TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN XXXX:2026

Xuất bản lần 1

GIAO DỊCH ĐIỆN TỬ - GIAO THỨC TẠO CHỮ KÝ SỐ CHO MÔ HÌNH KÝ SỐ TỪ XA

Electronic Transactions – Digital Signature Creation Protocol for Remote Signing Models

HÀ NỘI – 2026

Mục lục

Lời nói đầu

TCVN XXXX:2026 được tham khảo Tiêu chuẩn quốc tế ETSI TS 119 432 v1.2.1 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.

Lời giới thiệu

Sự phát triển của hệ thống phân tán, điện toán đám mây và thiết bị di động đã thúc đẩy mô hình ký số từ xa, trong đó các bước của quá trình tạo chữ ký số được thực hiện bởi nhiều hệ thống, dịch vụ hoặc thành phần khác nhau và khóa ký được quản lý tại dịch vụ từ xa.

Tiêu chuẩn này quy định các giao thức và giao diện giữa các thành phần tham gia quá trình tạo chữ ký số từ xa và tạo lập chữ ký điện tử nâng cao (AdES), nhằm bảo đảm khả năng kết nối và triển khai thống nhất. Việc cung cấp dịch vụ chữ ký số từ xa công cộng tại Việt Nam đồng thời phải tuân thủ pháp luật và quy chuẩn kỹ thuật quốc gia hiện hành.

Giao dịch điện tử - Giao thức tạo chữ ký số cho mô hình ký số từ xa

Electronic Transactions - Digital Signature Creation Protocol for Remote Signing Models

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu chung đối với giao thức tạo chữ ký số trong mô hình ký số từ xa, nhằm hỗ trợ việc triển khai, kết nối và cung cấp dịch vụ ký số từ xa thống nhất.

Tiêu chuẩn giới hạn ở mô hình ký số từ xa trên máy chủ, trong đó khóa ký được lưu giữ tại dịch vụ dùng chung từ xa; không áp dụng cho mô hình ký cục bộ mà khóa ký được lưu giữ trên thiết bị cá nhân của chủ thể ký.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau là cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng 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).

- Cloud Signature Consortium Standard (Version 1.0.3.0): "Architectures and protocols for remote signature applications".
- OASIS Standard: "Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0", Committee Specification 02.
- OASIS Standard: "Advanced Electronic Signature Profiles of the OASIS Digital Signature Service Version 2.0", Working Draft 02.
- IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
- OASIS Standard: "Asynchronous Processing Abstract Profile of the OASIS Digital Signature Services Version 1.0".
- EN 419 241-1: "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements" (produced by CEN).
- IETF RFC 5646: "Tags for Identifying Languages".https://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-asynchronous_processing-spec-
- IETF RFC 4514: "Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names".
- IETF RFC 3061: "A URN Namespace of Objects Identifiers".
- IETF RFC 7468: "Textual Encodings of PKIX, PKCS, and CMS Structures".
- ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

- ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".
- ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".
- TCVN 7217-1:2007 (ISO 3166-1:2006), Mã biểu thị tên quốc gia và các mảnh lãnh thổ hành chính - Phần 1: Mã quốc gia.

3 Thuật ngữ và chữ viết tắt

Trong tiêu chuẩn này sử dụng các thuật ngữ, định nghĩa sau:

3.1 Thuật ngữ

3.1.1

Chữ ký (số) AdES (AdES digital signature)

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

3.1.2

Ứng dụng khách (client application)

Ứng dụng chạy trong môi trường của chủ thể ký để truy cập các dịch vụ do SCASC và/hoặc SSASC cung cấp.

3.1.3

Chữ ký số (digital signature)

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.

3.1.4

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 dữ liệu chứng minh nguồn gốc và tính toàn vẹn của đơn vị dữ liệu, đồng thời bảo vệ chống giả mạo

3.1.5

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 chủ thể ký và cung cấp khả năng kiểm soát thao tác ký thay mặt chủ thể ký.

3.1.6

Ứng dụng ký số trên 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 chủ thể ký.

3.1.7

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

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

3.1.8

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

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

3.1.9

Nhà cung cấp dịch vụ ứng dụng ký số trên máy chủ (server signing application service provider)

TSP vận hành thành phần dịch vụ ứng dụng ký số trên máy chủ.

3.1.10

Ứng dụng tạo chữ ký số (signature creation application)

Ứng dụng trong hệ thống tạo chữ ký số thực hiện việc tạo chữ ký số AdES và sử dụng SCDev để tạo giá trị chữ ký số.

CHÚ THÍCH: SCDev có thể được quản lý bởi SSASC.

3.1.11

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 số.

3.1.12

Nhà cung cấp dịch vụ ứng dụng tạo chữ ký số (signature creation application service provider)

TSP vận hành thành phần dịch vụ ứng dụng tạo chữ ký số.

3.1.13

Ràng buộc tạo chữ ký số (signature creation constraint)

Tiêu chí được sử dụng khi tạo chữ ký số.

3.1.14

Thiết bị tạo chữ ký số (signature creation device)

Phần mềm hoặc phần cứng được cấu hình để sử dụng dữ liệu tạo chữ ký số và tạo giá trị chữ ký số.

3.1.15

Chính sách tạo chữ ký số (signature creation policy)

Tập hợp các ràng buộc tạo chữ ký số được hoặc sẽ được xử lý bởi SCASC hoặc SSASC.

3.1.16

Dịch vụ tạo chữ ký số (signature creation service)

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

3.1.17

Nhà cung cấp dịch vụ tạo chữ ký số (signature creation service provider)

TSP cung cấp dịch vụ tạo chữ ký số.

CHÚ THÍCH: Theo định nghĩa trong CEN EN 419 241-1.

3.1.18

Thông tin xác thực chữ ký (signature credential)

Tập hợp bao gồm khóa ký và chứng thư chữ ký số tương ứng.

3.1.19

Thông điệp dữ liệu (data message)

Thông tin được tạo ra, được gửi, được nhận, được lưu trữ bằng phương tiện điện tử.

3.1.20

Chữ ký điện tử (electronic signature)

Chữ ký được tạo lập dưới dạng dữ liệu điện tử gắn liền hoặc kết hợp một cách lô gíc với thông điệp dữ liệu để xác nhận chủ thể ký và khẳng định sự chấp thuận của chủ thể đó đối với thông điệp dữ liệu.

3.1.21

Ký số (digital signing)

Việc đưa khóa bí mật vào một chương trình phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu.

3.1.22

Chứng thư chữ ký số (digital signature certificate)

Một dạng chứng thư chữ ký điện tử do Tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp nhằm cung cấp thông tin về khóa công khai của một cá nhân, tổ chức từ đó xác nhận cá nhân, tổ chức là chủ thể ký thông qua việc sử dụng khóa bí mật tương ứng.

3.1.23

Dấu thời gian (timestamp)

Dữ liệu điện tử gắn với thông điệp dữ liệu cho phép xác định thời gian của thông điệp dữ liệu đó tồn tại ở một thời điểm cụ thể.

3.1.24

Cặp khóa không đối xứng (asymmetric key pair)

Khóa công khai và khóa bí mật tương ứng.

3.1.25

Khóa bí mật (private key)

Thành phần của cặp khóa không đối xứng được sử dụng để ký thông điệp dữ liệu.

3.1.26

Khóa công khai (public key)

Thành phần của cặp khóa không đối xứng được sử dụng để xác thực chữ ký số trên thông điệp dữ liệu.

3.1.27

Hàm băm (hash function)

Một thuật toán chuyển đổi thông điệp dữ liệu đầu vào thành một chuỗi có độ dài cố định, gọi là mã băm. Hàm băm được sử dụng để kiểm tra tính toàn vẹn của thông điệp dữ liệu và tạo chữ ký số.

3.1.28

Chủ thể ký (signer)

Cá nhân hoặc tổ chức sở hữu chứng thư chữ ký số và sử dụng khóa bí mật tương ứng để thực hiện ký số trên thông điệp dữ liệu.

3.1.29

Xác thực (authentication)

Việc cung cấp sự đảm bảo rằng đặc tính được tuyên bố của một thực thể là chính xác.

3.1.30

Dịch vụ tin cậy (trust service)

Dịch vụ điện tử cho các hoạt động: tạo, kiểm tra và xác minh chữ ký số và chứng thư liên quan; tạo, kiểm tra và xác minh dấu thời gian và chứng thư liên quan; chuyển phát điện tử và chứng thư liên quan; tạo, kiểm tra và xác minh chứng thư xác thực trang web; lưu trữ chữ ký số hoặc chứng thư liên quan đến các dịch vụ trên.

3.1.31

Khóa ký (signing key)

Khóa bí mật được sử dụng để tạo chữ ký số.

3.2 Ký hiệu

Không có.

3.3 Chữ viết tắt

AdES	Advanced Electronic Signature	Chữ ký điện tử nâng cao
API	Application Program Interface	Giao diện lập trình ứng dụng
ASN.1	Abstract Syntax Notation One	Ký pháp cú pháp trừu tượng phiên bản 1
CA	Certification Authority	Tổ chức chứng thực chữ ký số
CAdES	CMS Advanced Electronic Signatures	Chữ ký điện tử nâng cao dựa trên CMS

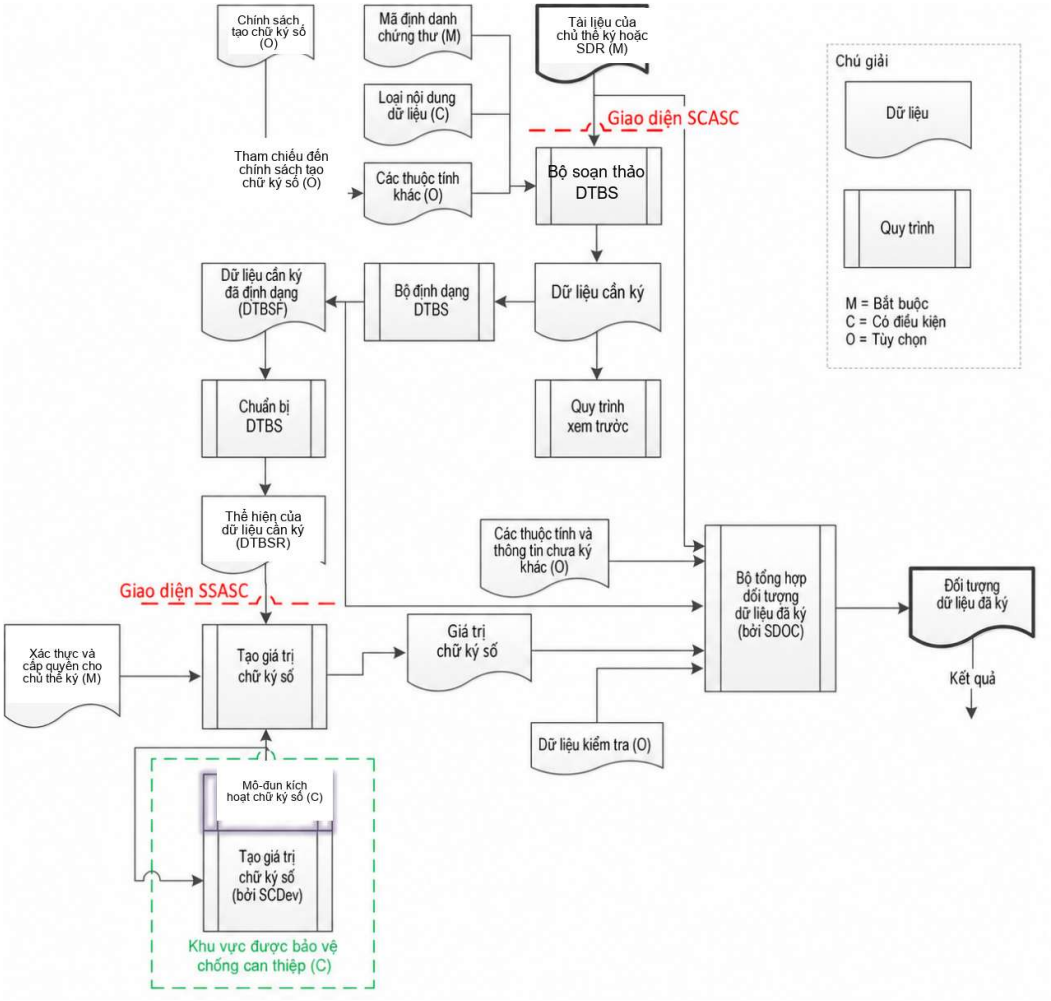
CEN	European Committee for Standardization	Ủy ban Tiêu chuẩn hóa Châu Âu
CMS	Cryptographic Message Syntax	Cú pháp thông điệp mật mã
CRL	Certificate Revocation List	Danh sách chứng thư bị thu hồi
CSC	Cloud Signature Consortium	Liên minh chữ ký số đám mây
DER	Distinguished Encoding Rules	Quy tắc mã hóa phân biệt
DSS-X	Digital Signature Services eXtended	Dịch vụ chữ ký số mở rộng
DSV	Digital Signature Value	Giá trị chữ ký số
DTBS	Data To Be Signed	Dữ liệu cần ký
DTBSF	Data To Be Signed Formatted	Dữ liệu cần ký đã định dạng
DTBSR	Data To Be Signed Representation	Thể hiện của dữ liệu cần ký
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số dựa trên đường cong elliptic
EN	European Norm	Tiêu chuẩn Châu Âu
ETSI	European Telecommunications Standards Institute	Viện Tiêu chuẩn Viễn thông Châu Âu
HTTP	Hyper Text Transfer Protocol	Giao thức truyền tải siêu văn bản
IETF	Internet Engineering Task Force	Lực lượng đặc nhiệm kỹ thuật Internet
ISO	International Organization for Standardization	Tổ chức tiêu chuẩn hóa quốc tế
JPEG	Joint Photographic Experts Group	Định dạng ảnh JPEG
JSON	JavaScript Object Notation	Định dạng trao đổi dữ liệu JSON
JWT	JSON Web Token	Mã thông báo web JSON
LDAP	Lightweight Directory Access Protocol	Giao thức truy cập thư mục hạng nhẹ
LT	Long Term	Ký số dài hạn
LTA	Long Term Archival	Lưu trữ ký số dài hạn
OAI	OpenAPI Initiative	Sáng kiến OpenAPI
OASIS	Organization for the Advancement of Structured Information Standards	Tổ chức thúc đẩy các tiêu chuẩn thông tin cấu trúc
OAuth	Open Authorization	Ủy quyền mở
OCSP	Online Certificate Status Protocol	Giao thức kiểm tra trạng thái chứng thư trực tuyến
OID	Object Identifier	Mã định danh đối tượng
PAdES	PDF Advanced Electronic Signatures	Chữ ký điện tử nâng cao cho PDF
PNG	Portable Network Graphics	Định dạng ảnh PNG
QES	Qualified Electronic Signature	Chữ ký điện tử đủ điều kiện
QSCD	Qualified electronic Signature Creation Device	Thiết bị tạo chữ ký điện tử đủ điều kiện
RA	Registration Authority	Tổ chức/Đại lý đăng ký
RFC	Request for Comments	Tài liệu yêu cầu nhận xét
RSA	Rivest, Shamir, & Adleman	Thuật toán mã hóa bất đối xứng RSA
SAD	Signature Activation Data	Dữ liệu kích hoạt chữ ký số
SAM	Signature Activation Module	Mô-đun kích hoạt chữ ký số
SAML	Security Assertion Markup Language	Ngôn ngữ đánh dấu xác nhận bảo mật
SCA	Signature Creation Application	Ứng dụng tạo chữ ký số

SCAL	Sole Control Assurance Level	Mức bảo đảm kiểm soát duy nhất
SCAL1	Sole Control Assurance Level 1	Mức bảo đảm kiểm soát duy nhất cấp 1
SCAL2	Sole Control Assurance Level 2	Mức bảo đảm kiểm soát duy nhất cấp 2
SCASC	Signature Creation Application Service Component	Thành phần dịch vụ ứng dụng tạo chữ ký số
SCDev	Signature Creation Device	Thiết bị tạo chữ ký số
SCS	Signature Creation Service	Dịch vụ tạo chữ ký số
SCSP	Signature Creation Service Provider	Nhà cung cấp dịch vụ tạo chữ ký số
SD	Signer's Document	Tài liệu của chủ thể ký
SDO	Signed Data Object	Đối tượng dữ liệu đã ký
SDOC	Signed Data Object Composer	Thành phần cấu thành đối tượng dữ liệu đã ký
SDR	Signer's Document Representation	Thể hiện tài liệu của chủ thể ký
SHA	Secure Hash Algorithm	Thuật toán băm an toàn
SSA	Server Signing Application	Ứng dụng ký số trên máy chủ
SSASC	Server Signing Application Service Component	Thành phần dịch vụ ứng dụng ký số trên máy chủ
TSP	Trust Service Provider	Tổ chức cung cấp dịch vụ tin cậy
URI	Uniform Resource Identifier	Định danh tài nguyên thống nhất
URL	Uniform Resource Locator	Bộ định vị tài nguyên thống nhất
URN	Uniform Resource Name	Tên tài nguyên thống nhất
UTF-8	Unicode Transformation Format - 8-bit	Định dạng chuyển đổi Unicode 8 bit
XAdES	XML Advanced Electronic Signatures	Chữ ký điện tử nâng cao dựa trên XML
XML	Extensible Markup Language	Ngôn ngữ đánh dấu mở rộng
XMLDSIG	XML Digital Signature	Chữ ký số XML
XSD	XML Schema Definition	Định nghĩa cấu trúc tài liệu XML

4 Quy trình tạo chữ ký số, sự phân tách dịch vụ

4.1 Các bước trong quy trình tạo chữ ký số và các phần tử dữ liệu liên quan

Hình 1 thể hiện các bước khác nhau và các phần tử dữ liệu liên quan đối với một quy trình tạo chữ ký số. Đối với việc tạo chữ ký số từ xa, các bước khác nhau của quy trình này được thực hiện dựa trên sự phân tách thành nhiều thành phần, các thành phần này phải truy cập hoặc cung cấp các phần tử dữ liệu tương ứng. Quy trình được minh họa trong hình dưới đây giới hạn ở các khối chức năng và thông tin cần thiết để tạo một chữ ký số mà không xem xét đến các vấn đề như xác thực chủ thể ký, cấp quyền sử dụng khóa ký hoặc tính sẵn sàng của chứng thư chữ ký số. Mô-đun kích hoạt chữ ký số (SAM) trong vùng bảo vệ chống can thiệp vật lý chỉ cần thiết khi Dịch vụ tạo chữ ký số (SCS) tuân thủ cơ chế kích hoạt chữ ký số thuộc Mức bảo đảm kiểm soát duy nhất cấp 2 (SCAL2).



Hình 1: Các bước và thành phần dữ liệu của quy trình tạo chữ ký số

4.2 Các thành phần chính và giao diện của dịch vụ

Quá trình trên chỉ ra các kịch bản trong đó chữ ký điện tử nâng cao (AdES) và/hoặc Giá trị chữ ký số (DSV) được tạo ra bằng cách sử dụng khóa ký lưu trữ trong một mô-đun bảo mật mật mã có tên gọi là Thiết bị tạo chữ ký số (SCDev), do Nhà cung cấp dịch vụ tạo chữ ký số (SCSP) vận hành.

Dựa trên các loại dữ liệu khác nhau được quản lý trong các yêu cầu và phản hồi, hai thành phần chính có thể được xác định trong sơ đồ trên nhằm cung cấp các giao diện khác nhau cho việc quản lý ký số: Thành phần dịch vụ ứng dụng ký số trên máy chủ (SSASC) và Thành phần dịch vụ ứng dụng tạo chữ ký số (SCASC) được định nghĩa dưới đây.

SSASC là thành phần hỗ trợ tạo các giá trị chữ ký số. SSASC có khả năng tương tác với SCDev lưu trữ khóa bí mật của chủ thể ký. Khi SSASC sử dụng SCDev, chủ thể ký được ủy quyền có khả năng kiểm soát khóa ký với một mức độ tin cậy nhất định.

Giao diện SSASC có đầu vào chính là Thể hiện của dữ liệu cần ký (DTBSR) cùng các tham số khác, và đầu ra chính là giá trị chữ ký số.

SCASC là thành phần hỗ trợ tạo chữ ký số AdES và thực hiện một số phần cụ thể của quy trình tạo chữ ký số. SCASC có khả năng tương tác với SSASC để yêu cầu tạo các giá trị chữ ký số. Giao diện SCASC có đầu vào chính là tài liệu cần ký (SD) hoặc thể hiện của tài liệu cần ký (SDR) cùng các tham số khác, và đầu ra chính là tài liệu đã ký hoặc chữ ký số.

SCS biểu thị một dịch vụ của Tổ chức cung cấp dịch vụ tin cậy (TSP) triển khai Ứng dụng tạo chữ ký số (SCA) và/hoặc Ứng dụng ký số trên máy chủ (SSA).

Một số biến thể của các giao diện này có thể xảy ra tùy thuộc vào việc phân chia chức năng giữa SCS và hệ thống nội bộ của chủ thể ký.

Các khoảng mục sau đây quy định chi tiết về các đối tượng thông tin và quy trình chính trong SCASC và SSASC.

4.3 Ứng dụng tạo chữ ký số

4.3.1 Tài liệu của chủ thể ký và quá trình băm

Quy trình tạo chữ ký số bắt đầu với tài liệu của chủ thể ký (SD) cần được ký. Tài liệu của chủ thể ký (SD) được thể hiện (SDR) bằng một giá trị băm trong Dữ liệu cần ký (DTBS). Các nhận xét sau đây được đưa ra:

- Việc tạo thể hiện tài liệu của chủ thể ký (SDR) (quá trình băm) có thể được thực hiện tại nơi lưu trữ tài liệu của chủ thể ký (SD) hoặc do Thành phần dịch vụ ứng dụng tạo chữ ký số (SCASC) thực hiện. Trong trường hợp đầu tiên, thể hiện tài liệu của chủ thể ký (SDR) được chuyển đến SCASC; trong khi ở trường hợp sau, tài liệu của chủ thể ký (SD) được chuyển đến SCASC.
- Tài liệu của chủ thể ký (SD) là một phần của Đối tượng dữ liệu đã ký (SDO) cuối cùng. Một phần chức năng của Thành phần cấu thành đối tượng dữ liệu đã ký (SDOC) (xây dựng định dạng AdES cuối cùng) là liên kết giá trị chữ ký số với tài liệu của chủ thể ký (SD).

Một quyết định thiết kế quan trọng đối với các dịch vụ tạo chữ ký số từ xa là nơi tài liệu của chủ thể ký (SD), và do đó là nội dung của tài liệu này, cần phải có sẵn. Việc chỉ cung cấp thể hiện tài liệu của chủ thể ký (SDR) giúp hạn chế các mối đe dọa đối với tính bảo mật, nhưng có thể dẫn đến những hạn chế về mặt chức năng của giải pháp tạo chữ ký số từ xa (ví dụ: khi cần tạo chữ ký số bao bọc - enveloping hoặc chữ ký bị bao bọc - enveloped, hoặc khi cần bao gồm cả phần thể hiện trực quan của chữ ký số).

4.3.2 Cấu thành và định dạng dữ liệu cần ký (DTBS)

Trong hai quy trình cấu thành và định dạng dữ liệu cần ký (DTBS), mà trong ngữ cảnh của tài liệu này được xem xét cùng nhau, thể hiện tài liệu của chủ thể ký (SDR) (giá trị băm của tài liệu cần ký) và các giá trị băm của tất cả các thuộc tính được ký phải được tập hợp thành Dữ liệu cần ký đã định dạng (DTBSF). Ngoài mã định danh chứng thư chữ ký số (giá trị băm của chứng

thư chữ ký số, có thể bao gồm cả các chứng thư chữ ký số khác trong chuỗi chứng thư chữ ký số) như được chỉ ra trong hình vẽ, các thuộc tính được ký bổ sung được yêu cầu hoặc được phép bởi các định dạng chữ ký số tiêu chuẩn ETSI (C/X/PAdES). Ví dụ, tất cả các biến thể CAdES và XAdES cơ bản (baseline) đều yêu cầu sự hiện diện của các thuộc tính được ký bao gồm "loại tài liệu" (của SD) và "thời gian ký tự khai".

Các thuộc tính được ký hoặc các giá trị băm của chúng, với sự hiện diện là cần thiết trong DTBS, luôn sẵn sàng cho SCASC khi DTBSF được tạo ra bởi SCASC.

4.3.3 Chuẩn bị dữ liệu cần ký (DTBS)

Bước này bao gồm việc tạo ra DTBSR từ DTBSF. SCASC chuẩn bị toàn bộ DTBSF, tính toán giá trị băm, và gửi giá trị băm (DTBSR) làm đầu vào cho một SSASC.

4.3.4 Thành phần cấu thành đối tượng dữ liệu đã ký (SDO)

Là bước cuối cùng, Đối tượng dữ liệu đã ký (SDO) (định dạng AdES) được cấu thành. Quá trình này bao gồm việc kết hợp giá trị chữ ký số với các tham số khác vào định dạng được yêu cầu. Tùy thuộc vào định dạng, chữ ký số được cung cấp cho tài liệu của chủ thể ký (SD) được gọi là:

- **Bị bao bọc (Enveloped):** Chữ ký được thêm vào bên trong tài liệu của chủ thể ký (SD) (ví dụ: chữ ký PAdES).
- **Bao bọc (Enveloping):** Chữ ký bao bọc bên ngoài tài liệu của chủ thể ký (SD) (ví dụ: một số định dạng CAdES nhất định).
- **Tách biệt (Detached):** Chữ ký là một đối tượng riêng biệt được liên kết với tài liệu của chủ thể ký (SD).

Việc cấu thành SDO được thực hiện bởi một thực thể dịch vụ tách biệt hoặc được tích hợp với các chức năng khác trong Thành phần dịch vụ ứng dụng tạo chữ ký số (SCASC).

4.4 Ứng dụng ký số trên máy chủ

4.4.1 Tạo chữ ký số

4.4.1.1 Giới thiệu

Mục đích của quá trình tạo chữ ký số là sử dụng DTBSR để tạo ra giá trị chữ ký số dưới sự kiểm soát của chủ thể ký.

Trong ngữ cảnh của TCVN này, việc tạo giá trị chữ ký số được quản lý bởi một SSASC sử dụng khóa ký được lưu trong mô-đun bảo mật mật mã (SCDev), mà chủ thể ký có thể kích hoạt thông qua quy trình xác thực và kích hoạt an toàn.

4.4.1.2 Kích hoạt chữ ký số

Thành phần dịch vụ ứng dụng ký số trên máy chủ (SSASC) sử dụng một Thiết bị tạo chữ ký số (SCDev) từ xa nhằm tạo, duy trì và sử dụng các khóa ký dưới sự kiểm soát của chủ thể ký được ủy quyền. Chủ thể ký được ủy quyền thực hiện kiểm soát từ xa đối với khóa ký với một mức độ tin cậy nhất định, về cơ bản là thông qua Mô-đun kích hoạt chữ ký số (SAM).

SAM là một thành phần phần mềm sử dụng Dữ liệu kích hoạt chữ ký số (SAD) để xác thực chủ thể ký và nhận sự cấp quyền từ chủ thể ký nhằm kích hoạt khóa ký của họ cho mục đích ký lên Thể hiện của dữ liệu cần ký (DTBSR). Quy trình này bảo đảm mức độ tin cậy rằng các khóa ký nằm dưới sự kiểm soát của chủ thể ký.

Hai mức độ tin cậy khác nhau về quyền kiểm soát khóa ký, được định nghĩa trong tiêu chuẩn CEN EN 419 241-1, được xem xét trong tài liệu này bao gồm:

Mức bảo đảm kiểm soát duy nhất cấp 1 (SCAL1):

- Các khóa ký được sử dụng, với một mức độ tin cậy thấp, dưới sự kiểm soát duy nhất của chủ thể ký.
- Việc sử dụng khóa để ký của chủ thể ký được ủy quyền do SSASC thực thi thông qua quá trình xác thực chủ thể ký. Việc kích hoạt khóa ký có thể được duy trì trong một khoảng thời gian nhất định và/hoặc cho một số lượng chữ ký nhất định.

CHÚ THÍCH: Các triển khai thực tế như vậy không được kỳ vọng sẽ đáp ứng các yêu cầu về quyền kiểm soát duy nhất giống như yêu cầu đối với một thiết bị tạo chữ ký điện tử đủ điều kiện độc lập (QSCD) được định nghĩa trong Quy chế eIDAS

Mức bảo đảm kiểm soát duy nhất cấp 2 (SCAL2):

- Các khóa ký được sử dụng, với một mức độ tin cậy cao, dưới sự kiểm soát duy nhất của chủ thể ký.
- Việc sử dụng khóa để ký của chủ thể ký được ủy quyền do mô-đun kích hoạt chữ ký số thực thi thông qua dữ liệu kích hoạt chữ ký số do chủ thể ký cung cấp, sử dụng một giao thức kích hoạt chữ ký số, nhằm cho phép sử dụng khóa ký tương ứng để ký các tài liệu cụ thể.

4.4.1.3 Tạo chữ ký số bằng thiết bị tạo chữ ký số (SCDev)

Quá trình tạo chữ ký số được thực hiện bởi SCDev. Trong bối cảnh của TCVN này, chỉ những kiến trúc mà quá trình tạo chữ ký số được thực hiện bởi một SCDev từ xa mới được xem xét. Theo các mức bảo đảm kiểm soát duy nhất nêu trên, khóa ký có thể được sử dụng để tạo giá trị chữ ký số sau khi xác thực chủ thể ký thành công bởi SSASC (SCAL1) hoặc sau khi xác minh SAD thành công bởi SAM.

5 Kiến trúc cho việc ký số trên máy chủ

5.1 Tổng quan

Khoản mục này mô tả kiến trúc của các hệ thống hỗ trợ ký số trên máy chủ từ xa, chỉ ra các tương tác cơ bản của SCASC và SSASC với các bên khác tham gia vào quy trình ký số từ xa, đồng thời xem xét đến mức độ tin cậy về quyền kiểm soát các khóa ký.

Một sơ đồ điển hình biểu diễn các hệ thống hỗ trợ ký số trên máy chủ từ xa (cung cấp QES và/hoặc AdES) bao gồm một SCASC được kết nối với một SSASC lưu trữ SCDev từ xa. Các dịch vụ như CA/RA, OCSP và CRL, cấp dấu thời gian, cùng các máy chủ xác thực và/hoặc cấp quyền được coi là bên ngoài sơ đồ này.

Hai kịch bản chính được xem xét bao gồm:

- Ứng dụng khách ký số gửi các yêu cầu tạo một hoặc nhiều chữ ký số AdES đến nhà cung cấp dịch vụ tạo chữ ký số;
- Ứng dụng khách ký số gửi các yêu cầu tạo một hoặc nhiều giá trị chữ ký số đến nhà cung cấp dịch vụ tạo chữ ký số, sau đó hoàn thiện cấu trúc chữ ký số AdES.

Các giao thức được định nghĩa cho phép cả SCASC và SSASC thực hiện ký số hàng loạt đối với các tài liệu, các giá trị băm của tài liệu và các DTBSR. Trong các quy trình ký số hàng loạt tài liệu như vậy, chủ thể ký không cần phải chấp thuận một cách tường minh cho từng chữ ký trên tài liệu.

5.2 Giới thiệu về các kiến trúc

Hai kiến trúc khác nhau được trình bày trong các khoản mục tiếp theo, trong đó SCASC và SSASC triển khai các cơ chế xác thực và cấp quyền khác nhau tùy theo mức độ tin cậy về quyền kiểm soát các khóa ký, có xem xét đến việc TSP quản lý SCASC và/hoặc SSASC có thể ủy quyền quy trình xác thực và cấp quyền cho một bên thứ ba bên ngoài (ví dụ: cho một nhà cung cấp danh tính và/hoặc nhà cung cấp dịch vụ xác thực).

Các kiến trúc này bao gồm hai môi trường chính: môi trường của chủ thể ký và môi trường được bảo vệ của TSP.

CHÚ THÍCH: Trong trường hợp SCS tuân thủ SCAL2, môi trường được bảo vệ của TSP bao gồm một thiết bị bảo vệ chống can thiệp vật lý (ví dụ: mô-đun mật mã tuân thủ tiêu chuẩn CEN EN 419 221-5).

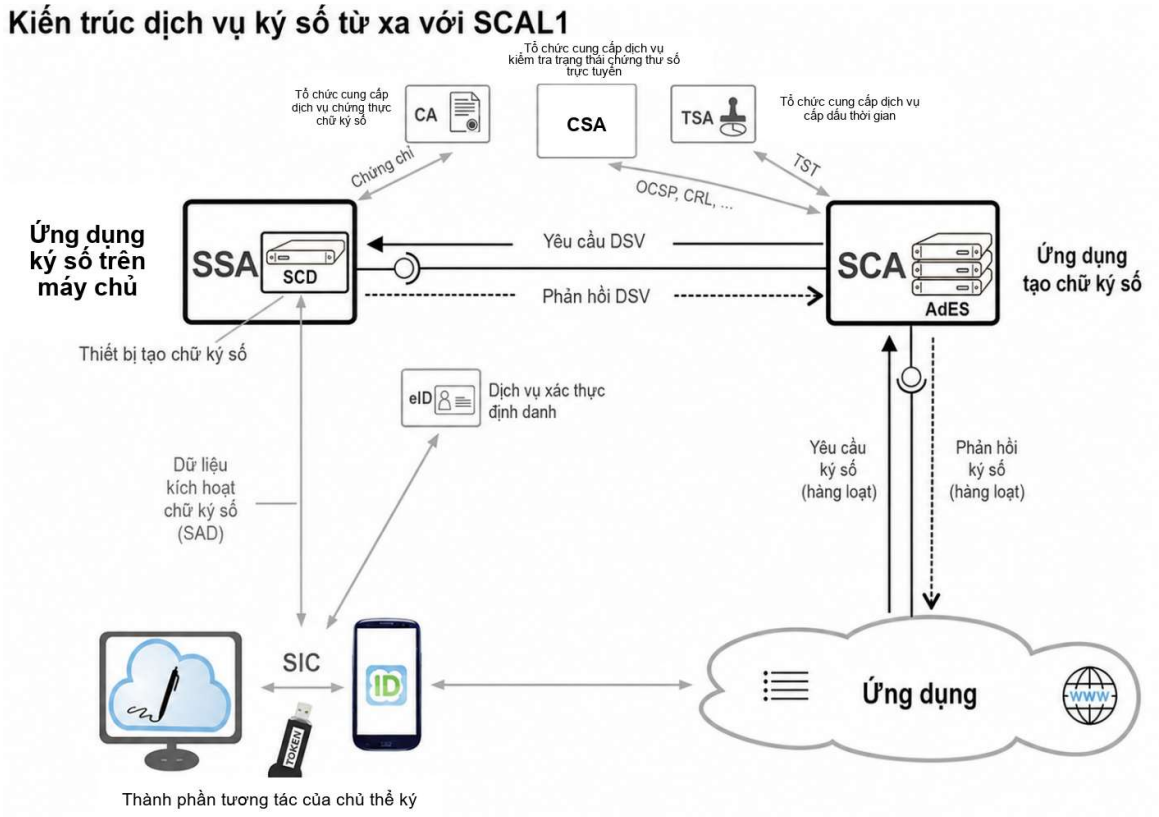
Môi trường của chủ thể ký mang tính chất nội bộ đối với chủ thể ký và việc bảo vệ môi trường này thuộc trách nhiệm của chủ thể ký. Môi trường được bảo vệ của TSP được vận hành theo chính sách an toàn thông tin do TSP lựa chọn nhằm bảo đảm an toàn cho các hoạt động của SCS, đồng thời có thể lưu trữ dưới dạng được bảo vệ các khóa ký và mối liên kết giữa các khóa ký với chủ thể ký tương ứng.

Trong các mô hình tiếp theo, các đường nét đứt được sử dụng để biểu diễn các luồng dữ liệu không thuộc các giao thức được định nghĩa trong tài liệu này, và chỉ được hiển thị nhằm mục đích làm rõ các tính năng có thể có của các dịch vụ được minh họa.

5.3 Dịch vụ ký số từ xa với SCAL1

Trong mô hình này, tính bí mật và tính toàn vẹn của khóa ký được bảo đảm bởi SCDev có thể được kích hoạt bởi SSASC. Việc kích hoạt như vậy có thể được duy trì trong một khoảng thời gian nhất định và/hoặc cho một số lượng chữ ký nhất định.

Chủ thể ký có thể được xác thực bởi một SCASC hoặc một SSASC tùy thuộc vào việc SCSP có lưu trữ một SCASC và/hoặc một SSASC hay không. Nếu SCSP chỉ lưu trữ SSASC thì SCASC có thể được cung cấp trực tiếp trong môi trường của chủ thể ký hoặc bởi một SCSP khác. SCASC và SSASC có thể ủy quyền quy trình xác thực chủ thể ký cho một bên thứ ba bên ngoài. Khi việc xác thực chủ thể ký thành công, khóa ký tương ứng có thể được sử dụng cho các hoạt động ký số thay mặt cho chủ thể ký trong một khung thời gian nhất định và/hoặc một số lượng hoạt động ký số nhất định, từ đó cho phép quản lý các hoạt động ký số hàng loạt.



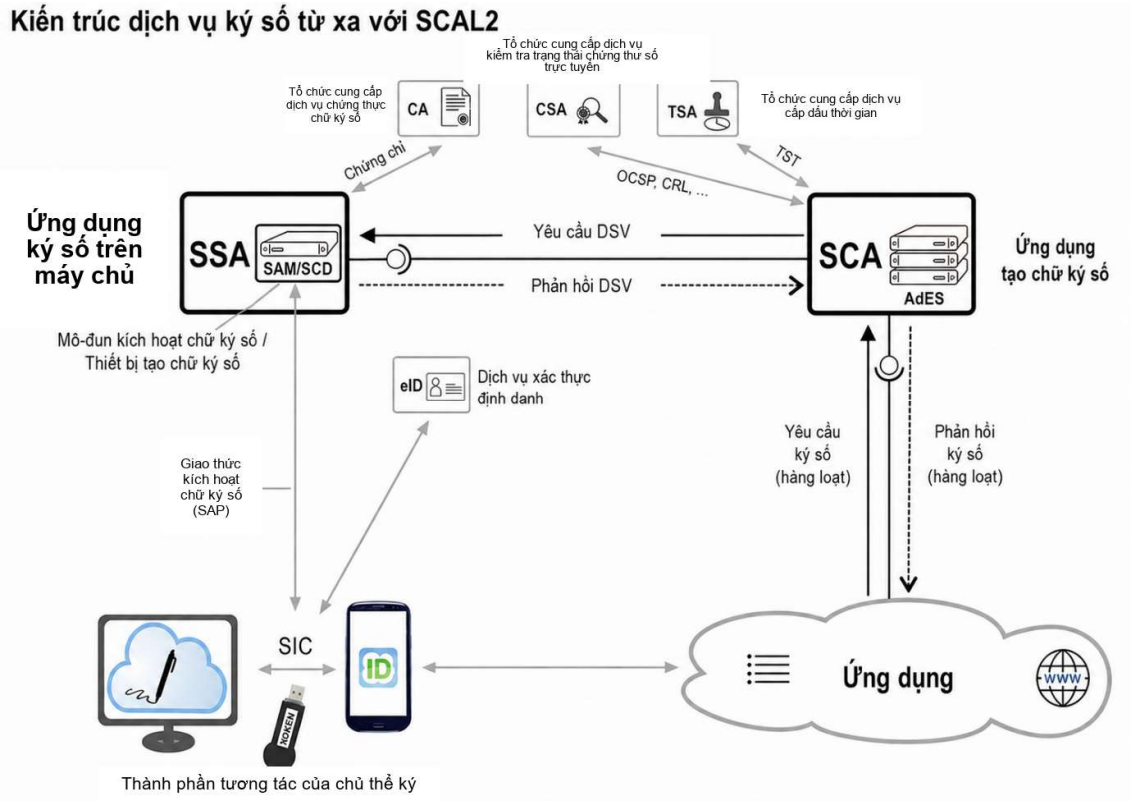
Hình 2: Kiến trúc dịch vụ ký số từ xa với SCAL1

5.4 Dịch vụ ký số từ xa với SCAL2

Trong mô hình này, một môi trường chính thứ ba được định nghĩa ngoài các môi trường được bảo vệ của chủ thể ký và của TSP: môi trường được bảo vệ chống giả mạo. Nó được vận hành

trong môi trường được bảo vệ của TSP, bảo vệ việc sử dụng các khóa ký và thực thi việc kích hoạt chữ ký số phải nằm dưới sự kiểm soát của chủ thể ký với mức độ tin cậy cao hơn so với mô hình trước đó.

Trong mô hình này, tính bảo mật và toàn vẹn của khóa ký được bảo đảm bởi SAM có thể được kích hoạt bởi SSASC. SAM xác minh SAD để có thể ủy quyền hoạt động ký được yêu cầu. SAM có thể ủy quyền xác thực chủ thể ký cho một bên ngoài. Khi quá trình xác thực SAD thành công, khóa ký tương ứng có thể được sử dụng cho các hoạt động ký thay mặt chủ thể ký.



Hình 3: Kiến trúc dịch vụ ký số từ xa với SCAL2

5.5 Bảo mật, tính toàn vẹn và bí mật

Cung cấp các yêu cầu cho các TSP vận hành một SCASC hỗ trợ việc tạo chữ ký số AdES.

Đưa ra các yêu cầu đối với các TSP vận hành một SSASC hỗ trợ việc tạo giá trị chữ ký số.

6 Quy định đặc tả hồ sơ giao thức

6.1 Giới thiệu

TCVN này quy định ngữ nghĩa giao thức để yêu cầu tạo chữ ký số tới một máy chủ từ xa và để nhận phản hồi liên quan.

Đối với ngữ nghĩa đã đề cập ở trên, tiêu chuẩn này quy định hai ràng buộc, mỗi ràng buộc ở một định dạng khác nhau (XML và JSON).

Trong phạm vi có thể và phù hợp, các hồ sơ được quy định trong tài liệu này đã lấy làm điểm khởi đầu một số đặc tả kỹ thuật của Ủy ban Kỹ thuật OASIS DSS-X, cụ thể là OASIS DSS-v2.0, các hồ sơ OASIS AdES cho DSS-v2.0 và tiêu chuẩn CSC.

Phần còn lại của tài liệu này được tổ chức như sau:

- Mục 6.2 và 6.3 đưa ra nhận xét chung về các giao thức XML và JSON.
- Mục 7 quy định rõ các thành phần của các giao thức để tạo chữ ký số từ xa (XML và JSON) được sử dụng bởi SSASC và SCASC.
- Mục 8 quy định các thông điệp mà các ứng dụng khách và SCS có thể trao đổi bằng cách sử dụng các thành phần được định nghĩa trong mục 7.

Đối với mỗi thành phần của các giao thức được đề cập ở trên, tài liệu này:

- Xác định các yêu cầu về ngữ nghĩa của thành phần (tức là các nội dung bắt buộc, các nội dung tùy chọn của nó, v.v.). Các yêu cầu này được định nghĩa trong các mục "Ngữ nghĩa của thành phần".
- Xác định các yêu cầu đối với thành phần XML. Các yêu cầu này được xác định trong các mục có tên "thành phần liên quan đến XML".
- Xác định các yêu cầu đối với JSON. Các yêu cầu này được xác định trong các mục có tên là "thành phần liên quan đến JSON".

6.2 Giao thức liên quan đến XML theo chuẩn OASIS DSS-X

Các cấu trúc được mô tả trong tài liệu này được chứa trong các tệp lược đồ [DSS_Core_XSD], [XMLDSIG_XSD] và bốn tệp lược đồ xml được xác định đồng nhất bằng [XSDSIGCREATIONPROT] trong suốt tài liệu này và vị trí của chúng được định nghĩa trong phụ lục A. Các phần tử và kiểu mới được định nghĩa trong lược đồ đó được định nghĩa trong không gian tên XML có giá trị URI là: http://uri.etsi.org/19432/v1.1.1#.

Bảng 1 trình bày các giá trị URI của các không gian tên XML khác và các tiền tố tương ứng của chúng được sử dụng trong các tệp lược đồ đã đề cập ở trên và trong tiêu chuẩn này.

Bảng 1

Giá trị URI của Không gian tên XML	Tiền tố
http://uri.etsi.org/19432/v1.1.1#	etsisig
http://www.w3.org/2000/09/xmldsighttp://www.w3.org/2000/09/xmldsig#	ds
http://docs.oasis-open.org/dss-x/ns/basehttp://docs.oasis-open.org/dss-x/ns/base	dsb
http://docs.oasis-open.org/dss-x/ns/corehttp://docs.oasis-open.org/dss-x/ns/core	dss2

Tài liệu này đề cập đến các thành phần trong các tệp lược đồ đã nêu trên và mô tả chi tiết hơn một số trong số đó.

Trong trường hợp không có bất kỳ yêu cầu bổ sung nào được định nghĩa trong tài liệu này, các yêu cầu được định nghĩa trong các tệp lược đồ được đề cập ở trên đối với từng yếu tố có trong tài liệu này phải được áp dụng.

Ngoài ra, tiêu chuẩn này quy định các phần tử không được quy định trong các tệp lược đồ đã đề cập ở trên. Đối với các phần tử này, tiêu chuẩn này cũng định nghĩa mô hình xử lý cho máy chủ. Mô hình xử lý này được quy định bên dưới chỉ dẫn Mô hình xử lý trong mỗi mục quy định một trong các phần tử này.

6.3 Giao thức liên quan đến JSON theo chuẩn CSC

Các cấu trúc được mô tả trong tài liệu này được chứa trong các tệp lược đồ [ETSI_SIG_CORE_JSCHEMA].

Ngoài ra, tiêu chuẩn này quy định các phần tử không được quy định trong tiêu chuẩn CSC. Đối với các phần tử này, tiêu chuẩn này cũng định nghĩa mô hình xử lý cho máy chủ. Mô hình xử lý này được quy định bên dưới chỉ dẫn Mô hình xử lý trong mỗi mục quy định một trong các phần tử này.1

7 Định nghĩa các thành phần giao thức

7.1 Giới thiệu

Mục 7 định nghĩa các thành phần giao thức để tạo chữ ký số từ xa. Các thành phần này đại diện cho dữ liệu có thể được truyền đến hoặc trả về bởi SCS để yêu cầu và thực thi các chức năng của SCS. Mục 8 định nghĩa các hồ sơ được SCS triển khai, sử dụng các thành phần được định nghĩa trong mục này.

7.2 Thành phần lựa chọn chế độ hoạt động đồng bộ/không đồng bộ

7.2.1 Ngữ nghĩa của thành phần

Thuật ngữ chế độ hoạt động đồng bộ có nghĩa là ứng dụng khách, sau khi gửi bất kỳ yêu cầu nào đến SCS, phải đợi cho đến khi yêu cầu đó hoàn tất trước khi chuyển sang một tác vụ khác. Trong chế độ hoạt động này, SCS phải thực hiện thao tác được yêu cầu và trả về (các) kết quả tương ứng cho ứng dụng khách. Thuật ngữ chế độ hoạt động không đồng bộ có nghĩa là ứng dụng khách, sau khi gửi bất kỳ yêu cầu nào đến SCS, có thể chuyển sang một tác vụ khác trước khi thao tác được yêu cầu hoàn tất. Trong chế độ hoạt động này, SCS phải chấp nhận yêu cầu và trả về một thông báo cho ứng dụng khách biết về việc chấp nhận yêu cầu của nó. Ứng dụng khách phải có thể yêu cầu (các) kết quả tương ứng từ SCS sau này.

Thành phần này phải được một ứng dụng khách sử dụng để yêu cầu chế độ hoạt động đồng bộ hoặc không đồng bộ từ SCS.

CHÚ THÍCH 1: Khi thành phần này không được ứng dụng khách chỉ định, SCS có thể thực hiện một trong các hành vi sau để xử lý yêu cầu, tùy theo chính sách dịch vụ được lựa chọn:

- Chỉ xử lý yêu cầu theo chế độ đồng bộ;
- Chỉ xử lý yêu cầu theo chế độ không đồng bộ;
- Xử lý yêu cầu theo chế độ đồng bộ và trong một số điều kiện nhất định có thể quyết định chuyển sang xử lý theo chế độ không đồng bộ.

CHÚ THÍCH 2: Khi việc xử lý không đồng bộ được SCS khởi tạo, SCS phải trả về phản hồi bao gồm:

- Mã kết quả thông báo cho ứng dụng khách về việc yêu cầu đang được xử lý theo chế độ không đồng bộ (xem mục 7.24); và
- Một mã định danh phản hồi duy nhất để ứng dụng khách sử dụng nhằm lấy kết quả xử lý của yêu cầu từ SCS (xem mục 7.26).

Chi tiết về chế độ xử lý không đồng bộ được mô tả tại mục 8.4.

7.2.2 Thành phần liên quan đến JSON

Thành phần để yêu cầu lựa chọn chế độ hoạt động phải được thể hiện bằng những mục sau:

- Tham số operationMode kiểu chuỗi.

Được chỉ định theo bảng 2.

Bảng 2

Tham số	Loại	Mô tả
operationMode	Chuỗi	Loại chế độ hoạt động được yêu cầu gửi đến SCS. Nó phải nhận một trong các giá trị sau: "A": chế độ hoạt động không đồng bộ được yêu cầu. "S": chế độ hoạt động đồng bộ được yêu cầu.

7.2.3 Thành phần liên quan đến XML

Phần tử để chọn chế độ hoạt động không đồng bộ/đồng bộ phải là etsisig:OperationMode, phần tử con của phần tử dss2:OptionalInputs.
Phần tử OperationMode được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết trong mục A.2, và được sao chép dưới đây để tham khảo:

```
<xs:element name="OperationMode" type="etsisig:OperationModeType" />
<xs:simpleType name="OperationModeType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Synchronous" />
    <xs:enumeration value="Asynchronous" />
  </xs:restriction>
</xs:simpleType>
```

7.2.4 Mô hình xử lý

Khi thành phần này không được ứng dụng khách cung cấp, SCS phải thực hiện một trong các hành vi sau để thực hiện thao tác được yêu cầu, theo chính sách dịch vụ đã chọn:

- Xử lý yêu cầu chỉ ở chế độ đồng bộ; hoặc
- Xử lý yêu cầu chỉ ở chế độ không đồng bộ; hoặc
- Xử lý yêu cầu ở chế độ đồng bộ và quyết định trong những điều kiện cụ thể để xử lý yêu cầu ở chế độ không đồng bộ.

Khi SCS áp dụng quá trình xử lý đồng bộ, nó phải trả về:

- Phản hồi được định nghĩa trong mục 8.2.2 trong trường hợp các yêu cầu tạo chữ ký số AdES;
- Phản hồi được định nghĩa trong mục 8.3.2 trong trường hợp các yêu cầu tạo DSV.

Khi quá trình xử lý không đồng bộ được SCS áp dụng, nó phải trả về một phản hồi ban đầu bao gồm:

- Mã kết quả thông báo cho ứng dụng khách về việc xử lý hoạt động được yêu cầu ở chế độ không đồng bộ (xem mục 7.24); và
- Một mã định danh phản hồi duy nhất mà ứng dụng khách phải sử dụng để lấy kết quả của hoạt động được yêu cầu từ SCS (xem mục 7.26).

Chế độ xử lý không đồng bộ được định nghĩa tại mục 8.4.

7.3 Thành phần định danh yêu cầu

7.3.1 Ngữ nghĩa của thành phần

Thành phần này chứa một giá trị chuỗi do ứng dụng khách cung cấp, được sử dụng để đối chiếu yêu cầu với phản hồi tương ứng sau đó hoặc để thăm dò kết quả của một hoặc nhiều yêu cầu không đồng bộ.

7.3.2 Thành phần liên quan đến JSON

Thành phần định danh yêu cầu phải được thể hiện bằng những mục sau:

- requestID tham số kiểu chuỗi.

Được chỉ định theo bảng 3.

Bảng 3

Tham số	Loại	Mô tả
requestID	Chuỗi	Dữ liệu từ ứng dụng khách thường được sử dụng để xử lý một mã định danh giao dịch chữ ký.

7.3.3 Thành phần liên quan đến XML

Phần tử để tương quan các yêu cầu với các phản hồi tiếp theo phải là thuộc tính RequestID của phần tử gốc dss2:SignRequest và thuộc tính RequestId của phần tử gốc dss2:SignResponse được định nghĩa trong OASIS DSS-v2.0, mục 4.4.1.2.,

7.4 Thành phần ủy quyền thông tin xác thực

7.4.1 Ngữ nghĩa của thành phần

Thành phần này phải chứa thông tin cần thiết để cho phép sử dụng khóa ký.

Khi Mức bảo đảm kiểm soát duy nhất cấp 1 (SCAL1) được triển khai, thành phần này chứa dữ liệu được sử dụng để kiểm soát, với mức độ tin cậy thấp, rằng một thao tác ký nhất định được thực hiện thay mặt chủ thể ký dưới sự kiểm soát duy nhất của chủ thể ký.

Khi Mức bảo đảm kiểm soát duy nhất cấp 2 (SCAL2) được triển khai, thành phần này chứa dữ liệu được sử dụng để kiểm soát, với mức độ tin cậy cao, rằng một thao tác ký nhất định được thực hiện thay mặt chủ thể ký dưới sự kiểm soát duy nhất của chủ thể ký.

7.4.2 Thành phần liên quan đến JSON

Thành phần để gửi ủy quyền thông tin xác thực phải được thể hiện bằng những mục sau:

- SAD: tham số kiểu chuỗi.

Được chỉ định theo bảng 4.

Bảng 4

Tham số	Loại	Mô tả
SAD	Chuỗi	Dữ liệu xác thực dùng để ủy quyền việc sử dụng khóa ký.

Phần tử "SAD" được định nghĩa trong mục 11.6 của tiêu chuẩn CSC.

7.4.3 Thành phần liên quan đến XML

Phần tử để ủy quyền thông tin xác thực phải là etsisig:SignatureActivationData, phần tử con của phần tử dss2:OptionalInputs. Nếu giá trị được gửi không phải là kiểu chuỗi, nó phải được mã hóa thành một giá trị chuỗi sử dụng mã hóa Base64.

Phần tử SignatureActivationData được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết trong mục A.2, và được sao chép dưới đây để tham khảo:

```
<xs:element name="SignatureActivationData" type="etsisig:SignatureActivationDataType" />
<xs:complexType name="SignatureActivationDataType">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="type" type="xs:string" use="optional" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
```

7.5 Thành phần để định nghĩa dữ liệu tùy chọn được trả về

7.5.1 Ngữ nghĩa của thành phần

Thành phần này định nghĩa một tập hợp các đầu ra bổ sung liên quan đến việc xử lý yêu cầu truy xuất thông tin chữ ký hoặc chứng thư chữ ký số và phải được ứng dụng khách sử dụng để

định nghĩa dữ liệu tùy chọn được trả về từ SCS. Phần tử này phải chứa một danh sách các tên phần tử của dữ liệu tùy chọn được yêu cầu.

Dưới đây là danh sách các thành phần con cấu thành nên thành phần này:

- Phần tử tùy chọn returnSigningCertificateInfo, nếu có, phải chứa một giá trị Boolean. Giá trị mặc định là 'false'. Phần tử này có thể được ứng dụng khách sử dụng để lấy thông tin liên quan đến chứng thư chữ ký số, chuỗi chứng thư và khóa ký được SCS sử dụng để tạo chữ ký số hoặc được xác định trong yêu cầu truy xuất thông tin xác thực chữ ký.
- Thành phần được định nghĩa trong mục 7.10 phải được sử dụng để chỉ định cho SCS thông tin nào liên quan đến chứng thư chữ ký số/chuỗi/khóa ký phải được trả về.
- Phần tử tùy chọn returnSupportMultiSignatureInfo, nếu có, phải chứa một giá trị Boolean. Giá trị mặc định của nó là 'false'. Phần tử này có thể được ứng dụng khách sử dụng để lấy thông tin liệu khóa ký có hỗ trợ việc tạo nhiều chữ ký với một yêu cầu ủy quyền duy nhất hay không.
- Phần tử returnServicePolicyInfo tùy chọn, nếu có, phải chứa một giá trị Boolean. Giá trị mặc định của nó là 'false'. Phần tử này có thể được ứng dụng khách sử dụng để lấy tên của chính sách dịch vụ được máy chủ sử dụng để thực hiện thao tác được yêu cầu.
- Phần tử tùy chọn returnSignatureCreationPolicyInfo, nếu có, phải chứa một giá trị Boolean. Giá trị mặc định của nó là 'false'. Phần tử này có thể được ứng dụng khách sử dụng để lấy tên của chính sách tạo chữ ký số được máy chủ sử dụng để thực hiện thao tác tạo chữ ký số được yêu cầu.
- Phần tử tùy chọn returnCredentialAuthorizationModeInfo, nếu có, phải chứa một giá trị Boolean. Giá trị mặc định là 'false'. Phần tử này có thể được ứng dụng khách sử dụng để lấy chế độ ủy quyền được yêu cầu bởi thông tin xác thực chữ ký được xác định trong yêu cầu truy xuất thông tin xác thực chữ ký.
- Phần tử tùy chọn returnSoleControlAssuranceLevelInfo, nếu có, phải chứa một giá trị Boolean. Giá trị mặc định là 'false'. Phần tử này có thể được ứng dụng khách sử dụng để lấy mức bảo đảm kiểm soát duy nhất được yêu cầu bởi thông tin xác thực chữ ký được xác định trong yêu cầu truy xuất thông tin xác thực chữ ký.

7.5.2 Thành phần liên quan đến JSON

Thành phần để chỉ định dữ liệu tùy chọn được trả về từ SCS phải được biểu thị bằng các tham số sau:

- returnSigningCertificateInfo
- returnSupportMultiSignatureInfo
- returnServicePolicyInfo
- returnSignatureCreationPolicyInfo

- returnCredentialAuthorizationModeInfo
- returnSoleControlAssuranceLevelInfo

Được quy định theo bảng 5.

Bảng 5

Tham số	Sự hiện diện	Loại
returnSigningCertificateInfo	Tùy chọn	Boolean
returnSupportMultiSignatureInfo	Tùy chọn	Boolean
returnServicePolicyInfo	Tùy chọn	Boolean
returnSignatureCreationPolicyInfo	Tùy chọn	Boolean
returnCredentialAuthorizationModeInfo	Tùy chọn	Boolean
returnSoleControlAssuranceLevelInfo	Tùy chọn	Boolean

Các phần tử "ReturnSigningCertificateInfo", "ReturnSupportMultiSignatureInfo", "ReturnServicePolicyInfo", "ReturnSignatureCreationPolicyInfo", "ReturnCredentialAuthorizationModeInfo" và "ReturnSoleControlAssuranceLevelInfo" không được định nghĩa trong tiêu chuẩn CSC.

7.5.3 Thành phần liên quan đến XML

Phần tử để yêu cầu dữ liệu tùy chọn được trả về phải là phần tử tùy chọn etsisig:ReturnOptionalData, được chứa trong phần tử dss2:OptionalInputs.

Phần tử ReturnOptionalData được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết trong mục A.2, và được sao chép bên dưới để tham khảo:

```
<xs:element name="ReturnOptionalData" type="etsisig:ReturnOptionalDataType"/>
<xs:complexType name="ReturnOptionalDataType">
    <xs:sequence>
        <xs:element ref="etsisig:SigningCertificateInfo" minOccurs="0"/>
        <xs:element ref="etsisig:SupportMultiSignatureInfo" minOccurs="0"/>
        <xs:element ref="etsisig:ServicePolicyInfo" minOccurs="0"/>
        <xs:element ref="etsisig:SignatureCreationPolicyInfo" minOccurs="0"/>
        <xs:element ref="etsisig:CredentialAuthorizationModeInfo" minOccurs="0"/>
        <xs:element ref="etsisig:SoleControlAssuranceLevelInfo" minOccurs="0"/>
</xs:sequence>
</xs:complexTy
            pe>
<xs:element name="SigningCertificateInfo" type="xs:Boolean"/>
<xs:element name="SupportMultiSignatureInfo" type="xs:Boolean"/>
<xs:element name="ServicePolicyInfo" type="xs:Boolean"/>
<xs:element name="SignatureCreationPolicyInfo" type="xs:Boolean"/>
<xs:element name="CredentialAuthorizationModeInfo" type="xs:Boolean"/>
<xs:element name="SoleControlAssuranceLevelInfo" type="xs:Boolean"/>
```

7.5.4 Mô hình xử lý

Nếu SCS không nhận diện được hoặc không thể xử lý bất kỳ dữ liệu tùy chọn nào cần trả về, nó phải từ chối yêu cầu và trả về lỗi.

7.6 Thành phần để xác định thời hạn hiệu lực cho các yêu cầu không đồng bộ

7.6.1 Ngữ nghĩa của thành phần

Thành phần này phải được sử dụng để chỉ định một khoảng thời gian tối đa mà SCS phải giữ (các) kết quả yêu cầu có sẵn để ứng dụng khách truy xuất. Thời hạn hiệu lực phải được tính bắt đầu từ thời điểm chấp nhận yêu cầu. SCS không cần trả về bất kỳ kết quả nào sau khi hết thời gian tối đa và có thể hủy bỏ bất kỳ kết quả nào đã được tạo ra.

7.6.2 Thành phần liên quan đến JSON

Thành phần để yêu cầu cài đặt khoảng thời gian tối đa phải được thể hiện như sau:

- validityPeriod tham số kiểu số.

Được quy định theo bảng 6

Bảng 6

Tham số	Loại	Mô tả
validityPeriod	Số nguyên	Khoảng thời gian tối đa tính bằng mili giây.

7.6.3 Thành phần liên quan đến XML

Phần tử để định nghĩa thời gian hiệu lực cho các yêu cầu không đồng bộ phải là etsisig:ValidityPeriod, phần tử con của phần tử dss2:OptionalInputs. Giá trị này chỉ định khoảng thời gian tối đa, bắt đầu từ thời điểm chấp nhận yêu cầu không đồng bộ và được biểu thị bằng mili giây, trong đó việc truy xuất (các) kết quả của yêu cầu không đồng bộ có thể được hoàn tất. Phần tử ValidityPeriod được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết trong mục A.2, và được sao chép dưới đây để tham khảo:

<xs:element name="ValidityPeriod" type="xs:int" />

7.6.4 Mô hình xử lý

Nếu thành phần có mặt, SCS phải thực hiện các thao tác được yêu cầu và giữ cho kết quả tương ứng có sẵn trong khoảng thời gian được chỉ định trong thành phần này. Nếu SCS không hoàn thành các thao tác được yêu cầu hoặc ứng dụng khách không yêu cầu (các) kết quả có sẵn trong khoảng thời gian đã chỉ định, việc xử lý yêu cầu của ứng dụng khách phải không được hoàn thành thành công.

7.7 Thành phần thực hiện xác thực ứng dụng khách

7.7.1 Ngữ nghĩa của thành phần

Thành phần này phải chứa thông tin để xác thực ứng dụng khách để truy cập vào SCASC hoặc SSASC.

CHÚ THÍCH 1: Cách một ứng dụng khách xác thực với SCASC hoặc SSASC nằm ngoài phạm vi của tài liệu này.

CHÚ THÍCH 2: SCSP có thể định nghĩa các cách khác mà một ứng dụng khách có thể xác thực với SCASC hoặc SSASC, ngoài hoặc thay thế cho việc sử dụng thành phần này.

7.7.2 Thành phần liên quan đến JSON

Thành phần ủy quyền phải được đưa vào tiêu đề HTTP Authorization của mọi cuộc gọi.

7.7.3 Thành phần liên quan đến XML

Phần tử dùng để xác thực ứng dụng khách phải là dss2:ClaimedIdentity, phần tử con của phần tử dss2:OptionalInputs, được định nghĩa trong OASIS DSS-v2.0, mục 4.4.9.2. Ngữ nghĩa của thành phần được định nghĩa là danh tính của dịch vụ yêu cầu. Cơ chế xác thực chính xác (tức là việc sử dụng SupportingInfo, v.v.) nằm ngoài phạm vi của tiêu chuẩn này và phải được định nghĩa bởi dịch vụ triển khai.,

7.8 Thành phần để xác định thông tin xác thực chữ ký

7.8.1 Ngữ nghĩa của thành phần

Thành phần này được sử dụng để xác định duy nhất khóa bí mật và chứng thư chữ ký số tương ứng của chủ thể ký phải được dùng để tạo chữ ký số.

7.8.2 Thành phần liên quan đến JSON

Thành phần để yêu cầu lựa chọn chế độ hoạt động phải được biểu thị bằng những mục sau:

- credentialID tham số kiểu Chuỗi.

Được chỉ định theo bảng 7.

Bảng 7

Tham số	Loại	Mô tả
credentialID	Chuỗi	Mã định danh được liên kết với khóa bí mật và chứng thư chữ ký số tương ứng.

Phần tử "credentialID" được định nghĩa trong mục 11.6 của tiêu chuẩn CSC.

7.8.3 Thành phần liên quan đến XML

Phần tử "credentialID" được định nghĩa trong mục 11.6 của tiêu chuẩn CSC.

7.9 Thành phần chọn ngôn ngữ

7.9.1 Ngữ nghĩa của thành phần

Thành phần này phải được sử dụng để yêu cầu một ngôn ngữ ưu tiên cho phản hồi và phải được quy định theo IETF RFC 5646.

Dịch vụ nên cung cấp các phản hồi theo ngôn ngữ cụ thể sử dụng ngôn ngữ được yêu cầu. Trong trường hợp ngôn ngữ được yêu cầu không được hỗ trợ thì phải không có lỗi nào được đưa ra và các phản hồi phải được tạo ra bằng ngôn ngữ mặc định của SCS.

7.9.2 Thành phần liên quan đến JSON

Thành phần để chọn cài đặt ngôn ngữ và khu vực phải được thể hiện bằng những mục sau:

- lang tham số kiểu chuỗi

Được chỉ định theo bảng 8.

Bảng 8

Tham số	Loại	Mô tả
Lang	Chuỗi	ngôn ngữ phản hồi được yêu cầu được quy định như trong IETF RFC 5646

Phần tử "Lang" được định nghĩa trong mục 11.1 của tiêu chuẩn CSC.

7.9.3 Thành phần liên quan đến XML

Phần tử để chọn ngôn ngữ và văn hóa phải là dsb:Language, phần tử con của
phần tử dss2:OptionalInputs, được định nghĩa trong OASIS DSS-v2.0 mục 4.2.8.2.,

7.10 Thành phần để chỉ định nội dung thông tin xác thực chữ ký được trả về

7.10.1 Ngữ nghĩa của thành phần

Thành phần này được sử dụng để chỉ định những nội dung nào của chuỗi chứng thư chữ ký số phải được trả về. Nếu thành phần này không được định nghĩa, SCS phải chỉ trả về chứng thư chữ ký số thực thể cuối.

7.10.2 Thành phần liên quan đến JSON

Thành phần để chỉ định nội dung nào của chuỗi chứng thư chữ ký số phải được SCS trả về phải được thể hiện bằng những mục sau:

- certificates tham số kiểu chuỗi
- authInfo Tham số kiểu Boolean.
- certInfo Tham số kiểu Boolean.

Được chỉ định theo bảng 9.

Bảng 9

Tham số	Sự hiện diện	Loại	Mô tả
certificates	Tùy chọn	Chuỗi	Chỉ định những chứng thư chữ ký số nào từ chuỗi chứng thư chữ ký số phải được trả về trong phản hồi SCS: "none": không có chứng thư chữ ký số nào được trả về. "single": chỉ chứng thư chữ ký số thực thể cuối cùng được trả về. "chain": chuỗi chứng thư chữ ký số đầy đủ được trả về. Giá trị mặc định là "single".
certInfo	Tùy chọn có điều kiện	Boolean	Chỉ định xem liệu thông tin trên chứng thư chữ ký số thực thể cuối có được trả về dưới dạng chuỗi có thể in được hay không. Giá trị mặc định là "false", vì vậy nếu tham số bị bỏ qua thì thông tin phải không được trả về. Phần tử này phải mang một giá trị chỉ khi tham số certificates chứa một giá trị khác "none".
authInfo	Tùy chọn có điều kiện	Boolean	Chỉ định xem liệu thông tin về các cơ chế ủy quyền được hỗ trợ bởi thông tin xác thực này có được trả về hay không. Giá trị mặc định là "false", vì vậy nếu tham số bị bỏ qua thì thông tin phải không được trả về. Phần tử này phải mang một giá trị chỉ khi tham số certificates chứa một giá trị khác với "none".

Các phần tử "certificates", "certInfo" và "authInfo" được định nghĩa trong mục 11.5 của tiêu chuẩn CSC

7.10.3 Thành phần liên quan đến XML

Phần tử để liệt kê chuỗi chứng thư chữ ký số phải là etsisig:ReturnSigningCertificate, phần tử con của phần tử etsisig:OptionalInputs.

Phần tử ReturnSigningCertificate được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết trong mục A.2, và được sao chép bên dưới để tham khảo.

```
<xs:element name="ReturnSigningCertificate" type="etsisig:ReturnSigningCertificateType" />
<xs:complexType name="ReturnSigningCertificateType">
    <xs:attribute name="ReturnCertificates" type="etsisig:ReturnCertificatesType" use="optional" />
    <xs:attribute name="CertificateInfo" type="xs:Boolean" use="optional" />
    <xs:attribute name="AuthorizationInfo" type="xs:Boolean" use="optional" />
</xs:complexType>

<xs:simpleType name="ReturnCertificatesType">
    <xs:restriction base="xs:string">
        <xs:enumeration value="None" />
        <xs:enumeration value="Single" />
        <xs:enumeration value="Chain" />
    </xs:restriction>
</xs:simpleType>
```

7.10.4 Mô hình xử lý

Nếu thành phần có mặt, SCS phải kiểm tra các giá trị được truyền trong các tham số thành phần.

Nếu tham số chỉ định các chứng thư chữ ký số cần được trả về có mặt, SCS phải trả về trong phản hồi của nó không có chứng thư chữ ký số nào, chỉ chứng thư chữ ký số hoặc toàn bộ chuỗi chứng thư chữ ký số nếu giá trị tham số tương ứng là "none", "single" hoặc "chain".

Nếu tham số cho biết liệu thông tin chứng thư chữ ký số có được trả về dưới dạng chuỗi hay không có giá trị "true", thì SCS phải trả về trong phản hồi của mình thông tin chứng thư chữ ký số như đã quy định tại mục 7.22.

Nếu tham số chỉ định liệu thông tin ủy quyền khóa ký và chứng thư chữ ký số có được trả về hay không có giá trị "true", SCS phải trả về trong phản hồi của nó thông tin ủy quyền khóa ký và chứng thư chữ ký số như được quy định trong mục 7.28.

7.11 Thành phần quản lý giao dịch chữ ký số

7.11.1 Ngữ nghĩa của thành phần

Thành phần này có thể được sử dụng để khởi tạo và quản lý một chuỗi các chữ ký với số lượng đã thỏa thuận, được coi là một đơn vị công việc duy nhất (được gọi là giao dịch trong mục này) giữa khách hàng và SCS.

Giao dịch phải được xác định bởi thành phần được định nghĩa trong mục 7.3, thành phần này phải được xử lý để tạo ra một mã định danh giao dịch duy nhất trong SCS.

VÍ DỤ 1: Một giao dịch đang hoạt động trong đó chủ thể ký cần đặt vào một tài liệu một số lượng chữ ký PAdES nhất định ở các phần khác nhau để xác nhận các nội dung khác nhau trong tài liệu. Trong trường hợp như vậy, một DTBS mới được tính toán trước mỗi chữ ký mới. Sử dụng một giao dịch đang hoạt động để hoàn thành tất cả các chữ ký cho phép chủ thể ký kiểm soát tốt hơn toàn bộ quá trình ký.

VÍ DỤ 2: Một chủ thể ký đang yêu cầu ký một số lượng rất lớn tài liệu, trong đó mỗi tài liệu được đưa vào yêu cầu một cách toàn vẹn và mỗi tài liệu khá lớn. Thành phần này có thể được sử dụng để ngăn yêu cầu trở nên quá lớn. Thay vì gửi tất cả tài liệu đến SCASC cùng một lúc, các tài liệu có thể được gửi từng cái một, và chúng sẽ được ký bằng cùng một hành động của chủ thể ký. Khóa phiên sẽ được sử dụng để bảo đảm rằng các tài liệu tiếp theo thuộc cùng một giao dịch.

CHÚ THÍCH: Định nghĩa về giao thức ủy quyền nằm ngoài phạm vi của tài liệu này.

7.11.2 Thành phần liên quan JSON

Thành phần để khởi tạo và quản lý một giao dịch phải được đại diện bởi những mục sau:

- numSignatures tham số kiểu số nguyên.

Được quy định theo bảng 10.

Bảng 10

Tham số	Loại	Mô tả
numSignatures	Số nguyên	Số lượng chữ ký cần thực hiện trong ngữ cảnh của giao dịch. SCS phải kiểm tra giá trị này trong ngữ cảnh của giao dịch.

Phần tử "numSignatures" được định nghĩa trong mục 11.6 của tiêu chuẩn CSC.

7.11.3 Thành phần liên quan đến XML

Phần tử để quản lý giao dịch chữ ký số phải là phần tử etsisig:NumberOfSignatures, phần tử con của dss2:OptionalInputs.

Phần tử etsisig:NumberOfSignatures phải được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết trong mục A.2, và được sao chép bên dưới để tham khảo.

<xs:element name="NumberOfSignatures" type="xs:int"/>

7.11.4 Mô hình xử lý

Nếu thành phần có mặt, SCS phải kiểm tra và lưu trữ giá trị được truyền trong tham số thành phần. Phản hồi của SCS phải bao gồm một định danh duy nhất trong thành phần để định danh phản hồi như được định nghĩa trong mục 7.26. Bất kỳ yêu cầu ký tiếp theo nào có chứa định danh duy nhất này trong thành phần định danh yêu cầu, phải được coi là một phần của giao dịch ký. Phản hồi cho bất kỳ yêu cầu ký nào là một phần của giao dịch phải bao gồm cùng một giá trị trong thành phần để định danh phản hồi. Sau khi SCS đã nhận đủ số lượng yêu cầu ký dự kiến trong giao dịch, bất kỳ yêu cầu tiếp theo nào bao gồm cùng giá trị định danh yêu cầu phải bị SCS từ chối và SCS phải trả về một phản hồi không thành công.

7.12 Thành phần để lựa chọn chính sách dịch vụ

7.12.1 Ngữ nghĩa của thành phần

Thành phần này phải chứa một định danh không mơ hồ của chính sách dịch vụ mà theo đó máy chủ phải thực hiện thao tác được yêu cầu.

7.12.2 Thành phần liên quan đến JSON

Thành phần để chỉ định mã định danh của chính sách dịch vụ theo đó máy chủ phải thực hiện thao tác được yêu cầu phải được biểu thị bằng những mục sau:

- policy tham số kiểu chuỗi

Được chỉ định theo bảng 11.

Bảng 11

Tham số	Loại	Mô tả
policy	Chuỗi	Yếu tố xác định một chính sách dịch vụ cụ thể liên quan đến SCS. Chính sách Phần tử có thể được sử dụng để chọn một chính sách dịch vụ cụ thể nếu một SCS hỗ trợ nhiều chính sách, hoặc như một kiểm tra sơ bộ để bảo đảm SCS triển khai chính sách dịch vụ mà khách hàng mong đợi.

7.12.3 Thành phần liên quan đến XML

Phần tử để chọn chính sách dịch vụ phải là dsb:ServicePolicy, phần tử con của phần tử dss2:OptionalInputs, được định nghĩa trong OASIS DSS-v2.0, mục 4.2.8.2.,

7.13 Thành phần để chọn chính sách tạo chữ ký số

7.13.1 Ngữ nghĩa của thành phần

Thành phần này phải chứa chính sách tạo chữ ký số phải được sử dụng khi ký DTBSR(s) và phải có giá trị là một định danh duy nhất của chính sách tạo chữ ký số dưới dạng URI. Nếu định danh của chính sách tạo chữ ký số là một OID, thì giá trị của phần tử này phải là một URN chỉ ra giá trị của OID đã đề cập ở trên như được quy định trong IETF RFC 3061.

Thay vì việc xác định rõ ràng chính sách tạo chữ ký số, thông tin chỉ định thuật toán chữ ký số phải được sử dụng có thể được cung cấp.

7.13.2 Thành phần liên quan đến JSON

Thành phần để chỉ định định danh chính sách tạo chữ ký số được SCS sử dụng phải được thể hiện như sau:

- signaturePolicyID tham số kiểu chuỗi;
- signAlgo tham số kiểu chuỗi
- signAlgoParams tham số kiểu chuỗi.

Được chỉ định theo bảng 12.

Bảng 12

Tham số	Sự hiện diện	Loại	Mô tả
signaturePolicyID	Bắt buộc có điều kiện	Chuỗi	Thành phần xác định một chính sách tạo chữ ký số cụ thể liên quan đến SCS. Phần tử này phải mang một giá trị nếu tham số signAlgo không được chỉ định.
signAlgo	Bắt buộc có điều kiện	Chuỗi	Phần tử chỉ định OID thuật toán được sử dụng để ký. Phần tử này phải có một giá trị nếu tham số signaturePolicyID không được chỉ định.
signAlgoParams	Tùy chọn có điều kiện	Chuỗi	Phần tử chỉ định mã hóa Base64 của các tham số chữ ký ASN.1 được mã hóa DER. Phần tử này có thể mang một giá trị chỉ khi được yêu cầu và/hoặc cho phép bởi thuật toán chữ ký số, ví dụ như

Tham số	Sự hiện diện	Loại	Mô tả
			Sơ đồ chữ ký mật mã RSA-PSS (IETF RFC 8017 [i.8]).

Phần tử "signaturePolicyID" không được định nghĩa trong tiêu chuẩn CSC. Các phần tử "signAlgo" và "signAlgoParams" được định nghĩa trong mục 11.9 của tiêu chuẩn CSC.

7.13.3 Thành phần liên quan đến XML

Phần tử để chọn thuật toán chữ ký số phải là dss2:SignatureAlgorithm, phần tử con của phần tử dss2:OptionalInputsSign, được định nghĩa trong OASIS DSS-v2.0, mục 4.4.4.2.,

Phần tử để chọn chính sách tạo chữ ký số phải là etsisig:SignaturePolicyId, phần tử con của phần tử dss2:OptionalInputs.

Phần tử cho các tham số thuật toán chữ ký số phải là etsisig:SignatureAlgorithmParameters, phần tử con của phần tử dss2:OptionalInputs.

Phần tử etsisig:SignaturePolicyId phải được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết trong mục A.2, và được sao chép bên dưới để tham khảo.

<xs:element name="SignaturePolicyId" type="xs:anyURI"/>

Phần tử etsisig:SignatureAlgorithmParameters phải được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết trong mục A.2, và được sao chép bên dưới để tham khảo.

<xs:element name="SignatureAlgorithmParameters" type="xs:base64Binary"/>

7.14 Thành phần lựa chọn thuộc tính/đặc tính chữ ký tùy chọn

7.14.1 Ngữ nghĩa của thành phần

Yêu cầu có thể bao gồm thành phần này nếu có các thuộc tính/đặc tính đã ký nhất định mà SCASC được yêu cầu đưa vào chữ ký.

Dưới đây là danh sách tên các thuộc tính/đặc tính có thể được tham chiếu trong thành phần này để yêu cầu đưa vào các thuộc tính/đặc tính đã ký tương ứng trong chữ ký. Thay vì tên các thuộc tính/đặc tính, cũng có thể sử dụng các OID thuộc tính/đặc tính tương ứng:

- Phần tử commitment-type-indication, nếu có, phải chứa mã hóa Base64 của thuộc tính chỉ báo loại cam kết được định nghĩa trong mục 5.2.3 của ETSI EN 319 122-1
- Phần tử content-hints, nếu có, phải chứa mã hóa Base64 của thuộc tính content-hints được định nghĩa trong mục 5.2.4.1 của ETSI EN 319 122-1 .
- Phần tử mime-type, nếu có, phải chứa mã hóa Base64 của thuộc tính mime-type được định nghĩa trong mục 5.4.2.2 của ETSI EN 319 122-1

- Phần tử signer-location, nếu có, phải chứa mã hóa Base64 của thuộc tính signer-location được định nghĩa trong mục 5.2.5 của ETSI EN 319 122-1
- Phần tử signer-attributes-v2, nếu có, phải chứa mã hóa Base64 của thuộc tính signer-attributes-v2 được định nghĩa trong mục 5.2.6.1 của ETSI EN 319 122-1
- Phần tử content-time-stamp, nếu có, phải chứa mã hóa Base64 của thuộc tính content-time-stamp được định nghĩa trong mục 5.2.8 của ETSI EN 319 122-1.
- Phần tử signature-policy-identifier, nếu có, phải chứa mã hóa Base64 của thuộc tính signature-policy-identifier được định nghĩa trong mục 5.2.9 của ETSI EN 319 122-1.
- Phần tử content-reference, nếu có, phải chứa mã hóa Base64 của thuộc tính content-reference được định nghĩa trong mục 5.2.11 của ETSI EN 319 122-1.
- Phần tử content-identifier, nếu có, phải chứa mã hóa Base64 của thuộc tính content-identifier được định nghĩa trong mục 5.2.12 của ETSI EN 319 122-1.
- Phần tử Location, nếu có, phải chứa mã hóa Base64 của thuộc tính Location được định nghĩa trong mục 5.3 của ETSI EN 319 142-1.
- Phần tử Reason, nếu có, phải chứa mã hóa Base64 của thuộc tính Reason được định nghĩa trong mục 5.3 của ETSI EN 319 142-1.
- Phần tử Name, nếu có, phải chứa mã hóa Base64 của thuộc tính Name được định nghĩa trong mục 5.3 của ETSI EN 319 142-1.
- Phần tử ContactInfo, nếu có, phải chứa mã hóa Base64 của thuộc tính ContactInfo được định nghĩa trong mục 5.3 của ETSI EN 319 142-1.
- Phần tử SignerRoleV2, nếu có, phải chứa mã hóa Base64 của thuộc tính SignerRoleV2 được định nghĩa trong mục 5.2.6 của ETSI EN 319 132-1.
- Phần tử CommitmentTypeIndication, nếu có, phải chứa mã hóa Base64 của thuộc tính CommitmentTypeIndication được định nghĩa trong mục 5.2.3 của ETSI EN 319 132-1.
- Phần tử SignatureProductionPlaceV2, nếu có, phải chứa mã hóa Base64 của thuộc tính SignatureProductionPlaceV2 được định nghĩa trong mục 5.2.5 của ETSI EN 319 132-1.
- Phần tử AllDataObjectsTimeStamp, nếu có, phải chứa mã hóa Base64 của thuộc tính AllDataObjectsTimeStamp được định nghĩa trong mục 5.2.8.1 của ETSI EN 319 132-1.
- Phần tử IndividualDataObjectsTimeStamp, nếu có, phải chứa mã hóa Base64 của thuộc tính IndividualDataObjectsTimeStamp được định nghĩa trong mục 5.2.8.2 của ETSI EN 319 132-1.
- Phần tử SignaturePolicyIdentifier, nếu có, phải chứa mã hóa Base64 của thuộc tính SignaturePolicyIdentifier được định nghĩa trong mục 5.2.8.2 của ETSI EN 319 132-1.

7.14.2 Thành phần liên quan đến JSON

Thành phần để lựa chọn các thuộc tính/đặc tính phải được đưa vào chữ ký phải được biểu diễn bằng mảng sau:

• signedProps chứa danh sách các thuộc tính phải được thêm vào các thuộc tính đã ký của chữ ký. Được chỉ định theo bảng 13.

Bảng 13

Tham số	Loại	Mô tả
signedProps	Mảng Đối tượng Thuộc tính	Danh sách các thuộc tính đã ký. Các thuộc tính có thể được bao gồm phụ thuộc vào định dạng chữ ký số và chính sách tạo chữ ký số.

'Đối tượng Thuộc tính' là một Đối tượng JSON bao gồm các thuộc tính sau:

• attribute_name tham số kiểu chuỗi;

• attribute_value tham số kiểu mảng chuỗi.

Được chỉ định theo bảng 14.

Bảng 14

Tham số	Sự hiện diện	Loại	Mô tả
attribute_name	Bắt buộc	Chuỗi	Tên hoặc OID của thuộc tính/đặc tính được đưa vào chữ ký. Tên của các thuộc tính và/hoặc đặc tính được định nghĩa trong mục 7.14.1 phải được sử dụng. Các thuộc tính và/hoặc đặc tính khác có tên được định nghĩa trong bảng ở mục 6.3 của ETSI EN 319 122-1, ETSI EN 319 132-1, ETSI, Các tài liệu EN 319 142-1 có thể được SCS hỗ trợ.
attribute_value	Điều kiện	Chuỗi	Tùy thuộc vào thuộc tính/đặc tính được chỉ định trong tham số attribute_name, tham số này chứa giá trị phải được sử dụng cho thuộc tính/đặc tính đó để đưa vào chữ ký. Khi một số yếu tố của mục này tham số không được định nghĩa SCASC phải tính toán nó, nếu cần.

7.14.3 Thành phần liên quan đến XML

Phần tử cho các thuộc tính/đặc tính chữ ký tùy chọn phải là dss2:Properties, phần tử con của phần tử dss2:OptionalInputs, được định nghĩa trong OASIS DSS-v2.0, mục 4.4.15.2.,

7.14.4 Mô hình xử lý

Ứng dụng khách có thể truyền cho SCASC một giá trị cụ thể để sử dụng cho từng thuộc tính/đặc tính hoặc để SCASC tự xác định giá trị. Nếu không có giá trị nào được truyền và SCASC không thể tính toán được, thuộc tính/đặc tính tương ứng phải không được đưa vào chữ ký. SCASC có thể bao gồm các thuộc tính/đặc tính bổ sung trong chữ ký, ngay cả khi những thuộc tính/đặc tính này không được ứng dụng khách yêu cầu rõ ràng (tức là vì các thuộc tính/đặc tính đó được yêu cầu bởi các hồ sơ chữ ký).

7.15 Thành phần chứa mã định danh giao thức

7.15.1 Ngữ nghĩa của thành phần

Thành phần này có thể được ứng dụng khách sử dụng để cho máy chủ biết giao thức nào đang được sử dụng để giao tiếp với chính máy chủ đó. Giá trị của thành phần này phải là một định danh thông báo rằng yêu cầu đã được xây dựng bằng cách sử dụng các giao thức được định nghĩa bởi tiêu chuẩn này.

Mã định danh cho giao thức được định nghĩa bởi tài liệu này phải là:

- http://uri.etsi.org/19432/v1.1.1#/creationprofile#

Yêu cầu có thể chứa các thành phần bổ sung mà giá trị của chúng là các định danh của các giao thức khác cũng đã được sử dụng để xây dựng yêu cầu.

Thành phần này phải được sử dụng để thông báo cho máy chủ rằng ứng dụng khách mong muốn xử lý yêu cầu theo các giao thức được định nghĩa bởi tiêu chuẩn này.

7.15.2 Thành phần liên quan đến JSON

Thành phần để chỉ ra giao thức được ứng dụng khách sử dụng phải được thể hiện như sau:

- profiletham số kiểu chuỗi

Được chỉ định theo bảng 15.

Bảng 15

Tham số	Loại	Mô tả
profile	Chuỗi	Chuỗi định danh giao thức mà ứng dụng khách đang sử dụng để giao tiếp với SCS.

7.15.3 Thành phần liên quan đến XML

Phần tử được sử dụng để thông báo cho máy chủ về hồ sơ phải là phần tử dsb:Profile của dss2:SignRequest, được định nghĩa trong OASIS DSS-v2.0, mục 4.2.10.2.,

7.16 Thành phần để yêu cầu các định dạng chữ ký số cụ thể

7.16.1 Ngữ nghĩa của thành phần

Thành phần này được sử dụng để yêu cầu một định dạng chữ ký số cụ thể. Định dạng chữ ký số và mức độ tuân thủ phải giống nhau cho mỗi tài liệu phải được ký trong yêu cầu chữ ký đã xác định.

Các mức độ tuân thủ của các tiêu chuẩn "hồ sơ cơ sở", được định nghĩa trong ETSI EN 319 122-1, ETSI

EN 319 132-1, ETSI EN 319 142-1 nên được sử dụng. Các mức độ tuân thủ của các tiêu chuẩn "hồ sơ cơ sở", được định nghĩa trong ETSI TS 103 171, ETSI TS 103 172 và ETSI TS 103 173, có thể được sử dụng.

Bảng 16

Định dạng chữ ký số	Mức độ tuân thủ	URI
CAdES/PAdES/XAdES	AdES-B-B	http://uri.etsi.org/ades/191x2/level/baseline/B-B#
CAdES/PAdES/XAdES	AdES-B-T	http://uri.etsi.org/ades/191x2/level/baseline/B-T#
CAdES/PAdES/XAdES	AdES-B-LT	http://uri.etsi.org/ades/191x2/level/baseline/B-LT#
CAdES/PAdES/XAdES	AdES-B-LTA	http://uri.etsi.org/ades/191x2/level/baseline/B-LTA#
CAdES/PAdES/XAdES	AdES-B	http://uri.etsi.org/ades/etsits/level/baseline/B-B#
CAdES/PAdES/XAdES	AdES-T	http://uri.etsi.org/ades/etsits/level/baseline/B-T#
CAdES/PAdES/XAdES	AdES-LT	http://uri.etsi.org/ades/etsits/level/baseline/B-LT#
CAdES/PAdES/XAdES	AdES-LTA	http://uri.etsi.org/ades/etsits/level/baseline/B-LTA#

Tùy thuộc vào loại chữ ký được chọn, khách hàng cũng có thể chỉ định các thuộc tính chữ ký sau đây.

Bảng 17

Định dạng chữ ký số	Thuộc tính bao chữ ký	URI
CAdES	Detached Attached Parallel	http://uri.etsi.org/cades/detached# http://uri.etsi.org/cades/attached# http://uri.etsi.org/cades/parallel#
PAdES	Certification Revision	http://uri.etsi.org/pades/certification# http://uri.etsi.org/pades/revision#
XAdES	Enveloped Enveloping Detached	http://uri.etsi.org/xades/enveloped# http://uri.etsi.org/xades/enveloping# http://uri.etsi.org/xades/detached#

7.16.2 Thành phần liên quan đến JSON

Thành phần để yêu cầu một định dạng chữ ký số cụ thể phải được biểu thị bằng các tham số sau:

- signatureFormat tham số kiểu chuỗi;
- conformanceLevel tham số kiểu chuỗi;
- signedEnvelopeProperty tham số kiểu chuỗi.

Được chỉ định theo bảng 18.

Bảng 18

Tham số	Sự hiện diện	Loại	Mô tả
signatureFormat	Bắt buộc	Chuỗi	Định dạng chữ ký số yêu cầu: "C" phải được sử dụng để yêu cầu tạo một chữ ký CAdES; "X" phải được sử dụng để yêu cầu tạo một chữ ký XAdES; "P" phải được sử dụng để yêu cầu tạo chữ ký số PAdES.
conformanceLevel	Tùy chọn	Chuỗi	"AdES-B-B" phải được sử dụng để yêu cầu tạo một chữ ký cấp B cơ sở 191x2. "AdES-B-T" phải được sử dụng để yêu cầu tạo một chữ ký cấp T cơ sở 191x2. "AdES-B-LT" phải được sử dụng để yêu cầu tạo một chữ ký LT mức 191x2 cơ sở. "AdES-B-LTA" phải được sử dụng để yêu cầu tạo một chữ ký LTA cấp độ 191x2 cơ sở. "AdES-B" phải được sử dụng để yêu cầu tạo ra một chữ ký etsits cấp độ B cơ sở. "AdES-T" phải được sử dụng để yêu cầu tạo một chữ ký etsits cấp T cơ sở. "AdES-LT" phải được sử dụng để yêu cầu tạo một chữ ký LT cấp etsits cơ sở. "AdES-LTA" phải được sử dụng để yêu cầu tạo một chữ ký LTA cấp độ etsits cơ sở. Tham số là tùy chọn. Mức cơ sở mặc định là AdES-B-B trong trường hợp nó bị bỏ qua. Nếu cần một dấu thời gian, việc yêu cầu và đưa vào đó được SCS quản lý theo cấu hình và chính sách của SCS.
signedEnvelopeProperty	Tùy chọn có điều kiện	Chuỗi	Thuộc tính bắt buộc liên quan đến phong bì đã ký mà các giá trị có thể có phụ thuộc vào giá trị của tham số signatureFormat.

7.16.3 Thành phần liên quan đến XML

Phần tử để yêu cầu một định dạng chữ ký số cụ thể phải là etsisig:SignatureType, phần tử con của phần tử dss2:OptionalInputs. Nó phải chứa một tham chiếu URI đến loại chữ ký được định nghĩa trước mà máy chủ phải tạo ra, với các giá trị được quy định trong mục 7.16.1.

Phần tử để yêu cầu một mức độ tuân thủ chữ ký cụ thể phải là etsisig:ConformanceLevel, phần tử con của phần tử dss2:OptionalInputs. Nó phải chứa một tham chiếu URI đến mức độ tuân thủ được định nghĩa trước mà tại đó máy chủ phải tạo ra chữ ký.

Phần tử để chỉ định thuộc tính phong bì phải là etsisig:SignedEnvelopeProperty. Các giá trị có thể của nó phụ thuộc vào loại phong bì được chỉ định và được định nghĩa trong mục 7.16.1.

<xs:element name="ConformanceLevel" type="xs:anyURI"/>
<xs:element name="SignatureType" type="xs:anyURI"/>
<xs:element name="SignedEnvelopeProperty" type="xs:anyURI"/>

Bảng được định nghĩa trong mục 7.16.1 liệt kê các URI cho các cấp độ được quy định cho chữ ký AdES trong ETSI EN 319 122-1, ETSI EN 319 132-1, ETSI EN 319 142-1, ETSI TS 103 171, ETSI TS 103 172, và ETSI TS 103 173

7.17 Thành phần để định danh chủ thể ký

7.17.1 Ngữ nghĩa của thành phần

Thành phần này được sử dụng để định danh duy nhất chủ thể ký. Thành phần này thể hiện mã định danh chủ thể ký được liên kết với danh tính chủ thể ký trong SCS.

Một yêu cầu phải chứa một thành phần để định danh chủ thể ký.

CHÚ THÍCH: Thành phần này có thể được máy chủ chấp nhận hoặc từ chối dựa trên xác thực dịch vụ hiện tại (tức là để tránh lấy danh sách thông tin xác thực liên quan đến chủ thể ký không ràng buộc với xác thực dịch vụ hiện tại).

7.17.2 Thành phần liên quan đến JSON

Thành phần để chỉ định định danh chủ thể ký phải được thể hiện như sau:

- SignerIdentity: Tham số kiểu chuỗi.

Được chỉ định theo bảng 19.

Bảng 19

Tham số	Loại	Mô tả
SignerIdentity	Chuỗi	Mã định danh liên quan đến danh tính chủ thể ký.

7.17.3 Thành phần liên quan đến XML

Phần tử để định danh chủ thể ký phải là phần tử etsisig:SignerIdentity, phần tử con của etsisig: OptionalInputs.

Phần tử etsisig:SignerIdentity được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết trong mục A.2, và được sao chép bên dưới để tham khảo:

<xs:element name="SignerIdentity" type="dss2:ClaimedIdentityType"/>

Kiểu dss2:ClaimedIdentityType được định nghĩa trong OASIS DSS-v2.0, mục 4.4.9.2.

7.18 Thành phần để chỉ định URL phản hồi

7.18.1 Ngữ nghĩa của thành phần

Với thành phần này, một ứng dụng khách có thể thông báo cho SCS về một URL phản hồi, nơi ứng dụng khách mong đợi nhận được thông báo khi SCS đã hoàn thành thao tác được yêu cầu. Thành phần này phải chứa một URL tuyệt đối.

7.18.2 Thành phần liên quan đến JSON

Thành phần để chỉ định URL phản hồi nơi ứng dụng khách yêu cầu nhận thông báo về hoạt động đã hoàn thành phải được thể hiện bằng những mục sau:

- responseUri tham số kiểu chuỗi.

Được quy định theo bảng 20.

Bảng 20

Tham số	Loại	Mô tả
responseUri	Chuỗi	Phần tử phải có giá trị là một địa điểm mà SCS phải thông báo việc hoàn thành thao tác tạo chữ ký số, dưới dạng giá trị URI.

7.18.3 Thành phần liên quan XML

Phần tử để chỉ định URL phản hồi phải là etsisig:ResponseURL, phần tử con của dss2:OptionalInputs phần tử.

Phần tử etsisig:ResponseURL phải được định nghĩa như trong tệp lược đồ XML "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết trong mục A.2 và được sao chép bên dưới để tham khảo:

```
<xs:element name="ResponseURL" type="xs:anyURI"/>
```

7.18.4 Mô hình xử lý

Nếu thành phần này hiện diện và SCS thực hiện thao tác được yêu cầu ở chế độ hoạt động không đồng bộ, SCS phải gọi đến vị trí được chỉ định bởi thành phần này sau khi hoàn thành thao tác được yêu cầu. SCS phải cung cấp làm tham số đầu vào thành phần được chỉ định trong mục 7.26 mà ứng dụng khách có thể đưa vào yêu cầu tiếp theo, để thăm dò kết quả chữ ký đang chờ xử lý.

7.19 Thành phần dùng để gửi tài liệu hoặc giá trị băm để ký

7.19.1 Ngữ nghĩa của thành phần

Thành phần này phải được sử dụng để truyền cho SCS danh sách tài liệu hoặc danh sách mã băm mà việc tạo chữ ký số được yêu cầu.

Tài liệu và mã băm phải được cung cấp dưới một trong các dạng sau:

- một vùng chứa chứa nội dung (các nội dung) được mã hóa base-64 của tài liệu (các tài liệu) cần ký; hoặc trong
- một vùng chứa chứa các giá trị băm được mã hóa base-64 của (các) tài liệu cần ký và thuật toán băm được sử dụng để tính toán các giá trị băm đó.

Do đó, một thể hiện của thành phần này không được chứa đồng thời cả một danh sách các tài liệu và một danh sách các hàm băm. Bảng 20 chứa một danh sách các thuật toán băm được khuyến nghị trong ETSI TS 119 312 [i.4].

Bảng 21

Thuật toán băm OID	Tên thuật toán băm	Thuật toán băm URI
2.16.840.1.101.3.4.2.1	SHA-256	http://www.w3.org/2001/04/xmlenc#sha256
2.16.840.1.101.3.4.2.2	SHA-384	http://www.w3.org/2001/04/xmldsig-more#sha384
2.16.840.1.101.3.4.2.3	SHA-512	http://www.w3.org/2001/04/xmlenc#sha512
2.16.840.1.101.3.4.2.8	SHA3-256	http://www.w3.org/2007/05/xmldsig-more#sha3-256
2.16.840.1.101.3.4.2.9	SHA3-384	http://www.w3.org/2007/05/xmldsig-more#sha3-384
2.16.840.1.101.3.4.2.10	SHA3-512	http://www.w3.org/2007/05/xmldsig-more#sha3-512

7.19.2 Thành phần liên quan đến JSON

Thành phần để gửi tài liệu hoặc mã băm cần ký phải được đại diện bởi các thông số (loại trừ lẫn nhau) sau:

- documents: tham số kiểu mảng chuỗi.
- documentDigests: Đối tượng JSON chứa (các) giá trị băm cần ký và OID thuật toán băm được sử dụng để tính toán (các) giá trị băm được chỉ định theo bảng 22.

Bảng 22

Tham số	Sự hiện diện	Loại	Mô tả
documents	Bắt buộc có điều kiện	Mảng Chuỗi	Nội dung (các) tài liệu được mã hóa Base64, để ký. Tham số này phải không được sử dụng nếu tham số documentDigests được thông qua.
documentDigests	Bắt buộc có điều kiện	Đối tượng JSON	Đối tượng JSON chứa (các) giá trị băm cần ký và OID thuật toán băm được sử dụng để tính toán (các) giá trị băm đó. Tham số này phải không được sử dụng nếu tham số documents được truyền vào.

Phần tử documentDigests phải là một JSONObject chứa các tham số sau:

- hashes tham số mảng kiểu chuỗi.
- hashAlgorithmOID tham số kiểu chuỗi.

Được quy định theo bảng 23.

Bảng 23

Tham số	Sự hiện diện	Loại	Mô tả
hashes	Bắt buộc	Mảng Chuỗi	Mã băm tài liệu được mã hóa Base64, để ký.

Tham số	Sự hiện diện	Loại	Mô tả
hashAlgorithmOID	Bắt buộc	Chuỗi	Thuật toán băm OID được sử dụng để tính toán mã băm tài liệu.

7.19.3 Thành phần liên quan đến XML

Phần tử để gửi tài liệu và mã băm phải là dss2:InputDocuments, với các giá trị được quy định trong OASIS DSS-v2.0, mục 4.5.1.2.,

7.20 Thành phần để trả về thông tin dịch vụ

7.20.1 Thành phần ngữ nghĩa

Phần tử này phải bao gồm:

1) mô tả chung về dịch vụ;
2) một tên gọi chung định danh dịch vụ;
3) một đường dẫn đến logo của dịch vụ;
4) quốc gia nơi dịch vụ đang hoạt động;
5) thông tin liên quan đến giao thức được hỗ trợ, tức là URI http://uri.etsi.org/19432/v1.1.1/creationprofile# chỉ định sự hỗ trợ của hồ sơ được quy định trong tài liệu này
6) danh sách các phiên bản giao thức được hỗ trợ;
7) một danh sách các ngôn ngữ được hỗ trợ, ngôn ngữ đầu tiên trong danh sách là ngôn ngữ mặc định của SCS;
8) một danh sách các chính sách tiêu biểu được thực hiện bởi SCS;
9) một danh sách các chính sách dịch vụ được thực hiện bởi SCS;
10) danh sách các chế độ hoạt động được chấp nhận;
11) một danh sách các chế độ xác thực được hỗ trợ;
12) một danh sách định dạng chữ ký số, mức độ tuân thủ và thuộc tính phong bì đã ký;
13) danh sách tên của tất cả các phương thức API được triển khai và hỗ trợ bởi SCS.

Một số mục trên có thể trống hoặc không có, cho biết một tính năng không được SCS hỗ trợ.

7.20.2 Thành phần liên quan đến JSON

Thành phần để trả về thông tin dịch vụ phải được thể hiện như sau

1) description là kết quả kiểu chuỗi;
2) name là kết quả kiểu chuỗi;
3) logo là kết quả kiểu chuỗi;
4) region là kết quả kiểu chuỗi;
5) protocol là kết quả kiểu chuỗi;
6) versions là kết quả kiểu mảng chuỗi;

7) lang là kết quả kiểu mảng chuỗi;

8) signaturePolicies là kết quả kiểu mảng chuỗi;

9) servicePolicies là kết quả kiểu mảng chuỗi;

10) operationModes là kết quả kiểu mảng chuỗi;

11) authType là kết quả kiểu mảng chuỗi;

12) signatureFormats là một mảng các giá trị về định dạng chữ ký số, mức phù hợp và thuộc tính bao chữ ký, xác định các giá trị có thể được truyền trong thành phần được định nghĩa tại mục 7.16;

13) methods là kết quả kiểu mảng chuỗi.

Được chỉ định theo bảng 24.

Bảng 24

Tham số	Sự hiện diện	Giá trị	Mô tả
description	Bắt buộc	Chuỗi	Mô tả ngắn về dịch vụ.
name	Bắt buộc	Chuỗi	Tên của dịch vụ.
logo	Bắt buộc	Chuỗi	URI của tệp hình ảnh chứa logo của Dịch vụ. Hình ảnh phải ở định dạng JPEG hoặc PNG và không lớn hơn 256x256 pixel.
region	Bắt buộc	Chuỗi	Mã quốc gia alpha-2 ISO 3166-1 nơi dịch vụ đang hoạt động.
protocol	Bắt buộc	Chuỗi	URI xác định giao thức được SCS hỗ trợ.
versions	Bắt buộc	Mảng Chuỗi	Các phiên bản của các đặc tả giao thức được SCS hỗ trợ. Định dạng của các chuỗi là Major.Minor.x.
lang	Bắt buộc	Mảng Chuỗi	Danh sách các ngôn ngữ được hỗ trợ trong các phản hồi của dịch vụ, được chỉ định theo IETF RFC 5646.
signaturePolicies	Bắt buộc	Mảng Chuỗi	Danh sách các chính sách tạo chữ ký số được hỗ trợ.
servicePolicies	Bắt buộc	Mảng Chuỗi	Danh sách các chính sách dịch vụ được hỗ trợ.
operationModes	Bắt buộc	Mảng Chuỗi	Danh sách các chế độ hoạt động được hỗ trợ.
authType	Bắt buộc	Mảng Chuỗi	Danh sách các cơ chế xác thực được dịch vụ hỗ trợ để truy cập các phương thức API.
signatureFormats	Bắt buộc	Mảng đối tượng JSON	Danh sách các JSONObject chỉ định các định dạng chữ ký số được SCS hỗ trợ và chứa các tham số sau: Tham số kiểu chuỗi định dạng chữ ký số; tham số kiểu chuỗi conformanceLevel; tham số signedEnvelopeProperty kiểu chuỗi. như được quy định trong mục 7.16.2.
methods	Bắt buộc	Mảng Chuỗi	Danh sách tên các phương thức API được hỗ trợ.

Các phần tử "signatureFormats", "signaturePolicies", "servicePolicies" và "operationModes" không được định nghĩa trong tiêu chuẩn CSC. Các phần tử khác được định nghĩa trong mục 11.1 của tiêu chuẩn CSC.

7.20.3 Thành phần liên quan đến XML

Phần tử để trả về thông tin dịch vụ phải là phần tử con etsisig:ServiceInformation của etsisig: OptionalOutputs

Phần tử ServiceInformation được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết trong mục A.2, và được sao chép bên dưới để tham khảo:

```
<xs:element name="ServiceInformation" type="etsisig:ServiceInformationType"/>
<xs:complexType name="ServiceInformationType">
    <xs:sequence>
        <xs:element name="Description" type="xs:string"/>
        <xs:element name="Version" type="xs:string"/>
        <xs:element name="Logo" type="xs:anyURI"/>
        <xs:element name="Region" type="xs:string"/>
        <xs:element name="SupportedProtocol" type="xs:anyURI" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="SupportedLanguage" type="xs:language" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="SupportedSignaturePolicy" type="xs:anyURI" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="SupportedServicePolicy" type="xs:anyURI" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="SupportedOperationMode" type="xs:string" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="SupportedSignatureFormat" type="etsisig:SupportedSignatureFormatType" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="SupportedAuthMode" type="xs:string" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="SupportedMethod" type="xs:string" minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexTy
        pe>
<xs:complexType name="SupportedSignatureFormatType">
    <xs:sequence>
        <xs:element name="SupportedSignatureType" type="xs:anyURI" minOccurs="0"/>
        <xs:element name="SupportedConformanceLevel" type="xs:anyURI" minOccurs="0"/>
        <xs:element name="SupportedEnvelope" type="xs:string" minOccurs="0"/>
</xs:sequence>
</xs:complexTy
        pe>
```

7.21 Thành phần để trả về tài liệu đã ký hoặc chữ ký

7.21.1 Ngữ nghĩa của thành phần

Thành phần này phải được sử dụng để trả về các chữ ký được yêu cầu. Giao thức phải cho phép trả về các chữ ký trong hai vùng chứa khác nhau theo các quy tắc sau:

1) Nếu chữ ký nằm trong tài liệu đã ký, nó phải được chứa trong một vùng chứa cụ thể được xác định là vùng chứa cho tài liệu đã ký.

2) Nếu chữ ký không được bao bọc thì nó phải được đưa vào một vùng chứa cụ thể được xác định là vùng chứa bao bọc chữ ký.

Giao thức hỗ trợ mối quan hệ 1-đến-1 giữa các tài liệu đầu vào và chữ ký, hoặc mối quan hệ nhiều-đến-1 trong đó tất cả các tài liệu đầu vào được bao phủ bởi một chữ ký.

7.21.2 Thành phần liên quan đến JSON

Thành phần để trả về các tài liệu đã ký hoặc chữ ký được yêu cầu phải được đại diện bởi những mục sau đây:

- DocumentWithSignature: mảng JSON kiểu chuỗi kết quả;
- SignatureObject: Mảng JSON kết quả dạng chuỗi;

Được quy định theo bảng 25.

Bảng 25

Tham số	Sự hiện diện	Loại	Mô tả
DocumentWithSignature	Bắt buộc có điều kiện	Mảng Chuỗi	Chữ ký được mã hóa Base64 được bao bọc trong tài liệu. Thành phần này phải mang một giá trị chỉ khi ứng dụng khách yêu cầu tạo chữ ký số được lồng vào trong tài liệu đã ký.
SignatureObject	Bắt buộc có điều kiện	Mảng Chuỗi	Chữ ký được mã hóa Base64 tách rời khỏi tài liệu. Phần tử này phải có giá trị chỉ khi ứng dụng khách yêu cầu tạo chữ ký số không bao bọc.

7.21.3 Thành phần liên quan XML

Phần tử để trả về chữ ký phải là dss2:SignatureObject, với các giá trị như được quy định trong OASIS DSS-v2.0, mục 4.5.6.2. Trong trường hợp chữ ký được bao bọc trong tài liệu, phần tử dss2:DocumentWithSignature, được định nghĩa trong OASIS DSS-v2.0 mục 4.4.19.2, phải được sử dụng.,

7.22 Thành phần để trả về thông tin xác thực chữ ký

7.22.1 Ngữ nghĩa của thành phần

Thành phần này được sử dụng để trả về chuỗi chứng thư chữ ký số và thông tin xác thực chữ ký.

Thành phần này phải chứa thông tin về thông tin xác thực chữ ký và chuỗi chứng thư chữ ký số được sử dụng hoặc phải được sử dụng trong hoạt động tạo DSV hoặc tạo chữ ký số.

Thành phần này phải chứa các dữ liệu sau:

1) Chứng thư chữ ký số/chuỗi chứng thư X.509 dùng để ký;

2) Thông tin về khóa ký:

- trạng thái của khóa;
- thuật toán được hỗ trợ;
- chiều dài của khóa;
- đường cong;

3) Chi tiết thuộc tính chứng thư chữ ký số của chủ thể ký:

- trạng thái;
- validFrom;
- validTo;
- issuerDN;
- serialNumber;
- subjectDN;

4) Việc hỗ trợ tạo nhiều chữ ký với một đặc tả yêu cầu ủy quyền duy nhất bởi thông tin xác thực.

Việc bao gồm thành phần này trong phản hồi có thể được yêu cầu bởi ứng dụng khách sử dụng "Thành phần để định nghĩa dữ liệu tùy chọn được trả về" được định nghĩa trong mục 7.5. Thông tin về chứng thư chữ ký số/chuỗi chứng thư X.509 và/hoặc khóa ký phải được bao gồm trong thành phần này có thể được chỉ định bởi ứng dụng khách sử dụng "Thành phần để chỉ định nội dung thông tin xác thực chữ ký được trả về" được định nghĩa trong mục 7.10.

7.22.2 Thành phần liên quan đến JSON

Thành phần để trả về thông tin xác thực chữ ký phải được thể hiện bằng những mục sau:

- cert/certificates: mảng kiểu chuỗi kết quả;
- key/status: kết quả kiểu chuỗi;
- key/algo: mảng kiểu chuỗi kết quả;
- key/len: kết quả kiểu số nguyên;
- key/curve: kết quả kiểu chuỗi;

- cert/status: kiểu chuỗi kết quả;
- cert/validFrom: kết quả kiểu chuỗi;
- cert/validTo: kết quả kiểu chuỗi;
- cert/IssuerDN: kết quả kiểu chuỗi;
- cert/serialNumber: kết quả kiểu chuỗi;
- cert/subjectDN: kết quả kiểu chuỗi;
- multisign: kết quả kiểu Boolean.

Được quy định theo bảng 26.

Bảng 26

Tham số	Sự hiện diện	Loại	Mô tả
cert/certificates	Bắt buộc có điều kiện	Mảng Chuỗi	Chứa một hoặc nhiều chứng thư chữ ký số X.509v3 được mã hóa Base64 từ chuỗi chứng thư chữ ký số. Nếu tham số chứng thư chữ ký số được định nghĩa trong mục 7.10.1.2 là "chain", toàn bộ chuỗi chứng thư chữ ký số phải được trả về với chứng thư chữ ký số thực thể cuối cùng ở đầu mảng. Nếu tham số chứng thư chữ ký số là "single", chỉ chứng thư chữ ký số thực thể cuối cùng phải được trả về. Nếu tham số chứng thư chữ ký số là "none", mục này tham số phải không được trả về.
key/status	Bắt buộc	Chuỗi	Đã bật | Đã tắt: Trạng thái kích hoạt khóa ký của thông tin xác thực: "đã bật": khóa ký đã được bật và có thể được sử dụng để ký. "đã vô hiệu hóa": khóa ký đã bị vô hiệu hóa và không thể dùng để ký. Mục này có thể xảy ra khi chủ sở hữu đã vô hiệu hóa nó hoặc khi SCS đã phát hiện chứng thư chữ ký số liên quan đã hết hạn hoặc bị thu hồi.
key/algo	Bắt buộc	Chuỗi	Danh sách các OID của các thuật toán khóa được hỗ trợ. Ví dụ: 1.2.840.113549.1.1.1 = RSA encryption, 1.2.840.10045.4.3.2 = ECDSA with SHA256, 1.2.840.113549.1.1.10 = RSASSA-PSS, 1.2.840.10045.4.3.4 = ECDSA with SHA512.
key/len	Bắt buộc	Số	Độ dài của khóa mật mã tính bằng bit.
key/curve	Bắt buộc có điều kiện	Chuỗi	OID của đường cong ECDSA. Giá trị này phải chỉ được trả về nếu keyAlgo dựa trên ECDSA.
cert/status	Tùy chọn	Chuỗi	hợp lệ | hết hạn | bị thu hồi | bị tạm ngừng: Trạng thái hiệu lực của chứng thư chữ ký số thực thể cuối. Giá trị này là tùy chọn. SCS chỉ được trả về một giá trị chính xác và nhất quán với trạng thái hiệu lực thực tế của chứng thư tại thời điểm phản hồi được tạo, nếu không thì tham số này phải không được đưa vào phản hồi. Trạng thái "hợp lệ" phải được trả về khi chứng thư nằm trong thời gian

Tham số	Sự hiện diện	Loại	Mô tả
			hiệu lực, được tạo bởi một CA được SCS tin cậy và không bị thu hồi hoặc tạm ngừng. Do đó, SCS phải không đưa tham số này vào phản hồi nếu không thể kiểm tra xem chứng thư chữ ký số có phải là bị thu hồi, bị đình chỉ hay không.
cert/validFrom	Bắt buộc	Chuỗi	Ngày bắt đầu hiệu lực từ chứng thư chữ ký số X.509v3 ở định dạng chuỗi có thể in được, được mã hóa theo định dạng GeneralizedTime (IETF RFC 5280) (ví dụ "YYYYMMDDHHMMSSZ"). Tham số này phải được trả về khi certInfo được định nghĩa trong mục 7.10 là "true".
cert/validTo	Bắt buộc	Chuỗi	Ngày hết hạn hiệu lực của chứng thư chữ ký số X.509v3 ở định dạng chuỗi có thể in, được mã hóa theo định dạng GeneralizedTime (IETF) RFC 5280 (ví dụ "YYYYMMDDHHMMSSZ"). Tham số này phải được trả về khi certInfo được định nghĩa trong mục 7.10 là "true".
cert/IssuerDN	Bắt buộc có điều kiện	Chuỗi	Tên phân biệt của Tổ chức phát hành từ chứng thư chữ ký số thực thể cuối X.509v3 ở định dạng chuỗi có thể in, được mã hóa UTF-8 theo IETF RFC 4514. Tham số này phải được trả về khi certInfo được định nghĩa trong mục 7.10 là "true".
cert/serialNumber	Bắt buộc có điều kiện	Chuỗi	Số sê-ri từ chứng thư chữ ký số X.509v3 dưới định dạng mã hóa lục phân (hex). Tham số này phải được trả về khi certInfo được định nghĩa trong mục 7.10 là "true".
cert/subjectDN	Bắt buộc có điều kiện	Chuỗi	Tên phân biệt của Chủ thể từ chứng thư chữ ký số X.509v3 dưới định dạng chuỗi có thể in được, mã hóa UTF-8 theo IETF RFC 4514. Tham số này phải được trả về khi certInfo được định nghĩa trong mục 7.10 là "true".
multisign	Bắt buộc có điều kiện	Boolean	Chỉ định xem thông tin xác thực (credential) có hỗ trợ tạo nhiều chữ ký số (ký số hàng loạt/đa thông điệp) chỉ với một yêu cầu cấp quyền duy nhất hay không.

Các phần tử trên được định nghĩa trong mục 11.5 của tiêu chuẩn CSC.

7.22.3 Thành phần liên quan đến XML

Phần tử để trả về thông tin xác thực chữ ký phải là ds:KeyInfo, phần tử con của dss2:OptionalOutputs phần tử gốc.

Phần tử để trả về thông tin xác thực chữ ký phải là ds:X509Data, phần tử con của phần tử ds:KeyInfo. Để bao gồm các thuộc tính bổ sung như được liệt kê tại điểm 3 trong mục ngữ nghĩa ở trên, phần tử etsisig:X509Details phải được sử dụng trong phần tử ds:KeyInfo tương ứng.

Phần tử X509Details được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết tại mục A.2, và được sao chép bên dưới để tham khảo:

```
<xs:element name="X509Details" type="etsisig:X509DetailsType"/>
<xs:complexType name="X509DetailsType">
    <xs:sequence>
        <xs:element ref="etsisig:Status"/>
        <xs:element ref="etsisig:NotBefore"/>
        <xs:element ref="etsisig:NotAfter"/>
</xs:sequence>
</xs:complexTy
        pe>

<xs:element name="NotBefore" type="xs:dateTime"/>
<xs:element name="NotAfter" type="xs:dateTime"/>

<xs:element name="Status" type="etsisig:CertificateStatusType"/>
<xs:simpleType name="CertificateStatusType">
    <xs:restriction base="xs:string">
        <xs:enumeration value="Valid"/>
        <xs:enumeration value="Expired"/>
        <xs:enumeration value="Revoked"/>
        <xs:enumeration value="Suspended"/>
    </xs:restriction>
</xs:simpleType>

<xs:element name="Enabled" type="xs:Boolean"/>
<xs:element name="Algorithm" type="xs:anyURI"/>
<xs:element name="Length" type="xs:int"/>
<xs:element name="Curve" type="xs:anyURI"/>

<xs:element name="KeyDetails" type="etsisig:KeyDetailsType"/>
<xs:complexType name="KeyDetailsType">
    <xs:sequence>
        <xs:element ref="etsisig:Enabled"/>
        <xs:element ref="etsisig:Algorithm"/>
        <xs:element ref="etsisig:Length"/>
        <xs:element ref="etsisig:Curve"/>
</xs:sequence>
</xs:complexTy
        pe>
<xs:element name="MultipleSignaturesEnabled" type="xs:Boolean"/>
```

VÍ DỤ:

```
<ds:KeyInfo>
    <ds:X509Data>
        <etsisig:X509Details>
            <etsisig:Status>Valid</etsisig:Status>
            <etsisig:NotBefore>2002-05-30T09:00:00</etsisig:NotBefore>
            <etsisig:NotAfter>2022-05-30T09:00:00</etsisig:NotAfter>
        </etsisig:X509Details>
        <etsisig:KeyDetails>
            <etsisig:Enabled>true</etsisig:Enabled>
            <etsisig:Algorithm>1.2.840.10045.4.3.2</etsisig:Algorithm>
            <etsisig:Length>4096</etsisig:Length>
            <etsisig:Curve>1.2.840.10045.3.1.1.7</etsisig:Curve>
        </etsisig:KeyDetails>
        <etsisig:MultipleSignaturesEnabled>false</etsisig:MultipleSignaturesEnabled>
    </ds:X509Data>
</ds:KeyInfo>
```

7.23 Thành phần dùng để trả về danh sách chứng thư chữ ký số

7.23.1 Ngữ nghĩa của thành phần

Thành phần này phải được sử dụng để trả về (các) chứng thư chữ ký số khả dụng của chủ thể ký. Mỗi chứng thư chữ ký số cũng có thể bao gồm chuỗi của nó.

7.23.2 Thành phần liên quan đến JSON

Thành phần để trả về (các) chứng thư chữ ký số khả dụng của chủ thể ký phải được thể hiện bằng những mục sau:

- credentialIDs mảng các tham số kiểu chuỗi;
- certificates mảng các tham số kiểu chuỗi.

Được chỉ định theo bảng 27.

Bảng 27

Tham số	Sự hiện diện	Loại	Mô tả
credentialIDs	Bắt buộc	Mảng Chuỗi	Một hoặc nhiều credentialID liên kết với định danh chủ thể ký được cung cấp hoặc được ngầm định.
certificates	Có điều kiện	Mảng chuỗi (Array of Chuỗi)	Mỗi chuỗi phải chứa một hoặc nhiều chứng thư trong chuỗi chứng thư chữ ký số, trong đó mỗi chứng thư được mã hóa dạng văn bản theo quy định tại IETF RFC 7468. Nếu tham số certificates được định nghĩa tại 7.10.1.2 có giá trị là “chain”, mỗi chuỗi phải chứa toàn bộ chuỗi chứng thư với chứng thư thực thể cuối (end entity certificate) ở đầu chuỗi, tiếp theo là các chứng thư CA bổ sung. Nếu tham số certificates có giá trị là “single”, mỗi chuỗi chỉ được chứa chứng thư thực thể cuối. Nếu tham số certificates có giá trị là “none”, tham số này không được trả về.

7.23.3 Thành phần liên quan XML

Phần tử để trả về danh sách (các) chứng thư chữ ký số phải là ds:KeyInfo, phần tử con của etsisig:OptionalOutputs phần tử gốc.

Nếu tham số ReturnCertificates được định nghĩa trong mục 7.10.3 là "Chain", toàn bộ chuỗi chứng thư chữ ký số phải được trả về với chứng thư chữ ký số thực thể cuối cùng là phần tử ds:Keyinfo đầu tiên. Nếu tham số ReturnCertificates là "Single", chỉ chứng thư chữ ký số thực thể cuối cùng phải được trả về. Nếu tham số ReturnCertificates là "None", không có phần tử ds:Keyinfo nào phải được trả về.

7.24 Thành phần để thông báo kết quả hoạt động

7.24.1 Ngữ nghĩa của thành phần

Thành phần này phải chứa thông tin thể hiện kết quả của yêu cầu.

CHÚ THÍCH: Khi chế độ yêu cầu là đồng bộ, thành phần này sẽ trả về kết quả(s) của quá trình xử lý.

Khi chế độ yêu cầu là không đồng bộ, thành phần này phải trả về xác nhận việc chấp nhận yêu cầu hay không.

7.24.2 Thành phần liên quan đến JSON

Khi trạng thái HTTP của yêu cầu khác 200 OK, kết quả của thao tác được yêu cầu phải được trả về trong phần thân của phản hồi HTTP sử dụng kiểu phương tiện "application/json". Cấu trúc JSON bao gồm các mục sau:

- error giá trị kiểu chuỗi;
- error_description giá trị kiểu chuỗi.

Được chỉ định theo bảng 28.

Bảng 28

Tham số	Sự hiện diện	Loại	Mô tả
error	Bắt buộc	Chuỗi	Chuỗi mã lỗi.
error_description	Tùy chọn	Chuỗi	Mô tả dễ hiểu đối với người dùng, được viết theo ngôn ngữ phù hợp với đặc tả của tham số lang, cung cấp thông tin bổ sung về lỗi nhằm hỗ trợ ứng dụng khách hiểu được lỗi đã xảy ra.

Các mã trạng thái và thông báo lỗi được định nghĩa trong mục 10.1 của tiêu chuẩn CSC phải được sử dụng nếu phù hợp.

7.24.3 Thành phần liên quan đến XML

Phần tử để thông báo kết quả phải là dsb:Result với các giá trị của các phần tử con dss2:ResultMajor và

dss2:ResultMinor như được quy định trong OASIS DSS-v2.0, mục 4.2.7.2.,

7.25 Thành phần định danh chính sách dịch vụ

7.25.1 Ngữ nghĩa của thành phần

Thành phần này phải được sử dụng để trả về tên của chính sách dịch vụ được máy chủ sử dụng để thực hiện thao tác được yêu cầu.

Việc bao gồm thành phần này trong phản hồi có thể được khách hàng yêu cầu bằng cách sử dụng "Thành phần để định nghĩa dữ liệu tùy chọn phải được trả về" được định nghĩa trong mục 7.5.

7.25.2 Thành phần liên quan đến JSON

Thành phần để trả về định danh chính sách dịch vụ phải được biểu thị bằng những mục sau:

- policy: kết quả loại chuỗi

Được chỉ định theo bảng 29.

Bảng 29

Tham số	Loại	Mô tả
policy	Chuỗi	Phần tử dùng để định danh một chính sách dịch vụ cụ thể liên kết với SCS.

7.25.3 Thành phần liên quan đến XML

Phần tử để định danh chính sách dịch vụ phải là dsb:AppliedPolicy, phần tử con của phần tử dss2:OptionalOutputs, được định nghĩa trong OASIS DSS-v2.0, mục 4.2.9.2.,

7.26 Thành phần để định danh phản hồi

7.26.1 Ngữ nghĩa của thành phần

Thành phần này chứa một giá trị chuỗi được tạo bởi SCS để định danh duy nhất phản hồi có nguồn gốc từ chính SCS. Thành phần này chủ yếu được sử dụng trong chế độ hoạt động không đồng bộ, nơi ứng dụng khách phải cung cấp giá trị responseID nhận được cùng với phản hồi ban đầu được bao gồm trong thành phần requestID của bất kỳ yêu cầu tiếp theo nào thăm dò kết quả chữ ký đang chờ xử lý.

7.26.2 Thành phần liên quan đến JSON

Thành phần định danh yêu cầu chữ ký có kết quả được yêu cầu phải được thể hiện bằng những mục sau đây:

- responseID: tham số kiểu chuỗi.

Được chỉ định theo bảng 30.

Bảng 30

Tham số	Loại	Mô tả
responseID	Chuỗi	Giá trị kiểu chuỗi bất kỳ do SCS sinh ra nhằm định danh duy nhất phản hồi có nguồn gốc từ chính SCS.

7.26.3 Thành phần liên quan đến XML

Phần tử để xác định yêu cầu ký mà kết quả của nó được yêu cầu phải là thuộc tính responseID của phần tử gốc dss2:SignResponse, được định nghĩa trong OASIS DSS-v2.0, mục 4.3.2.2.,

7.27 Thành phần để xác định chính sách tạo chữ ký số

7.27.1 Ngữ nghĩa của thành phần

Thành phần này phải chứa thông tin được sử dụng để tạo chữ ký số và/hoặc DSV. Thông tin phải bao gồm:

a) Việc xác định chính sách tạo chữ ký số được sử dụng khi tạo DSV(s).

b) Các tham số tùy chọn khác chứa các vị trí của tài liệu chính sách tạo chữ ký số.

Việc bao gồm thành phần này trong phản hồi có thể được khách hàng yêu cầu bằng cách sử dụng "Thành phần để định nghĩa dữ liệu tùy chọn được trả về" được định nghĩa trong mục 7.5.
CHÚ THÍCH: Chính sách tạo chữ ký số có thể là một phần của chính sách dịch vụ. Do đó, chính sách tạo chữ ký số có thể được xác định một cách ngầm định bởi chính sách dịch vụ được áp dụng.

7.27.2 Thành phần liên quan đến JSON

Thành phần để trả về định danh chính sách tạo chữ ký số phải được thể hiện bằng những mục sau:

- signaturePolicyID tham số kiểu chuỗi;
- signaturePolicyLocations tham số kiểu mảng chuỗi.

Được chỉ định theo bảng 31.

Bảng 31

Tham số	Presence	Loại	Mô tả
signaturePolicyID	Bắt buộc	Chuỗi	“Phần tử định danh một chính sách cụ thể liên kết với SCS. Phần tử này phải có giá trị là mã định danh duy nhất của chính sách tạo chữ ký số dưới dạng URI. Nếu mã định danh của chính sách tạo chữ ký số là một OID thì giá trị của phần tử này phải là một URN biểu thị giá trị của OID nêu trên theo quy định tại IETF RFC 3061.
signaturePolicyLocations	Tùy chọn	Mảng hoặc Chuỗi	Mỗi phần tử chuỗi phải có giá trị URI là một địa chỉ mà tại đó tài liệu chính sách tạo chữ ký số có thể được truy cập.”

7.27.3 Thành phần liên quan đến XML

Phần tử để xác định chính sách tạo chữ ký số phải là dsb:AppliedPolicy, phần tử con của phần tử dss2:OptionalOutputs, được định nghĩa trong OASIS DSS-v2.0, mục 4.2.9.2.,

7.28 Thành phần để trả về chế độ ủy quyền thông tin xác thực

7.28.1 Ngữ nghĩa của thành phần

Thành phần này chỉ định chế độ ủy quyền được yêu cầu bởi thông tin xác thực chữ ký đã được định danh.
VÍ DỤ: SCSP có thể chỉ định các chế độ ủy quyền được hỗ trợ trong chính sách dịch vụ hoặc trong các mục và điều kiện của dịch vụ.
Các giá trị trả về có thể là:
1) "Ngầm định": quá trình ủy quyền được SCS quản lý một cách tự chủ. Ở chế độ này, SCS phải làm việc trực tiếp với người dùng để thực hiện quá trình ủy quyền mà không có bất kỳ sự can thiệp nào từ ứng dụng khách;

2) "Tường minh": ứng dụng khách cung cấp các yếu tố bảo mật cần thiết cho SCS để SCS thực hiện quá trình ủy quyền;

3) "AuthorizationCode": quá trình ủy quyền được quản lý bởi SCS sử dụng một cơ chế dựa trên mã ủy quyền, ví dụ một cơ chế OAuth 2.0 dựa trên mã ủy quyền như được mô tả trong IETF RFC 6749

4) "IdentificationToken": quá trình ủy quyền được quản lý bởi SCS sử dụng một cơ chế dựa trên các mã thông báo bảo mật chứa thông tin hồ sơ người dùng (như tên người dùng, email, v.v.), được biểu thị dưới dạng các xác nhận (ví dụ: một JWT như được mô tả trong IETF RFC 7519 hoặc một xác nhận SAML); hoặc

5) Các giá trị khác nhau tùy theo các chế độ ủy quyền được SCSP hỗ trợ và quy định.

7.28.2 Thành phần liên quan đến JSON

Thành phần để trả về chế độ ủy quyền của thông tin xác thực chữ ký đã được xác định phải được thể hiện bằng những mục sau:

- authMode Kết quả kiểu chuỗi.

Được chỉ định theo bảng 32.

Bảng 32

Tham số	Loại	Mô tả
authMode	Chuỗi	Quy định chế độ cấp quyền đối với thông tin chứng thư ký.

Phần tử "authMode" được định nghĩa trong mục 11.5 của tiêu chuẩn CSC. Giá trị "identificationToken", được đề cập trong mục 7.28.1, không được định nghĩa trong tiêu chuẩn CSC

7.28.3 Thành phần liên quan đến XML

Phần tử để trả về chế độ ủy quyền thông tin xác thực phải là etsisig:AuthorizationMode, phần tử con của phần tử etsisig:OptionalOutputs.

Phần tử etsisig:AuthorizationMode được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết trong mục A.2, và được sao chép dưới đây để tham khảo:

```
<xs:element name="AuthorizationMode" type="AuthorizationModeType"/>
<xs:simpleType name="AuthorizationModeType">
    <xs:restriction base="xs:string"
        <xs:enumeration value="Implicit"/>
        <xs:enumeration value="Explicit"/>
        <xs:enumeration value="AuthorizationCode"/>
        <xs:enumeration value="IdentificationToken"/>
    </xs:restriction>
```

</xs:simpleType>

7.29 Thành phần để trả về giá trị chữ ký số

7.29.1 Ngữ nghĩa của thành phần

Thành phần này phải chứa một danh sách các giá trị chữ ký số được mã hóa base64 tương ứng với (các) DTBSR được truyền vào
tham số documentDigests được quy định tại mục 7.19.
Vị trí của giá trị(các) chữ ký số trong danh sách phải trùng với vị trí của các giá trị băm được bao gồm trong thành phần DTBSR(s).
Các giá trị được trả về trong thành phần này có thể được chỉ định tùy theo các hành vi thay thế khả dĩ của SCS:

1) Khi một hoặc nhiều chữ ký được yêu cầu không thành công, thành phần này không được trả về và một mã lỗi được trả về làm kết quả đầu ra của việc tạo chữ ký số.

2) Khi một hoặc nhiều chữ ký được yêu cầu không thành công, các DSV tương ứng được trả về dưới dạng giá trị rỗng.

7.29.2 Thành phần liên quan đến JSON

Thành phần để trả về DSV(s) phải được thể hiện như sau:

- mảng chữ ký kiểu chuỗi kết quả. Được chỉ định theo bảng 33.

Bảng 33

Tham số	Loại	Mô tả
signatures	Mảng hoặc Chuỗi	Một hoặc nhiều giá trị chữ ký số được mã hóa base64. Trong trường hợp có nhiều chữ ký, các giá trị chữ ký số phải được trả về theo cùng thứ tự với các giá trị băm tương ứng được cung cấp trong tham số đầu vào.

7.29.3 Thành phần liên quan đến XML

Phần tử để trả về giá trị chữ ký số phải là dss2:SignatureObject, phần tử con của phần tử gốc dss2:SignResponse, được định nghĩa trong OASIS DSS-v2.0, mục 4.5.6.2. Sẽ có một dss2:SignatureObject cho mỗi DSV. Thuộc tính tùy chọn WhichDoc phải chứa định danh của tài liệu liên quan từ yêu cầu tạo chữ ký số.,

7.30 Thành phần để trả về mức bảo đảm kiểm soát duy nhất được yêu cầu

7.30.1 Ngữ nghĩa của thành phần

Thành phần này quy định mức bảo đảm kiểm soát duy nhất được yêu cầu bởi thông tin xác thực chữ ký đã xác định, như được định nghĩa trong CEN EN 419 241-1. Chỉ hai giá trị của mức bảo đảm kiểm soát duy nhất phải được hỗ trợ: "SCAL1" và "SCAL2". Các giá trị đó xác định hai mức độ tin cậy khác nhau của việc kiểm soát khóa ký, như được quy định trong mục 4.4.1.1.

CHÚ THÍCH: Đối với tiêu chuẩn này, giá trị "SCAL2" cho biết rằng dữ liệu kích hoạt chữ ký số, được sử dụng để bảo đảm chủ thể ký được ủy quyền sử dụng khóa ký của mình, được liên kết với tài liệu hoặc các tài liệu cần ký và cần có xác thực hai yếu tố để ủy quyền chữ ký.

7.30.2 Thành phần liên quan đến JSON

Thành phần để trả về mức bảo đảm kiểm soát duy nhất được yêu cầu bởi thông tin xác thực chữ ký đã xác định phải được thể hiện bằng những mục sau:

- SCAL kết quả kiểu chuỗi.

Được quy định theo bảng 34.

Bảng 34

Tham số	Loại	Mô tả
SCAL	Chuỗi	Quy định Mức bảo đảm kiểm soát duy nhất (Sole Control Assurance Level - SCAL) được yêu cầu bởi thông tin xác thực chữ ký: “1”: mức bảo đảm kiểm soát duy nhất cấp 1 được yêu cầu đối với thông tin xác thực chữ ký đã được định danh; “2”: mức bảo đảm kiểm soát duy nhất cấp 2 được yêu cầu đối với thông tin xác thực chữ ký đã được định danh.”

Phần tử "SCAL" được định nghĩa tại mục 11.5 của tiêu chuẩn CSC.

7.30.3 Thành phần liên quan đến XML

Phần tử để trả về mức SCAL yêu cầu phải là etsisig:SoleControlAssuranceLevel, phần tử con của phần tử etsisig:OptionalOutputs.

Phần tử SoleControlAssuranceLevel được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", có vị trí được trình bày chi tiết trong mục A.2, và được sao chép dưới đây để tham khảo:

```
<xs:element name="SoleControlAssuranceLevel" type="SoleControlAssuranceLevelType"/>
<xs:simpleType name="SoleControlAssuranceLevelType">
        <xs:restriction base="xs:string">
                <xs:enumeration value="SCAL1"/>
                <xs:enumeration value="SCAL2"/>
        </xs:restriction>
 </xs:simpleType>
```

8 Các thông điệp tạo chữ ký số từ xa

8.1 Giới thiệu

Trong tiêu chuẩn này, các thông điệp thể hiện cách thức mà bất kỳ ứng dụng khách nào có thể tương tác với bất kỳ SCS nào tuân thủ đặc tả. Các điều sau định nghĩa các thông điệp mà ứng dụng khách và SCS có thể trao đổi. Đối với mỗi cặp yêu cầu và phản hồi, bảng tương ứng quy định thành phần nào trong số các thành phần được định nghĩa tại điều trước có thể được sử dụng và cung cấp các thông tin sau:

- tham chiếu đến mục nơi thành phần được quy định;
- mô tả ngắn gọn về thành phần;

- sự hiện diện của thành phần.

Giá trị được bao gồm trong cột "Sự hiện diện" của các bảng từ 36 đến 47 có ý nghĩa được định nghĩa trong bảng 35.

Bảng 35

Giá trị	Mô tả
M	Thành phần phải được bao gồm trong yêu cầu gửi tới hoặc phản hồi trả về từ SCS.
Tùy chọn	Thành phần có thể được bao gồm trong yêu cầu gửi tới hoặc phản hồi trả về từ SCS.
Bắt buộc có điều kiện	Thành phần phải được bao gồm trong yêu cầu hoặc phản hồi tùy thuộc vào việc xuất hiện của các điều kiện nhất định.

8.2 Các thông điệp tạo chữ ký số AdES

8.2.1 Thông điệp yêu cầu (A)

8.2.1.1 Thành phần yêu cầu tạo chữ ký số AdES

Thông điệp yêu cầu tạo chữ ký số AdES gửi đến một SCASC phải bao gồm các thành phần cho:

1) Nộp một trong hai các tài liệu cần ký hoặc SDR (đại diện tài liệu của chủ thể ký, ví dụ giá trị băm của tài liệu).

CHÚ THÍCH 1: Thông điệp có thể chứa một hoặc nhiều tài liệu và/hoặc một hoặc nhiều bản trình bày tài liệu để tạo chữ ký số. Một chữ ký AdES sẽ được tạo cho mỗi thành phần đầu vào này. Các thành phần khác được sử dụng để chọn loại chữ ký sẽ được tạo cho mỗi tài liệu hoặc hàm băm tài liệu.

2) Cung cấp ủy quyền thông tin xác thực dưới dạng dữ liệu kích hoạt chữ ký số.

3) Xác định một hoặc nhiều giao thức và/hoặc hồ sơ mà thông điệp yêu cầu tuân thủ. Thành phần đầu tiên trong số đó phải có URI sau đây làm giá trị, xác định thông điệp yêu cầu là thông điệp đã được xây dựng bằng cách sử dụng giao thức "tạo chữ ký số AdES" được quy định trong tài liệu này:

http://uri.etsi.org/19432/v1.1.1/signaturecreationprotocol#

CHÚ THÍCH 2: Giao thức được định nghĩa bởi tài liệu này có thể được kết hợp với các hồ sơ khác để yêu cầu các tính năng hoặc chức năng bổ sung do SCASC cung cấp miễn là các hồ sơ này không xung đột với các yêu cầu được quy định trong tài liệu này.

Thông điệp yêu cầu tạo chữ ký số AdES gửi đến SCASC có thể chứa các thành phần khác để yêu cầu các tính năng bổ sung. Mục 7.5 liệt kê một số thành phần tùy chọn này và chứa các tham chiếu đến các mục chỉ định các yêu cầu ngữ nghĩa cho từng thành phần.

Thông báo này bao gồm các thành phần sau.

Bảng 36

Tham chiếu.	Thành phần dùng cho	Sự hiện diện
7.2	lựa chọn chế độ hoạt động đồng bộ/không đồng bộ	Tùy chọn
7.3	định danh yêu cầu	Tùy chọn
7.4	xác thực thông tin xác thực	M
7.5	xác định dữ liệu tùy chọn cần trả về	Tùy chọn
7.6	xác định khoảng thời gian hiệu lực cho yêu cầu không đồng bộ	Tùy chọn
7.7	xác thực dịch vụ	Tùy chọn
7.8	định danh thông tin xác thực chữ ký	Bắt buộc có điều kiện
7.9	lựa chọn ngôn ngữ	Tùy chọn
7.10	nội dung thông tin xác thực chữ ký cần trả về	Tùy chọn
7.11	quản lý giao dịch ký số	Tùy chọn
7.12	lựa chọn chính sách dịch vụ	Tùy chọn
7.13	lựa chọn chính sách tạo chữ ký số	Tùy chọn
7.14	lựa chọn thuộc tính/đặc tính chữ ký tùy chọn	Tùy chọn
7.15	mã định danh giao thức	M
7.16	yêu cầu định dạng chữ ký số cụ thể	Tùy chọn
7.18	chỉ định URL phản hồi	Tùy chọn
7.19	gửi tài liệu hoặc giá trị băm để ký	M

Thành phần để định danh thông tin xác thực chữ ký có thể không được đưa vào thông điệp nếu người dùng chỉ có một thông tin xác thực chữ ký đã được xác thực trước đó.

8.2.1.2 Thành phần liên quan JSON

Phương thức signatures/signDoc phải được gọi để yêu cầu chữ ký của một hoặc nhiều tài liệu hoặc bản trình bày tài liệu. Phương thức này tính toán chữ ký của các tài liệu hoặc bản trình bày tài liệu được cung cấp trong đầu vào. Các thành phần để yêu cầu chữ ký của một tài liệu hoặc một bản trình bày tài liệu phải là tập hợp các tham số bắt buộc và tùy chọn, được quy định trong mục 8.2.1.1, để gọi chữ ký tài liệu bằng phương thức signatures/signDoc.

Mô hình xử lý

Máy chủ phải xử lý các thành phần nhận được cùng với các chữ ký/signDoc để tính toán chữ ký số từ xa của một hoặc nhiều tài liệu hoặc SDR như được chỉ ra trong mục 8.2.1.1 của tài liệu này.

8.2.1.3 Thành phần liên quan đến XML

Phần tử phải là thành phần chính để yêu cầu tạo chữ ký số AdES phải là phần tử gốc của thông điệp dss:SignRequest như được quy định trong OASIS DSS-v2.0.

Mô hình xử lý

Máy chủ phải xử lý các thành phần trong dss:SignRequest như được chỉ ra trong các mục tương ứng của OASIS DSS-v2.0.

Máy chủ phải xử lý từng phần tử con của các thành phần dss:OptionalInputs và dss:InputDocuments như được chỉ ra trong mục tương ứng của tiêu chuẩn này nếu phần tử con không được quy định trong bất kỳ tài liệu OASIS được tham chiếu nào. Nếu không, máy chủ phải tuân theo mô hình xử lý được định nghĩa trong tài liệu OASIS tương ứng.

8.2.2 Thông điệp phản hồi (B)

8.2.2.1 Thành phần phản hồi đối với các yêu cầu tạo chữ ký số AdES

Thông điệp phản hồi tạo chữ ký số AdES phát sinh từ một yêu cầu tạo chữ ký số AdES, phải bao gồm thành phần để thông báo kết quả tổng thể của hoạt động ký được yêu cầu bởi ứng dụng khách.

Thông điệp phản hồi tạo chữ ký số AdES có thể bao gồm một hoặc nhiều phần tử tài liệu đã ký hoặc chữ ký như được định nghĩa trong mục 7.21.

Thông báo này bao gồm các thành phần sau.

Bảng 37

Tham chiếu.	Thành phần dùng cho	Sự hiện diện
7.21	trả về tài liệu đã ký hoặc chữ ký	Tùy chọn
7.22	trả về thông tin chứng thư chữ ký số	Tùy chọn
7.24	thông báo kết quả xử lý	M
7.25	định danh chính sách dịch vụ	Tùy chọn
7.26	định danh phản hồi	Bắt buộc có điều kiện
7.27	định danh chính sách tạo chữ ký số	Tùy chọn

Mã định danh phản hồi có thể được bao gồm trong thông điệp phản hồi. Mã định danh phản hồi phải được bao gồm trong thông điệp phản hồi nếu một trong các điều kiện sau xảy ra:

1) Yêu cầu tạo chữ ký số AdES bao gồm thành phần chỉ ra chế độ hoạt động không đồng bộ tới SCASC, như được quy định trong mục 7.2.

2) SCASC chọn xử lý yêu cầu ở chế độ không đồng bộ.

8.2.2.2 Thành phần liên quan JSON

Thành phần phản hồi yêu cầu ký tài liệu phải là tập hợp các thành phần như được chỉ ra trong mục 8.2.2.1.

8.2.2.3 Thành phần liên quan đến XML

Phần tử đóng vai trò là thành phần chính để phản hồi yêu cầu tạo chữ ký số AdES phải là phần tử gốc của thông điệp dss2:SignResponse như được quy định trong OASIS DSS-v2.0.

8.3 Các thông điệp tạo giá trị chữ ký số (DSV)

8.3.1 Thông điệp yêu cầu (C)

8.3.1.1 Thành phần yêu cầu tạo các giá trị chữ ký số (DSV)

Trong kịch bản này, SCASC hoặc một ứng dụng trong môi trường của chủ thể ký chuẩn bị (các) DTBSR được gửi đến SSASC cùng với các thông tin khác cần thiết để tính toán chữ ký.

Thông điệp yêu cầu tạo các DSV gửi tới một SSASC phải chứa các thành phần cho:

1) Nộp các DTBSR.

CHÚ THÍCH 1: Thông báo có thể chứa một hoặc nhiều thể hiện của dữ liệu cần ký để tạo DSV. Một DSV sẽ được tạo cho mỗi thành phần đầu vào này.

2) Cung cấp ủy quyền thông tin xác thực dưới dạng dữ liệu kích hoạt chữ ký số.

3) Xác định một hoặc nhiều giao thức và/hoặc hồ sơ mà thông điệp yêu cầu tuân thủ. Thành phần đầu tiên trong số các thành phần đó phải có URI sau đây làm giá trị, xác định thông điệp yêu cầu là thông điệp đã được xây dựng bằng cách sử dụng giao thức "tạo giá trị chữ ký số" được quy định trong tài liệu này:

http://uri.etsi.org/19432/v1.1.1/dsvcreationprotocol#

CHÚ THÍCH 2: Giao thức được định nghĩa bởi tài liệu này có thể được kết hợp với các hồ sơ khác để yêu cầu các tính năng hoặc chức năng bổ sung do SSASC cung cấp miễn là các hồ sơ này không xung đột với các yêu cầu được quy định trong tài liệu này.

SSASC tạo ra các giá trị chữ ký số sử dụng khóa bí mật của chủ thể ký được lưu giữ trên SCDev và trả về các kết quả của hoạt động ký và thông tin để truy xuất các DSV.

Thông điệp yêu cầu tạo DSV gửi đến SSASC có thể chứa các thành phần khác để yêu cầu các tính năng bổ sung. Mục 7.5 liệt kê một số thành phần tùy chọn này và chứa các tham chiếu đến các mục quy định các yêu cầu ngữ nghĩa cho từng thành phần.

Thông báo này bao gồm các thành phần sau.

Bảng 38

Tham chiếu.	Thành phần dùng cho	Sự hiện diện
7.2	lựa chọn chế độ hoạt động đồng bộ/không đồng bộ	Tùy chọn
7.3	định danh yêu cầu	Tùy chọn
7.4	xác thực thông tin xác thực	M
7.5	xác định dữ liệu tùy chọn cần trả về	Tùy chọn
7.6	xác định khoảng thời gian hiệu lực cho yêu cầu không đồng bộ	Tùy chọn
7.7	xác thực dịch vụ	Tùy chọn
7.8	định danh thông tin xác thực chữ ký	Bắt buộc có điều kiện
7.9	lựa chọn ngôn ngữ	Tùy chọn

Tham chiếu.	Thành phần dùng cho	Sự hiện diện
7.10	nội dung thông tin xác thực chữ ký cần trả về	Tùy chọn
7.11	quản lý giao dịch ký số	Tùy chọn
7.12	lựa chọn chính sách dịch vụ	Tùy chọn
7.13	lựa chọn chính sách tạo chữ ký số	Tùy chọn
7.15	mã định danh giao thức	M
7.18	chỉ định URL phản hồi	Tùy chọn
7.19	gửi giá trị băm để ký	M

Thành phần định danh thông tin xác thực chữ ký có thể không được bao gồm trong thông điệp nếu người dùng đã được xác thực trước đó chỉ có một thông tin xác thực chữ ký.

8.3.1.2 Thành phần liên quan JSON

Thành phần để yêu cầu chữ ký trên một DTBSR phải là tập hợp các tham số bắt buộc để gọi chữ ký thông qua phương thức signatures/signHash như được quy định trong tiêu chuẩn CSC. Thành phần chính sách tạo chữ ký số có thể được sử dụng để chỉ định thuật toán chữ ký số và các tham số thuật toán chữ ký số nếu có, thay thế cho các tham số signAlgo và signAlgoParams được định nghĩa trong tiêu chuẩn CSC.

Mô hình xử lý

Máy chủ phải xử lý các thành phần như được chỉ ra trong mô tả chữ ký/signHash của tiêu chuẩn CSC.

Máy chủ phải xử lý từng thành phần như được chỉ ra trong mục 8.3.1.1 của tài liệu này nếu phần tử con không được chỉ định trong mô tả chữ ký/signHash của tiêu chuẩn CSC.

8.3.1.3 Thành phần liên quan XML

Phần tử yêu cầu (các) chữ ký băm phải là phần tử gốc của thông điệp dss2:SignRequest.

Mô hình xử lý

Máy chủ phải xử lý các thành phần được kế thừa từ dsb:RequestBaseType như được chỉ ra trong mục (Xử lý cho Chữ ký XML), đặc biệt là trong biến thể cho <DocumentHash> của OASIS DSS-v2.0 ..

8.3.2 Thông điệp phản hồi (D)

8.3.2.1 Thành phần phản hồi đối với các yêu cầu tạo các giá trị chữ ký số (DSV)

Thông điệp phản hồi tạo chữ ký số DSV phát sinh từ một yêu cầu tạo DSV, phải bao gồm thành phần để thông báo kết quả tổng thể của thao tác ký được ứng dụng khách yêu cầu.

Thông báo phản hồi tạo DSV có thể bao gồm một hoặc nhiều phần tử DSV như được định nghĩa trong mục 7.29. Thông báo này bao gồm các thành phần sau.

Bảng 39

Tham chiếu.	Thành phần dùng cho	Sự hiện diện
7.22	trả về thông tin chứng thư chữ ký số	Tùy chọn
7.24	thông báo kết quả xử lý	M
7.25	định danh chính sách dịch vụ	Tùy chọn
7.26	định danh phản hồi	Bắt buộc có điều kiện
7.27	định danh chính sách tạo chữ ký số	Tùy chọn
7.29	trả về DSV	Tùy chọn

Mã định danh phản hồi có thể được bao gồm trong thông điệp phản hồi. Mã định danh phản hồi phải được bao gồm trong thông điệp phản hồi nếu một trong các điều kiện sau xảy ra:

1) Yêu cầu tạo DSV bao gồm thành phần chỉ ra chế độ hoạt động không đồng bộ tới SCASC, như được quy định trong mục 7.2.

2) SSASC lựa chọn xử lý yêu cầu ở chế độ không đồng bộ.

8.3.2.2 Thành phần liên quan JSON

Phản hồi cho yêu cầu chữ ký băm (hash) phải bao gồm tập hợp các tham số được trả về trong phản hồi của phương thức signatures/signHash như được quy định trong tiêu chuẩn CSC.

8.3.2.3 Thành phần liên quan đến XML

Phần tử để phản hồi yêu cầu ký DTBS(s) phải là phần tử gốc dss2:SignResponse như được chỉ ra trong mục 8.5.1 và trong các đặc tả kỹ thuật OASIS DSS-v2.0 .

8.4 Các thông điệp phục vụ xử lý không đồng bộ (E)

8.4.1 Thành phần quản lý các yêu cầu đang chờ xử lý (pending-requests)

Thành phần này phải quản lý các thông điệp để yêu cầu SCS trả về các phản hồi tương ứng với các yêu cầu tạo chữ ký số (ban đầu) hoặc DSV đã gửi trước đó, được định nghĩa trong các mục 8.2.1 và 8.3.1, khi được SCS xử lý ở chế độ không đồng bộ. Các yêu cầu loại này sau đây được gọi là yêu cầu đang chờ xử lý.

Trong xử lý không đồng bộ, một ứng dụng khách gửi yêu cầu tạo chữ ký số hoặc DSV ban đầu đến máy chủ. Yêu cầu ban đầu có thể chứa, trong số những thứ khác, một thành phần mà qua đó chế độ hoạt động không đồng bộ được yêu cầu gửi đến SCS, như được quy định trong mục 7.2 và một mã định danh yêu cầu được tạo bởi ứng dụng khách, như được quy định trong mục 7.3.

Máy chủ có thể trả về một phản hồi cho biết rằng yêu cầu tạo chữ ký số đã được chấp nhận nhưng nó chưa được hoàn thành, hoặc do ứng dụng khách đã yêu cầu chế độ hoạt động không đồng bộ tới SCS hoặc do SCS đã chọn thực hiện thao tác được yêu cầu ở chế độ không đồng bộ. Trong phản hồi ban đầu này, SCS phải truyền một mã định danh phản hồi, như được quy định trong mục 7.26. Nếu yêu cầu ban đầu chứa mã định danh yêu cầu, cả ứng dụng khách và SCS có thể tương quan mã định danh phản hồi này với mã định danh yêu cầu ban đầu.

Theo mô hình xử lý này, ứng dụng khách, sau yêu cầu ban đầu, có thể gửi một yêu cầu đang chờ xử lý (pending-request) đến SCS. Yêu cầu đang chờ xử lý này phải bao gồm trong thành phần định danh yêu cầu, như được định nghĩa trong mục 7.3, giá trị của mã định danh phản hồi đã được SCS trả về trước đó trong phản hồi của nó đối với yêu cầu tạo chữ ký số ban đầu. Giá trị mã định danh phản hồi này cho phép SCS liên kết yêu cầu đang chờ xử lý này với yêu cầu tạo chữ ký số ban đầu. SCS phải trả về kết quả tạo chữ ký số hoặc một lần nữa là chỉ báo "chưa hoàn thành".

Nếu mục sau xảy ra, ứng dụng khách có thể gửi các yêu cầu tiếp theo cho đến khi SCS trả về một phản hồi với kết quả tạo chữ ký số.

Thông điệp yêu cầu đang chờ xử lý phải chứa các thành phần cho:

1) Xác định yêu cầu là một yêu cầu đang chờ xử lý liên quan đến yêu cầu tạo chữ ký số ban đầu hoặc DSV. Thành phần được chỉ định trong mục 7.3 phải được sử dụng để bao gồm định danh phản hồi xác định yêu cầu đang chờ xử lý.

2) Xác định một hoặc nhiều giao thức và/hoặc hồ sơ mà thông điệp yêu cầu đang chờ xử lý tuân thủ. Thành phần đầu tiên trong số các thành phần đó phải có URI sau đây làm giá trị, xác định thông điệp yêu cầu đang chờ xử lý là một thông điệp đã được xây dựng bằng cách sử dụng giao thức "xử lý không đồng bộ" được quy định trong tài liệu này:

http://uri.etsi.org/19432/v1.1.1/asynchronousprotocol#

CHÚ THÍCH: Giao thức được định nghĩa bởi tài liệu này có thể được kết hợp với các hồ sơ khác để yêu cầu các tính năng hoặc chức năng bổ sung do SCS cung cấp, miễn là các hồ sơ này không xung đột với các yêu cầu được quy định trong tài liệu này.

Phản hồi cho một yêu cầu đang chờ xử lý có định dạng giống như phản hồi cho yêu cầu tạo chữ ký số hoặc DSV ban đầu. Một thông điệp yêu cầu đang chờ xử lý bao gồm các thành phần sau.

Bảng 40

Tham chiếu.	Thành phần dùng cho	Sự hiện diện
7.3	định danh yêu cầu/kết quả truy vấn chữ ký	M
7.7	xác thực dịch vụ	Tùy chọn
7.9	lựa chọn ngôn ngữ	Tùy chọn

Tham chiếu.	Thành phần dùng cho	Sự hiện diện
7.15	mã định danh giao thức	M

8.4.2 Thành phần liên quan đến JSON

Yếu tố phải cho SCS biết rằng ứng dụng khách đang yêu cầu phản hồi tương ứng với một yêu cầu đã gửi trước đó (ban đầu) (như một phần của giao thức không đồng bộ) phải là tập hợp các tham số bắt buộc và tùy chọn được định nghĩa trong mục 8.4.1 để gọi phương thức signatures/signPolling.

Mô hình xử lý

Máy chủ phải xử lý từng thành phần như được chỉ ra trong mục 8.4.1.

Máy chủ phải kiểm tra việc hoàn thành các hoạt động liên quan đến yêu cầu được xác định bởi thuộc tính requestID và phản hồi tương ứng, trả về các DSV đã tạo hoặc tài liệu đã ký hoặc chữ ký hoặc chỉ báo rằng các hoạt động chưa hoàn thành hoặc một mã lỗi (ví dụ vì yêu cầu không thể hoàn thành hoặc vì thời gian cho phép yêu cầu kết quả đã hết hạn).

8.4.3 Thành phần liên quan đến XML

Phần tử phải chỉ ra cho SCS rằng ứng dụng khách đang yêu cầu phản hồi tương ứng với một yêu cầu đã gửi trước đó (ban đầu) (như một phần của giao thức không đồng bộ) phải là phần tử dss2:PendingRequest như được quy định trong OASIS DSS-v2.0.

8.5 Thông điệp danh sách chứng thư chữ ký số

8.5.1 Thông điệp yêu cầu (F)

8.5.1.1 Thành phần yêu cầu danh sách chứng thư chữ ký số

Thông điệp yêu cầu danh sách chứng thư chữ ký số của một chủ thể ký phải chứa thành phần để:

1) Xác định một hoặc nhiều giao thức và/hoặc hồ sơ mà thông điệp yêu cầu tuân thủ. Thành phần đầu tiên trong số các thành phần đó phải có URI sau đây làm giá trị, xác định thông điệp yêu cầu là một thông điệp đã được xây dựng bằng cách sử dụng giao thức "danh sách chứng thư chữ ký số" được quy định trong tài liệu này:

http://uri.etsi.org/19432/v1.1.1/certificateslistprotocol#

CHÚ THÍCH: Giao thức được định nghĩa bởi tài liệu này có thể được kết hợp với các hồ sơ khác để yêu cầu các tính năng hoặc chức năng bổ sung do SCS cung cấp miễn là các hồ sơ này không xung đột với các yêu cầu được quy định trong tài liệu này.

Một chủ thể ký có thể có một hoặc nhiều thông tin xác thực được liên kết trong một định danh chủ thể ký duy nhất. Thông báo này bao gồm các thành phần sau.

Bảng 41

Tham chiếu.	Thành phần dùng cho	Sự hiện diện
7.3	định danh yêu cầu	Tùy chọn
7.7	xác thực dịch vụ	Tùy chọn
7.9	lựa chọn ngôn ngữ	Tùy chọn
7.10	nội dung chuỗi chứng thư cần trả về	Tùy chọn
7.15	mã định danh giao thức	M
7.17	định danh chủ thể ký	Bắt buộc có điều kiện

Thành phần định danh chủ thể ký có thể không được bao gồm trong thông điệp nếu nó đã được ngầm định trong xác thực dịch vụ đã thực hiện.

8.5.1.2 Thành phần liên quan đến JSON

Thành phần để truy xuất thông tin xác thực phải là tập hợp các tham số được yêu cầu bởi phương thức credentials/list như được quy định trong tiêu chuẩn CSC.

Mô hình xử lý

Máy chủ phải xử lý các thành phần như được chỉ ra trong mô tả thông tin xác thực/danh sách của tiêu chuẩn CSC.

Máy chủ phải xử lý từng thành phần như được chỉ ra trong mục 8.5.1.1 của tài liệu này nếu thành phần con không được quy định trong bất kỳ tiêu chuẩn CSC tham chiếu nào . Ngược lại, máy chủ phải tuân theo mô hình xử lý được định nghĩa trong tiêu chuẩn CSC tương ứng.

8.5.1.3 Thành phần liên quan đến XML

Phần tử chính để yêu cầu danh sách chứng thư chữ ký số phải là phần tử gốc của thông điệp etsisig:InformationRequest.

Phần tử etsisig:InformationRequest được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết tại mục A.2.

Phần tử etsisig:SignerIdentity, phần tử con của phần tử etsisig:OptionalInputs phải được thiết lập để xác định chủ thể ký mà danh sách các thông tin xác thực chữ ký đang được yêu cầu.

Mô hình xử lý

Máy chủ phải xử lý các thành phần được kế thừa từ phần tử etsisig:SignerIdentity để truy xuất và trả về danh sách thông tin xác thực liên quan đến định danh người dùng.

8.5.2 Thông điệp phản hồi (G)

8.5.2.1 Thành phần phản hồi đối với yêu cầu danh sách chứng thư chữ ký số

Thông điệp phản hồi danh sách chứng thư chữ ký số, phát sinh từ yêu cầu liệt kê chứng thư chữ ký số, phải bao gồm thành phần để thông báo kết quả tổng thể của thao tác được ứng dụng khách yêu cầu.

Thông điệp phản hồi danh sách chứng thư chữ ký số có thể bao gồm một hoặc nhiều phần tử chứng thư chữ ký số như được định nghĩa trong mục 7.23. Thông điệp này bao gồm các thành phần sau.

Bảng 42

Tham chiếu.	Thành phần dùng cho	Sự hiện diện
7.23	trả về danh sách chứng thư chữ ký số	Tùy chọn
7.24	thông báo kết quả xử lý	M

SCS phải trả về lỗi trong trường hợp yêu cầu lấy danh sách chứng thư chữ ký số được liên kết với một chủ thể ký khác với người đã xác thực với dịch vụ.

8.5.2.2 Thành phần liên quan JSON

Phản hồi cho yêu cầu truy xuất danh sách thông tin xác thực của người dùng phải bao gồm tập hợp các kết quả được quy định trong mục 8.5.2.1 như được định nghĩa trong các mục 7.23.2 và 7.24.2.

8.5.2.3 Thành phần liên quan XML

Phần tử đóng vai trò là thành phần chính để phản hồi danh sách chứng thư chữ ký số phải là phần tử gốc của thông điệp etsisig:InformationResponse.

Phần tử etsisig:InformationResponse được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết tại mục A.2.

Phần tử con ds:KeyInfo của phần tử etsisig:OptionalOutputs phải trả về danh sách chứng thư chữ ký số được yêu cầu.

8.6 Các thông điệp truy xuất thông tin xác thực chữ ký

8.6.1 Thông điệp yêu cầu (H)

8.6.1.1 Thành phần yêu cầu thông tin xác thực chữ ký

Thông điệp để yêu cầu thông tin về một thông tin xác thực chữ ký gửi đến SCS phải chứa các thành phần cho:

1) Xác định thông tin xác thực chữ ký.

2) Xác định một hoặc nhiều giao thức và/hoặc hồ sơ mà thông điệp yêu cầu tuân thủ. Thành phần đầu tiên trong số đó phải có URI sau đây làm giá trị, xác định thông điệp yêu cầu là một thông điệp được xây dựng bằng giao thức "thông tin xác thực" được quy định trong tài liệu này: http://uri.etsi.org/19432/v1.1.1/credentialinfoprotocol#

CHÚ THÍCH: Giao thức được định nghĩa bởi tài liệu này có thể được kết hợp với các hồ sơ khác để yêu cầu các tính năng hoặc chức năng bổ sung do SSASC cung cấp, miễn là các hồ sơ này không xung đột với các yêu cầu được quy định trong tài liệu này.

Thông điệp yêu cầu thông tin xác thực chữ ký gửi đến SCS có thể chứa các thành phần khác để yêu cầu các tính năng bổ sung. Mục 7.5 liệt kê một số thành phần tùy chọn này và chứa các tham chiếu đến các mục quy định yêu cầu ngữ nghĩa cho từng thành phần.

Thông báo này bao gồm các thành phần sau.

Bảng 43

Tham chiếu.	Thành phần dùng cho	Sự hiện diện
7.3	định danh yêu cầu	Tùy chọn
7.5	xác định dữ liệu tùy chọn cần trả về	Tùy chọn
7.7	xác thực dịch vụ	Tùy chọn
7.8	định danh thông tin xác thực chữ ký	Bắt buộc có điều kiện
7.9	lựa chọn ngôn ngữ	Tùy chọn
7.10	nội dung thông tin xác thực chữ ký cần trả về	Tùy chọn
7.15	mã định danh giao thức	M

Thành phần để xác định thông tin xác thực chữ ký có thể không được bao gồm trong thông điệp nếu người dùng đã được xác thực trước đó chỉ có một thông tin xác thực chữ ký.

8.6.1.2 Thành phần liên quan đến JSON

Thành phần để yêu cầu thông tin xác thực phải là tập hợp các tham số được quy định trong mục 8.6.1.1.

Mô hình xử lý

Máy chủ phải xử lý các thành phần như được chỉ ra trong mô tả thông tin xác thực/thông tin của tiêu chuẩn CSC.

Máy chủ phải xử lý từng thành phần như được chỉ ra trong mục 8.6.1.1 của tiêu chuẩn này nếu thành phần con không được quy định trong bất kỳ tiêu chuẩn CSC tham chiếu nào . Ngược lại, máy chủ phải tuân theo mô hình xử lý được định nghĩa trong tiêu chuẩn CSC tương ứng.

8.6.1.3 Thành phần liên quan đến XML

Phần tử chính để yêu cầu truy xuất thông tin xác thực chữ ký phải là phần tử gốc của thông điệp etsisig:InformationRequest.

Phần tử etsisig:InformationRequest được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", có vị trí được trình bày chi tiết trong mục A.2.

Phần tử con dss2:KeySelector của phần tử etsisig:InformationRequest phải được thiết lập để xác định thông tin xác thực chữ ký mà thông tin của nó cần được trả về làm đầu ra chính của hồ sơ.

8.6.2 Thông điệp phản hồi (I)

8.6.2.1 Thành phần phản hồi đối với yêu cầu thông tin xác thực chữ ký

Thông điệp phản hồi thông tin xác thực chữ ký phát sinh từ yêu cầu thông tin xác thực chữ ký phải bao gồm thành phần để thông báo kết quả tổng thể của hoạt động được ứng dụng khách yêu cầu.

Thông điệp phản hồi thông tin xác thực chữ ký có thể bao gồm một hoặc nhiều phần tử thông tin xác thực chữ ký như được định nghĩa trong mục 7.22.

Thông báo này bao gồm các thành phần sau.

Bảng 44

Tham chiếu.	Thành phần dùng cho	Sự hiện diện
7.22	trả về thông tin xác thực chữ ký	Tùy chọn
7.24	thông báo kết quả xử lý	M
7.28	trả về chế độ ủy quyền đối với thông tin xác thực chữ ký	Tùy chọn
7.30	trả về mức SCAL yêu cầu	Tùy chọn

8.6.2.2 Thành phần liên quan đến JSON

Phản hồi yêu cầu truy xuất thông tin xác thực chữ ký phải bao gồm tập hợp các kết quả được quy định trong mục 8.6.2.1 và được trả về như trong phản hồi của phương thức credentials/info được quy định trong tiêu chuẩn CSC.

8.6.2.3 Thành phần liên quan XML

Phần tử đóng vai trò là thành phần chính của phản hồi truy xuất thông tin xác thực chữ ký phải là phần tử gốc của thông điệp etsisig:InformationResponse.

Phần tử etsisig:InformationResponse được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết trong mục A.2.

Phần tử con ds:KeyInfo của phần tử etsisig:InformationResponse phải trả về chứng thư chữ ký số và thông tin khóa được yêu cầu.

8.7 Các thông điệp thông tin dịch vụ (J)

8.7.1 Thông điệp yêu cầu (J)

8.7.1.1 Thành phần yêu cầu thông tin dịch vụ

Thông điệp yêu cầu thông tin dịch vụ phải bao gồm thành phần cho:

1) Xác định một hoặc nhiều giao thức và/hoặc hồ sơ mà thông điệp yêu cầu tuân thủ. Thành phần đầu tiên trong số các thành phần đó phải có URI sau đây làm giá trị, xác định thông điệp yêu cầu là một thông điệp đã được xây dựng bằng giao thức "thông tin dịch vụ" được quy định trong tài liệu này:

http://uri.etsi.org/19432/v1.1.1/serviceinformationprotocol#

CHÚ THÍCH: Giao thức được định nghĩa bởi tài liệu này có thể được kết hợp với các hồ sơ khác để yêu cầu các tính năng hoặc chức năng bổ sung do SCS cung cấp, miễn là các hồ sơ này không xung đột với các yêu cầu được quy định trong tài liệu này.

Thông báo này bao gồm các thành phần sau.

Bảng 45

Tham chiếu.	Thành phần dùng cho	Sự hiện diện
7.9	lựa chọn ngôn ngữ	Tùy chọn
7.15	mã định danh giao thức	M

8.7.1.2 Thành phần liên quan đến JSON

Thành phần để yêu cầu thông tin dịch vụ phải là tập hợp các tham số được quy định trong mục 8.7.1.1.

Mô hình xử lý

Máy chủ phải xử lý các thành phần như được chỉ ra trong mô tả thông tin của tiêu chuẩn CSC.

Máy chủ phải xử lý từng thành phần như được chỉ ra trong mục 8.7.1.1 của tiêu chuẩn này nếu thành phần con không được quy định trong bất kỳ tiêu chuẩn CSC tham chiếu nào . Nếu không, máy chủ phải tuân theo mô hình xử lý được định nghĩa trong tiêu chuẩn CSC tương ứng.

8.7.1.3 Thành phần liên quan đến XML

Phần tử phải là thành phần chính để yêu cầu thông tin dịch vụ phải là phần tử gốc của thông điệp etsisig:InformationRequest.

Phần tử etsisig:InformationRequest được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết trong mục A.2.

Phần tử dsb:Language, phần tử con của phần tử etsisig:OptionalInputs, có thể được thiết lập để chọn ngôn ngữ và văn hóa.

8.7.2 Thông điệp phản hồi (K)

8.7.2.1 Thành phần để phản hồi các yêu cầu thông tin dịch vụ

Hồ sơ này bao gồm các thành phần sau.

Bảng 46

Tham chiếu.	Thành phần dùng cho	Sự hiện diện
7.20	trả về thông tin dịch vụ	M

8.7.2.2 Thành phần liên quan đến JSON

Phản hồi yêu cầu thông tin dịch vụ phải bao gồm tập hợp các tham số được quy định trong mục 8.7.2.1 và được trả về như trong phản hồi của phương thức info như được quy định trong tiêu chuẩn CSC.

8.7.2.3 Thành phần liên quan XML

Phần tử phải là thành phần chính để phản hồi thông tin dịch vụ phải là phần tử gốc của thông điệp etsisig:InformationResponse.

Phần tử etsisig:InformationResponse được định nghĩa trong tệp XML Schema "[XSDSIGCREATIONPROT]", vị trí của nó được trình bày chi tiết tại mục A.2.

etsisig:ServiceInformation, phần tử con của phần tử etsisig:OptionalOutputs phải trả về thông tin dịch vụ được yêu cầu.

8.8 Tóm tắt việc sử dụng các thành phần

A = Hồ sơ đối với yêu cầu chữ ký số (yêu cầu tạo chữ ký số AdES)

B = Hồ sơ đối với phản hồi chữ ký số (phản hồi tạo chữ ký số AdES)

C = Hồ sơ đối với yêu cầu giá trị chữ ký số (DSV)

D = Hồ sơ đối với phản hồi giá trị chữ ký số (DSV)

E = Hồ sơ đối với xử lý không đồng bộ

F = Hồ sơ đối với yêu cầu danh sách chứng thư chữ ký số

G = Hồ sơ đối với phản hồi danh sách chứng thư chữ ký số

H = Hồ sơ đối với yêu cầu truy xuất thông tin xác thực chữ ký

I = Hồ sơ đối với phản hồi thông tin xác thực chữ ký

J = Hồ sơ đối với yêu cầu thông tin dịch vụ

K = Hồ sơ đối với phản hồi thông tin dịch vụ

Bảng 47

Tham chiếu	Thành phần dùng cho:	A	B	C	D	E	F	G	H	I	J	K
7.2	Lựa chọn chế độ hoạt động đồng bộ/không đồng bộ	O		O								
7.3	Định danh yêu cầu	O		O		M	O			O		
7.4	Cấp quyền đối với thông tin xác thực chữ ký	O		O								
7.5	Xác định dữ liệu tùy chọn được trả về	O		O					O			
7.6	Xác định thời hạn hiệu lực đối với các yêu cầu không đồng bộ	O		O								
7.7	Xác thực dịch vụ	O		O		O	O			O		
7.8	Định danh thông tin xác thực chữ ký	C		C					C			
7.9	Lựa chọn ngôn ngữ	O		O		O	O			O		O
7.10	Nội dung thông tin xác thực chữ ký được trả về	O		O					O			
7.11	Quản lý các giao dịch chữ ký số	O		O								
7.12	Lựa chọn chính sách dịch vụ	O		O								
7.13	Lựa chọn chính sách tạo chữ ký số	O		O								
7.14	Lựa chọn các thuộc tính/tính chất chữ ký số tùy chọn	O										
7.15	Định danh giao thức	M		M		M	M			M		M
7.16	Yêu cầu các định dạng chữ ký số cụ thể	O										
7.17	Định danh chủ thể ký					C						
7.18	Xác định URL phản hồi	O		O								
7.19	Gửi tài liệu hoặc giá trị băm cần ký	M		M								
7.20	Trả về thông tin dịch vụ											M
7.21	Trả về các tài liệu đã ký hoặc các chữ ký số		O									
7.22	Trả về thông tin xác thực chữ ký		O		O					O		
7.23	Trả về danh sách các chứng thư chữ ký số					O						
7.24	Thông báo kết quả hoạt động		M		M			M			M	
7.25	Định danh chính sách dịch vụ		O		O							

7.26	Định danh phản hồi		C		C							
7.27	Định danh chính sách tạo chữ ký số		O		O							
7.28	Trả về chế độ cấp quyền đối với thông tin xác thực chữ ký						O					
7.29	Trả về giá trị chữ ký số				O							
7.30	Trả về mức bảo đảm kiểm soát duy nhất yêu cầu						O					

Phụ lục A

(quy định)

Tệp lược đồ XML và JSON

A.1 Vị trí tệp lược đồ JSON đối với "$schema" "http://uri.etsi.org/19432/v1.2.1/json#"

Tệp 19432-schema.json có trong tệp lưu trữ ts_119432v010201p0.zip đi kèm ETSI TS 119 432 V1.2.1 và có tại https://forge.etsi.org/rep/esi/x19_432_sign_creation_protocol/raw/v1.2.1/19432-schema.json. Tệp này chứa các định nghĩa phần tử và kiểu trong lược đồ JSON có giá trị "$schema" là "http://uri.etsi.org/19432/v1.2.1/json#".

A.2 Vị trí tệp lược đồ XML đối với không gian tên http://uri.etsi.org/19432/v1.1.1#

Bốn tệp etsi-org-19432-xmlSchema-common.xsd, etsi-org-19432-xmlSchema-dsv-creation.xsd, etsi-org-19432-xmlSchema-service-information.xsd và etsi-org-19432-xmlSchema-signature-creation.xsd chứa các định nghĩa phần tử và kiểu trong không gian tên có URI http://uri.etsi.org/19432/v1.1.1#. Các tệp này có trong tệp lưu trữ ts_119432v010201p0.zip đi kèm ETSI TS 119 432 V1.2.1 và được công bố tại các địa chỉ sau:

https://forge.etsi.org/rep/esi/x19_432_sign_creation_protocol/raw/v1.1.1/etsi-org-19432-xmlSchema-common.xsd

https://forge.etsi.org/rep/esi/x19_432_sign_creation_protocol/raw/v1.1.1/etsi-org-19432-xmlSchema-dsv-creation.xsd

https://forge.etsi.org/rep/esi/x19_432_sign_creation_protocol/raw/v1.1.1/etsi-org-19432-xmlSchema-service-information.xsd

https://forge.etsi.org/rep/esi/x19_432_sign_creation_protocol/raw/v1.1.1/etsi-org-19432-xmlSchema-signature-creation.xsd

Phụ lục B

(tham khảo)

Tệp mô tả OpenAPI™

Tệp mô tả OpenAPI 3.0 (19432-openapi.yaml), theo định nghĩa của OpenAPI Initiative (OAI), có trong tệp lưu trữ ts_119432v010201p0.zip đi kèm ETSI TS 119 432 V1.2.1 và có tại https://forge.etsi.org/rep/esi/x19_432_sign_creation_protocol/raw/v1.2.1/19432-openapi.yaml.

Tệp này chứa các định nghĩa lược đồ JSON cho từng thành phần và mô tả từng thông điệp của giao thức được quy định trong tiêu chuẩn này.

Phụ lục C

(tham khảo)

Thư mục tài liệu tham khảo

ETSI TS 119 441, Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services.

ETSI TS 119 442, Electronic signatures and infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services.

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

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

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