùng công vụ phải đáp ứng yêu cầu kỹ thuật tương tự chữ ký số công cộng³⁷. Tuy nhiên, với đặc thù phạm vi sử dụng, chữ ký này được cấp bởi một chủ thể đặc biệt – Cục Chứng thực số và Bảo mật thông tin, trực thuộc Ban Cơ yếu Chính phủ – thay vì các CA công cộng, nhằm bảo đảm an ninh, tính pháp lý và bảo mật tuyệt đối cho hoạt động công vụ³⁸.

Về giá trị pháp lý, CKĐT không bị phủ nhận giá trị pháp lý chỉ vì được thể

²⁸ Điều 22.1a Luật Giao dịch điện tử năm 2023.

²⁹ Điều 22.2 Luật Giao dịch điện tử năm 2023.

³⁰ Điều 3.11 Luật Giao dịch điện tử năm 2023.

³¹ Điều 3.12, 22.2, 22.3 Luật Giao dịch điện tử năm 2023.

³² Điều 9.2 Nghị định 23/2025/NĐ-CP. Quy định này chỉ áp dụng với CKĐT chuyên dùng đảm bảo an toàn.

³³ Điều 22.1b Luật Giao dịch điện tử năm 2023.

³⁴ Điều 22.3 Luật Giao dịch điện tử năm 2023.

³⁵ Điều 18 Nghị định 23/2025/NĐ-CP.

³⁶ Điều 22.1c Luật Giao dịch điện tử 2023; Điều 5.1 Luật Cán bộ, công chức năm 2025.

³⁷ Điều 22.3 Luật Giao dịch điện tử năm 2023.

³⁸ Điều 3.4 Nghị định 68/2024/NĐ-CP.

hiện dưới dạng điện tử³⁹, tương tự nguyên tắc được ghi nhận trong E-SIGN, UETA và eIDAS. Tuy nhiên, pháp luật Việt Nam chỉ ghi nhận giá trị tương đương chữ ký tay đối với chữ ký số và CKĐT chuyên dùng đảm bảo an toàn⁴⁰. Riêng đối với các hình thức xác nhận khác bằng phương tiện điện tử (FIDO, OTP, SMS, chữ ký scan...), dù không được công nhận là CKĐT nhưng cũng không bị phủ nhận hoàn toàn, mà vẫn được phép sử dụng trong những lĩnh vực cụ thể theo quy định pháp luật liên quan⁴¹. Lý giải của cơ quan lập pháp, quy định này cần thiết để phù hợp với thực tiễn, hỗ trợ giao dịch số diễn ra thuận lợi, đồng thời phân biệt rõ với CKĐT nhằm bảo đảm tính pháp lý chặt chẽ khi cần.

4. So sánh cách tiếp cận phân loại chữ ký điện tử của Hoa Kỳ, Liên minh châu Âu, Việt Nam và định hướng giải pháp

4.1 So sánh cách tiếp cận phân loại chữ ký điện tử của Hoa Kỳ, Liên minh châu Âu và Việt Nam

Trên cơ sở phân tích pháp luật Hoa Kỳ, EU và Việt Nam về phân loại CKĐT, phân tiếp theo sẽ tiến hành so sánh ba hệ thống pháp luật dựa trên ba tiêu chí sau:

Thứ nhất, về xu hướng tiếp cận.

Trong các xu hướng tiếp cận khi xây dựng khung pháp lý về CKĐT, Hoa Kỳ theo hướng tối thiểu. Đạo luật E-SIGN và UETA công nhận mọi hình thức dữ liệu điện tử là CKĐT, không đặt nặng yếu tố kỹ thuật, không phân loại chữ ký và không ưu tiên giá trị pháp lý cho bất kỳ loại nào. Các đạo luật này thậm chí không đề cập đến chữ ký số – loại chữ ký được các quốc gia xem là chuẩn mực. Điều đó phản ánh triết lý pháp luật Hoa Kỳ đề cao tự do giao kết: luật chỉ đảm bảo CKĐT không bị phân biệt đối xử, còn lại do các bên tự đánh giá.

Ngược lại, Việt Nam theo hướng tiếp cận chặt chẽ khi chỉ công nhận những CKĐT đáp ứng yêu cầu kỹ thuật. Từng loại CKĐT được quy định cụ thể về phạm vi sử dụng, đơn vị cung cấp và quy trình chứng thực, phản ánh mục tiêu quản lý và bảo đảm an toàn cho giao dịch. Quan điểm này dựa trên bối cảnh Việt Nam, nơi giao dịch điện tử phát triển nhanh, nhưng hạ tầng công nghệ và pháp lý vẫn đang hoàn thiện, cùng với nhu cầu hội nhập thúc đẩy việc phải xây dựng

³⁹ Điều 23.1 Luật Giao dịch điện tử năm 2023.

⁴⁰ Điều 23.2 Luật Giao dịch điện tử năm 2023. Xem thêm điều kiện công nhận CKĐT chuyên dùng đảm bảo an toàn tại Điều 9.1, 4.4, 10, 11 Nghị định 23/2025/NĐ-CP.

⁴¹ Điều 22.4 Luật Giao dịch điện tử năm 2023.

khung pháp lý chặt chẽ.

Dung hòa hai xu hướng trên, EU lựa chọn cách tiếp cận hai cấp. eIDAS công nhận mọi hình thức xác nhận điện tử là CKĐT, đồng thời thiết lập hai cấp độ: “trung” (AdES) và “cao” (QES), kèm theo giá trị pháp lý tương ứng. Cách tiếp cận này phù hợp với bối cảnh EU – nơi 27 quốc gia thành viên cần một khuôn khổ hài hòa để áp dụng thống nhất, không quá linh hoạt cũng không cứng nhắc. Ngoài ra, nhu cầu giao dịch xuyên biên giới đòi hỏi chuẩn CKĐT đủ tin cậy để tạo điều kiện công nhận lẫn nhau trên toàn khối.

Thứ hai, về tiêu chí phân loại CKĐT.

Cùng theo xu hướng tiếp cận chặt chẽ, nhưng EU và Việt Nam lại có tiêu chí phân loại CKĐT khác nhau. EU phân loại theo mức độ tin cậy và an toàn, trong khi Việt Nam dựa vào phạm vi sử dụng. Hai tiêu chí tưởng chừng khác biệt nhưng thực tế có sự giao thoa. Việt Nam tuyên bố phân loại CKĐT theo phạm vi sử dụng nhưng trước đó đã dùng tiêu chí kỹ thuật để loại trừ các hình thức xác nhận đơn giản. Sau đó, tiêu chí công nghệ được dùng để phân biệt chữ ký số và CKĐT chuyên dùng. Trong cùng tầng chữ ký số, pháp luật mới tiếp tục phân loại theo phạm vi sử dụng.

Xét thêm về chữ ký số công cộng và chữ ký số chuyên dùng công vụ, pháp luật EU và Hoa Kỳ không phân loại tách bạch như Việt Nam nhưng vẫn thiết lập chữ ký số riêng cho khu vực công. Ở châu Âu, QES thường dùng trong hoạt động công vụ, và nhiều quốc gia EU đã xây dựng hệ thống QES riêng cho khu vực công. Chẳng hạn, tại Đức, QES được sử dụng trong dịch vụ công và hành chính điện tử, với hạ tầng của các nhà cung cấp dịch vụ tin cậy đủ điều kiện như D-Trust để cấp chứng thư số cho công chức⁴². Tương tự, tại Hoa Kỳ, dù E-SIGN và UETA không phân loại CKĐT, các cơ quan công quyền vẫn sử dụng Hạ tầng khóa công khai (Public Key Infrastructure – PKI) riêng cho hoạt động công vụ, gồm PKI liên bang, PKI riêng của các tiểu bang, và Federal Bridge CA (FBCA) đóng vai trò kết nối, công nhận chéo giữa các cấp thông qua việc cấp chứng nhận chéo (cross-certification)⁴³.

⁴² Bundesdruckerei, *Digital signatures – legally binding and mobile*, truy cập tại <https://www.bundesdruckerei.de/en/innovation-hub/digital-signatures-legally-binding-convenient-and-mobile>, truy cập ngày 19/8/2025.

⁴³ U.S. General Services Administration, *Federal Public Key Infrastructure 101*, truy cập tại <https://www.idmanagement.gov/university/fpki/>, truy cập ngày 19/8/2025.

Thứ ba, về việc công nhận giá trị pháp lý của các loại CKĐT.

Trong khi pháp luật Hoa Kỳ không phân biệt giá trị pháp lý giữa các loại CKĐT, thì EU và Việt Nam lại đề cao các loại CKĐT có mức độ bảo đảm cao hơn. Cụ thể, EU công nhận QES có giá trị pháp lý tương đương chữ ký tay và hiệu lực này được thừa nhận trong toàn bộ khối thành viên. Tương tự, pháp luật Việt Nam cũng công nhận giá trị tương đương chữ ký tay đối với chữ ký số và CKĐT chuyên dùng đảm bảo an toàn. Với các loại CKĐT không thuộc nhóm trên, cả EU và Việt Nam đều không mặc nhiên công nhận giá trị tương đương chữ ký tay, dù vẫn cho phép sử dụng. Trong những trường hợp này, hiệu lực pháp lý sẽ phụ thuộc vào thỏa thuận giữa các bên hoặc do cơ quan tổ tụng xem xét, đánh giá.

4.2 Giải pháp gợi mở cho Việt Nam

Mỗi quốc gia sẽ lựa chọn cách tiếp cận phù hợp tùy theo bối cảnh và mục tiêu lập pháp riêng. EU được đánh giá cao với eIDAS – khuôn khổ pháp lý kiểu mẫu tạo dựng niềm tin vào QES⁴⁴, giúp thúc đẩy giao dịch trong khối⁴⁵. Ngược lại, Hoa Kỳ theo hướng linh hoạt, tin vào thị trường, với E-SIGN và UETA khuyến khích mạnh mẽ CKĐT nhờ thủ tục đơn giản, chi phí thấp, qua đó thúc đẩy ứng dụng rộng rãi trong thương mại cũng như được chấp nhận trong hệ thống tư pháp⁴⁶.

Tại Việt Nam, Luật Giao dịch điện tử năm 2023 thể hiện định hướng quản lý chặt chẽ hơn và thực tế đã đạt được những kết quả nhất định trong mục tiêu chuyển đổi số quốc gia⁴⁷. Liên quan đến vấn đề phân loại CKĐT, như đã phân tích, Việt Nam phân CKĐT thành ba loại và không bao gồm các hình thức xác nhận điện tử đơn giản. Cách tiếp cận này phản ánh quan điểm cần xây dựng hệ thống CKĐT đáp ứng tiêu chuẩn kỹ thuật, hướng đến an toàn giao dịch và khả năng được công nhận rộng rãi ở nước ngoài, nhất là khi công nghệ đã phát triển hơn so với thời điểm ban hành Luật Giao dịch điện tử năm 2005. Tuy nhiên,

⁴⁴ Bundesdruckerei, tld số 42.

⁴⁵ EDICOM Group, *eIDAS: 5 years making transactions more secure in the European Union*, <https://edicomgroup.com/blog/eidas-5-years-making-transactions-more-secure-in-the-european-union>, truy cập ngày 19/8/2025.

⁴⁶ Parker Poe, *Using Electronic Signatures*, truy cập tại <https://www.parkerpoe.com/news/2016/10/using-electronic-signatures>, truy cập ngày 19/8/2025.

⁴⁷ Bộ Thông tin và Truyền thông (2023), *Báo cáo tình hình ứng dụng và phát triển chữ ký số tại Việt Nam năm 2024*, NXB Thông tin và Truyền thông.

tác giả cho rằng việc loại trừ các hình thức xác nhận điện tử đơn giản là chưa thực sự phù hợp.

Thứ nhất, các hình thức xác nhận điện tử đơn giản vẫn mang bản chất của CKĐT.

CKĐT dù được thể hiện dưới hình thức phi truyền thống nhưng vẫn mang bản chất của chữ ký truyền thống: xác nhận chủ thể ký và sự chấp thuận với nội dung ký. Với bản chất và chức năng đó, các hình thức xác nhận điện tử dù đơn giản hay phức tạp đều phù hợp với bản chất CKĐT. Khi đó, dù chỉ là tên đánh máy trong email, nhưng nếu xác định được danh tính người gửi và sự đồng ý của họ với nội dung email, thì cũng được xem là CKĐT.

Minh chứng cho nhận định trên, nhiều án lệ tại Hoa Kỳ đã khẳng định tính hợp lệ của các hình thức xác nhận đơn giản, như vụ *Cloud Corp. v. Hasbro, Inc.* (2002) công nhận việc gõ tên trong email là đủ để hành vi ký kết có hiệu lực⁴⁸. Tòa án cũng từng thừa nhận việc nhập tên trên hợp đồng là đủ để tạo thành sự chấp thuận trong vụ kiện *Zulkiewski v. General American Life Insurance Co* (2021)⁴⁹. Trong khi đó, một số án lệ khác cho thấy CKĐT, dù tạo qua nền tảng uy tín như DocuSign, vẫn có thể bị Tòa bác bỏ nếu không chứng minh được ý định ký kết rõ ràng hoặc thiếu bằng chứng xác thực về danh tính và công nghệ sử dụng. Chẳng hạn, vụ *Park v. NMSI, Inc.* (2023), vụ *AJ Equity Group LLC v. The Office Connection, Inc.* (2023) hay vụ *Fabian v. Renovate America, Inc.* (2019)⁵⁰.

Quan điểm học thuật cũng đồng tình rằng điều cốt yếu của chữ ký là thể hiện danh tính và ý chí, không phụ thuộc vào hình thức kỹ thuật. Chẳng hạn, Báo cáo nghiên cứu của Ủy ban pháp luật Anh nhấn mạnh không nên phủ nhận giá trị chỉ vì hình thức điện tử đơn giản, miễn có ý định rõ ràng⁵¹. Tương tự, quan điểm ủng hộ nguyên tắc trung lập công nghệ cũng được thể hiện trong các nghiên cứu pháp lý ở Việt Nam⁵².

⁴⁸ Roaa Al-Heeti, *Electronic Signatures*, truy cập tại <https://www.atgf.com/tools-publications/pubs/electronic-signatures>, truy cập ngày 19/8/2025.

⁴⁹ UnicornForms, *ESIGN & UETA Compliance*, truy cập tại <https://www.unicornforms.com/blog/esign-ueta-compliance#>, truy cập ngày 19/8/2025.

⁵⁰ UnicornForms, tld số 49.

⁵¹ Law Commission (UK) (2019), *Electronic Execution of Documents*, Law Commission Electronic execution of documents, truy cập ngày 19/8/2025.

⁵² Nguyễn Thị Kim Hồng, Nguyễn Hào Khang, *Công nhận các loại chữ ký điện tử khác theo pháp luật Việt Nam và một số quốc gia*, truy cập tại <https://tapchitoaan.vn/cong-nhan-cac-loai-chu-ky-dien-tu-khac-theo-phap-luat-viet-nam-va-mot-so-quoc-gia13224.html>, truy cập ngày 19/8/2025.

Thứ hai, việc không công nhận các hình thức xác nhận điện tử đơn giản sẽ ảnh hưởng đến giá trị pháp lý của chúng.

Dù pháp luật Việt Nam vẫn cho phép sử dụng các hình thức xác nhận điện tử đơn giản nhằm tránh xung đột với pháp luật chuyên ngành, đáp ứng nhu cầu thực tiễn⁵³ và đảm bảo quyền tự định đoạt trong giao dịch dân sự, nhưng việc không công nhận các hình thức này là CKĐT sẽ ảnh hưởng đến giá trị pháp lý và độ tin cậy của chúng. Nếu được xem là CKĐT, các hình thức này sẽ chịu sự điều chỉnh của Luật Giao dịch điện tử. Khi đó, giá trị pháp lý sẽ được ghi nhận rõ ràng, đặc biệt là nguyên tắc không phủ nhận giá trị pháp lý chỉ vì hình thức thể hiện. Dù không thể có giá trị tương đương chữ ký tay do chưa đáp ứng yêu cầu kỹ thuật, các hình thức này vẫn có độ tin cậy nhất định trong giao dịch và được chấp nhận làm chứng cứ trong tố tụng. Ngược lại, nếu không được công nhận là CKĐT, chúng sẽ nằm ngoài phạm vi điều chỉnh của Luật Giao dịch điện tử, không được khẳng định giá trị pháp lý, từ đó giảm độ tin cậy và giá trị chứng cứ. Đây là sự loại trừ không cần thiết, không giúp giảm chi phí thực thi luật, trong khi việc công nhận lại mang nhiều lợi ích, nhất là khi các hình thức này vẫn được sử dụng phổ biến.

Từ những bất cập nêu trên, tác giả cho rằng pháp luật Việt Nam nên cân nhắc thừa nhận mọi hình thức xác nhận điện tử là CKĐT, miễn đáp ứng chức năng xác thực danh tính và thể hiện sự chấp thuận của người ký. Cách tiếp cận này tương đồng với pháp luật Hoa Kỳ, EU và cũng từng được quy định trong Luật Giao dịch điện tử 2005. Song song đó, Luật Giao dịch điện tử cũng cần bổ sung một số quy định:

Một là, trao quyền cho luật chuyên ngành quy định loại CKĐT phù hợp với đặc thù của từng lĩnh vực. Theo đó, Luật Giao dịch điện tử chỉ dừng ở việc thừa nhận mọi hình thức xác nhận điện tử, nếu đáp ứng chức năng xác thực danh tính và thể hiện sự chấp thuận, đều được coi là CKĐT. Đồng thời, luật cần quy định mở, cho phép từng lĩnh vực chuyên ngành xác định loại CKĐT phù hợp để áp dụng bắt buộc. Trên cơ sở đó, luật chuyên ngành có thể đặt ra yêu cầu riêng tùy theo tính chất của lĩnh vực. Chẳng hạn, trong lĩnh vực công chứng, vốn yêu cầu

⁵³ Thái Mạnh Cường, *Chuyển đổi số gặp trở ngại vì quy định chữ ký*, truy cập tại <https://thesaigontimes.vn/chuyen-doi-so-gap-tro-ngai-vi-quy-dinh-chu-ky/>, truy cập ngày 19/8/2025.

mức độ xác thực danh tính cao và ràng buộc pháp lý chặt chẽ, thì bắt buộc phải sử dụng chữ ký số⁵⁴. Ngược lại, trong các giao dịch dân sự thông thường, pháp luật không can thiệp, đồng nghĩa với việc chấp nhận cả những hình thức xác nhận điện tử đơn giản.

Hai là, ràng buộc trách nhiệm lưu trữ và xác thực lâu dài đối với các phương thức xác nhận điện tử đơn giản. Chẳng hạn, với clickwrap, hệ thống cần ghi nhận đầy đủ log: thời gian, địa chỉ IP, trình duyệt, nội dung đồng ý... để chứng minh hành vi người dùng. Với OTP, cần lưu bằng chứng gửi mã, thời điểm, số điện thoại nhận và xác nhận thành công. Hướng quy định này tương tự UETA (Hoa Kỳ), theo đó: “Bên lưu trữ hồ sơ điện tử phải bảo đảm tài liệu được giữ an toàn, toàn vẹn, có thể truy cập và kiểm tra khi cần thiết”⁵⁵. Việc quy định rõ nghĩa vụ kỹ thuật này giúp bảo đảm tính toàn vẹn hồ sơ, đồng thời tăng giá trị chứng cứ trong xử lý tranh chấp giao dịch điện tử.

5. Kết luận

Cách phân loại CKĐT ở ba hệ thống pháp luật có sự giao thoa nhưng cũng tồn tại những khác biệt. Hoa Kỳ có xu hướng không phân loại rạch ròi CKĐT nhằm thúc đẩy sự linh hoạt trong giao dịch, trong khi EU và Việt Nam lại phân loại CKĐT để khuyến khích phát triển và sử dụng các loại CKĐT an toàn. So sánh tổng thể, nội hàm CKĐT trong pháp luật Việt Nam là hẹp nhất và có tiêu chí phân loại chi tiết nhất. Sự khác biệt này xuất phát từ định hướng phát triển rõ ràng và nhu cầu quản lý chặt chẽ từng loại CKĐT. Tuy vậy, việc thu hẹp nội hàm có thể không phù hợp với bản chất CKĐT, đồng thời làm giảm giá trị pháp lý của các hình thức xác nhận điện tử đơn giản. Đây là vấn đề mà nhà làm luật cần cân nhắc, vì việc công nhận các hình thức này không tạo gánh nặng quản lý, không ảnh hưởng đáng kể đến định hướng phát triển công nghệ, mà còn góp phần tăng tính pháp lý và tạo thuận lợi cho các bên giao dịch cũng như cơ quan tài phán khi giải quyết tranh chấp.

DANH MỤC TÀI LIỆU THAM KHẢO

1. Quốc hội (2005), Luật Giao dịch điện tử số 51/2005/QH11, ngày 29/11/2005

⁵⁴ Điều 63-65 Luật Công chứng năm 2024.

⁵⁵ UETA, Section 12.

2. Quốc hội (2023), Luật Giao dịch điện tử số 20/2023/QH15, ngày 22/6/2023
3. Chính phủ (2025), Nghị định số 23/2025/NĐ-CP ngày 21/02/2025 quy định về chữ ký điện tử và dịch vụ tin cậy.
4. Electronic Signatures in Global and National Commerce Act (E-SIGN Act) 2000
5. Uniform Electronic Transactions Act (UETA) 1999
6. Regulation (EU) No 910/2014 (eIDAS Regulation)
7. Regulation (EU) 2024/1183 (eIDAS 2.0)
8. Adobe, *A global overview of electric signatures*, https://www.adobe.com/content/dam/dx-dc/pdf/ue/dc_esignatures_global_overview_ue.pdf
9. Bộ Thông tin và Truyền thông (2023), *Báo cáo tình hình ứng dụng và phát triển chữ ký số tại Việt Nam năm 2024*, NXB Thông tin và Truyền thông.
10. Bundesdruckerei, *Digital signatures – legally binding and mobile*, <https://www.bundesdruckerei.de/en/innovation-hub/digital-signatures-legally-binding-convenient-and-mobile>, truy cập ngày 19/8/2025.
11. EDICOM Group, *eIDAS: 5 years making transactions more secure in the European Union*, <https://edicomgroup.com/blog/eidas-5-years-making-transactions-more-secure-in-the-european-union>, truy cập ngày 19/8/2025.
12. emSigner, *The Legal Landscape of eSignatures: Understanding Global Regulations*, <https://blogs.emsigner.com/the-legal-landscape-of-esignatures-understanding-global-regulations>, truy cập ngày 19/8/2025.
13. Harbhajan S. Kehal Varinder P. Singh (2005), *Digital Economy: Impacts, Influences and Challenges*, IGI Global, Chapter VI.
14. Law Commission (UK) (2019), *Electronic Execution of Documents*, Law Commission Electronic execution of documents
15. NEAC, *OTP không phải là chữ ký điện tử*, truy cập tại <https://neac.gov.vn/vi/tin-tuc-su-kien/detail/otp-khong-phai-la-chu-ky-dien-tu-577.htm>, truy cập ngày 19/8/2025.
16. Nguyễn Thị Kim Hồng, Nguyễn Hào Khang, *Công nhận các loại chữ ký điện tử khác theo pháp luật Việt Nam và một số quốc gia*, truy cập tại

<https://tapchitoaan.vn/cong-nhan-cac-loai-chu-ky-dien-tu-khac-theo-phap-luat-viet-nam-va-mot-so-quoc-gia13224.html>, truy cập ngày 19/8/2025.

17. Parker Poe, *Using Electronic Signatures*, truy cập tại <https://www.parkerpoe.com/news/2016/10/using-electronic-signatures>, truy cập ngày 19/8/2025.

18. Roaa Al-Heeti, *Electronic Signatures*, truy cập tại <https://www.atgf.com/tools-publications/pubs/electronic-signatures>, truy cập ngày 19/8/2025.

19. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001