TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN XXXX:2026

Xuất bản lần 1

GIAO DỊCH ĐIỆN TỬ - YÊU CẦU CHUNG VỀ VẬN HÀNH VÀ KIỂM SOÁT ĐỐI VỚI TỔ CHỨC CUNG CẤP DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG THEO MÔ HÌNH KÝ SỐ TỪ XA (REMOTE SIGNING)

Electronic Transactions – General requirements for operation and control of Public Digital Signature Certification Service Providers under the remote digital digning model

HÀ NỘI - 2026

Mục lục

Lời nói đầu

TCVN XXXX:2026 được xây dựng trên cơ sở tham khảo Tiêu chuẩn quốc tế ETSI TS 119 431 của Viện Tiêu chuẩn Viễn thông Châu Âu (ETSI), có điều chỉnh, sửa đổi, bổ sung để phù hợp với điều kiện của Việt Nam.

TCVN XXXX:2026 do Trung tâm Chứng thực điện tử Quốc gia biên soạn, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Trong bối cảnh chuyển đổi số, chữ ký số ngày càng được sử dụng rộng rãi trong các hoạt động quản lý nhà nước, giao dịch dân sự, thương mại và cung cấp dịch vụ công. Chữ ký số cho phép xác nhận chủ thể ký, thể hiện sự chấp thuận đối với thông điệp dữ liệu và bảo đảm tính toàn vẹn của thông điệp dữ liệu theo quy định của pháp luật về giao dịch điện tử. Khi đáp ứng các điều kiện theo quy định của pháp luật, chữ ký số có giá trị pháp lý tương đương chữ ký tay, góp phần thiết lập lòng tin và bảo đảm an toàn cho các giao dịch điện tử.

Cùng với sự phát triển của hạ tầng số và công nghệ điện toán đám mây, mô hình ký số từ xa (Remote Signing) được triển khai nhằm nâng cao tính thuận tiện, khả năng mở rộng và khả năng tích hợp với các hệ thống thông tin, nền tảng số. Trong mô hình này, khóa bí mật của thuê bao được tạo lập, lưu trữ và sử dụng trong môi trường kỹ thuật do Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng quản lý và kiểm soát; việc ký số được thực hiện thông qua cơ chế xác thực và chấp thuận phù hợp, bảo đảm khóa bí mật không bị lộ, không bị sao chép và không bị sử dụng trái phép.

Việc cung cấp dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa đặt ra yêu cầu nghiêm ngặt đối với công tác quản lý, vận hành hệ thống, bảo vệ khóa bí mật, xác thực thuê bao, kiểm soát truy cập, ghi nhật ký và giám sát an toàn thông tin. Các rủi ro phát sinh từ thay đổi công nghệ, thuật toán mật mã, lỗ hổng kỹ thuật hoặc sai sót trong vận hành cần được nhận diện, đánh giá và kiểm soát thông qua các chính sách, quy trình và biện pháp kỹ thuật phù hợp.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa giữ vai trò then chốt trong việc bảo đảm rằng hoạt động ký số được thực hiện đúng chủ thể, đúng ý chí, đúng thời điểm và trong môi trường an toàn, tin cậy. Để thực hiện vai trò này, tổ chức phải thiết lập và duy trì hệ thống quản lý, quy trình vận hành, biện pháp kỹ thuật và cơ chế kiểm soát nhằm bảo đảm tính bảo mật, tính toàn vẹn, tính xác thực và khả năng kiểm tra của dịch vụ ký số từ xa.

Tiêu chuẩn này quy định các yêu cầu về vận hành và kiểm soát đối với Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa. Tiêu chuẩn làm cơ sở cho việc thiết kế, triển khai, vận hành, giám sát và đánh giá sự phù hợp của dịch vụ, góp phần tăng cường độ tin cậy, giá trị pháp lý của chữ ký số và thúc đẩy phát triển giao dịch điện tử an toàn.

Giao dịch điện tử - Yêu cầu chung về vận hành và kiểm soát đối với Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa (Remote Signing)

Electronic Transactions – General requirements for operation and control of Public Digital Signature Certification Service Providers under the remote digital signing model

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa, khi cung cấp dịch vụ này, phải áp dụng đầy đủ toàn bộ nội dung của tiêu chuẩn này, bao gồm phần nội dung chính, Phụ lục A và Phụ lục B.

Phụ lục A quy định các yêu cầu được xây dựng trên cơ sở ETSI TS 119 431-1 đối với việc vận hành thiết bị tạo chữ ký số từ xa và quản lý vòng đời khóa ký số.

Phụ lục B quy định các yêu cầu được xây dựng trên cơ sở ETSI TS 119 431-2 đối với thành phần hỗ trợ tạo chữ ký số AdES.

Việc bố trí các yêu cầu tại hai phụ lục không tạo ra lựa chọn áp dụng riêng lẻ, áp dụng thay thế hoặc loại trừ một trong hai phụ lục.

Các yêu cầu bao quát việc thiết lập chính sách, quản trị và vận hành, sinh và quản lý vòng đời khóa ký số, xác thực và kích hoạt chữ ký, giao diện dịch vụ, tạo chữ ký số AdES, ghi nhật ký, bảo đảm liên tục hoạt động và chấm dứt dịch vụ.

Tiêu chuẩn này cung cấp cơ sở cho việc thiết kế, vận hành, giám sát và đánh giá sự phù hợp của dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa.

Tiêu chuẩn này không quy định giao thức truy cập dịch vụ, phương pháp đánh giá của tổ chức đánh giá sự phù hợp hoặc yêu cầu đối với tổ chức đánh giá sự phù hợp.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi (nếu có)

TCVN 14617:2026, *Công nghệ thông tin - Dịch vụ tin cậy - Yêu cầu đối với chữ ký số và chứng thư chữ ký số*

TCVN 14618:2026, Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về đối với tổ chức cung cấp dịch vụ tin cậy

ETSI EN 319 403-1 V2.3.1 (2020-06), *Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers* (Chữ ký điện tử và hạ tầng tin cậy (ESI) - Đánh giá sự phù hợp của tổ chức cung cấp dịch vụ tin cậy - Phần 1: Yêu cầu đối với tổ chức đánh giá sự phù hợp thực hiện đánh giá tổ chức cung cấp dịch vụ tin cậy)

ETSI EN 319 411-1 V1.4.1 (2023-10), *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements* (Chữ ký điện tử và hạ tầng tin cậy (ESI) - Yêu cầu về chính sách và an toàn đối với tổ chức cung cấp dịch vụ tin cậy cấp chứng thư chữ ký số - Phần 1: Yêu cầu chung)

EN 419221-5:2018, *Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services* (Hồ sơ bảo vệ đối với mô-đun mật mã của tổ chức cung cấp dịch vụ tin cậy - Phần 5: Mô-đun mật mã cho dịch vụ tin cậy)

EN 419241-1:2018, *Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements* (Hệ thống tin cậy hỗ trợ ký số phía máy chủ - Phần 1: Yêu cầu chung về an toàn hệ thống)

ETSI TS 119 101 V1.1.1 (2016-03), *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation* (Chữ ký điện tử và hạ tầng tin cậy (ESI) - Yêu cầu về chính sách và an toàn đối với ứng dụng tạo chữ ký số và xác thực chữ ký số)

3 Thuật ngữ, định nghĩa và chữ viết tắt

3.1 Thuật ngữ và định nghĩa

Trong tiêu chuẩn này sử dụng các thuật ngữ được áp dụng theo ETSI TR 119 001 và các thuật ngữ dưới đây.

3.1.1

Xác thực (authentication)

Việc cung cấp sự bảo đảm về danh tính được khai báo bởi một thực thể.

[Nguồn: ISO/IEC 18014-2]

3.1.2

Chữ ký số (digital signature)

Chữ ký số là chữ ký điện tử sử dụng thuật toán khóa không đối xứng, gồm khóa bí mật và khóa công khai, trong đó khóa bí mật được dùng để ký số và khóa công khai được dùng để kiểm tra chữ ký số. Chữ ký số bảo đảm tính xác thực, tính toàn vẹn và tính chống chối bỏ nhưng không bảo đảm tính bí mật của thông điệp dữ liệu.

Nguồn: Tài liệu tham khảo số [1]

3.1.3

Giá trị chữ ký số (digital signature value)

Kết quả của phép biến đổi mật mã đối với một đơn vị dữ liệu, cho phép bên nhận xác minh nguồn gốc và tính toàn vẹn của dữ liệu, đồng thời bảo vệ chống giả mạo.

3.1.4

Định danh điện tử (electronic identification – eID)

Quy trình sử dụng dữ liệu định danh cá nhân dưới dạng điện tử để đại diện duy nhất cho một cá nhân, pháp nhân hoặc một cá nhân đại diện cho pháp nhân.

3.1.5

Phương tiện định danh điện tử (electronic identification means)

Thiết bị vật lý và/hoặc phi vật lý chứa dữ liệu định danh cá nhân và được sử dụng để xác thực cho một dịch vụ trực tuyến.

3.1.6

Tham chiếu phương tiện định danh điện tử (electronic identification means reference)

Dữ liệu được sử dụng trong SSAS làm tham chiếu tới phương tiện định danh điện tử nhằm xác thực người ký.

3.1.7

Khóa ký sử dụng một lần (one-time signing key)

Khóa ký được ràng buộc, cấp chứng nhận, sử dụng và hủy bỏ trên cơ sở một lần cấp quyền, gắn với một phiên ký duy nhất đối với DTBS/R(s).

3.1.8

Thiết bị tạo chữ ký số từ xa (remote signature creation device)

Thiết bị tạo chữ ký số được sử dụng từ xa theo góc nhìn của người ký và cho phép kiểm soát quá trình ký thay mặt người ký.

3.1.9

Thiết bị tạo chữ ký số (Signature Creation Device – SCDev)

Phần mềm hoặc phần cứng được cấu hình để triển khai dữ liệu tạo chữ ký và tạo ra giá trị chữ ký số.

3.1.10

Dịch vụ tin cậy (trust service)

Dịch vụ tin cậy bao gồm:

a) Dịch vụ cấp dấu thời gian;

b) Dịch vụ chứng thực thông điệp dữ liệu;

c) Dịch vụ chứng thực chữ ký số công cộng.

Nguồn: Tài liệu tham khảo số [1]

3.1.11

Tổ chức cung cấp dịch vụ tin cậy (Trust Service Provider – TSP)

Tổ chức cung cấp một hoặc nhiều dịch vụ tin cậy.

3.1.12

Chữ ký số nâng cao (AdES digital signature)

Chữ ký số thuộc một trong các loại: CAdES, PAdES hoặc XAdES.

3.1.13

Dịch vụ ứng dụng ký số phía máy chủ (Server Signing Application Service – SSAS)

Dịch vụ tin cậy bao gồm thành phần ứng dụng ký số phía máy chủ và SCDev để tạo giá trị chữ ký số thay người ký.

3.1.14

Tổ chức cung cấp dịch vụ ứng dụng ký số phía máy chủ (Server Signing Application Service Provider – SSASP)

Tổ chức cung cấp dịch vụ tin cậy vận hành dịch vụ ứng dụng ký số phía máy chủ.

3.1.15

Ứng dụng ký phía máy chủ (server signing application)

Ứng dụng sử dụng thiết bị tạo chữ ký số từ xa để tạo giá trị chữ ký số thay mặt người ký.

3.1.16

Thành phần dịch vụ ứng dụng ký phía máy chủ (server signing application service component)

Thành phần dịch vụ của TSP sử dụng ứng dụng ký số phía máy chủ.

3.1.17

Quy tắc áp dụng chữ ký số (signature applicability rules)

Tập hợp các quy tắc áp dụng cho một hoặc nhiều chữ ký số nhằm xác định chữ ký số có phù hợp với mục đích nghiệp vụ hoặc pháp lý cụ thể hay không.

CHÚ THÍCH: Có thể sử dụng ETSI TS 119 172-1.

3.1.18

Ứng dụng tạo chữ ký (signature creation application)

Ứng dụng trong hệ thống tạo chữ ký số dùng để tạo chữ ký số AdES và dựa vào thiết bị tạo chữ ký số để tạo giá trị chữ ký số.

CHÚ THÍCH: Thiết bị tạo chữ ký số có thể được quản lý bởi thành phần dịch vụ liên quan.

3.1.19

Thành phần dịch vụ ứng dụng tạo chữ ký số (signature creation application service component)

Thành phần dịch vụ của TSP sử dụng ứng dụng tạo chữ ký.

3.1.20

Ràng buộc tạo chữ ký (signature creation constraint)

Các tiêu chí được sử dụng khi tạo chữ ký số.

3.1.21

Chính sách tạo chữ ký (signature creation policy)

Tập hợp các ràng buộc tạo chữ ký được hoặc sẽ được xử lý bởi ứng dụng tạo chữ ký.

3.1.22

Dịch vụ tạo chữ ký (signature creation service)

Dịch vụ của TSP triển khai ứng dụng tạo chữ ký và/hoặc ứng dụng ký phía máy chủ.

3.1.23

Tổ chức cung cấp dịch vụ tạo chữ ký (signature creation service provider)

Tổ chức cung cấp dịch vụ tạo chữ ký.

CHÚ THÍCH: Nguồn: EN 419241-1.

3.1.24

Bên tin cậy (relying party)

Bên nhận dữ liệu ký số hoặc sử dụng hoặc ứng dụng để xác minh/tin cậy dấu thời gian.

3.1.25

Thuê bao (subscriber)

Cá nhân hoặc tổ chức được cung cấp dịch vụ tin cậy và bị ràng buộc bởi các nghĩa vụ theo thỏa thuận với tổ chức cung cấp dịch vụ tin cậy.

3.1.26

Quyền kiểm soát duy nhất (sole control)

Trạng thái trong đó chỉ người ký có khả năng cho phép sử dụng khóa ký số tương ứng để tạo chữ ký số thông qua cơ chế xác thực và chấp thuận phù hợp.

3.1.27

Dữ liệu kích hoạt chữ ký (Signature Activation Data – SAD)

Dữ liệu được sử dụng để xác thực người ký và cho phép kích hoạt khóa ký số, đồng thời ràng buộc việc kích hoạt khóa ký số với dữ liệu được biểu diễn để ký số hoặc các tài liệu cụ thể cần ký.

3.1.28

Mô-đun kích hoạt chữ ký (Signature Activation Module – SAM)

Thành phần tin cậy thực hiện kiểm tra dữ liệu kích hoạt chữ ký và, khi dữ liệu này hợp lệ, cho phép kích hoạt khóa ký số trong thiết bị tạo chữ ký số từ xa để tạo giá trị chữ ký số.

3.2 Chữ viết tắt

Từ viết tắt	Tiếng Anh	Giải thích
CA	Certificate Authority	Tổ chức cung cấp dịch vụ chứng thực chữ ký số
DTBS/R	Data To Be Signed Representation	Dữ liệu được biểu diễn để ký số
eID	electronic Identification	Định danh điện tử
LSP	Lightweight SSAS Policy	Chính sách SSAS mức cơ bản
NSP	Normalized SSAS Policy	Chính sách SSAS chuẩn hóa
OID	Object Identifier	Định danh đối tượng
PIN	Personal Identification Number	Mã định danh cá nhân

SAD	Signature Activation Data	Dữ liệu kích hoạt chữ ký
SAM	Signature Activation Module	Mô-đun kích hoạt chữ ký
SAP	Signature Activation Protocol	Giao thức kích hoạt chữ ký
SCDev	Signature Creation Device	Thiết bị tạo chữ ký số
SP	SSAS Policy	Chính sách SSAS
SSAS	Server Signing Application Service	Dịch vụ ứng dụng ký phía máy chủ
SSASP	Server Signing Application Service Provider	Tổ chức cung cấp dịch vụ ứng dụng ký phía máy chủ
TSP	Trust Service Provider	Tổ chức cung cấp dịch vụ tin cậy
URI	Uniform Resource Identifier	Định danh tài nguyên thống nhất
SCA	Signature Creation Application	Ứng dụng tạo chữ ký
SCASC	Signature Creation Application Service Component	Thành phần dịch vụ ứng dụng tạo chữ ký
SCASP	Signature Creation Application Service Provider	Tổ chức cung cấp dịch vụ ứng dụng tạo chữ ký
SD	Signer's Document	Tài liệu của người ký
SLA	Service-Level Agreement	Thỏa thuận mức dịch vụ
SSASC	Server Signing Application Service Component	Thành phần dịch vụ ứng dụng ký phía máy chủ
TSA	Time-Stamping Authority	Tổ chức cung cấp dịch vụ cấp dấu thời gian

3.3 Ký hiệu

Các yêu cầu không có dấu hiệu bổ sung áp dụng cho mọi dịch vụ thuộc phạm vi của điều tương ứng. Các dấu hiệu sau được sử dụng:

- [CÓ ĐIỀU KIỆN]: yêu cầu chỉ áp dụng khi điều kiện nêu trong yêu cầu được đáp ứng;

- [LSP]: yêu cầu áp dụng cho dịch vụ được cung cấp theo Chính sách SSAS mức cơ bản;

- [NSP]: yêu cầu áp dụng cho dịch vụ được cung cấp theo Chính sách SSAS chuẩn hóa.

4 Khái niệm dịch vụ, nguyên tắc áp dụng và kiến trúc

4.1 Khái quát

Tiêu chuẩn này kết hợp hai lớp dịch vụ có quan hệ trực tiếp. Lớp SSAS quản lý thiết bị tạo chữ ký số từ xa, việc sinh, liên kết, kích hoạt, sao lưu và hủy khóa ký số. Lớp SCASC nhận tài liệu hoặc giá trị băm, chuẩn bị biểu diễn dữ liệu cần ký, nhận giá trị chữ ký số từ SCDev và tạo chữ ký số AdES.

Các yêu cầu chung đối với TSP được áp dụng theo TCVN 14618:2026. Đối với SSAS, các yêu cầu về hệ thống tin cậy hỗ trợ ký phía máy chủ được áp dụng theo EN 419241-1 và các yêu cầu liên quan đến cấp chứng thư chữ ký số được xem xét theo ETSI EN 319 411-1. Đối với SCASC, các yêu cầu bổ sung tập trung vào việc tiếp nhận dữ liệu, chuẩn bị DTBSR, tương tác với SCDev và tạo chữ ký số AdES.

CHÚ THÍCH: Các viện dẫn đến hệ thống tin cậy hỗ trợ ký phía máy chủ (TW4S) trong EN 419241-1 được hiểu là viện dẫn áp dụng cho SSAS.

4.2 Các lớp và thành phần dịch vụ

SSAS được phân chia thành các dịch vụ thành phần sau nhằm phân loại yêu cầu:

- Dịch vụ sinh khóa ký số;

- Dịch vụ liên kết chứng thư chữ ký số;

- Dịch vụ liên kết phương tiện định danh điện tử hoặc liên kết trực tiếp với danh tính đối với khóa ký sử dụng một lần;

- Dịch vụ kích hoạt chữ ký;

- Dịch vụ hủy khóa ký số;

- Dịch vụ cung cấp phương tiện định danh điện tử, khi được triển khai.

SCASC nhận tài liệu và/hoặc giá trị băm của tài liệu cần ký cùng với các tham số ký tùy chọn, thu thập thông tin cần thiết, chuẩn bị DTBSR và gửi DTBSR đến SCDev. SCDev có thể nằm trong môi trường của người dùng hoặc được quản lý bởi SSASC. SCASC đưa giá trị chữ ký số do SCDev trả về vào chữ ký số AdES.

CHÚ THÍCH: Việc phân chia dịch vụ chỉ nhằm làm rõ yêu cầu chính sách và không đặt ra hạn chế đối với cách phân chia vật lý hoặc tổ chức trong triển khai.

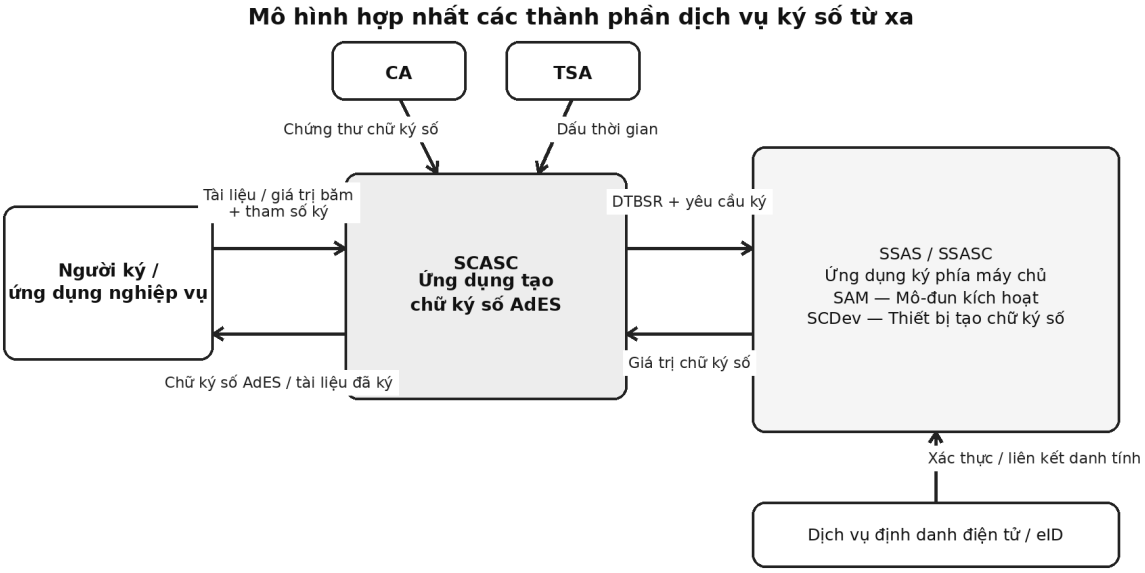
4.3 Nguyên tắc áp dụng toàn bộ tiêu chuẩn

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa tại Việt Nam phải áp dụng đầy đủ các quy định từ Điều 1 đến Điều 4, Phụ lục A và Phụ lục B của tiêu chuẩn này.

Phụ lục A và Phụ lục B là các bộ phận quy định không tách rời của tiêu chuẩn này và phải được áp dụng đồng thời khi tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa.

4.4 Kiến trúc logic hợp nhất

Mối quan hệ logic giữa người ký hoặc ứng dụng nghiệp vụ, SCASC, SSAS/SSASC, SCDev và các dịch vụ hỗ trợ được minh họa tại Hình 1.



CHÚ THÍCH: Hình 1 minh họa quan hệ giữa các thành phần và không biểu diễn một luồng xử lý bắt buộc.

Hình 1 - Mô hình logic hợp nhất các thành phần dịch vụ ký số từ xa

Phụ lục A

(quy định)

Yêu cầu về chính sách và an toàn vận hành đối với thiết bị tạo chữ ký số từ xa

A.1 Tổng quan

A.1.1 Khái niệm chung về yêu cầu chính sách

Tài liệu này được cấu trúc về cơ bản phù hợp với ETSI EN 319 411-1 nhằm hỗ trợ Tổ chức cung cấp dịch vụ tin cậy (TSP) áp dụng các yêu cầu này vào tài liệu chính sách và quy chế chứng thực (CP/CPS) của mình.

Tài liệu này tích hợp theo hình thức viện dẫn các yêu cầu của EN 419241-1. EN 419241-1 quy định các mức bảo đảm đối với kiểm soát duy nhất.

CHÚ THÍCH 1: Mọi yêu cầu áp dụng và được viện dẫn đối với Hệ thống tin cậy hỗ trợ ký phía máy chủ (TW4S) trong EN 419241-1 là yêu cầu áp dụng đối với dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa (SSAS).

Tài liệu này tích hợp theo hình thức viện dẫn các yêu cầu của TCVN 14618:2026 và bổ sung các yêu cầu liên quan đến Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa (SSASP).

Các yêu cầu được thể hiện dưới dạng các mục tiêu an toàn, kèm theo các yêu cầu cụ thể hơn đối với các biện pháp kiểm soát nhằm đáp ứng các mục tiêu đó, khi được xem là cần thiết để bảo đảm mức độ tin cậy cần thiết rằng các mục tiêu này được đáp ứng.

A.1.2 Tài liệu áp dụng đối với SSAS

A.1.2.1 Quy chế chứng thực SSAS

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa phải xây dựng, triển khai, thực thi và cập nhật quy chế chứng thực dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa, là quy chế chứng thực dịch vụ tin cậy theo định nghĩa tại điều 6.1 TCVN 14618:2026, được cụ thể hóa cho SSAS.

Quy chế chứng thực SSAS mô tả cách thức SSASP vận hành dịch vụ của mình và thuộc sở hữu của SSASP. Quy chế chứng thực SSAS được điều chỉnh phù hợp với cơ cấu tổ chức, quy trình vận hành, cơ sở vật chất và môi trường tính toán của TSP. Đối tượng tiếp nhận quy chế chứng thực có thể bao gồm tổ chức đánh giá, thuê bao và Bên tin cậy.

CHÚ THÍCH: Sự hiện diện của một số thành phần trong quy chế chứng thực SSAS là yêu cầu bắt buộc của tài liệu này; tuy nhiên, tài liệu này không đặt ra hạn chế về hình thức của quy chế chứng thực SSAS. Quy chế chứng thực này có thể được tích hợp trong tài liệu quy chế chứng thực chung của TSP tổng thể các dịch vụ khác do TSP cung cấp hoặc được xây dựng như một tài liệu độc lập.

Tài liệu này quy định các yêu cầu được xác định là cần thiết đối với các chính sách SSAS được quy định tại Điều A.1.3.2, phải được SSASP phê duyệt và được thể hiện trong quy chế chứng thực của mình.

A.1.2.2 Chính sách SSAS

Chính sách SSAS (SP) mô tả những gì được cung cấp và có thể bao gồm nhiều thông tin vượt ra ngoài phạm vi của tài liệu này nhằm chỉ ra phạm vi áp dụng của SSAS. Một SP được xác định độc lập với các

chi tiết cụ thể của môi trường vận hành của SSASP. Đối tượng sử dụng SP có thể bao gồm kiểm toán viên, thuê bao và Bên tin cậy.

Tài liệu này định nghĩa ba loại SP:

1) Chính sách SSAS mức cơ bản (LSP) cung cấp mức chất lượng dịch vụ cơ bản.

2) Chính sách SSAS chuẩn hóa (NSP) đáp ứng các thông lệ tốt nhất được công nhận chung đối với các TSP vận hành thiết bị ký số từ xa (SCDev) phục vụ cho mọi loại giao dịch.

SP không nhất thiết phải là một phần trong bộ tài liệu của SSASP. Ngoài ra, tài liệu này không đặt ra ràng buộc về hình thức của SP; SP có thể là một tài liệu độc lập hoặc được cung cấp như một phần của Cp/CPS và/hoặc các điều khoản, điều kiện chung.

A.1.2.3 Điều khoản và điều kiện

Bên cạnh hoặc như một phần của SCP và CP/CPS SSAS, TSP phải ban hành các điều khoản và điều kiện. Các điều khoản và điều kiện có thể bao quát nội dung thương mại hoặc kỹ thuật. Các điều khoản và điều kiện là đặc thù đối với SSASP. Đối tượng tiếp nhận các điều khoản và điều kiện là thuê bao và Bên tin cậy.

CHÚ THÍCH: Sự hiện diện của một số nội dung là bắt buộc trong các điều khoản và điều kiện theo yêu cầu của tài liệu này; tuy nhiên, tài liệu này không đặt ra hạn chế về hình thức của các điều khoản và điều kiện. Các điều khoản và điều kiện có thể là một tài liệu độc lập công khai, hoặc được phân tách trong (các) thỏa thuận với thuê bao và thông tin cung cấp cho Bên tin cậy. Hình thức và nội dung của các điều khoản và điều kiện cũng có thể phụ thuộc vào quy định pháp luật quốc gia.

A.1.3 Các dịch vụ thành phần của SSAS

CHÚ THÍCH 1: Tài liệu này không bắt buộc bất kỳ cách thức phân chia dịch vụ nào của TSP. Các yêu cầu được quy định tại các mục tiếp theo.

Trong tài liệu này, các dịch vụ SSAS được phân chia thành các dịch vụ thành phần sau nhằm mục đích phân loại yêu cầu:

- Dịch vụ tạo khóa ký số: tạo khóa ký số trên thiết bị từ xa (the remote device). Bằng chứng sở hữu đối với khóa ký số được tạo ra được chuyển đến dịch vụ đăng ký của TSP phát hành chứng thư chữ ký số tương ứng.

- Dịch vụ liên kết chứng thư chữ ký số: liên kết các chứng thư chữ ký số được tạo bởi dịch vụ tạo chứng thư chữ ký số của TSP với các khóa ký số tương ứng.

- Định danh điện tử (eID)/dịch vụ liên kết danh tính (identity linking service): liên kết định danh điện tử hoặc danh tính chủ thể với các khóa ký số tương ứng nhằm bảo đảm quyền kiểm soát duy nhất.

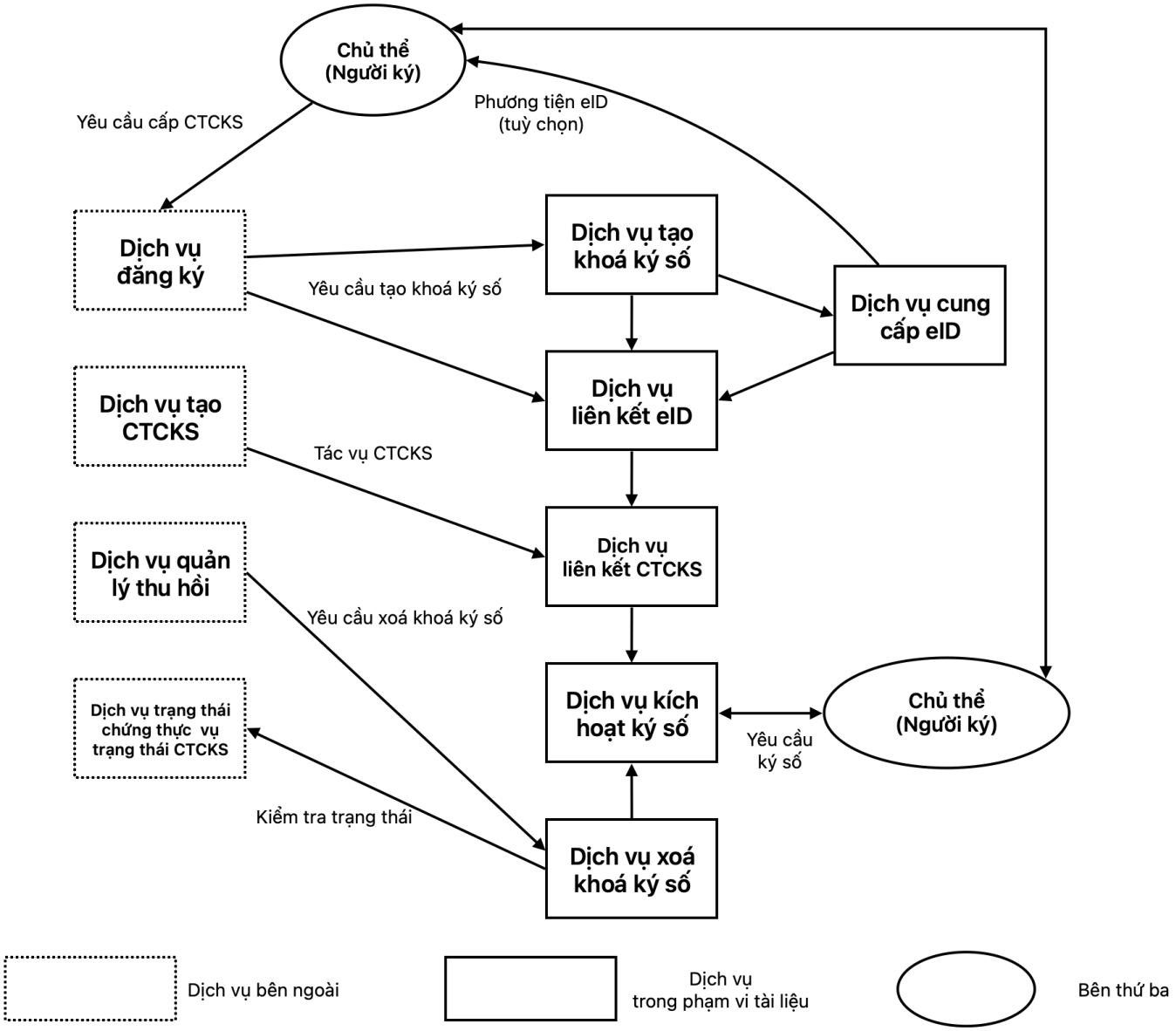
- Dịch vụ kích hoạt ký số: xác minh dữ liệu kích hoạt ký số và kích hoạt khóa ký số tương ứng để tạo chữ ký số.

- Dịch vụ xóa khóa ký số: hủy khóa ký số theo cách bảo đảm rằng khóa ký số không thể được sử dụng.

- Dịch vụ cung cấp phương tiện định danh điện tử (tùy chọn): chuẩn bị và cung cấp phương tiện định danh điện tử đảm bảo sẵn sàng cho người ký.

Việc phân chia các dịch vụ nêu trên chỉ nhằm mục đích làm rõ các yêu cầu chính sách và không đặt ra bất kỳ hạn chế nào đối với việc phân chia thực tế trong triển khai dịch vụ của TSP.

Hình 1 minh họa các mối quan hệ tương tác giữa các thành phần dịch vụ trong tài liệu này và mối quan hệ với các thành phần bên ngoài của TSP cấp chứng thư chữ ký số.



Hình 1 - Minh họa việc phân chia các thành phần SSAS

A.2 Quy định chung về quy chế chứng thực và chính sách

A.2.1 Yêu cầu đối với Quy chế chứng thực

A.2.1.1 Áp dụng các yêu cầu được quy định tại điều 6.1 của TCVN 14618:2026.

Ngoài ra, áp dụng bổ sung các yêu cầu cụ thể sau:

CHÚ THÍCH 1: Một TSP có thể tài liệu hóa các yêu cầu chính sách SSAS cụ thể tách biệt khỏi CP/CPS.

A.2.1.2 CP/CPS của TSP phải bao gồm các thuật toán ký số và các tham số được áp dụng, các thuật toán được sử dụng để tạo cặp khóa và bất kỳ thuật toán, tham số nào khác có vai trò quan trọng đối với an toàn vận hành SSAS.

A.2.1.3 TSP phải công bố công khai CP/CPS của mình thông qua phương tiện trực tuyến, bảo đảm khả dụng 24 giờ mỗi ngày và 7 ngày mỗi tuần (24×7).

CHÚ THÍCH 2: TSP không bắt buộc phải công bố các nội dung chứa thông tin nhạy cảm.

A.2.2 Tên và định danh chính sách dịch vụ ký số từ xa

A.2.2.1: Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng theo mô hình ký số từ xa phải xây dựng, công bố và duy trì chính sách dịch vụ ký số từ xa.

A.2.2.2: Mỗi chính sách dịch vụ ký số từ xa phải có tên và định danh duy nhất để nhận biết chính xác chính sách được áp dụng đối với dịch vụ do tổ chức cung cấp.

A.2.2.3: Tên và định danh chính sách phải được thể hiện thống nhất trong quy chế chứng thực, chính sách cung cấp dịch vụ và các tài liệu có liên quan được tổ chức công bố.

A.2.2.4: Trường hợp sử dụng định danh đối tượng (OID) để định danh chính sách, OID phải được cấp, quản lý và sử dụng theo quy định của pháp luật Việt Nam.

A.2.2.5: Khi chính sách được sửa đổi làm thay đổi phạm vi, đối tượng, điều kiện áp dụng hoặc mức bảo đảm của dịch vụ, tổ chức phải thay đổi định danh chính sách tương ứng và công bố rõ thời điểm áp dụng chính sách mới.

A.2.3 Các bên tham gia

A.2.3.1 SSASP

A.2.2.1.1 SSASP có thể sử dụng các bên khác để cung cấp một phần dịch vụ; tuy nhiên, SSASP luôn duy trì trách nhiệm tổng thể và phải bảo đảm rằng các yêu cầu chính sách được quy định trong tài liệu này được đáp ứng.

A.2.3.2 Thuê bao và người ký

Trong khuôn khổ các chính sách này, người ký gắn với khóa ký số có thể là:

a) Cá nhân;

b) Cá nhân được định danh liên kết với một pháp nhân;

c) Pháp nhân (có thể là một tổ chức, đơn vị hoặc bộ phận được định danh liên kết với một tổ chức); hoặc

d) Thiết bị hoặc hệ thống được vận hành bởi hoặc thay mặt cho cá nhân hoặc pháp nhân.

CHÚ THÍCH: Tài liệu này không đặt ra bất kỳ hạn chế cụ thể nào đối với việc đại diện pháp lý được thể hiện bởi chữ ký điện tử hoặc con dấu điện tử được tạo theo tài liệu này.

Mối quan hệ giữa người ký và thuê bao tương đương với mối quan hệ giữa chủ thể và thuê bao như được quy định tại Điều 5.4.2 ETSI EN 319 411-1.

A.3 Yêu cầu thực hành của Tổ chức cung cấp dịch vụ tin cậy

A.3.1 Trách nhiệm công khai và kho lưu trữ

A.3.1.1 TSP phải cung cấp cho thuê bao và Bên tin cậy các chính sách dịch vụ (SP), CP/CPS và các điều khoản, điều kiện áp dụng liên quan đến việc sử dụng khóa ký số.

A.3.1.2 Các điều khoản và điều kiện áp dụng phải được nhận biết rõ ràng đối với một khóa ký số cụ thể hoặc đối với chứng thư chữ ký số liên quan.

A.3.1.3 Các thông tin được nêu tại A.3.1.1 và A.3.1.2 phải được cung cấp 24 giờ mỗi ngày, 7 ngày mỗi tuần. Trong trường hợp hệ thống bị lỗi, gián đoạn dịch vụ hoặc các yếu tố khác ngoài khả năng kiểm soát của TSP, TSP phải nỗ lực tối đa để đảm bảo dịch vụ này không bị gián đoạn quá thời gian tối đa được quy định trong bản tuyên bố thực hành SSAS.

A.3.1.4 Các thông tin được nêu tại A.3.1.1 nên được công bố công khai và có thể truy cập trên phạm vi quốc tế.

A.3.2 Khởi tạo khóa ký số

A.3.2.1 Sinh khóa ký số

A.3.2.1.1 [LSP] Áp dụng các yêu cầu tại điều SRG_KM.1.1 1.1 của EN 419241-1.

A.3.2.1.2 [NSP] Áp dụng các yêu cầu tại điều SRA_SKM.1.1 của EN 419241-1.

A.3.2.1.2.1 Khóa ký số của người ký phải được sinh và sử dụng trong thiết bị tạo chữ ký (SCDev) được chứng nhận phù hợp với EN 419221-5 [5].

A.3.2.1.3 Áp dụng các yêu cầu tại điều SRG_KM.1.2 của EN 419241-1 .

A.3.2.1.4 Áp dụng các yêu cầu tại điều SRG_KM.1.3 của EN 419241-1.

A.3.2.1.5 Áp dụng các yêu cầu tại điều SRG_KM.1.4 của EN 419241-1.

A.3.2.1.6 Điều khoản SRC_SKS.1.1 của EN 419241-1, quy định về tham số thuật toán, phải được áp dụng.

A.3.2.1.7 Điều khoản SRC_SKS.1.3 của EN 419241-1, quy định về thời điểm sinh khóa, phải được áp dụng.

A.3.2.1.8 [CÓ ĐIỀU KIỆN] Nếu SSAS và dịch vụ tạo chứng thư chữ ký số được quản lý riêng biệt, SSAS phải hỗ trợ yêu cầu quy định tại 6.3.1.1 của ETSI EN 319 411-1..

A.3.2.2 Phương tiện định danh điện tử (eID means) hoặc liên kết danh tính

CHÚ THÍCH 1: Khóa ký số được liên kết với một phương tiện eID mà phương tiện này được liên kết với danh tính thuê bao, hoặc Khóa ký số được liên kết trực tiếp với danh tính.

A.3.2.2.2 [LSP] Áp dụng yêu cầu được quy định tại điều SRC_SA.1.1 của EN 419241-1.

A.3.2.2.3 [NSP] [CÓ ĐIỀU KIỆN] Nếu người ký là cá nhân, việc chứng minh và xác minh danh tính phải theo quy định tại điều khoản A.1.2 của EN 419241-1, đối với mức đảm bảo “substantial” hoặc cao hơn.

A.3.2.2.4 [NSP] [CÓ ĐIỀU KIỆN] Nếu người ký là pháp nhân, việc chứng minh và xác minh danh tính phải theo quy định tại điều khoản A.1.3 của EN 419241-1, đối với mức đảm bảo “substantial” hoặc cao hơn.

A.3.2.2.5 [NSP] Việc nộp hồ sơ và đăng ký trong quá trình đăng ký ban đầu (enrolment) của người ký phải thực hiện theo quy định tại điều khoản A.1.1 của EN 419241-1.

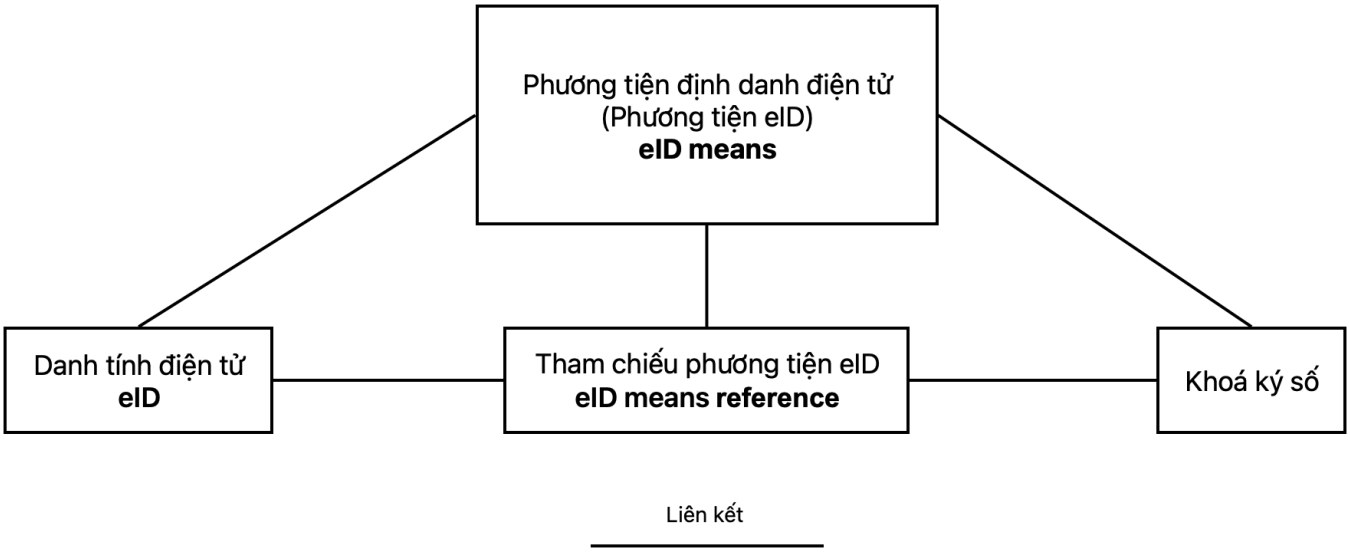
A.3.2.2.6 [NSP] [CÓ ĐIỀU KIỆN] Trong trường hợp việc xác thực được liên kết với một phương tiện eID, các đặc tính và thiết kế của phương tiện eID phải theo quy định tại điều khoản A.2.1 của EN 419241-1, đối với mức đảm bảo “substantial” hoặc cao hơn.

A.3.2.2.7 [NSP] [CÓ ĐIỀU KIỆN] Trong trường hợp việc xác thực được liên kết với một phương tiện eID, cơ chế xác thực phải theo quy định tại điều khoản A.2.2 của EN 419241-1, đối với mức đảm bảo “substantial” hoặc cao hơn.

A.3.2.2.8 [CÓ ĐIỀU KIỆN] Trong trường hợp việc xác thực được liên kết với một phương tiện eID, SSASP phải liên kết các khóa ký số với tham chiếu phương tiện eID (eID means reference) của người ký tương ứng.

A.3.2.2.10 SSASP có thể tạo tham chiếu phương tiện eID (eID means reference) và cung cấp phương tiện eID tương ứng cho người ký (xem điều khoản A.3.2.4).

A.3.2.2.11 SSASP phải bảo đảm rằng dữ liệu định danh cá nhân được liên kết với tham chiếu phương tiện eID hoặc liên kết với dữ liệu định danh gắn với chủ thể của chứng thư chữ ký số tương ứng.



Hình 2 - Minh hoạ liên kết giữa các đối tượng trong việc định danh điện tử

A.3.2.2.12 Tham chiếu phương tiện eID của người ký có thể được cung cấp bởi một bên (bên ngoài) được ủy quyền**.**

A.3.2.2.13 [LSP] [CÓ ĐIỀU KIỆN] Trường hợp toàn bộ hoặc một phần quy trình xác thực được ủy quyền cho một bên bên ngoài, SSASP phải bảo đảm rằng bên bên ngoài đó đáp ứng các yêu cầu quy định tại A.3.2.2.2 và A.3.2.2.8.

A.3.2.2.14 [NSP] [CÓ ĐIỀU KIỆN] Trường hợp toàn bộ hoặc một phần quy trình xác thực được ủy quyền cho một bên bên ngoài, SSASP phải bảo đảm rằng bên bên ngoài đó đáp ứng các yêu cầu quy định tại A.3.2.2.3**,** A.3.2.2.4**,** A.3.2.2.5**,** A.3.2.2.6**,** A.3.2.2.7 và A.3.2.2.8.

A.3.2.2.15 [NSP] [CÓ ĐIỀU KIỆN] Trường hợp toàn bộ quy trình xác thực được ủy quyền cho một bên bên ngoài, SSASP phải bảo đảm rằng vật liệu khóa bí mật được sử dụng để xác thực bên được ủy quyền với SAM phải được lưu trữ trong một mô-đun mật mã đã được chứng nhận, phù hợp với yêu cầu quy định tại SRG_KM.1.1 của ETSI EN 419 241-1.

A.3.2.2.16 [NSP] [CÓ ĐIỀU KIỆN] Trường hợp toàn bộ hoặc một phần quy trình xác thực được ủy quyền cho một bên bên ngoài, SSASP phải bảo đảm rằng:

- bên ngoài đáp ứng đầy đủ các yêu cầu liên quan của tài liệu này và các yêu cầu về đăng ký theo quy định pháp lý áp dụng; hoặc

- quy trình xác thực được ủy quyền cho bên bên ngoài sử dụng phương tiện eID, phương tiện eID này đã được cơ quan có thẩm quyền công nhận/đăng ký chính thức, phù hợp với các quy định pháp lý áp dụng.

A.3.2.2.17 SSASP phải bảo vệ tính toàn vẹn của các liên kết giữa khóa ký số của người ký với tham chiếu phương tiện eID của họ (nếu được sử dụng), hoặc với danh tính đã cung cấp trong trường hợp khác.

A.3.2.3 Liên kết chứng thư chữ ký số

A.3.2.3.1 Áp dụng yêu cầu được quy định tại điều SRC_SKS.1.2 của EN 419241-1.

A.3.2.3.2 Áp dụng yêu cầu được quy định tại điều SRC_SKS.1.4 của EN 419241-1

A.3.2.3.3 Áp dụng yêu cầu được quy định tại điều SRC_SKS.1.5 của EN 419241-1.

A.3.2.4 Cung cấp phương tiện định danh điện tử

A.3.2.4.1 [CÓ ĐIỀU KIỆN] Nếu SSASP cung cấp phương tiện eID cho người ký, phương tiện đó phải được chuyển giao an toàn cho người ký.

A.3.2.4.2 [CÓ ĐIỀU KIỆN] Nếu SSASP cá nhân hóa phương tiện eID với dữ liệu kích hoạt người dùng (ví dụ mã PIN), dữ liệu kích hoạt phải được chuẩn bị và phân phối an toàn, tách biệt với phương tiện định danh điện tử.

A.3.3 Yêu cầu vận hành vòng đời khóa ký

A.3.3.1 Kích hoạt chữ ký

A.3.3.1.1 Áp dụng yêu cầu được quy định tại điều SRC_SA.1.2 của EN 419241-1

A.3.3.1.2 Áp dụng yêu cầu được quy định tại điều SRC_SA.1.3 của EN 419241-1

A.3.3.1.3 Áp dụng yêu cầu được quy định tại điều SRC_SA.1.4 của EN 419241-1

A.3.3.1.4 Áp dụng yêu cầu được quy định tại điều SRC_SA.1.5 của EN 419241-1

A.3.3.1.5 [NSP] Áp dụng yêu cầu được quy định tại điều SRA_SKM.2.1 của EN 419241-1

A.3.3.1.6 [NSP] Áp dụng yêu cầu được quy định tại điều SRA_SAP.1.2 của EN 419241-1

A.3.3.1.7 [NSP] Áp dụng yêu cầu được quy định tại điều SRA_SKM.2.5 của EN 419241-1

A.3.3.1.8 SSASP nên đảm bảo chứng thư chữ ký số chứa khóa công khai có hiệu lực trước khi sử dụng khóa ký số tương ứng.

CHÚ THÍCH 1: valid = chưa hết hạn, không bị thu hồi, không bị tạm ngừng; có thể được đáp ứng bằng cách áp dụng điều A.3.3.2.1 nếu không sử dụng việc tạm ngừng.

A.3.3.1.9 Khóa ký số chỉ được sử dụng trong các trường hợp đã có sự đồng ý của người ký.

A.3.3.1.10 Áp dụng yêu cầu được quy định tại điều SRC_DSC.1.1 của EN 419241-1.

A.3.3.1.11 [CÓ ĐIỀU KIỆN] Trong trường hợp việc xác thực được liên kết trực tiếp với danh tính, SAD phải chứa định danh duy nhất của phiên ký, định danh này phải được liên kết duy nhất với SSAS.

A.3.3.1.12 [CÓ ĐIỀU KIỆN] Trong trường hợp việc xác thực được liên kết trực tiếp với danh tính, SAD phải chứa định danh duy nhất của quá trình xác minh danh tính.

A.3.3.1.13 [CÓ ĐIỀU KIỆN] Trong trường hợp việc xác thực được liên kết trực tiếp với danh tính, phiên ký phải được liên kết:

1) chính xác với một SAD, trong đó SAD này chứa các tham chiếu của tất cả các tài liệu sẽ được ký số trong phiên này;

2) hoặc với nhiều giá trị SAD nếu và chỉ nếu nhiều chữ ký số liên tiếp được áp dụng lên cùng một tài liệu, trong đó mỗi chữ ký số mới bao phủ các chữ ký trước đó.

VÍ DỤ 1: Trong PAdES, mỗi chữ ký mới bao phủ các chữ ký trước đó.

CHÚ THÍCH 2: Định danh duy nhất của phiên ký có thể được sử dụng để xác định khóa ký “mặc định hoặc được chọn” trong SAD như được yêu cầu tại SRA_SAP.2.3 của EN 419241-1.

CHÚ THÍCH 3: Định danh duy nhất của quá trình xác minh danh tính có thể được sử dụng để xác định người ký đã được xác thực trong SAD như được yêu cầu tại SRA_SAP.2.3 của EN 419241-1.

A.3.3.1.14 [CÓ ĐIỀU KIỆN] Trong trường hợp việc xác thực được liên kết trực tiếp với danh tính, phiên ký phải kết thúc chậm nhất là 2 giờ sau khi kết thúc quy trình xác minh danh tính.

CHÚ THÍCH 4: Quy trình xác minh danh tính không chỉ bao gồm việc tương tác với đối tượng được xác minh danh tính, mà còn bao gồm tất cả các xử lý cần thiết để có được kết quả đã được xác minh ở cuối cùng.

CHÚ THÍCH 5: Trong trường hợp việc xác thực được liên kết với một eID, thì việc xác minh danh tính của liên kết eID có thể được sử dụng trong thời gian dài hơn, bởi vì các yếu tố xác thực cho phép đảm bảo một liên kết mạnh với danh tính.

A.3.3.1.15 [NSP] [CÓ ĐIỀU KIỆN] Trong trường hợp người ký là cá nhân và việc xác thực được liên kết trực tiếp với danh tính, SAP phải bao gồm một hành động rõ ràng (không chỉ là một ô tích chọn) của người ký để chấp thuận việc ủy quyền ký số nội dung của các tài liệu cụ thể được tham chiếu trong SAD.

A.3.3.1.16 [NSP] [CÓ ĐIỀU KIỆN] Trong trường hợp người ký là pháp nhân và việc xác thực được liên kết trực tiếp với danh tính, SAP phải bao gồm một hành động rõ ràng (không chỉ là một ô tích chọn) của cá nhân đã được xác định trong quá trình xác minh danh tính và được phép ký số thay mặt pháp nhân để chấp thuận việc ủy quyền xác nhận nguồn gốc và tính toàn vẹn của các tài liệu cụ thể được tham chiếu trong SAD.

VÍ DỤ 2: Một hành động rõ ràng có thể là cuộn đến cuối tài liệu trước khi nhấn nút chấp nhận hoặc gõ “Tôi đồng ý ký hợp đồng này”.

A.3.3.2 Xóa khóa ký số

A.3.3.2.1 Áp dụng yêu cầu được quy định tại điều SRG_KM.7.1 của EN 419241-1 phải được áp dụng. Nếu chứng thư chữ ký số bị thu hồi, khóa ký số tương ứng phải bị hủy.

A.3.3.2.2 SSASP phải hủy khóa ký số khi có yêu cầu từ người ký.

A.3.3.2.3 Áp dụng yêu cầu được quy định tại điều SRG_KM.7.2 của EN 419241-1.

A.3.3.2.4 Áp dụng yêu cầu được quy định tại điều SRG_KM.7.3 của EN 419241-1.

A.3.3.3 Sao lưu và khôi phục khóa ký

A.3.3.3.1 Áp dụng yêu cầu được quy định tại điều SRG_KM.2.1 của EN 419241-1.

A.3.3.3.2 Áp dụng yêu cầu được quy định tại điều SRG_KM.2.2 của EN 419241-1.

A.3.3.3.3 Áp dụng yêu cầu được quy định tại điều SRG_KM.2.3 của EN 419241-1.

A.3.3.3.4 Số lượng bản sao dữ liệu không được vượt quá mức tối thiểu cần thiết để đảm bảo tính liên tục của dịch vụ.

A.3.4 Kiểm soát về cơ sở vật chất, quản lý và vận hành

A.3.4.1 Quy định chung

A.3.4.1.1 Áp dụng yêu cầu được quy định tại điều 5, 6.3 và 7.3 của TCVN 14618:2026.

A.3.4.2 Kiểm soát an ninh vật lý

A.3.4.2.1 Áp dụng yêu cầu được quy định tại điều 7.6 của TCVN 14618:2026 .

A.3.4.2.2 Áp dụng tương ứng (mutatis mutandis) yêu cầu đối với dịch vụ tạo và quản lý kích hoạt khóa ký được quy định tại điều 6.4.2.2 đến 6.4.2.10 của ETSI EN 319 411-1.

A.3.4.3 Kiểm soát thủ tục

A.3.4.3.1 Áp dụng yêu cầu được quy định tại điều 7.4.3X, REQ-7.4-04X và REQ-7.4-07X đến REQ-7.4-12X quy định tại TCVN 14618:2026.

A.3.4.4 Kiểm soát nhân sự

A.3.4.4.1 Áp dụng yêu cầu được quy định tại điều 7.2 của TCVN 14618:2026.

A.3.4.5 Thủ tục ghi nhật ký kiểm toán

A.3.4.5.1 Áp dụng yêu cầu được quy định tại điều 7.10 của TCVN 14618:2026.

A.3.4.5.2 Tất cả các sự kiện an toàn phải được ghi nhật ký, bao gồm:

a) thay đổi liên quan đến chính sách ATTT;

b) khởi động và tắt hệ thống;

c) sự cố hệ thống và lỗi phần cứng;

d) hoạt động của tường lửa và bộ định tuyến;

e) các lần truy cập và các nỗ lực truy cập hệ thống SSAS.

A.3.4.5.3 Áp dụng yêu cầu được quy định tại điều SRG_AA.1 của EN 419241-1.

A.3.4.5.4 Các yêu cầu quy định tại điều khoản SRG_AA.2 của EN 419241-1, về khả năng sẵn sàng của dữ liệu kiểm toán, phải được áp dụng.

A.3.4.5.5 Áp dụng yêu cầu được quy định tại điều SRG_AA.3 của EN 419241-1.

A.3.4.5.6 Áp dụng yêu cầu được quy định tại điều SRG_AA.7 của EN 419241-1.

A.3.4.5.7 Áp dụng yêu cầu được quy định tại điều SRG_AA.8 của EN 419241-1.

A.3.4.6 Lưu trữ bản ghi

A.3.4.6.1 SSASP phải lưu giữ các bản ghi dữ liệu kiểm toán (audit data records) trong ít nhất 7 năm sau khi bất kỳ chứng thư chữ ký số nào dựa trên các bản ghi này không còn hợp lệ, phù hợp với quy định pháp luật hiện hành.

A.3.4.7 Thay đổi khóa

Không có yêu cầu chính sách.

A.3.4.8 Xử lý sự cố và khôi phục thảm họa

A.3.4.8.1 Áp dụng yêu cầu được quy định tại điều 7.9 và 7.11 của TCVN 14618:2026.

A.3.4.9 Chấm dứt dịch vụ SSASP

A.3.4.9.1 Áp dụng yêu cầu được quy định tại điều 7.12 của TCVN 14618:2026.

A.3.5 Kiểm soát an toàn kỹ thuật

A.3.5.1 Quản lý hệ thống và an toàn thông tin

A.3.5.1.1 Áp dụng yêu cầu được quy định tại điều SRG_M.1 của EN 419241-1.

A.3.5.2 Hệ thống và vận hành

A.3.5.2.1 Áp dụng yêu cầu được quy định tại điều SRG_SO.1 của EN 419241-1.

A.3.5.2.2 Áp dụng yêu cầu được quy định tại điều SRG_SO.2 của EN 419241-1.

A.3.5.3 Kiểm soát an toàn máy tính

A.3.5.3. Áp dụng yêu cầu được quy định tại điều REQ-7.4-01, REQ-7.4-02X, REQ-7.4-05X, REQ-7.4-06X và REQ-7.4-13X quy định tại TCVN 14618:2026.

CHÚ THÍCH: Các yêu cầu đối với hệ thống tin cậy có thể được đáp ứng bằng các hệ thống phù hợp với EN 419241-1 hoặc hồ sơ bảo vệ phù hợp được xác định theo ISO/IEC 15408.

A.3.5.3.2 Áp dụng yêu cầu được quy định tại điều SRG_AA.6.1 của EN 419241-1.

A.3.5.4 Kiểm soát an toàn vòng đời

A.3.5.4.1 Áp dụng yêu cầu được quy định tại điều 7.7 và 7.14 của TCVN 14618:2026.

A.3.5.5 Kiểm soát an toàn mạng

A.3.5.5.1 Áp dụng yêu cầu được quy định tại điều 7.8 của TCVN 14618:2026.

A.3.6 Đánh giá tuân thủ và đánh giá khác

Việc đánh giá tuân thủ phải thực hiện theo ETSI EN 319 403.

A.3.7 Các vấn đề kinh doanh và pháp lý khác

A.3.7.1 Phí dịch vụ

Các yêu cầu chính sách này không nhằm hạn chế việc TSP thu phí dịch vụ.

A.3.7.2 Trách nhiệm tài chính

Không có yêu cầu.

A.3.7.3 Bảo mật thông tin kinh doanh

Không có yêu cầu.

A.3.7.4 Bảo vệ dữ liệu cá nhân

A.3.7.4.1 Áp dụng yêu cầu được quy định tại điều REQ-7.13-05 quy định tại TCVN 14618:2026.

A.3.7.5 Quyền sở hữu trí tuệ

Không có yêu cầu chính sách.

A.3.7.6 Cam kết và bảo đảm

SSASP chịu trách nhiệm đảm bảo tuân thủ các thủ tục quy định trong chính sách này, kể cả khi chức năng được thuê ngoài.

A.3.7.7 Tuyên bố miễn trừ trách nhiệm

Áp dụng theo điều A.3.7.6.

A.3.7.8 Giới hạn trách nhiệm pháp lý

Áp dụng các yêu cầu được quy định trong điều khoản và điều kiện tại điều 6.8.4.

A.3.7.9 Bồi thường

Không có yêu cầu chính sách.

A.3.7.10 Thời hạn và chấm dứt

Không có yêu cầu chính sách.

A.3.7.11 Thông báo và trao đổi với các bên liên quan

Không có yêu cầu chính sách.

A.3.7.12 Sửa đổi

Không có yêu cầu chính sách.

A.3.7.13 Giải quyết tranh chấp

Không có yêu cầu chính sách.

A.3.7.14 Luật áp dụng

Không thuộc phạm vi tài liệu này.

A.3.7.15 Tuân thủ pháp luật

A.3.7.15.1 Áp dụng các yêu cầu được quy định tại điều 7.13-01 và REQ-7.13-02 quy định tại TCVN 14618:2026.

A.3.7.16 Các quy định khác

Không có yêu cầu chính sách.

A.3.8 Các quy định khác

A.3.8.1 Yêu cầu tổ chức

A.3.8.1.1 Áp dụng các yêu cầu được quy định tại điều 7.1 của TCVN 14618:2026.

A.3.8.2 Thử nghiệm bổ sung

Không có yêu cầu chính sách.

A.3.8.3 Người khuyết tật

A.3.8.3.1 Áp dụng các yêu cầu được quy định tại điều REQ-7.13-03 và REQ-7.13-04 quy định tại TCVN 14618:2026.

A.3.8.4 Điều khoản và điều kiện

A.3.8.4.1 Áp dụng các yêu cầu được quy định tại điều 6.2 của TCVN 14618:2026.

A.4 Khung xây dựng chính sách dịch vụ ứng dụng ký số phía máy chủ

A.4.1 [CÓ ĐIỀU KIỆN] Khi xây dựng một SP từ các yêu cầu được xác định trong tài liệu này, chính sách phải bao gồm, hoặc quy định chặt chẽ hơn, tất cả các yêu cầu được xác định tại các điều khoản A.2 và A.3.

A.4.2 [CÓ ĐIỀU KIỆN] Khi xây dựng một SP từ các yêu cầu được xác định trong tài liệu này, chính sách phải xác định bất kỳ sai khác nào mà nó lựa chọn áp dụng.

A.4.3 [CÓ ĐIỀU KIỆN] Khi xây dựng một SP từ các yêu cầu được xác định trong tài liệu này, người ký phải được thông báo, như một phần của việc triển khai các điều khoản và điều kiện, về các cách thức mà chính sách cụ thể bổ sung hoặc quy định chặt chẽ hơn các yêu cầu của chính sách như được xác định trong tài liệu này.

A.4.4 [CÓ ĐIỀU KIỆN] Khi xây dựng một SP từ các yêu cầu được xác định trong tài liệu này, phải có một cơ quan (ví dụ: cơ quan quản lý chính sách) có thẩm quyền và trách nhiệm cuối cùng trong việc xác định và phê duyệt chính sách.

A.4.5 [CÓ ĐIỀU KIỆN] Khi xây dựng một SP từ các yêu cầu được xác định trong tài liệu này, nên thực hiện đánh giá rủi ro để đánh giá các yêu cầu nghiệp vụ và xác định các yêu cầu an toàn cần được đưa vào chính sách cho cộng đồng và phạm vi áp dụng đã nêu.

A.4.6 [CÓ ĐIỀU KIỆN] Khi xây dựng một SP từ các yêu cầu được xác định trong tài liệu này, chính sách nên được phê duyệt và sửa đổi theo một quy trình xem xét đã được xác định, bao gồm cả trách nhiệm trong việc duy trì chính sách.

A.4.7 [CÓ ĐIỀU KIỆN] Khi xây dựng một SP từ các yêu cầu được xác định trong tài liệu này, nên tồn tại một quy trình xem xét đã được xác định để bảo đảm rằng chính sách được hỗ trợ bởi quy chế chứng thực.

A.4.8 [CÓ ĐIỀU KIỆN] Khi xây dựng một SP từ các yêu cầu được xác định trong tài liệu này, TSP nên cung cấp các chính sách mà mình hỗ trợ cho cộng đồng người sử dụng.

A.4.9 [CÓ ĐIỀU KIỆN] Khi xây dựng một SP từ các yêu cầu được xác định trong tài liệu này, các sửa đổi đối với các chính sách do TSP hỗ trợ nên được cung cấp cho người ký.

A.4.10 [CÓ ĐIỀU KIỆN] Khi xây dựng một SP từ các yêu cầu được xác định trong tài liệu này, phải có một định danh đối tượng duy nhất cho chính sách (ví dụ: OID hoặc URI).

Phụ lục B

(quy định)

Yêu cầu về chính sách và an toàn đối với thành phần dịch vụ hỗ trợ việc tạo chữ ký số AdES

B.1 Tổng quan

B.1.1 Khái niệm chung về yêu cầu chính sách

Tài liệu này được cấu trúc phù hợp với TCVN 14618:2026. Tài liệu này viện dẫn các yêu cầu của TCVN 14618:2026 [9] và bổ sung các yêu cầu liên quan đến SCASP.

Xem TCVN 14618:2026 [9], điều 4 để có hướng dẫn về các yêu cầu chính sách chung.

B.1.2 Tài liệu áp dụng đối với SCASC

B.1.2.1 Quy chế chứng thực SCASC

Tổ chức cung cấp dịch vụ ứng dụng tạo chữ ký (SCASP) xây dựng, triển khai, thực thi và cập nhật một quy chế chứng thực SCASC, đây là một quy chế chứng thực dịch vụ tin cậy như được định nghĩa trong TCVN 14618:2026, được áp dụng cụ thể cho thành phần dịch vụ ứng dụng tạo chữ ký số. Xem điều khoản 6.1.

Quy chế chứng thực SCASC mô tả cách SCASP vận hành dịch vụ của mình và thuộc sở hữu của SCASP. Thực hành SCASC được điều chỉnh phù hợp với cấu trúc tổ chức, quy trình vận hành, cơ sở vật chất và môi trường tính toán của một TSP. Người nhận quy chế chứng thực có thể là kiểm toán viên, người ký và Bên tin cậy.

Tài liệu này cung cấp các yêu cầu được xác định là cần thiết để hỗ trợ một chính sách SCASC ở mức cao, được SCASP phê duyệt và được phản ánh trong quy chế chứng thực của mình.

B.1.2.2 Chính sách SCASC

Một chính sách SCASC mô tả những gì được cung cấp và có thể chứa nhiều thông tin đa dạng vượt ra ngoài phạm vi của tài liệu này nhằm chỉ ra khả năng áp dụng của dịch vụ. Một chính sách SCASC được định nghĩa độc lập với các chi tiết cụ thể của môi trường vận hành cụ thể của một SSASP. Người nhận của chính sách dịch vụ có thể là kiểm toán viên, người ký và Bên tin cậy.

Tài liệu này có thể được một chính sách SCASC viện dẫn để cung cấp thông tin về mức độ của dịch vụ.

Một chính sách SCASC không nhất thiết là một phần của tài liệu của SCASP (theo TCVN 14618:2026, một quy chế chứng thực và các điều khoản và điều kiện chung là đủ). Ngoài ra, tài liệu này không đặt ra các ràng buộc về hình thức của các chính sách SCASC; một chính sách SCASC có thể là một tài liệu độc lập hoặc được cung cấp như một phần của quy chế chứng thực và/hoặc các điều khoản và điều kiện chung.

Tài liệu này không đặt ra bất kỳ giới hạn nào đối với nội dung của các chính sách SCASC, tuy nhiên yêu cầu SCASP phải cung cấp thông tin tối thiểu về dịch vụ mà mình cung cấp (xem các điều khoản 6.1 và 6.2).

B.1.2.3 Điều khoản và điều kiện

Ngoài quy chế chứng thực và chính sách SCASC (nếu được ban hành), SCASP cũng ban hành điều khoản và điều kiện, nội dung này bao quát một phạm vi rộng các điều khoản thương mại hoặc điều khoản kỹ thuật mà không nhất thiết phải được truyền đạt tới khách hàng, v.v. Các điều khoản và điều kiện là cụ thể đối với một SCASP. Người nhận các điều khoản và điều kiện có thể là người ký và Bên tin cậy.

B.1.2.4 Các tài liệu khác liên quan đến việc tạo chữ ký số

Bên cạnh việc mô tả các thực hành được SCASP sử dụng để cung cấp dịch vụ tạo chữ ký số AdES, điều quan trọng là phải ghi nhận các tiêu chí theo đó các chữ ký số được tạo ra và, hơn nữa, có thể xác định rằng chúng phù hợp với một nhu cầu nghiệp vụ cụ thể.

Hai loại tài liệu có thể được sử dụng cho các mục đích này:

- Chính sách tạo chữ ký số: là tập hợp các ràng buộc về việc tạo chữ ký số được xử lý bởi SCA. Một chính sách tạo chữ ký số có thể được định danh bằng một OID.

- Quy tắc áp dụng chữ ký số: có thể được cấu trúc theo ETSI TS 119 172-1 và có thể bao gồm một chính sách tạo chữ ký số chứa các ràng buộc tạo chữ ký số sẽ được SCA áp dụng, cũng như các tiêu chí khác thể hiện khả năng áp dụng của chữ ký số được tạo ra đối với các nhu cầu nghiệp vụ cụ thể.

CHÚ THÍCH: Việc sử dụng các quy tắc áp dụng chữ ký số nằm ngoài phạm vi của tài liệu này, nhưng có thể được áp dụng như một phần mở rộng đối với dịch vụ tạo chữ ký số được đề cập trong tài liệu này.

Quy chế chứng thực SCASC, chính sách tạo chữ ký số và quy tắc áp dụng chữ ký số là các loại tài liệu khác nhau; quy chế chứng thực SCASC mô tả cách SCASP vận hành dịch vụ của mình, trong khi chính sách tạo chữ ký số quy định các ràng buộc sẽ được SCA xử lý khi tạo chữ ký số. Vượt ra ngoài phạm vi của chính sách tạo chữ ký số, quy tắc áp dụng chữ ký số quy định các quy tắc và giả định được người sử dụng dùng để quyết định liệu một chữ ký số được tạo theo các quy tắc này có phù hợp với mục đích hay không.

Chủ sở hữu của quy chế chứng thực SCASC là SCASP, trong khi chủ sở hữu của quy tắc áp dụng chữ ký số thường là người ký.

B.1.3 Kiến trúc

Một thành phần dịch vụ của TSP hỗ trợ việc tạo chữ ký số AdES (SCASC**)** nhận (các) tài liệu và/hoặc (các) giá trị băm của (các) tài liệu cần được ký, và tùy chọn một số tham số ký, thu thập tất cả thông tin cần thiết để tạo chữ ký số, chuẩn bị biểu diễn dữ liệu cần được ký (DTBSR) và gửi dữ liệu này tới thiết bị tạo chữ ký số (SCDev)**.**

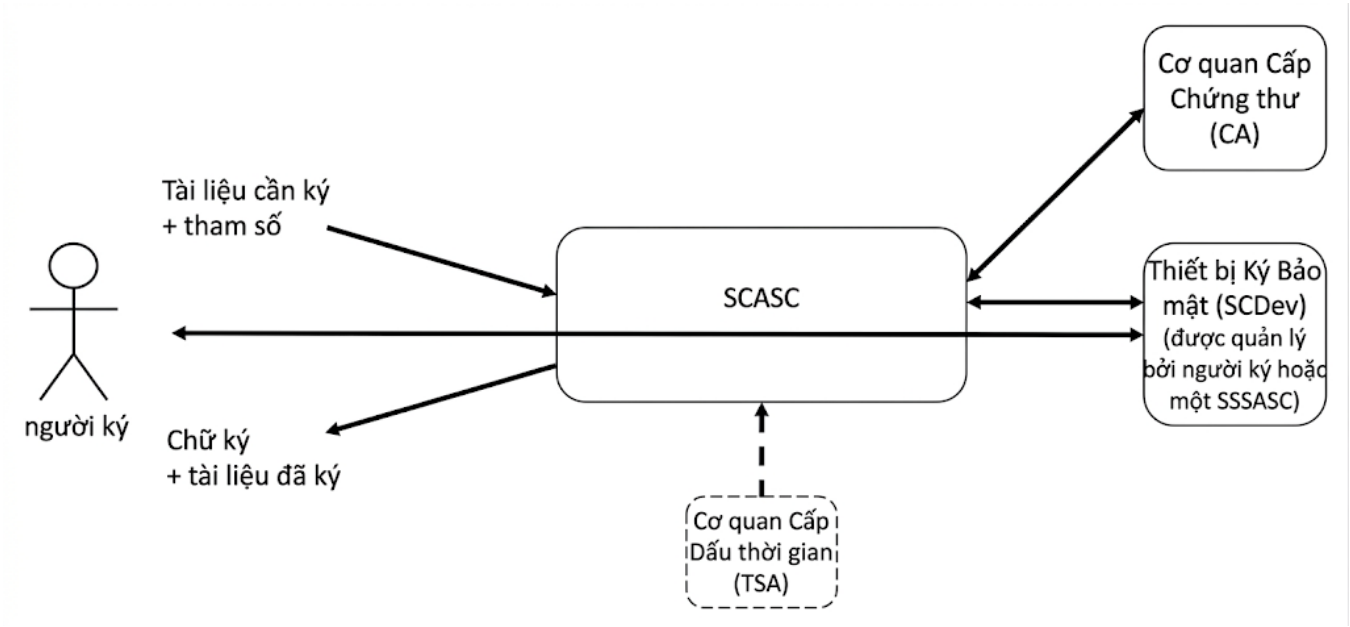
SCDev có thể nằm trong môi trường của người dùng hoặc được quản lý bởi một thành phần dịch vụ ứng dụng ký phía máy chủ (SSASC) **n**hư được mô tả trong ETSI TS 119 431-1.

Với mục đích của tài liệu này, giả định rằng SCDev thực hiện việc xác thực và sự đồng ý ký với người dùng và trả về giá trị chữ ký số, mà không đi vào chi tiết việc này được thực hiện bởi chính SCDev hay bởi thành phần quản lý SCDev.

Việc cho phép sử dụng khóa ký số trong SCDev có thể thông qua SCASC nhưng cũng có thể được thực hiện trực tiếp thông qua việc giao tiếp giữa người ký và SCDev.

Giá trị chữ ký số được SCASC đưa vào trong chữ ký số.

CHÚ THÍCH: SCASC đại diện cho ứng dụng tạo chữ ký số trong EN 419241-1.



Hình 3 - Mối quan hệ của thành phần dịch vụ TSP đối với việc tạo chữ ký số AdES

B.2 Đánh giá rủi ro

B.2.1 Áp dụng các yêu cầu được quy định tại điều 6.1 của TCVN 14618:2026.

B.3 Chính sách và quy chế chứng thực

B.3.1 Quy chế chứng thực

B.3.1.1 Áp dụng các yêu cầu được quy định tại Điều 6.1 của TCVN 14618:2026.

B.3.1.2 Khi SCASC hỗ trợ việc đưa dấu thời gian vào chữ ký số AdES, quy chế chứng thực SCASC phải liệt kê các TSA được sử dụng.

B.3.1.3 Quy chế chứng thực SCASC phải chỉ rõ tất cả các chính sách tạo chữ ký số được hỗ trợ.

B.3.1.4 Quy chế chứng thực SCASC phải chỉ rõ tất cả các định dạng chữ ký số được hỗ trợ.

B.3.1.5 Quy chế chứng thực SCASC phải chỉ rõ tất cả các lớp chữ ký số được hỗ trợ.

B.3.1.6 SCASP phải xác định trong quy chế chứng thực SCASC các nghĩa vụ của tất cả các tổ chức bên ngoài hỗ trợ dịch vụ của mình, bao gồm các chính sách và thực hành áp dụng.

B.3.2 Điều khoản và điều kiện

B.3.2.1 Áp dụng các yêu cầu được quy định tại Điều 6.2 của TCVN 14618:2026.

B.3.2.2 Để xác định chính sách dịch vụ tin cậy được áp dụng, điều khoản và điều kiện của SCASC phải liệt kê hoặc viện dẫn (ví dụ: thông qua OID), và mô tả ngắn gọn, các chính sách SCASC được hỗ trợ mà nó tuân thủ.

B.3.2.3 Để xác định chính sách dịch vụ tin cậy được áp dụng, điều khoản và điều kiện của SCASC có thể sử dụng các OID được quy định tại Điều B.1.2.2.

B.3.2.4 [CÓ ĐIỀU KIỆN] Trường hợp điều khoản và điều kiện của SCASC viện dẫn một chính sách dịch vụ tin cậy bằng một OID khác với các OID được quy định tại Điều B.1.2.2, thì chính sách dịch vụ tin cậy được viện dẫn đó phải tuân thủ các yêu cầu tại Điều B.6.

B.3.2.7 Điều khoản và điều kiện phải nêu rõ quyền và nghĩa vụ của SCASP và người ký.

B.3.2.8 Điều khoản và điều kiện phải mô tả các tùy chọn được dịch vụ hỗ trợ, tối thiểu bao gồm:

a) các định dạng chữ ký số được hỗ trợ;

b) các tham số ký số được hỗ trợ;

c) việc tài liệu cần ký số có thể chỉ được cung cấp dưới dạng giá trị băm hay không; và

d) các thiết bị tạo chữ ký số (SCDev) được hỗ trợ trong môi trường người dùng hoặc các SSASC được hỗ trợ tạo giá trị chữ ký số cho người ký.

B.3.2.9 Điều khoản và điều kiện phải bao gồm các nội dung của Thỏa thuận mức dịch vụ (SLA) liên quan đến khả năng sẵn sàng của dịch vụ và, khi áp dụng, các thông tin SLA khác như thời gian phản hồi.

B.3.2.10 Điều khoản và điều kiện phải cung cấp thông báo rằng SLA có thể bị ảnh hưởng bởi các thực hành, chính sách và SLA của các TSP khác không thuộc sự kiểm soát của SCASP, như CA phát hành chứng thư chữ ký số được sử dụng cho chữ ký hoặc TSA được sử dụng để đóng dấu thời gian.

B.3.2.11 Điều khoản và điều kiện phải giải thích cách SCASP xử lý dữ liệu cá nhân.

B.3.3 Chính sách an toàn thông tin

B.3.3.1 Áp dụng các yêu cầu được quy định tại Điều 6.3 của TCVN 14618:2026.

B.3.3.2 Chính sách an toàn thông tin nên ghi nhận các biện pháp kiểm soát về an toàn và quyền riêng tư được triển khai để bảo vệ dữ liệu cá nhân.

CHÚ THÍCH: Nếu SCASP có quyền truy cập vào dữ liệu cần ký số, thì dữ liệu này có thể chứa thông tin mật cũng như dữ liệu cá nhân.

B.4 Quản lý và vận hành SCAS

B.4.1 Tổ chức nội bộ

B.4.1.1 Áp dụng các yêu cầu được quy định tại Điều 7.1 của TCVN 14618:2026.

B.4.2 Nguồn nhân lực

B.4.2.1 Áp dụng các yêu cầu được quy định tại Điều 7.2 của TCVN 14618:2026.

B.4.3 Quản lý tài sản

B.4.3.1 Áp dụng các yêu cầu được quy định tại Điều 7.3 của TCVN 14618:2026.

B.4.4 Kiểm soát truy cập

B.4.4.1 Áp dụng các yêu cầu được quy định tại Điều 7.4 của TCVN 14618:2026.

B.4.5 Kiểm soát mật mã

B.4.5.1 Áp dụng các yêu cầu được quy định tại Điều 7.5 của TCVN 14618:2026.

B.4.6 An ninh vật lý và môi trường

B.4.6.1 Áp dụng các yêu cầu được quy định tại Điều 7.6 của TCVN 14618:2026.

B.4.6.2 Áp dụng các yêu cầu được quy định tại Điều 5.2 của ETSI TS 119 101

B.4.7 An ninh vận hành

B.4.7.1 Áp dụng các yêu cầu được quy định tại Điều 7.7 của TCVN 14618:2026.

Ngoài ra, áp dụng các yêu cầu sau:

B.4.7.2 Các yêu cầu sau được quy định tại Điều 5.2 của ETSI TS 119 101 nên được áp dụng đối với SCA: GSM 1.2 và GSM 1.3.

B.4.7.3 Các yêu cầu sau được quy định tại Điều 5.2 của ETSI TS 119 101 phải được áp dụng đối với SCA: GSM 2.4.

B.4.7.4 SCASC phải triển khai tất cả các yêu cầu bắt buộc từ ETSI TS 119 101 được viện dẫn ở trên, bất kể yêu cầu đó được áp dụng cho DA hay SCA.

B.4.8 An ninh mạng

B.4.8.1 Áp dụng các yêu cầu được quy định tại Điều 7.8 của TCVN 14618:2026.

B.4.9 Quản lý sự cố

B.4.9.1Áp dụng các yêu cầu được quy định tại Điều 7.9 của TCVN 14618:2026.

B.4.10 Thu thập bằng chứng

B.4.10.1 Áp dụng các yêu cầu được quy định tại Điều 7.10 của TCVN 14618:2026.

Ngoài ra, áp dụng các yêu cầu sau:

B.4.10.2 Mọi hoạt động tạo chữ ký số AdES phải được ghi nhật ký, cùng với thông tin định danh của người đăng ký khi thông tin này được biết.

B.4.10.3 Nhật ký sự kiện phải được gắn dấu thời gian của sự kiện.

B.4.10.4 Tần suất xử lý, thời gian lưu trữ, biện pháp bảo vệ, quy trình sao lưu của hệ thống thu thập, quy trình lưu trữ và đánh giá lỗ hổng đối với nhật ký sự kiện phải được ghi nhận trong quy chế chứng thực SCASC.

B.4.10.5 Việc triển khai các yêu cầu B.4.10.1 và B.4.10.2 phải tính đến các yêu cầu về quyền riêng tư áp dụng.

B.4.10.6 Nhật ký sự kiện nên bao gồm loại sự kiện, trạng thái thành công hoặc thất bại của sự kiện, và định danh của cá nhân và/hoặc thành phần phát sinh sự kiện đó.

B.4.11 Quản lý tính liên tục hoạt động

B.4.11.1 Áp dụng các yêu cầu được quy định tại Điều 7.11 của TCVN 14618:2026.

Ngoài ra, áp dụng các yêu cầu sau:

B.4.11.2 Cần triển khai các biện pháp để tránh gián đoạn dịch vụ do hành vi cố ý hoặc vô ý của người dùng hoặc Bên tin cậy.

B.4.11.3 [CÓ ĐIỀU KIỆN] Trường hợp bổ sung dấu thời gian vào chữ ký số, SLA của SCASP cần xem xét SLA của TSA tương ứng.

B.4.12 Chấm dứt dịch vụ và kế hoạch chấm dứt

B.4.12.1 Áp dụng các yêu cầu được quy định tại Điều 7.12 của TCVN 14618:2026.

B.4.13 Tuân thủ và yêu cầu pháp lý

B.4.13.1 Áp dụng các yêu cầu được quy định tại Điều 7.13 của TCVN 14618:2026.

Ngoài ra, áp dụng các yêu cầu sau:

B.4.13.2 Khi dữ liệu cá nhân được xử lý bởi Bên tin cậy, nếu pháp luật yêu cầu, phải thiết lập thỏa thuận phù hợp với các bên xử lý dữ liệu cá nhân nhằm bảo đảm họ tuân thủ các yêu cầu pháp lý, bao gồm việc triển khai các biện pháp kỹ thuật, tổ chức và pháp lý để bảo vệ dữ liệu cá nhân.

CHÚ THÍCH 1: Dữ liệu cần ký số được coi là dữ liệu cá nhân.

B.4.13.3 SCASC không được lưu trữ SD sau khi xử lý nếu không cần thiết.

CHÚ THÍCH 2: Nếu SCASP hoạt động kết hợp với dịch vụ lưu trữ lâu dài, có thể phát sinh nhu cầu lưu giữ dữ liệu này.

B.4.13.4 SCASP chịu trách nhiệm tổng thể trong việc đáp ứng các yêu cầu được quy định tại các Điều B.2 đến B.5, ngay cả khi một phần hoặc toàn bộ chức năng được thực hiện bởi các nhà thầu phụ.

B.5 Thành phần dịch vụ ứng dụng tạo chữ ký số

B.5.1 Giao diện

B.5.1.1 [CÓ ĐIỀU KIỆN] Trường hợp SCASC có giao thức cho phép máy truy cập để sử dụng dịch vụ, nên sử dụng giao thức được quy định tại ETSI TS 119 432.

B.5.1.2 Kết nối giữa SCASC và SCDev được sử dụng để tạo giá trị chữ ký số phải được bảo mật.

B.5.1.3 [CÓ ĐIỀU KIỆN] Trường hợp SCASC hiển thị tài liệu cho người ký, phải mô tả trong quy chế chứng thực SCASC cách thức bảo đảm nguyên tắc “những gì bạn thấy là những gì bạn ký” (What You See Is What You Sign - WYSIWYS).

B.5.1.4 [CÓ ĐIỀU KIỆN] Trường hợp SCASC hiển thị tài liệu cho người ký theo cách diễn giải, quy chế chứng thực SCASC phải nêu rõ cách thức diễn giải các dữ liệu cụ thể.

B.5.1.5 [CÓ ĐIỀU KIỆN] Trường hợp SCASC hiển thị tài liệu cho người ký, quy chế chứng thực SCASC hoặc điều khoản và điều kiện phải nêu rõ các loại nội dung có thể được hiển thị chính xác.

B.5.1.6 [CÓ ĐIỀU KIỆN] Trường hợp SCASC hiển thị tài liệu cho người ký, giao diện phải cảnh báo người ký nếu không thể hiển thị chính xác tất cả các phần của SD theo kiểu nội dung dữ liệu.

B.5.1.7 [CÓ ĐIỀU KIỆN] Trường hợp SCASC cung cấp giao diện người dùng đồ họa cho phía khách, các yêu cầu UI 1 và UI 2 của ETSI TS 119 101 nên được áp dụng.

B.5.1.8 [CÓ ĐIỀU KIỆN] Trường hợp SCASC hiển thị tài liệu cho người ký, phải có quy trình xử lý mà trong đó người ký nhận thức rõ việc mình đồng ý ký số tài liệu.

B.5.1.9 [CÓ ĐIỀU KIỆN] Trường hợp SCASC hiển thị tài liệu cho người ký, các yêu cầu SCP 13 và SCP 47 của ETSI TS 119 101 phải được áp dụng.

B.5.1.10 [CÓ ĐIỀU KIỆN] Trường hợp SCASC hiển thị tài liệu cho người ký, SCASC nên cho phép tải xuống tài liệu cần ký số.

B.5.1.11 [CÓ ĐIỀU KIỆN] Trường hợp SCASC hiển thị tài liệu cho người ký, SCASC nên ghi nhật ký thời gian tài liệu được hiển thị cho người ký.

B.5.1.12 [CÓ ĐIỀU KIỆN] Trường hợp SCASC hiển thị tài liệu cho người ký và tài liệu đã được tải xuống, SCASC nên ghi nhật ký sự kiện này.

B.5.2 Tạo chữ ký số AdES

B.5.2.1 SCASC phải bảo đảm tính toàn vẹn và tính bảo mật của thông tin nhận được.

B.5.2.2 Các thuật toán mật mã được sử dụng nên được lựa chọn từ các thuật toán được khuyến nghị trong TCVN 14617:2026.

B.5.2.3 Các thuật toán mật mã được áp dụng phải theo quy định trong chính sách tạo chữ ký số.

B.5.2.4 Các yêu cầu SCP 14, SCP 31, SCP 37 và SCP 61 của ETSI TS 119 101 phải được áp dụng.

B.5.2.5 SCASC phải thông báo cho người ký về loại cam kết (commitment type).

CHÚ THÍCH 2: Thông tin này có thể được cung cấp trong chính sách tạo chữ ký số.

B.5.2.6 SCASC nên bao gồm chuỗi chứng thư chữ ký số trong chữ ký số.

B.5.2.7 Người ký phải có khả năng biết chính sách tạo chữ ký số nào sẽ được áp dụng.

B.5.2.8 Người ký phải có khả năng biết chính sách tạo chữ ký số nào đã được áp dụng khi tạo một chữ ký số cụ thể.

B.5.2.9 SCASC nên cung cấp chữ ký số cho người ký.

B.5.2.10 Trường hợp SCASC có quyền truy cập vào dữ liệu đã ký số, nên cung cấp dữ liệu đã ký số cùng với chữ ký số cho người ký.

CHÚ THÍCH 3: Trường hợp chữ ký số được bao gói trong hoặc bao chứa dữ liệu đã ký, yêu cầu B.5.2.10 được suy ra trực tiếp từ yêu cầu B.5.2.9.

B.6 Khung định nghĩa chính sách thành phần dịch vụ ứng dụng tạo chữ ký số

CHÚ THÍCH: TSP có thể sử dụng trực tiếp các chính sách dịch vụ tin cậy được xác định tại Điều B.1.2.2, hoặc có thể viện dẫn một chính sách dịch vụ tin cậy được xây dựng dựa trên các chính sách tại Điều B.1.2.2 nhưng bổ sung thêm các yêu cầu hoặc ràng buộc so với các yêu cầu của tài liệu này. Trường hợp sau được hiểu là chính sách SCASC được xây dựng dựa trên một chính sách dịch vụ tin cậy được quy định trong tài liệu này.

B.6.2 [CÓ ĐIỀU KIỆN] Trường hợp xây dựng chính sách SCASC dựa trên một chính sách dịch vụ tin cậy được quy định trong tài liệu này, chính sách SCASC phải xác định chính sách dịch vụ tin cậy nào được sử dụng làm cơ sở.

B.6.3 [CÓ ĐIỀU KIỆN] Trường hợp xây dựng chính sách SCASC dựa trên một chính sách dịch vụ tin cậy được quy định trong tài liệu này, chính sách phải xác định mọi sai khác mà nó lựa chọn áp dụng.

B.6.4 [CÓ ĐIỀU KIỆN] Trường hợp xây dựng chính sách SCASC dựa trên một chính sách dịch vụ tin cậy được quy định trong tài liệu này, người đăng ký phải được thông báo, trong quá trình thực hiện điều khoản và điều kiện, về cách thức mà chính sách cụ thể bổ sung hoặc siết chặt các yêu cầu của chính sách được quy định trong tài liệu này.

B.6.5 [CÓ ĐIỀU KIỆN] Trường hợp xây dựng chính sách SCASC dựa trên một chính sách dịch vụ tin cậy được quy định trong tài liệu này, phải có một cơ quan (ví dụ: cơ quan quản lý chính sách) có thẩm quyền và trách nhiệm cuối cùng trong việc xác định và phê duyệt chính sách.

B.6.6 [CÓ ĐIỀU KIỆN] Trường hợp xây dựng chính sách SCASC dựa trên một chính sách dịch vụ tin cậy được quy định trong tài liệu này, nên thực hiện đánh giá rủi ro để đánh giá các yêu cầu nghiệp vụ và xác định các yêu cầu an toàn cần đưa vào chính sách cho cộng đồng và phạm vi áp dụng đã xác định.

B.6.7 [CÓ ĐIỀU KIỆN] Trường hợp xây dựng chính sách SCASC dựa trên một chính sách dịch vụ tin cậy được quy định trong tài liệu này, chính sách phải được phê duyệt và sửa đổi theo một quy trình rà soát được xác định, bao gồm trách nhiệm duy trì chính sách.

B.6.8 [CÓ ĐIỀU KIỆN] Trường hợp xây dựng chính sách SCASC dựa trên một chính sách dịch vụ tin cậy được quy định trong tài liệu này, phải tồn tại một quy trình rà soát được xác định để bảo đảm rằng chính sách được hỗ trợ bởi các quy chế chứng thực.

B.6.9 [CÓ ĐIỀU KIỆN] Trường hợp xây dựng chính sách SCASC dựa trên một chính sách dịch vụ tin cậy được quy định trong tài liệu này, TSP nên cung cấp các chính sách mà mình hỗ trợ cho cộng đồng người sử dụng.

B.6.10 [CÓ ĐIỀU KIỆN] Trường hợp xây dựng chính sách SCASC dựa trên một chính sách dịch vụ tin cậy được quy định trong tài liệu này, các phiên bản sửa đổi của chính sách được hỗ trợ bởi TSP nên được cung cấp cho người đăng ký.

B.6.11 [CÓ ĐIỀU KIỆN] Trường hợp xây dựng chính sách SCASC dựa trên một chính sách dịch vụ tin cậy được quy định trong tài liệu này, phải có một định danh đối tượng duy nhất cho chính sách (ví dụ: OID hoặc URI).

Thư mục tài liệu tham khảo

[1] Luật số 20/2023/QH15 ngày 22 tháng 6 năm 2023 của Quốc hội về giao dịch điện tử.

[2] ETSI TS 119 431-1 V1.3.1 (2024-12), Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev.

[3] ETSI TS 119 431-2 V1.2.1 (2023-06), Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation.

[4] ETSI TR 119 001, Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations.

[5] ETSI TS 119 172-1, Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents.

[6] ETSI TS 119 102-1 V1.2.1 (2018-08), Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.

[7] ETSI EN 319 122-1, Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures.

[8] ETSI EN 319 122-2, Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures.

[9] ETSI EN 319 132-1, Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures.

[10] ETSI EN 319 132-2, Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures.

[11] ETSI EN 319 142-1, Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures.

[12] ETSI EN 319 142-2, Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signature profiles.

[13] ETSI TS 119 432, Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation.

[14] EN 419241-2:2019, Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing.

[15] IETF RFC 3647 (November 2003), Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework.

[16] ISO/IEC 15408 (tất cả các phần), Information security, cybersecurity and privacy protection - Evaluation criteria for IT security.

[17] ISO/IEC 18014-2:2021, Information security - Time-stamping services - Part 2: Mechanisms producing independent tokens.