TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN XXXX:2026

Xuất bản lần 1

GIAO DỊCH ĐIỆN TỬ - YÊU CẦU VỀ CHÍNH SÁCH VÀ AN TOÀN ĐỐI VỚI TỔ CHỨC CUNG CẤP DỊCH VỤ LƯU TRỮ VÀ XÁC NHẬN TÍNH TOÀN VẸN CỦA THÔNG ĐIỆP DỮ LIỆU

Electronic transactions - Policy and security requirements for providers of data-message preservation and integrity validation services

HÀ NỘI - 2026

Mục lục

Lời giới thiệu 7
1 Phạm vi áp dụng 8
2 Tài liệu viện dẫn 8
3 Thuật ngữ, định nghĩa, ký hiệu và chữ viết tắt 9
3.1 Thuật ngữ và định nghĩa 9
3.2 Chữ viết tắt 16
3.3 Ký hiệu và quy ước 17
4 Khái niệm chung 17
4.1 Mô hình lưu trữ của dịch vụ bảo quản 17
4.1.1 Tổng quan 17
4.1.2 Dịch vụ bảo quản có lưu trữ [WST] 18
4.1.3 Dịch vụ bảo quản có lưu trữ tạm thời [WTS] 19
4.1.4 Dịch vụ bảo quản không lưu trữ [WOS] 20
4.2 Mục tiêu chức năng 21
4.3 Tài liệu áp dụng đối với dịch vụ bảo quản 22
4.3.1 Quy chế chứng thực dịch vụ bảo quản 22
4.3.2 Chính sách dịch vụ bảo quản 22
4.3.3 Lược đồ bảo quản và hồ sơ bảo quản 23
4.3.4 Chính sách bằng chứng bảo quản 23
4.3.5 Chính sách xác thực chữ ký số 24
4.4 Thời hạn dự kiến của bằng chứng 24
4.5 Thời hạn bảo quản 25
5 Đánh giá rủi ro 25
6 Chính sách và quy chế chứng thực 26
6.1 Quy chế chứng thực dịch vụ bảo quản 26
6.2 Điều khoản và điều kiện 26
6.3 Chính sách an toàn thông tin 27
6.4 Hồ sơ bảo quản 27
6.5 Chính sách bằng chứng bảo quản 29
6.6 Chính sách xác thực chữ ký số 29
6.7 Thỏa thuận với thuê bao 30
7 Quản lý và vận hành tổ chức cung cấp dịch vụ bảo quản 30
7.1 Tổ chức nội bộ 30
7.2 Nguồn nhân lực 30
7.3 Quản lý tài sản 30
7.4 Kiểm soát truy cập 30
7.5 Kiểm soát mật mã 30

7.6 An toàn vật lý và môi trường....31
7.7 An toàn vận hành....31
7.8 An toàn mạng....31
7.9 Quản lý sự cố....31
7.10 Thu thập bằng chứng....31
7.11 Quản lý tính liên tục hoạt động....32
7.12 Chấm dứt hoạt động và kế hoạch chấm dứt....32
7.13 Tuân thủ....32
7.14 Giám sát mật mã....32
7.15 Tăng cường bằng chứng....32
7.16 Gói xuất - nhập....33
7.17 Chuỗi cung ứng....33
8 Giao thức vận hành và thông báo....33
8.1 Giao thức bảo quản....33
8.2 Giao thức thông báo....35
9 Quy trình bảo quản....35
9.1 Lưu trữ dữ liệu và bằng chứng bảo quản....35
9.2 Bằng chứng bảo quản....35
9.3 Bảo quản chữ ký số....36
Thư mục tài liệu tham khảo....38

Lời nói đầu

TCVN XXXX:2026 được xây dựng trên cơ sở ETSI TS 119 511 V1.2.1 (2025-10) của Viện Tiêu chuẩn Viễn thông châu Âu (ETSI), có điều chỉnh và bổ sung để phù hợp với mục đích áp dụng tại Việt Nam.

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

Lời giới thiệu

Chữ ký số, dấu thời gian và các bằng chứng dựa trên cơ chế mật mã ngày càng được sử dụng rộng rãi trong giao dịch điện tử. Tuy nhiên, mức độ an toàn và sự phù hợp của thuật toán mật mã, độ dài khóa, hàm băm và công nghệ xác thực thay đổi theo thời gian.

Việc duy trì khả năng xác thực chữ ký số, trạng thái hiệu lực của chữ ký số và bằng chứng về sự tồn tại của dữ liệu trong thời gian dài đòi hỏi các cơ chế bảo quản phù hợp. Các cơ chế này có thể bao gồm thu thập và bảo vệ dữ liệu xác thực, sử dụng dấu thời gian hoặc bản ghi bằng chứng, giám sát mức độ an toàn của thuật toán và tăng cường bằng chứng trước khi cơ chế mật mã hiện tại suy yếu.

Tiêu chuẩn này sử dụng thuật ngữ “dịch vụ bảo quản” để gọi tắt dịch vụ lưu trữ và xác nhận tính toàn vẹn của thông điệp dữ liệu được thực hiện bằng kỹ thuật chữ ký số. Dịch vụ bảo quản có thể có lưu trữ, có lưu trữ tạm thời hoặc không lưu trữ dữ liệu; vì vậy, “bảo quản” trong tiêu chuẩn này không đồng nhất với chức năng lưu trữ dữ liệu thông thường.

Tiêu chuẩn quy định các yêu cầu về chính sách, quản lý, vận hành và an toàn đối với tổ chức cung cấp dịch vụ bảo quản, làm cơ sở cho việc triển khai, giám sát và đánh giá sự phù hợp của dịch vụ.

Giao dịch điện tử - Yêu cầu về chính sách và an toàn đối với tổ chức cung cấp dịch vụ lưu trữ và xác nhận tính toàn vẹn của thông điệp dữ liệu

Electronic transactions - Policy and security requirements for providers of data-message preservation and integrity validation services

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu về chính sách và an toàn đối với tổ chức cung cấp dịch vụ bảo quản dài hạn chữ ký số và dữ liệu tổng quát, bao gồm dữ liệu đã ký số hoặc chưa ký số, bằng kỹ thuật chữ ký số.

Tiêu chuẩn này áp dụng cho dịch vụ nhằm duy trì trong thời gian dài khả năng xác thực chữ ký số và trạng thái hiệu lực của chữ ký số, cung cấp bằng chứng về sự tồn tại của dữ liệu, và/hoặc tăng cường bằng chứng bảo quản do bên ngoài cung cấp. Tiêu chuẩn bao quát các mô hình dịch vụ có lưu trữ, có lưu trữ tạm thời và không lưu trữ.

Tiêu chuẩn này không quy định việc chuyển đổi dữ liệu gốc sang đối tượng dữ liệu khác có nội dung và ngữ nghĩa tương đương nhằm xử lý sự lỗi thời của định dạng dữ liệu hoặc phần mềm hiển thị.

2 Tài liệu viện dẫn

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

ETSI EN 319 401, *Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers* (Chữ ký điện tử và hạ tầng tin cậy (ESI) – Yêu cầu chung về chính sách đối với tổ chức cung cấp dịch vụ tin cậy).

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

ETSI EN 319 411-1, *Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements* (Chữ ký điện

tử và hạ tầng tin cậy (ESI) – Yêu cầu về chính sách và an toàn đối với tổ chức cung cấp dịch vụ tin cậy phát hành chứng thư chữ ký số – Phần 1: Yêu cầu chung).

ETSI TS 119 512, *Electronic Signatures and Trust Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services* (Chữ ký điện tử và hạ tầng tin cậy (ESI) – Giao thức dành cho tổ chức cung cấp dịch vụ tin cậy cung cấp dịch vụ bảo quản dữ liệu dài hạn).

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

EN 419241-2, *Trustworthy Systems Supporting Server Signing; Part 2: Protection Profile for QSCD for Server Signing (CEN)* (Hệ thống tin cậy hỗ trợ ký số trên máy chủ – Phần 2: Hồ sơ bảo vệ đối với thiết bị tạo chữ ký số đủ điều kiện dùng cho ký số trên máy chủ).

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

ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security* (Công nghệ thông tin – Kỹ thuật an toàn – Tiêu chí đánh giá an toàn công nghệ thông tin).

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules* (Công nghệ thông tin – Kỹ thuật an toàn – Yêu cầu an toàn đối với mô-đun mật mã).

IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* (Hạ tầng khóa công khai X.509 trên Internet – Hồ sơ chứng thư chữ ký số và danh sách chứng thư chữ ký số bị thu hồi).

IETF RFC 3161, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)* (Hạ tầng khóa công khai X.509 trên Internet – Giao thức dấu thời gian).

IETF RFC 4998, *Evidence Record Syntax (ERS)* (Cú pháp bản ghi bằng chứng).

IETF RFC 6283, *Extensible Markup Language Evidence Record Syntax (XMLERS)* (Cú pháp bản ghi bằng chứng sử dụng ngôn ngữ đánh dấu mở rộng).

3 Thuật ngữ, định nghĩa, ký hiệu và chữ viết tắt

3.1 Thuật ngữ và định nghĩa

3.1.1

Vùng chứa (container)

Đối tượng dữ liệu chứa một tập hợp các đối tượng dữ liệu và thông tin bổ sung tùy chọn mô tả các đối tượng dữ liệu được chứa, nội dung của chúng và mối quan hệ giữa chúng.

VÍ DỤ: Định dạng vùng chứa có thể dựa trên ZIP theo ISO/IEC 21320-1 hoặc XML. ASiC là một ví dụ của vùng chứa dựa trên ZIP.

CHÚ THÍCH 1: Thông tin bổ sung có thể bao gồm chữ ký số, dấu thời gian, bản ghi bằng chứng, dữ liệu xác thực (CRL, phản hồi OCSP) và báo cáo xác thực.

3.1.2

Đối tượng dữ liệu (data object)

Dữ liệu nhị phân hoặc dữ liệu octet thực tế được ứng dụng xử lý, ví dụ biến đổi, tính giá trị băm hoặc ký số, và có thể gắn với thông tin bổ sung như định danh, phương thức mã hóa, kích thước hoặc loại dữ liệu.

3.1.3

Vùng chứa đối tượng bảo quản dạng chênh lệch (delta preservation object container)

Vùng chứa đối tượng bảo quản đặc biệt mô tả sự khác biệt so với một vùng chứa đối tượng bảo quản đã tồn tại.

3.1.4

Kỹ thuật chữ ký số (digital signature techniques)

Các kỹ thuật dựa trên chữ ký số, dấu thời gian hoặc bản ghi bằng chứng.

3.1.5

Bản ghi bằng chứng (evidence record)

Đơn vị dữ liệu có thể được sử dụng để chứng minh sự tồn tại của một đối tượng dữ liệu được bảo quản hoặc một nhóm đối tượng dữ liệu được bảo quản tại một thời điểm xác định.

CHÚ THÍCH 1: Xem IETF RFC 4998, IETF RFC 6283 và ETSI TS 119 122-3.

3.1.6

Thời hạn dự kiến của bằng chứng (expected evidence duration)

Đối với dịch vụ bảo quản có lưu trữ tạm thời hoặc không lưu trữ, khoảng thời gian mà dịch vụ bảo quản dự kiến bằng chứng bảo quản có thể được sử dụng để đạt được mục tiêu bảo quản.

3.1.7

Gói xuất - nhập (export-import package)

Thông tin được trích xuất từ dịch vụ bảo quản, bao gồm đối tượng dữ liệu gửi (SubDO), bằng chứng bảo quản và siêu dữ liệu liên quan đến bảo quản, cho phép một dịch vụ bảo quản khác nhập thông tin và tiếp tục đạt được mục tiêu bảo quản.

3.1.8

Dài hạn (long-term)

Khoảng thời gian mà các thay đổi công nghệ có thể ảnh hưởng.

VÍ DỤ: Sự lỗi thời của thuật toán mật mã, kích thước khóa, hàm băm hoặc việc lộ khóa.

3.1.9

Bảo quản dài hạn (long-term preservation)

Việc kéo dài trạng thái hiệu lực của chữ ký số trong thời gian dài và/hoặc cung cấp bằng chứng về sự tồn tại của dữ liệu trong thời gian dài, bất chấp sự lỗi thời của thuật toán mật mã, độ dài khóa, hàm băm, việc khóa bị xâm phạm hoặc việc mất khả năng kiểm tra trạng thái hiệu lực của chứng thư chữ ký số.

3.1.10

Siêu dữ liệu (metadata)

Dữ liệu mô tả dữ liệu khác.

CHÚ THÍCH 1: Nguồn: ISO 14721:2012.

3.1.11

Giao thức thông báo (notification protocol)

Giao thức được dịch vụ bảo quản sử dụng để gửi thông báo tới máy khách dịch vụ bảo quản.

3.1.12

Máy khách dịch vụ bảo quản (preservation client)

Thành phần hoặc phần mềm tương tác với dịch vụ bảo quản thông qua giao thức bảo quản.

3.1.13

Bằng chứng bảo quản (preservation evidence)

Bằng chứng do dịch vụ bảo quản tạo ra, có thể được sử dụng để chứng minh một hoặc nhiều mục tiêu bảo quản đã được đáp ứng đối với một đối tượng bảo quản xác định.

3.1.14

Tăng cường bằng chứng bảo quản (preservation evidence augmentation)

Việc bổ sung dữ liệu vào bằng chứng bảo quản hiện có nhằm kéo dài thời hạn hiệu lực của bằng chứng đó.

VÍ DỤ: Thêm dấu thời gian mới bảo vệ dữ liệu xác thực bổ sung hoặc sử dụng hàm băm mạnh hơn.

3.1.15

Chính sách bằng chứng bảo quản (preservation evidence policy)

Tập hợp các quy tắc, quy định yêu cầu và quy trình nội bộ để tạo bằng chứng bảo quản hoặc quy định cách xác thực bằng chứng bảo quản.

3.1.16

Thời hạn lưu giữ bằng chứng bảo quản (preservation evidence retention period)

Là khoảng thời gian mà bằng chứng được tạo theo chế độ bất đồng bộ có thể được truy xuất từ dịch vụ bảo quản áp dụng đối với dịch vụ bảo quản có lưu trữ tạm thời [WTS].

3.1.17

Mục tiêu bảo quản (preservation goal)

Một trong các mục tiêu đạt được trong khoảng thời gian dài: duy trì trạng thái hiệu lực của chữ ký số, cung cấp bằng chứng về sự tồn tại của dữ liệu, hoặc tăng cường bằng chứng bảo quản do bên ngoài cung cấp.

CHÚ THÍCH 1: Dịch vụ bảo quản có thể đạt một hoặc nhiều mục tiêu.

3.1.18

Giao diện bảo quản (preservation interface)

Thành phần triển khai giao thức bảo quản ở phía dịch vụ bảo quản.

3.1.19

Danh mục bảo quản (preservation manifest)

Đối tượng dữ liệu trong vùng chứa đối tượng bảo quản, tham chiếu đến các đối tượng dữ liệu bảo quản, thông tin bổ sung hoặc siêu dữ liệu trong vùng chứa.

VÍ DỤ: Tệp bổ sung trong ASiC theo ETSI EN 319 162-1; versionManifest trong TR-ESOR-F; Phần tử manifest dạng XML trong vùng chứa dựa trên XML.

3.1.20

Đối tượng bảo quản (preservation object)

Đối tượng dữ liệu có kiểu được gửi tới, xử lý hoặc truy xuất từ dịch vụ bảo quản.

CHÚ THÍCH 1: Đối tượng bảo quản bao gồm đối tượng dữ liệu gửi, vùng chứa đối tượng bảo quản và bằng chứng bảo quản.

3.1.21

Vùng chứa đối tượng bảo quản (preservation object container)

Vùng chứa bao gồm một tập hợp các đối tượng dữ liệu và có thể bao gồm siêu dữ liệu liên quan, thông tin về các đối tượng dữ liệu và danh mục bảo quản mô tả nội dung và mối quan hệ giữa chúng.

3.1.22

Định danh đối tượng bảo quản (preservation object identifier)

Định danh duy nhất của một đối tượng bảo quản hoặc một tập hợp đối tượng bảo quản được gửi tới dịch vụ bảo quản.

3.1.23

Thời hạn bảo quản (preservation period)

Là khoảng thời gian mà dịch vụ duy trì việc bảo quản các đối tượng đã được gửi và các bằng chứng liên quan áp dụng đối với dịch vụ bảo quản có lưu trữ [WST].

CHÚ THÍCH 1: Các đối tượng bảo quản có thể được cập nhật trong thời hạn bảo quản.

3.1.24

Hồ sơ bảo quản (preservation profile)

Tập hợp các chi tiết triển khai được định danh duy nhất, liên quan đến một mô hình lưu trữ của dịch vụ bảo quản và một hoặc nhiều mục tiêu bảo quản, trong đó quy định cách thức tạo và xác thực các bằng chứng bảo quản.

CHÚ THÍCH 1: Xem 4.3 của tiêu chuẩn này và phần mô tả phiên bản máy có thể đọc được trong ETSI TS 119 512.

3.1.25

Giao thức bảo quản (preservation protocol)

Giao thức được sử dụng để trao đổi thông tin giữa dịch vụ bảo quản và máy khách dịch vụ bảo quản.

3.1.26

Lược đồ bảo quản (preservation scheme)

Tập hợp chung các quy trình và quy tắc liên quan đến một mô hình lưu trữ của dịch vụ bảo quản và một hoặc nhiều mục tiêu bảo quản, trong đó mô tả khái quát cách thức tạo và xác thực các bằng chứng bảo quản.

CHÚ THÍCH 1: Các hồ sơ bảo quản khác nhau có thể triển khai cùng một lược đồ bảo quản.

CHÚ THÍCH 2: Một lược đồ bảo quản có thể được triển khai bởi một hoặc nhiều hồ sơ bảo quản.

3.1.27

Dịch vụ bảo quản (preservation service)

Là dịch vụ lưu trữ và xác nhận tính toàn vẹn của thông điệp dữ liệu

3.1.28

Tổ chức cung cấp dịch vụ bảo quản (preservation service provider)

Tổ chức cung cấp dịch vụ tin cậy cung cấp dịch vụ bảo quản.

3.1.29

Chính sách dịch vụ bảo quản (preservation service policy)

Chính sách dịch vụ tin cậy áp dụng cho dịch vụ bảo quản.

3.1.30

Quy chế chứng thực dịch vụ bảo quản (preservation service practice statement)

Quy chế chứng thực dịch vụ tin cậy áp dụng cho dịch vụ bảo quản.

3.1.31

Mô hình lưu trữ của dịch vụ bảo quản (preservation storage model)

Một trong các phương thức triển khai dịch vụ bảo quản: có lưu trữ, có lưu trữ tạm thời hoặc không lưu trữ.

3.1.32

Bên gửi dữ liệu bảo quản (preservation submitter)

Cá nhân hoặc tổ chức sử dụng máy khách dịch vụ bảo quản để gửi đối tượng dữ liệu.

3.1.33

Thuê bao dịch vụ bảo quản (preservation subscriber)

Cá nhân hoặc tổ chức bị ràng buộc theo thỏa thuận với tổ chức cung cấp dịch vụ bảo quản về các nghĩa vụ của thuê bao.

3.1.34

Bằng chứng về sự tồn tại (proof of existence)

Bằng chứng xác lập rằng một đối tượng đã tồn tại tại một thời điểm cụ thể.

3.1.35

Bằng chứng về tính toàn vẹn (proof of integrity)

Bằng chứng xác lập rằng dữ liệu không bị thay đổi kể từ khi được bảo vệ.

CHÚ THÍCH 1: Bằng chứng về sự tồn tại đòi hỏi và đồng thời hàm ý có bằng chứng về tính toàn vẹn.

3.1.36

Thiết bị mật mã an toàn (secure cryptographic device)

Thiết bị lưu giữ khóa bí mật của người dùng, bảo vệ khóa khỏi bị xâm phạm và thực hiện chức năng ký số hoặc giải mã thay mặt người dùng.

3.1.37

Người ký (signer)

Thực thể tạo ra chữ ký số.

3.1.38

Đối tượng dữ liệu gửi (submission data object)

Đối tượng dữ liệu gốc do máy khách dịch vụ bảo quản cung cấp.

CHÚ THÍCH 1: Khi máy khách dịch vụ bảo quản cung cấp vùng chứa đối tượng bảo quản (POC), POC là một đối tượng dữ liệu gửi.

3.1.39

Xác nhận thời gian (time assertion)

Dấu thời gian hoặc bản ghi bằng chứng.

3.1.40

Dấu thời gian (TimeStamp)

Dấu thời gian là 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.

Nguồn: Tài liệu tham khảo số [1]

3.1.41

Tổ chức cấp dấu thời gian (Time Stamping Authority)

Tổ chức cung cấp dịch vụ tin cậy cung cấp dịch vụ cấp dấu thời gian.

3.1.42

Dịch vụ cấp dấu thời gian (Time Stamping service)

Dịch vụ tin cậy cung cấp dịch vụ cấp dấu thời gian, gắn thông tin về thời gian vào thông điệp dữ liệu.

Nguồn: Tài liệu tham khảo số [1]

3.1.43

Dữ liệu xác thực (validation data)

Dữ liệu được sử dụng để xác thực chữ ký số.

3.1.44

Bên thứ ba (relying party)

Bên tiếp nhận và dựa vào kết quả của dịch vụ tin cậy để đưa ra quyết định.

3.1.45

Thuê bao (subscriber)

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

3.1.46

Dịch vụ tin cậy (trust service)

Dịch vụ tin cậy bao gồm:

a) Dịch vụ cấp dấu thời gian;

b) Dịch vụ chứng thực thông điệp dữ liệu;

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

Nguồn: Tài liệu tham khảo số [1]

3.1.47

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

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

3.2 Chữ viết tắt

AdES	Advanced Electronic Signature	Chữ ký điện tử nâng cao
ASiC	Associated Signature Container	Vùng chứa chữ ký liên kết
AUG	Augmentation goal	Mục tiêu tăng cường bằng chứng bảo quản
CA	Certification Authority	Tổ chức cung cấp dịch vụ chứng thực chữ ký số
CSA	Certificate Status Authority	Tổ chức cung cấp thông tin trạng thái chứng thư chữ ký số
CRL	Certificate Revocation List	Danh sách chứng thư chữ ký số bị thu hồi
EAL	Evaluation Assurance Level	Mức bảo đảm đánh giá
OCSP	Online Certificate Status Protocol	Giao thức kiểm tra trạng thái chứng thư chữ ký số trực tuyến
OID	Object Identifier	Định danh đối tượng
PDS	Preservation of Digital Signatures	Bảo quản chữ ký số
PGD	Preservation of General Data	Bảo quản dữ liệu tổng quát
PO	Preservation Object	Đối tượng bảo quản
POC	Preservation Object Container	Vùng chứa đối tượng bảo quản
PRP	Preservation service Protocol	Giao thức dịch vụ bảo quản
PSP	Preservation Service Provider	Tổ chức cung cấp dịch vụ bảo quản
CP/CPS	—	Quy chế chứng thực dịch vụ bảo quản
SigS	Digital Signature creation Service	Dịch vụ tạo chữ ký số
SubDO	Submission Data Object	Đối tượng dữ liệu gửi
TSA	Time-Stamping Authority	Tổ chức cung cấp dịch vụ cấp dấu thời gian
TSP	Trust Service Provider	Tổ chức cung cấp dịch vụ tin cậy
URI	Uniform Resource Identifier	Định danh tài nguyên thống nhất
ValS	Validation Service	Dịch vụ xác thực chữ ký số
WOS	Without Storage	Dịch vụ bảo quản không lưu trữ
WST	With Storage	Dịch vụ bảo quản có lưu trữ

WTS	With Temporary Storage	Dịch vụ bảo quản có lưu trữ tạm thời

3.3 Ký hiệu và quy ước

Các yêu cầu, khuyến nghị hoặc sự cho phép trong tiêu chuẩn này được thể hiện như sau:

a) Điều khoản không kèm ký hiệu bổ sung áp dụng cho mọi tổ chức cung cấp dịch vụ bảo quản phù hợp với tiêu chuẩn này;

b) Điều khoản chỉ áp dụng trong điều kiện nhất định được đánh dấu "[CÓ ĐIỀU KIỆN]";

c) Điều khoản áp dụng cho nhóm dịch vụ bảo quản cụ thể được đánh dấu như sau:

- [WOS]: dịch vụ bảo quản không lưu trữ;
- [WTS]: dịch vụ bảo quản có lưu trữ tạm thời;
- [WST]: dịch vụ bảo quản có lưu trữ;
- [PDS]: bảo quản chữ ký số;
- [PGD]: bảo quản dữ liệu tổng quát;
- [PDS+PGD]: bảo quản kết hợp chữ ký số và dữ liệu tổng quát;
- [AUG]: tăng cường bằng chứng bảo quản được gửi tới dịch vụ.

4 Khái niệm chung

4.1 Mô hình lưu trữ của dịch vụ bảo quản

4.1.1 Tổng quan

Ba mô hình lưu trữ của dịch vụ bảo quản được phân biệt như sau:

1) Dịch vụ bảo quản có lưu trữ [WST]

Trong trường hợp này, dữ liệu cần bảo quản được dịch vụ bảo quản lưu trữ; bằng chứng bảo quản và dữ liệu được bảo quản được cung cấp theo yêu cầu cho máy khách dịch vụ bảo quản. Dịch vụ bảo quản lưu trữ một hoặc nhiều đối tượng dữ liệu gửi (SubDO), các đối tượng bảo quản (PO) được tạo từ SubDO và các bằng chứng bảo quản liên quan. PO được tạo từ SubDO bằng cách tăng cường hoặc bằng cách xây dựng vùng chứa đối tượng bảo quản (POC). Các điều khoản áp dụng riêng cho mô hình này được đánh dấu [WST], xem 3.3.

2) Dịch vụ bảo quản có lưu trữ tạm thời [WTS]

Trong trường hợp này, dữ liệu cần bảo quản được lưu trữ ở phía máy khách dịch vụ bảo quản. Dịch vụ bảo quản chỉ lưu trữ tạm thời dữ liệu hoặc giá trị băm của dữ liệu, muộn nhất đến khi bằng chứng bảo quản được tạo. Bằng chứng được tạo theo chế độ bất đồng bộ và được lưu giữ trong một khoảng thời gian xác định để máy khách truy xuất. Các điều khoản áp dụng riêng cho mô hình này được đánh dấu [WTS], xem 3.3.

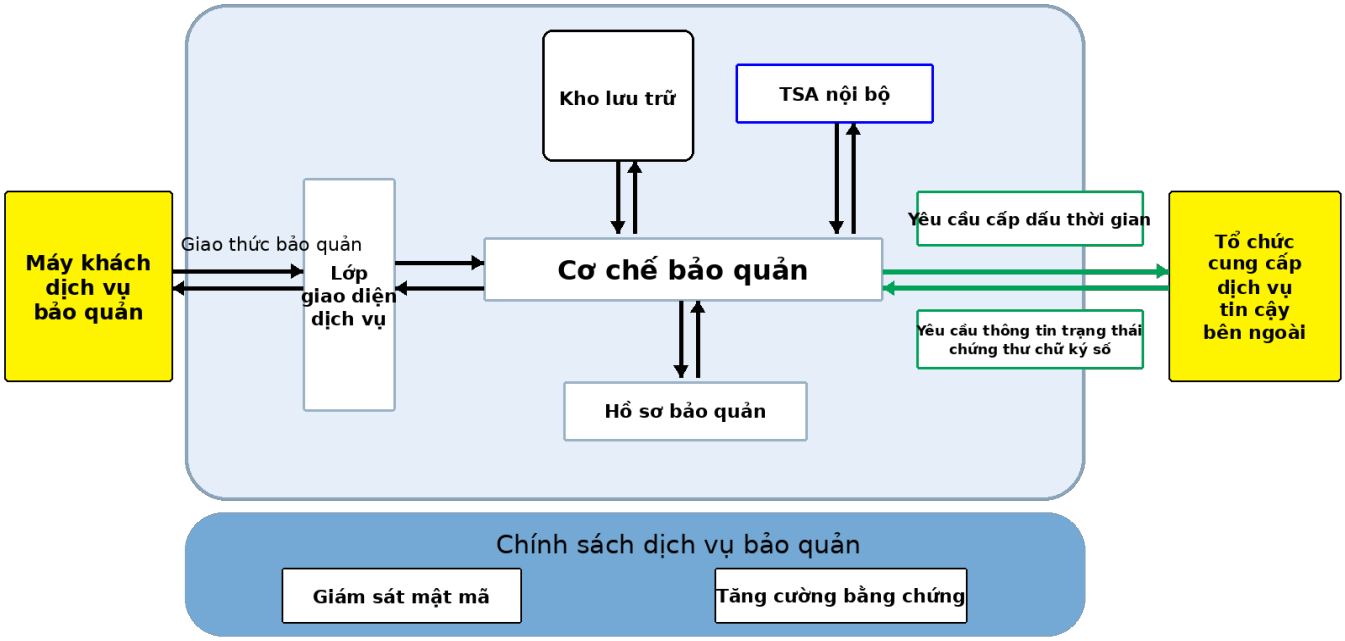
VÍ DỤ: Bản ghi bằng chứng có thể được tạo hằng ngày từ các giá trị băm của dữ liệu cần bảo quản được cung cấp trong vòng 24 giờ.

3) Dịch vụ bảo quản không lưu trữ [WOS]

Trong trường hợp này, dữ liệu cần bảo quản được lưu trữ ở phía máy khách dịch vụ bảo quản. Dịch vụ bảo quản không lưu trữ SubDO hoặc bằng chứng bảo quản. Bằng chứng được tạo theo chế độ đồng bộ và được bao gồm trong phản hồi. Dịch vụ bảo quản chỉ lưu giữ dấu vết hoạt động để có thể cung cấp hồ sơ về các hoạt động đó. Các điều khoản áp dụng riêng cho mô hình này được đánh dấu [WOS], xem 3.3.

Tùy thuộc vào mô hình lưu trữ, dịch vụ bảo quản triển khai các quy trình khác nhau. Ba mô hình được minh họa tại Hình 1, Hình 2 và Hình 3.

4.1.2 Dịch vụ bảo quản có lưu trữ [WST]



Hình 1 - Mô hình chức năng của dịch vụ bảo quản có lưu trữ [WST]

Giao thức bảo quản cho phép máy khách dịch vụ bảo quản tương tác với giao diện bảo quản.

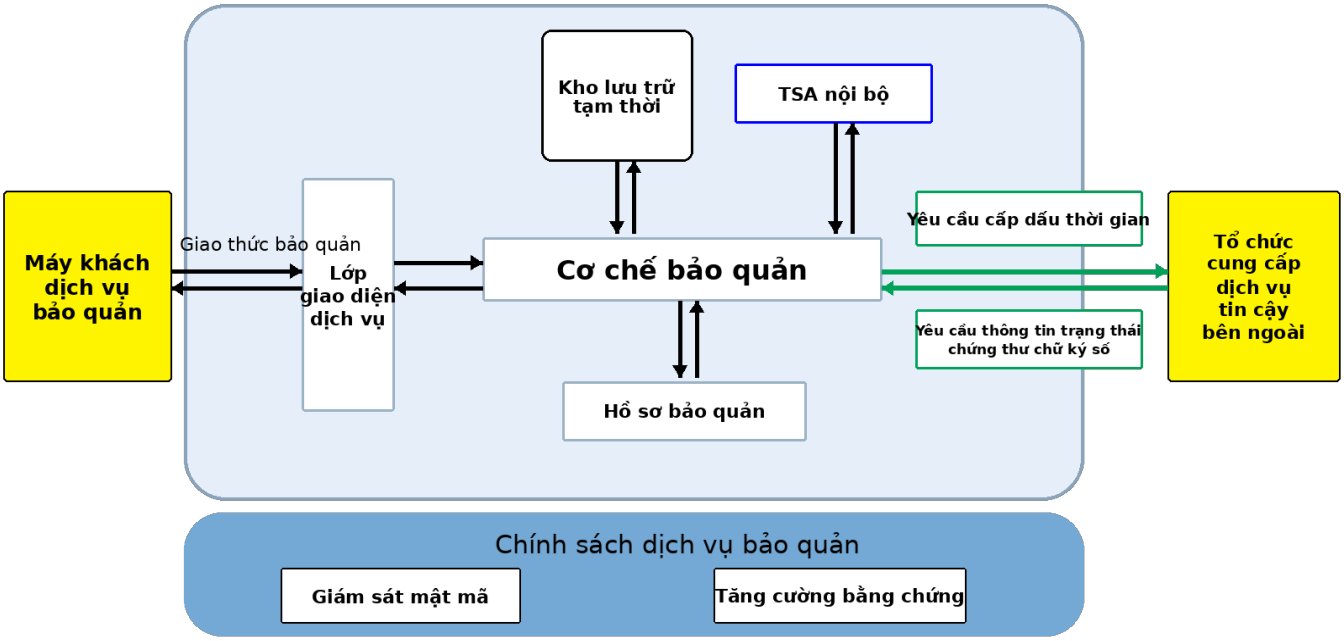
Dịch vụ bảo quản có lưu trữ lưu giữ SubDO và các đối tượng bảo quản (PO) được tạo từ SubDO bằng cách tăng cường hoặc xây dựng vùng chứa đối tượng bảo quản (POC), đồng thời tạo bằng chứng bảo quản theo yêu cầu, phù hợp với hồ sơ bảo quản đã được lựa chọn. Bên gửi sử dụng máy khách dịch vụ bảo quản để gửi một hoặc nhiều SubDO tới dịch vụ bảo quản và nhận lại định danh đối tượng bảo quản. Trong thời hạn bảo quản, máy khách có thể yêu cầu truy xuất một hoặc nhiều bằng chứng bảo quản và/hoặc PO. Dịch vụ bảo quản phải cung cấp khả năng xóa PO đã lưu trữ. Khi xóa bằng chứng bảo quản, SubDO và PO tương ứng được tạo từ SubDO đó cũng phải được xóa. Theo hồ sơ bảo quản đã lựa chọn, dịch vụ bảo quản có thể giữ lại bằng chứng bảo quản khi xóa SubDO, nhưng không được giữ lại SubDO khi đã xóa bằng chứng bảo quản, cho đến hết thời hạn bảo quản.

Một dịch vụ bảo quản có lưu trữ có thể cho phép cung cấp một phiên bản mới của một PO đã được nộp trước đó. Mối liên kết giữa các phiên bản khác nhau được thể hiện trong POC. Chức năng này cho phép xác định sự khác biệt so với phiên bản trước đó.

Dịch vụ bảo quản có thể liên hệ với các TSP bên ngoài để thu thập thông tin cần thiết nhằm tạo bằng chứng bảo quản. Các dịch vụ này có thể bao gồm tổ chức cung cấp thông tin trạng thái chứng thư chữ ký số (CSA), tổ chức cung cấp dịch vụ cấp dấu thời gian (TSA), dịch vụ tạo chữ ký số (SigS), dịch vụ xác thực chữ ký số (ValS) hoặc dịch vụ lưu trữ hồ sơ điện tử.

Dịch vụ bảo quản sử dụng TSA nội bộ hoặc bên ngoài để tạo bằng chứng bảo quản. Dịch vụ bảo quản giám sát các thuật toán mật mã được sử dụng trong các bằng chứng bảo quản đã lưu trữ (xem 7.14) và tăng cường bằng chứng bảo quản khi cần (xem 7.15).

4.1.3 Dịch vụ bảo quản có lưu trữ tạm thời [WTS]



Hình 2 - Mô hình chức năng của dịch vụ bảo quản có lưu trữ tạm thời [WTS]

Giao thức bảo quản cho phép máy khách dịch vụ bảo quản tương tác với giao diện bảo quản.

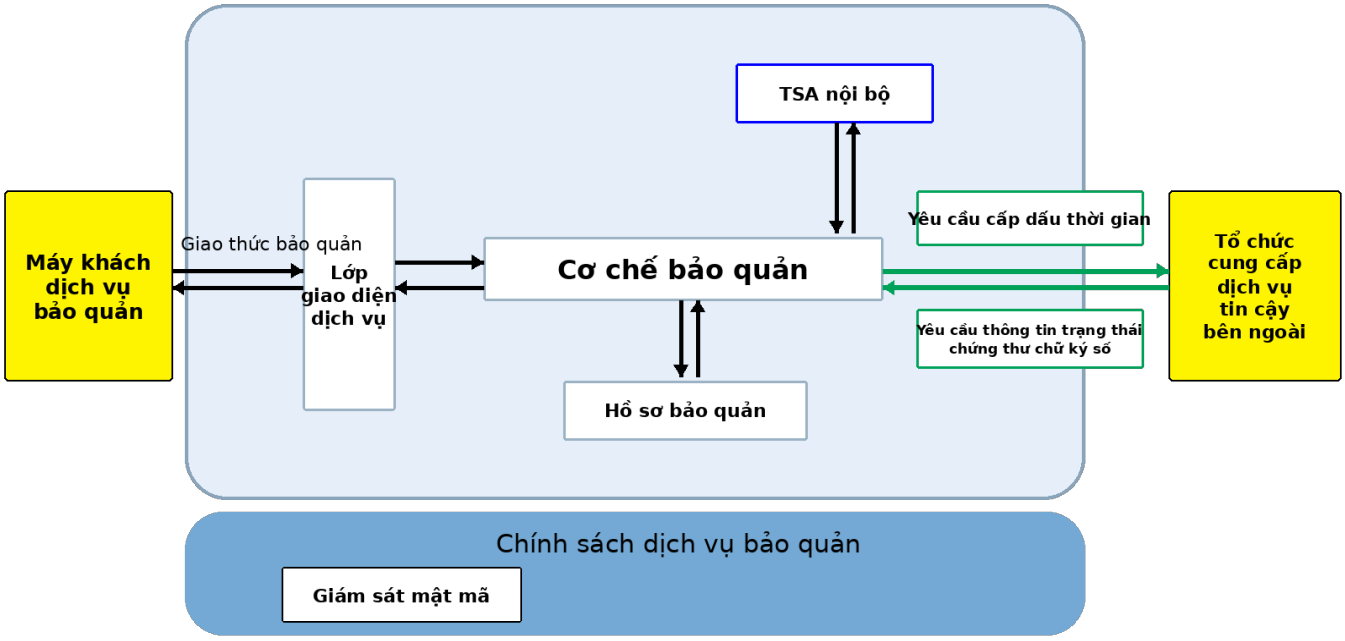
Dịch vụ bảo quản theo mô hình WTS lưu giữ tạm thời một hoặc nhiều SubDO hoặc một hoặc nhiều giá trị băm do máy khách dịch vụ bảo quản gửi, cho đến khi bằng chứng bảo quản sẵn sàng để máy khách truy xuất; sau đó dữ liệu tạm thời này phải được xóa.

Dịch vụ bảo quản tạo bằng chứng theo chế độ bất đồng bộ sau khoảng thời gian được quy định trong hồ sơ bảo quản. Sau khi được tạo, bằng chứng có thể được truy xuất theo yêu cầu trong suốt thời hạn lưu giữ bằng chứng bảo quản.

Dịch vụ bảo quản có thể liên hệ với các TSP bên ngoài để thu thập thông tin cần thiết nhằm tạo bằng chứng bảo quản. Các dịch vụ này có thể bao gồm CSA, TSA, dịch vụ tạo chữ ký số hoặc con dấu điện tử (SigS), hoặc dịch vụ xác thực chữ ký số (ValS).

Dịch vụ bảo quản sử dụng TSA nội bộ hoặc bên ngoài để tạo bằng chứng bảo quản. Dịch vụ bảo quản giám sát các thuật toán mật mã được sử dụng trong các hồ sơ bảo quản đang có hiệu lực (xem 7.14) và thay đổi tập hợp thuật toán áp dụng khi cần. Bằng chứng bảo quản được tạo theo hồ sơ đang có hiệu lực và được tăng cường khi cần (xem 7.15).

4.1.4 Dịch vụ bảo quản không lưu trữ [WOS]



Hình 3 - Mô hình chức năng của dịch vụ bảo quản không lưu trữ [WOS]

Giao thức bảo quản cho phép máy khách dịch vụ bảo quản tương tác với giao diện bảo quản.

Dịch vụ bảo quản theo mô hình WOS không lưu trữ dữ liệu cần bảo quản, giá trị băm của dữ liệu hoặc bằng chứng bảo quản.

Dịch vụ tạo bằng chứng theo chế độ đồng bộ, phù hợp với hồ sơ bảo quản. Bên gửi dữ liệu bảo quản gửi một hoặc nhiều SubDO và nhận ngay phản hồi chứa một hoặc nhiều bằng chứng bảo quản tương ứng.

Dịch vụ bảo quản giám sát các thuật toán mật mã được sử dụng trong các hồ sơ bảo quản đang có hiệu lực (xem 7.14) và thay đổi tập hợp thuật toán áp dụng khi cần. Bằng chứng bảo quản được tạo theo các hồ sơ bảo quản đang có hiệu lực.

Dịch vụ bảo quản có thể liên hệ với các TSP bên ngoài để thu thập thông tin cần thiết nhằm tạo bằng chứng bảo quản. Các dịch vụ này có thể bao gồm CSA, TSA, dịch vụ tạo chữ ký số hoặc con dấu điện tử (SigS), hoặc dịch vụ xác thực chữ ký số (ValS).

Dịch vụ bảo quản sử dụng một TSA nội bộ hoặc bên ngoài trong quá trình tạo các bằng chứng bảo quản.

4.2 Mục tiêu chức năng

Có thể phân biệt các trường hợp sử dụng khác nhau đối với dịch vụ bảo quản, mỗi trường hợp có các yêu cầu về chính sách và an toàn riêng. Dịch vụ bảo quản có thể cung cấp:

1) Việc cung cấp bằng chứng về sự tồn tại trong thời gian dài của dữ liệu nói chung, bất kể dữ liệu đó có được ký số hay không;

2) Việc duy trì trong thời gian dài khả năng xác thực chữ ký số, trạng thái hiệu lực của chữ ký số và bằng chứng về sự tồn tại của dữ liệu đã ký số; và/hoặc

3) Việc tăng cường bằng chứng bảo quản được gửi tới dịch vụ bảo quản.

Trong trường hợp thứ nhất, mục tiêu của dịch vụ bảo quản là tạo bằng chứng rằng dữ liệu hoặc tập hợp dữ liệu không bị thay đổi và đã tồn tại vào một thời điểm xác định.

Các yêu cầu, khuyến nghị hoặc quyền cụ thể cho trường hợp này được đánh dấu bằng [PGD], xem 3.3.

Trong trường hợp thứ hai, khả năng xác thực chữ ký số và duy trì trạng thái hiệu lực của chữ ký số đạt được bằng cách bảo đảm rằng tất cả dữ liệu xác thực cần thiết được thu thập, xác minh và bảo vệ bằng các kỹ thuật chữ ký số.

CHÚ THÍCH 1: ETSI EN 319 102-1 xác định các trạng thái kết quả xác thực chữ ký số, bao gồm TOTAL_PASSED, TOTAL_FAILED và INDETERMINATE.

CHÚ THÍCH 2: Sự khác biệt chính giữa trường hợp thứ nhất và trường hợp thứ hai là, trong trường hợp thứ hai, dữ liệu xác thực tương ứng với chữ ký số cũng được bảo quản; xem 9.3.3.

Các bằng chứng này cung cấp bằng chứng về sự tồn tại của chữ ký số và dữ liệu xác thực, chẳng hạn dấu thời gian, chuỗi chứng thư chữ ký số và thông tin thu hồi. Khi dữ liệu đã ký số được cung cấp cùng chữ ký số, các bằng chứng cũng cung cấp bằng chứng về sự tồn tại của dữ liệu đã ký số. Dữ liệu xác thực có thể được gửi tới dịch vụ bảo quản hoặc do dịch vụ bảo quản thu thập. Tiêu chuẩn này không hạn chế phương thức thu thập và bảo vệ dữ liệu xác thực trong bằng chứng bảo quản.

CHÚ THÍCH 3: Dữ liệu xác thực có thể được bao gồm trực tiếp trong bằng chứng hoặc trong báo cáo xác thực.

CHÚ THÍCH 4: Dịch vụ bảo quản không phải là dịch vụ xác thực chữ ký số. Dịch vụ bảo quản có thể sử dụng dịch vụ xác thực chữ ký số để tạo báo cáo xác thực hoặc hỗ trợ thu thập, xác minh dữ liệu xác thực; tuy nhiên, việc sử dụng dịch vụ xác thực không bắt buộc nếu dịch vụ bảo quản tự thu thập, xác minh và bảo vệ đầy đủ dữ liệu xác thực cần thiết để duy trì lâu dài khả năng xác thực và trạng thái hiệu lực của chữ ký số.

Khi không thể thu thập và xác minh đầy đủ dữ liệu xác thực cần thiết, hồ sơ bảo quản phải quy định cách thức dịch vụ bảo quản xử lý. Các phương án có thể bao gồm:

a) trả về thông báo lỗi;

b) bảo quản toàn bộ thông tin có thể thu thập được; hoặc

c) khi có thể, tiếp tục thu thập dữ liệu xác thực còn thiếu tại thời điểm sau.

Các yêu cầu, khuyến nghị hoặc quyền cụ thể cho trường hợp này được đánh dấu bằng [PDS], xem 3.3.

Dịch vụ bảo quản cũng có thể đồng thời duy trì trạng thái hiệu lực của chữ ký số được gửi và cung cấp bằng chứng về sự tồn tại của dữ liệu khác được gửi [PDS+PGD].

Ngoài các trường hợp trên, dịch vụ bảo quản có thể hỗ trợ mục tiêu tăng cường bằng chứng bảo quản được gửi tới. Dịch vụ cho phép máy khách dịch vụ bảo quản gửi một hoặc nhiều bằng chứng bảo quản để dịch vụ tăng cường khi cần.

VÍ DỤ 1: Dịch vụ bảo quản tiếp nhận bản ghi bằng chứng do dịch vụ bảo quản khác tạo cùng dữ liệu được bảo vệ, sau đó tiếp tục bảo quản dữ liệu bằng cách tăng cường bằng chứng đã được gửi ban đầu.

CHÚ THÍCH 5: Đối với dịch vụ bảo quản có lưu trữ, việc tăng cường bằng chứng bảo quản trong thời hạn bảo quản là độc lập với "mục tiêu tăng cường", vì nó tăng cường các bằng chứng bảo quản được lưu trữ nội bộ chứ không phải các bằng chứng được nộp.

Dịch vụ bảo quản có thể hỗ trợ riêng mục tiêu tăng cường hoặc kết hợp với các mục tiêu khác.

Mối liên kết giữa một hoặc nhiều tài liệu đã ký số và các giá trị băm của chúng được sử dụng trong một hoặc nhiều chữ ký số là thiết yếu khi bảo quản chữ ký số.

Tuy nhiên, vì lý do bảo mật, quyền riêng tư hoặc hiệu năng, trong một số trường hợp chỉ gửi giá trị băm của tài liệu đã ký số tới dịch vụ bảo quản. Khi đó, việc bảo quản tài liệu đã ký số nằm ngoài phạm vi kiểm soát và trách nhiệm của dịch vụ bảo quản; dịch vụ chỉ chịu trách nhiệm bảo quản các giá trị băm đã gửi. Bằng chứng về sự tồn tại của giá trị băm chỉ cung cấp bằng chứng về sự tồn tại của đối tượng được băm trong thời gian thuật toán băm còn được xem là đủ mạnh. Dịch vụ bảo quản có thể cho phép gửi các giá trị băm mới của tài liệu đã ký số trước khi thuật toán băm ban đầu suy yếu, ví dụ để gia hạn cây băm hoặc cập nhật bằng chứng. Tuy nhiên, dịch vụ bảo quản không thể kiểm tra liệu các giá trị băm mới có liên quan đến các giá trị băm đã cung cấp ban đầu hay không.

4.3 Tài liệu áp dụng đối với dịch vụ bảo quản

4.3.1 Quy chế chứng thực dịch vụ bảo quản

PSP phải xây dựng, triển khai, thực thi và cập nhật Quy chế chứng thực (CP/CPS). CP/CPS là quy chế chứng thực dịch vụ tin cậy theo ETSI EN 319 401, được cụ thể hóa cho dịch vụ bảo quản. Xem 6.1.

Quy chế chứng thực dịch vụ bảo quản mô tả cách PSP vận hành dịch vụ của mình và thuộc sở hữu của PSP. Các đối tượng nhận CP/CPS có thể bao gồm kiểm toán viên, thuê bao và bên thứ ba.

CHÚ THÍCH: Một số thành phần bắt buộc của CP/CPS dịch vụ bảo quản được quy định trong tiêu chuẩn này. CP/CPS dịch vụ bảo quản có thể là một phần của CP/CPS dịch vụ tin cậy chung bao quát các dịch vụ khác do TSP cung cấp hoặc là một tài liệu độc lập.

Tiêu chuẩn này đưa ra các yêu cầu được xác định là cần thiết để hỗ trợ một chính sách dịch vụ bảo quản ở mức cao, được PSP phê duyệt và được nêu trong các bản CP/CPS của mình.

4.3.2 Chính sách dịch vụ bảo quản

Chính sách dịch vụ bảo quản mô tả những gì được cung cấp và có thể bao gồm các thông tin khác vượt ra ngoài phạm vi của tiêu chuẩn này nhằm chỉ ra phạm vi áp dụng của dịch vụ.

Các đối tượng nhận chính sách dịch vụ có thể bao gồm kiểm toán viên, thuê bao và bên thứ ba. Chính sách này bao gồm các quy tắc cần tuân thủ khi cung cấp dịch vụ. Tuy nhiên, nội dung của nó không chỉ giới hạn ở mô tả kỹ thuật như được quy định trong hồ sơ bảo quản, mà còn bao gồm các yêu cầu tổng quát hơn về quản lý dịch vụ và vận hành.

Tiêu chuẩn này có thể được viện dẫn trong chính sách dịch vụ bảo quản nhằm cung cấp thông tin về mức độ của dịch vụ.

Theo ETSI EN 319 401, TSP phải định danh các chính sách dịch vụ mà mình hỗ trợ. Đối với dịch vụ bảo quản, định danh này được thông báo thông qua tài liệu cung cấp cho thuê bao và bên thứ ba.

Chính sách dịch vụ bảo quản không nhất thiết là một phần của tài liệu của PSP (theo ETSI EN 319 401, Quy chế chứng thực và các điều khoản, điều kiện chung là đủ); ví dụ, một chính sách dịch vụ bảo quản có thể được một cộng đồng sử dụng chung và không thuộc sở hữu của PSP. Tiêu chuẩn này cũng không đặt ra ràng buộc về hình thức của chính sách dịch vụ bảo quản; chính sách có thể là một tài liệu độc lập hoặc được cung cấp như một phần của, hoặc được viện dẫn bởi, Quy chế chứng thực và/hoặc các điều khoản, điều kiện chung.

4.3.3 Lược đồ bảo quản và hồ sơ bảo quản

Lược đồ bảo quản là một tập hợp chung các thủ tục và quy tắc liên quan đến một mô hình lưu trữ của dịch vụ bảo quản và một hoặc nhiều mục tiêu bảo quản, mô tả cách các bằng chứng bảo quản được tạo ra và xác thực. Lược đồ bảo quản có thể được hỗ trợ bởi một hoặc nhiều hồ sơ bảo quản.

Hồ sơ bảo quản xác định một tập hợp các chi tiết triển khai quy định cách các bằng chứng bảo quản được tạo ra và xác thực, và có liên quan đến một mô hình lưu trữ của dịch vụ bảo quản và một hoặc nhiều mục tiêu bảo quản. Một hồ sơ bảo quản có thể viện dẫn một lược đồ bảo quản để đặc tả các quy tắc chung.

VÍ DỤ 1: ETSI TS 119 512 Phụ lục G chứa các ví dụ về lược đồ bảo quản.

Một dịch vụ bảo quản cụ thể có thể triển khai nhiều hồ sơ bảo quản khác nhau. Mỗi hồ sơ bảo quản được định danh duy nhất.

VÍ DỤ 2: Việc định danh duy nhất có thể được thực hiện bằng URI (tuyệt đối hoặc tương đối), xem IETF RFC 3986
VÍ DỤ 3: Việc định danh duy nhất có thể được thực hiện bằng OID hoặc URI và một phiên bản cùng với ngày mà phiên bản cụ thể đó có hiệu lực.

Nội dung của hồ sơ bảo quản được mô tả tại 6.4.

4.3.4 Chính sách bằng chứng bảo quản

Chính sách bằng chứng bảo quản được viện dẫn bởi hồ sơ bảo quản. Chính sách này bao gồm toàn bộ thông tin về cách các bằng chứng bảo quản được tạo ra và cách chúng có thể được xác thực.

CHÚ THÍCH: Xem 6.4.4 c)-a.

4.3.5 Chính sách xác thực chữ ký số

Trong trường hợp bảo quản chữ ký số mà dịch vụ bảo quản thu thập dữ liệu xác thực cần thiết để xác định trạng thái của chữ ký số, hồ sơ bảo quản phải viện dẫn chính sách xác thực chữ ký số. Trong trường hợp này, chính sách xác thực chữ ký số mô tả các quy tắc được tuân thủ để thu thập dữ liệu xác thực.

CHÚ THÍCH: Xem 6.4.4 c).

4.4 Thời hạn dự kiến của bằng chứng

Thời hạn dự kiến của bằng chứng áp dụng đối với dịch vụ bảo quản có lưu trữ tạm thời hoặc không có lưu trữ.

Đây là khoảng thời gian mà trong đó, hoặc thời điểm mà đến đó, dịch vụ bảo quản dự kiến một bằng chứng bảo quản có thể được sử dụng để đạt mục tiêu bảo quản. Điều này có nghĩa là bằng chứng bảo quản vẫn có thể được xác thực và vẫn cung cấp sự bảo vệ bằng mật mã. Đối với một số định dạng bằng chứng bảo quản, ví dụ bản ghi bằng chứng hoặc chữ ký số AdES dùng cho lưu trữ dài hạn, chỉ cần có thể xác thực thành công dấu thời gian mới nhất bảo vệ toàn bộ bằng chứng bảo quản.

Đối với các bằng chứng bảo quản được tạo bằng các kỹ thuật chữ ký số, cần xem xét một số khoảng thời gian sau:

1) Thời hạn hiệu lực của khóa bí mật, tức là khoảng thời gian được xác định trước trong đó khóa bí mật có thể được sử dụng để tạo bằng chứng, trừ khi chứng thư chữ ký số liên quan đã bị thu hồi vì bất kỳ lý do nào;

2) Thời hạn hiệu lực của chứng thư chữ ký số;

3) Khoảng thời gian trong đó yêu cầu thu hồi chứng thư chữ ký số được tiếp nhận và xử lý, tức là khoảng thời gian chứng thư chữ ký số có thể bị thu hồi;

4) Khoảng thời gian trong đó thông tin thu hồi còn sẵn sàng;

5) Khoảng thời gian trong đó các hàm băm có khả năng chống lại tấn công va chạm; và

6) Khoảng thời gian trong đó khóa công khai có khả năng chống lại các tấn công mật mã.

Đối với chứng thư chữ ký số phù hợp với IETF RFC 5280, chứng thư chữ ký số chỉ có thể bị thu hồi trong thời hạn hiệu lực của chứng thư chữ ký số.

Đối với chứng thư chữ ký số phù hợp với IETF RFC 5280, thông tin thu hồi còn sẵn sàng ít nhất đến khi kết thúc thời hạn hiệu lực của chứng thư chữ ký số. Tuy nhiên, CA có thể tiếp tục cung cấp thông tin thu hồi sau khi chứng thư chữ ký số hết hiệu lực.

Một bằng chứng được tạo bằng các xác nhận thời gian (dấu thời gian hoặc bản ghi bằng chứng) cần được xác thực bằng cách xây dựng một đường dẫn chứng thư chữ ký số đến một điểm tin cậy.

CHÚ THÍCH: Một điểm tin cậy có thể nằm ở đỉnh của một hệ phân cấp CA hoặc là bất kỳ chứng thư CA nào trong hệ phân cấp CA.

Một bằng chứng bảo quản có thể được xác thực chừng nào các điều kiện sau còn được đáp ứng:

1) Không có chứng thư chữ ký số nào trong đường dẫn chứng thư chữ ký số bị thu hồi với lý do "lộ khóa";

2) Không có khóa công khai nào trong dữ liệu xác thực bị ảnh hưởng bởi các tấn công mật mã; và

3) Không có hàm băm nào được sử dụng trong dữ liệu xác thực bị ảnh hưởng bởi tấn công va chạm.

Điều kiện tại điểm 1) có thể được xác minh khi thông tin thu hồi còn sẵn có.

Nếu khóa bí mật và tất cả các bản sao dự phòng của nó được tiêu hủy một cách an toàn, không thể khôi phục khi kết thúc thời hạn hiệu lực của khóa bí mật, thì cách duy nhất để xâm phạm khóa bí mật là thực hiện thành công một cuộc tấn công mật mã đối với khóa công khai tương ứng hoặc đối với một trong các hàm băm được sử dụng.

Thời hạn dự kiến của bằng chứng phản ánh việc ước tính thời điểm đến khi các thuật toán chữ ký số và các hàm băm được sử dụng trong dữ liệu xác thực của bằng chứng bảo quản cuối cùng còn đủ khả năng chống chịu.

Thời hạn hiệu lực công nghệ là khoảng thời gian mà trong đó chữ ký số hoặc bằng chứng có thể được xác thực thành công và được tin cậy. Thời hạn này phụ thuộc vào thời điểm đến khi đường dẫn chứng thư chữ ký số còn có thể được xác minh và các thuật toán băm, thuật toán chữ ký số còn được tin cậy. Thời hạn hiệu lực công nghệ của chữ ký số tương tự thời hạn dự kiến của bằng chứng bảo quản dựa trên kỹ thuật chữ ký số.

4.5 Thời hạn bảo quản

Đối với dịch vụ bảo quản có lưu trữ [WST], thời hạn bảo quản là khoảng thời gian dịch vụ bảo quản các đối tượng bảo quản (PO). PO có thể bao gồm các đối tượng dữ liệu gửi (SubDO) và các PO được tạo từ SubDO bằng cách tăng cường hoặc bằng cách xây dựng POC có chứa các bằng chứng liên quan.

Thời hạn bảo quản có thể được xác định bằng một khoảng thời gian, ví dụ số năm kể từ thời điểm gửi; theo thời hạn lưu giữ bắt buộc; theo một tiêu chí; hoặc theo một ngày cụ thể. Trong thời hạn này, dịch vụ bảo quản tạo và tăng cường bằng chứng bảo quản khi cần để đạt mục tiêu bảo quản. Cách tạo bằng chứng có thể thay đổi trong thời hạn bảo quản, ví dụ do chứng thư chữ ký số hết hiệu lực hoặc thuật toán mật mã không còn đáng tin cậy. Dịch vụ bảo quản có thể sử dụng các nguồn thông tin bên ngoài để đánh giá thời điểm thuật toán mật mã, độ dài khóa hoặc hàm băm có khả năng không còn đáng tin cậy, ví dụ ETSI TS 119 312, và khi cần phát hành một hồ sơ bảo quản mới hoặc phiên bản mới của hồ sơ bảo quản.

5 Đánh giá rủi ro

5.1 Áp dụng các yêu cầu quy định tại Điều 5 của ETSI EN 319 401.

6 Chính sách và quy chế chứng thực

6.1 Quy chế chứng thực dịch vụ bảo quản

6.1.1 Áp dụng các yêu cầu quy định tại Điều 6.1 của ETSI EN 319 401.

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

6.1.2 PSP nên liệt kê hoặc viện dẫn, ví dụ thông qua OID, và mô tả ngắn gọn các chính sách dịch vụ bảo quản được hỗ trợ trong CP/CPS dịch vụ bảo quản.

6.1.3 PSP phải liệt kê trong CP/CPS dịch vụ bảo quản các hồ sơ bảo quản được hỗ trợ.

6.1.4 PSP phải nêu trong CP/CPS dịch vụ bảo quản cách thức đạt được các mục tiêu bảo quản.

6.1.5 PSP phải quy định trong CP/CPS cách thức bảo đảm tính sẵn sàng của các đối tượng dữ liệu đã gửi (SubDO) và các bằng chứng bảo quản liên quan.

6.1.6 PSP phải xác định trong CP/CPS nghĩa vụ của mọi tổ chức bên ngoài hỗ trợ dịch vụ bảo quản, bao gồm các chính sách và thực hành áp dụng.

6.1.7 [WST] PSP phải nêu trong CP/CPS các chi tiết về quy trình yêu cầu các gói xuất - nhập (export-import package).

6.1.8 [WST] PSP phải quy định trong CP/CPS các phương thức tạo lập các gói xuất - nhập, xem 7.16.

VÍ DỤ 1: Gói xuất - nhập có được mã hóa hay không.

6.1.9 [WST] PSP phải quy định trong CP/CPS việc xử lý dữ liệu khi kết thúc thời hạn bảo quản.

VÍ DỤ 2: Dữ liệu được xóa hoặc được chuyển tới một địa điểm khác.

6.2 Điều khoản và điều kiện

6.2.1 Áp dụng các yêu cầu quy định tại Điều 6.2 của ETSI EN 319 401.

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

6.2.2 PSP phải liệt kê trong điều khoản và điều kiện tất cả các chính sách dịch vụ bảo quản mà mình hỗ trợ.

6.2.3 PSP phải nêu rõ nơi có thể tìm thấy thông tin về các hồ sơ bảo quản được hỗ trợ.

6.2.4 [CÓ ĐIỀU KIỆN] Khi bên gửi dữ liệu bảo quản được phép tham gia vào quy trình bảo quản, ví dụ cung cấp dữ liệu xác thực cần thiết, PSP phải mô tả trong điều khoản và điều kiện các điều kiện áp dụng, đồng thời xác định rõ trách nhiệm của dịch vụ bảo quản và trách nhiệm của bên gửi.

6.2.5 [WST] PSP phải quy định trong điều khoản và điều kiện cách thức thực hiện yêu cầu đối với các gói xuất - nhập (export-import package).

VÍ DỤ 1: Yêu cầu có thể được thực hiện qua thư điện tử hoặc thư bảo đảm.

6.2.6 [PDS] PSP phải quy định trong điều khoản và điều kiện phương pháp sẽ áp dụng khi không thể thu thập và xác minh đầy đủ dữ liệu xác thực.

VÍ DỤ 2: Có gửi thông báo thất bại hay không.

VÍ DỤ 3: Có hủy bỏ yêu cầu bảo quản hay tiếp tục xử lý với dữ liệu xác thực không đầy đủ.

6.2.7 [CÓ ĐIỀU KIỆN] Khi bên gửi dữ liệu bảo quản được phép cung cấp các giá trị băm để sử dụng trong việc gia hạn cây băm, PSP phải quy định trong điều khoản và điều kiện rằng PSP không chịu trách nhiệm bảo đảm các giá trị băm mới tương ứng với các giá trị băm ban đầu của cây băm.

CHÚ THÍCH: PSP không có cách nào để biết các giá trị băm đó tương ứng với tài liệu nào, cũng như liệu chúng có thực sự tương ứng với một giá trị băm của một phép tính băm cụ thể hay không.

6.2.8 [CÓ ĐIỀU KIỆN] Khi bên gửi dữ liệu bảo quản được phép cung cấp giá trị băm của đối tượng cần bảo quản thay cho chính đối tượng đó, PSP phải nêu rõ trong điều khoản và điều kiện rằng dịch vụ chỉ bảo quản các giá trị băm đã gửi và bằng chứng về sự tồn tại của giá trị băm chỉ cho phép chứng minh sự tồn tại của đối tượng được băm trong thời gian thuật toán băm còn được xem là đủ mạnh.

6.3 Chính sách an toàn thông tin

6.3.1 Áp dụng các yêu cầu quy định tại Điều 6.3 của ETSI EN 319 401.

6.4 Hồ sơ bảo quản

6.4.1 Dịch vụ bảo quản phải hỗ trợ ít nhất một hồ sơ bảo quản.

6.4.2 Dịch vụ bảo quản có thể hỗ trợ nhiều hơn một hồ sơ bảo quản.

6.4.3 Mỗi hồ sơ bảo quản phải được định danh duy nhất.

6.4.4 Một hồ sơ bảo quản:

a) Phải bao gồm định danh để định danh duy nhất hồ sơ bảo quản.

b) Phải bao gồm các thao tác được hỗ trợ của giao thức bảo quản. Đối với mỗi thao tác:

- Phải bao gồm các định dạng đầu vào được hỗ trợ.

VÍ DỤ 1: Trong trường hợp có thể cung cấp giá trị băm của dữ liệu, danh sách các hàm băm được chấp nhận.
VÍ DỤ 2: Trong trường hợp [PDS], các định dạng chữ ký số được hỗ trợ.

- [CÓ ĐIỀU KIỆN] Phải bao gồm các định dạng đầu ra bổ sung, trong trường hợp có hỗ trợ các đầu ra khác với định dạng đầu vào được hỗ trợ và định dạng bằng chứng bảo quản.

c) Phải bao gồm một tập các chính sách kỹ thuật áp dụng. Tập chính sách này:

CHÚ THÍCH 1: Không bao gồm chính sách dịch vụ bảo quản.

- Phải viện dẫn chính sách bằng chứng bảo quản quy định tại 6.5.

CHÚ THÍCH 2: Phiên bản hiện tại của tiêu chuẩn giả định có chính sách ở dạng con người có thể đọc được. Phiên bản tương lai có thể viện dẫn đặc tả chính sách ở dạng máy có thể đọc được.

- [PDS][PDS+PGD] [CÓ ĐIỀU KIỆN] Phải viện dẫn chính sách xác thực chữ ký số theo 6.6 khi máy khách dịch vụ bảo quản không cung cấp dữ liệu xác thực.

d) Phải bao gồm thời hạn hiệu lực của hồ sơ. Thời hạn hiệu lực:

- Phải bao gồm thời điểm mà từ đó hồ sơ bảo quản đã có hiệu lực hoặc sẽ có hiệu lực.

- Có thể bao gồm thời điểm mà đến đó hồ sơ bảo quản còn hiệu lực.

e) Phải bao gồm mô hình lưu trữ của dịch vụ bảo quản (WST, WTS hoặc WOS).

f) Phải bao gồm các mục tiêu bảo quản (PDS, PGD, AUG hoặc kết hợp của chúng).

g) Phải bao gồm tất cả các định dạng bằng chứng được hỗ trợ.

h) Có thể bao gồm một đặc tả dùng để viện dẫn đến một đặc tả công khai mà trong đó hồ sơ bảo quản được mô tả.

i) Phải bao gồm hoặc viện dẫn đến mô tả của hồ sơ bảo quản bằng ngôn ngữ con người có thể hiểu được. Mô tả này có thể được cung cấp bằng nhiều ngôn ngữ.

VÍ DỤ 3: Một số quốc gia có thể yêu cầu sử dụng nhiều hơn một ngôn ngữ.

j) Có thể bao gồm một định danh dùng để viện dẫn đến một đặc tả công khai mà trong đó lược đồ bảo quản liên quan đến hồ sơ được mô tả.

6.4.5 [WTS] Đối với dịch vụ bảo quản có lưu trữ tạm thời, hồ sơ bảo quản phải quy định thời hạn lưu giữ bằng chứng bảo quản, tức khoảng thời gian bằng chứng được tạo theo chế độ bất đồng bộ có thể được máy khách dịch vụ bảo quản truy xuất từ dịch vụ.

6.4.6 [WTS][WOS] Đối với dịch vụ bảo quản có lưu trữ tạm thời hoặc không có lưu trữ, hồ sơ bảo quản nên bao gồm thời hạn dự kiến của bằng chứng.

6.4.7 [WTS][WOS] Thời hạn dự kiến của bằng chứng phải dựa trên việc ước lượng mức độ phù hợp của các thuật toán mật mã.

6.4.8 [WTS][WOS] Thời hạn dự kiến của bằng chứng nên dựa trên ETSI TS 119 312.

CHÚ THÍCH: Khuyến nghị về bộ thuật toán mật mã trong ETSI TS 119 312 có thể được thay thế bằng tiêu chuẩn hoặc khuyến nghị quốc gia hiện hành.

6.4.9 Các hồ sơ bảo quản được hỗ trợ phải được cung cấp trực tuyến.

6.4.10 Dịch vụ bảo quản phải công khai tất cả các hồ sơ bảo quản mà mình hỗ trợ hoặc đã từng hỗ trợ.

6.4.11 [WST] Cùng một hồ sơ bảo quản phải được áp dụng trong suốt thời hạn bảo quản.

6.4.12 [WTS] Cùng một hồ sơ bảo quản phải được áp dụng trong suốt toàn bộ thời hạn lưu giữ bằng chứng bảo quản.

6.4.13 Hồ sơ bảo quản không nên thay đổi theo thời gian, do đó tất cả các yếu tố động nên được quy định bên ngoài hồ sơ bảo quản (ví dụ: chính sách bằng chứng bảo quản hoặc chính sách xác thực chữ ký số).

6.4.14 Chính sách bằng chứng bảo quản hoặc chính sách xác thực chữ ký số được viện dẫn trong hồ sơ bảo quản có thể thay đổi theo thời gian. Tuy nhiên, tất cả phiên bản liên quan đến một hồ sơ bảo quản cụ thể phải được công khai và phải xác định rõ khoảng thời gian áp dụng của từng phiên bản.

VÍ DỤ 4: Chính sách bằng chứng bảo quản có thể thay đổi khi dịch vụ cấp dấu thời gian (TSA) được sử dụng thay đổi hoặc khi các thuật toán mật mã áp dụng thay đổi.

6.5 Chính sách bằng chứng bảo quản

6.5.1 Chính sách bằng chứng bảo quản được viện dẫn bởi hồ sơ bảo quản có thể trình bày dưới dạng con người có thể đọc được.

6.5.2 [CÓ ĐIỀU KIỆN] Nếu tồn tại nhiều định dạng hoặc nhiều ngôn ngữ khác nhau của chính sách bằng chứng bảo quản, PSP phải nêu rõ phiên bản nào có hiệu lực ưu tiên áp dụng.

6.5.3 Chính sách bằng chứng bảo quản phải mô tả cách thức tạo lập bằng chứng bảo quản, bao gồm các thuật toán mật mã được sử dụng.

6.5.4 Các thuật toán mật mã được sử dụng nên được lựa chọn theo ETSI TS 119 312.

CHÚ THÍCH 1: Khuyến nghị về bộ thuật toán mật mã trong ETSI TS 119 312 có thể được thay thế bằng tiêu chuẩn hoặc khuyến nghị quốc gia hiện hành.

6.5.5 Chính sách bằng chứng bảo quản phải mô tả các TSP mà dịch vụ bảo quản có thể sử dụng, ví dụ tổ chức cung cấp dịch vụ tạo chữ ký số, tổ chức cung cấp dịch vụ cấp dấu thời gian hoặc tổ chức cung cấp thông tin trạng thái chứng thư chữ ký số.

6.5.6 Chính sách bằng chứng bảo quản phải bao gồm cách thức mà bằng chứng bảo quản có thể được xác thực, bao gồm:

1) Các điểm tin cậy nào có thể được sử dụng để xác thực chữ ký số trong bằng chứng bảo quản.

2) Các điểm tin cậy nào có thể được sử dụng để xác thực dấu thời gian trong bằng chứng bảo quản.

6.5.7 [WST][WTS] Chính sách bằng chứng bảo quản phải quy định cách thức tăng cường bằng chứng.

CHÚ THÍCH 2: Xem 7.15 về các yêu cầu đối với việc tăng cường bằng chứng bảo quản.

6.5.8 Chính sách bằng chứng bảo quản phải mô tả định dạng của bằng chứng bảo quản.

6.5.9 Chính sách bằng chứng bảo quản phải nêu rõ bằng chứng có chứa thông tin tường minh về các nội dung áp dụng sau đây hay không và, nếu có, cách thức thể hiện:

a) Dịch vụ bảo quản;

b) Chính sách bằng chứng bảo quản; hoặc

c) Hồ sơ bảo quản.

6.6 Chính sách xác thực chữ ký số

6.6.1 Chính sách xác thực chữ ký số được bao gồm trong hồ sơ bảo quản (xem 6.4.4) có thể được trình bày dưới dạng con người có thể đọc được.

6.6.2 [CÓ ĐIỀU KIỆN] Nếu chính sách xác thực chữ ký số tồn tại dưới nhiều định dạng hoặc ngôn ngữ, PSP phải quy định phiên bản có giá trị ưu tiên áp dụng.

6.6.3 [CÓ ĐIỀU KIỆN] Nếu được bao gồm trong hồ sơ bảo quản, chính sách xác thực chữ ký số phải quy định chiến lược lựa chọn dữ liệu xác thực, ví dụ các điểm tin cậy, mô hình xác thực (chuỗi hoặc vỏ), và các tiêu chí liên quan.

6.7 Thỏa thuận với thuê bao

6.7.1 PSP phải cung cấp thỏa thuận với thuê bao, trong đó bao gồm việc chấp nhận các điều khoản và điều kiện.

6.7.2 [CÓ ĐIỀU KIỆN] Nếu dịch vụ bảo quản cung cấp giao thức thông báo, PSP phải quy định trong thỏa thuận với thuê bao việc thuê bao có nhận thông báo hay không và phương thức nhận thông báo.

6.7.3 [CÓ ĐIỀU KIỆN] Nếu dịch vụ bảo quản cung cấp giao thức thông báo, PSP phải cập nhật thỏa thuận với thuê bao khi phương thức thông báo được bổ sung hoặc loại bỏ.

6.7.4 [WST][WTS] PSP phải quy định trong thỏa thuận với thuê bao chủ thể có quyền truy cập các PO, bao gồm SubDO và bằng chứng bảo quản.

6.7.5 [WST][WTS] PSP phải quy định trong thỏa thuận với thuê bao chủ thể có quyền yêu cầu cung cấp dấu vết hoạt động liên quan đến các PO.

7 Quản lý và vận hành tổ chức cung cấp dịch vụ bảo quản

7.1 Tổ chức nội bộ

7.1.1 Áp dụng các yêu cầu quy định tại Điều 7.1 của ETSI EN 319 401.

7.2 Nguồn nhân lực

7.2.1 Áp dụng các yêu cầu quy định tại Điều 7.2 của ETSI EN 319 401.

7.3 Quản lý tài sản

7.3.1 Áp dụng các yêu cầu quy định tại Điều 7.3 của ETSI EN 319 401.

7.4 Kiểm soát truy cập

7.4.1 Áp dụng các yêu cầu quy định tại Điều 7.4 của ETSI EN 319 401.

7.5 Kiểm soát mật mã

7.5.1 Áp dụng các yêu cầu quy định tại 7.5 của ETSI EN 319 401.

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

7.5.2 PSP phải bảo đảm dấu thời gian được sử dụng trong quy trình bảo quản được cấp bởi TSA áp dụng các thực hành tiên tiến hiện hành về chính sách và an toàn đối với tổ chức cung cấp dịch vụ cấp dấu thời gian. Cụ thể, TSA nên phù hợp với ETSI EN 319 421.

7.5.3 PSP chỉ nên sử dụng trong quy trình bảo quản dấu thời gian có thể được xác thực bằng CRL hoặc phản hồi OCSP, trong đó có mã lý do khi chứng thư chữ ký số chứa khóa công khai bị thu hồi.

7.5.4 [CÓ ĐIỀU KIỆN] Khi PSP ký số một phần hoặc toàn bộ bằng chứng bảo quản, PSP nên lựa chọn chứng thư chữ ký số dùng để ký do CA tin cậy cấp, đáp ứng ETSI EN 319 411-1 hoặc ETSI EN 319 411-2.

7.5.5 [CÓ ĐIỀU KIỆN] Khi PSP ký số một phần hoặc toàn bộ bằng chứng bảo quản, khóa bí mật ký của PSP phải được lưu giữ và sử dụng trong một thiết bị mật mã an toàn đáp ứng một trong các điều kiện sau:

a) Là hệ thống tin cậy được bảo đảm ở mức EAL 4 trở lên theo ISO/IEC 15408 và chương trình đánh giá an toàn được công nhận, hoặc theo tiêu chí đánh giá an toàn công nghệ thông tin tương đương được công nhận ở cấp quốc gia hoặc quốc tế. Việc đánh giá phải dựa trên mục tiêu an toàn hoặc hồ sơ bảo vệ đáp ứng các yêu cầu của tiêu chuẩn này, trên cơ sở phân tích rủi ro và có tính đến các biện pháp an toàn vật lý và các biện pháp an toàn phi kỹ thuật khác; hoặc

b) Đáp ứng các yêu cầu quy định trong ISO/IEC 19790, FIPS PUB 140-2 mức 3 hoặc FIPS PUB 140-3 mức 3.

7.5.6 [CÓ ĐIỀU KIỆN] Khi PSP ký số một phần hoặc toàn bộ bằng chứng bảo quản, thiết bị mật mã an toàn quy định tại 7.5.5 nên đáp ứng phương án a) của 7.5.5.

7.5.7 [CÓ ĐIỀU KIỆN] Khi PSP ký (một phần của) bằng chứng bảo quản, mọi bản sao dự phòng của khóa bí mật ký của PSP phải được bảo vệ để bảo đảm tính toàn vẹn và tính bảo mật bởi thiết bị mật mã an toàn trước khi được lưu trữ bên ngoài thiết bị đó.

7.6 An toàn vật lý và môi trường

7.6.1 Áp dụng các yêu cầu quy định tại Điều 7.6 của ETSI EN 319 401.

7.7 An toàn vận hành

7.7.1 Áp dụng các yêu cầu quy định tại Điều 7.7 của ETSI EN 319 401.

7.8 An toàn mạng

7.8.1 Áp dụng các yêu cầu quy định tại Điều 7.8 của ETSI EN 319 401.

7.8.2 [WST] Dịch vụ bảo quản phải được tích hợp trong môi trường công nghệ thông tin sao cho mọi truy cập của thuê bao làm thay đổi nội dung lưu trữ chỉ được thực hiện thông qua dịch vụ bảo quản.

7.9 Quản lý sự cố

7.9.1 Áp dụng các yêu cầu quy định tại Điều 7.9 của ETSI EN 319 401.

7.10 Thu thập bằng chứng

7.10.1 Áp dụng các yêu cầu quy định tại Điều 7.10 của ETSI EN 319 401.

7.10.2 Dịch vụ bảo quản phải triển khai nhật ký sự kiện để thiết lập thông tin cần thiết phục vụ việc chứng minh sau này.

7.11 Quản lý tính liên tục hoạt động

7.11.1 Áp dụng các yêu cầu quy định tại Điều 7.11 của ETSI EN 319 401.

7.12 Chấm dứt hoạt động và kế hoạch chấm dứt

7.12.1 Áp dụng các yêu cầu quy định tại Điều 7.12 của ETSI EN 319 401.

7.12.2 [WST] Kế hoạch chấm dứt phải quy định việc xử lý các đối tượng bảo quản (PO) đã được lưu trữ khi dịch vụ bảo quản chấm dứt.s

7.13 Tuân thủ

7.13.1 Áp dụng các yêu cầu quy định tại Điều 7.13 của ETSI EN 319 401.

7.14 Giám sát mật mã

7.14.1 Đối với mỗi hồ sơ bảo quản đang có hiệu lực, PSP phải giám sát mức độ an toàn của từng thuật toán và tham số mật mã được sử dụng. Khi một thuật toán hoặc tham số được xem là trở nên kém an toàn hoặc chứng thư chữ ký số liên quan sắp hết hiệu lực, PSP phải cập nhật chính sách bằng chứng bảo quản liên quan hoặc tạo hồ sơ bảo quản mới để xử lý các PO được gửi mới.

7.14.2 [WST] [CÓ ĐIỀU KIỆN] Khi một thuật toán hoặc tham số đã được sử dụng trong bằng chứng bảo quản được xem là trở nên kém an toàn hoặc chứng thư chữ ký số liên quan sắp hết hiệu lực, dịch vụ bảo quản phải tăng cường bằng chứng theo phiên bản mới của chính sách bằng chứng bảo quản trong suốt thời hạn bảo quản.

7.14.3 Để đánh giá các thuật toán mật mã theo 7.14.1 và 7.14.2, nên tham chiếu ETSI TS 119 312.

CHÚ THÍCH: Khuyến nghị về bộ thuật toán mật mã trong ETSI TS 119 312 có thể được thay thế bằng tiêu chuẩn hoặc khuyến nghị quốc gia hiện hành.

7.15 Tăng cường bằng chứng

7.15.1 [WST] Trong suốt thời hạn bảo quản, dịch vụ bảo quản phải bảo đảm bằng chứng bảo quản có thể được sử dụng để đạt mục tiêu bảo quản tương ứng.

7.15.2 [WTS] Trong suốt thời hạn lưu giữ bằng chứng bảo quản, dịch vụ bảo quản phải bảo đảm bằng chứng bảo quản có thể được sử dụng để đạt mục tiêu bảo quản tương ứng.

CHÚ THÍCH 1: Điều này có thể bị ảnh hưởng trong trường hợp một thuật toán mật mã không còn được tin cậy hoặc không còn thu thập được thông tin thu hồi.

7.15.3 [WST][WTS] Dịch vụ bảo quản phải tăng cường bằng chứng bảo quản trước khi bằng chứng không còn có thể được sử dụng để đạt mục tiêu bảo quản tương ứng, nhằm đáp ứng 7.15.1 hoặc 7.15.2.

CHÚ THÍCH 2: Đối với chữ ký số, việc tăng cường có thể được thực hiện bằng cách tích hợp vào chữ ký số thông tin cần thiết để duy trì hiệu lực, như dấu thời gian và dữ liệu xác thực.

CHÚ THÍCH 3: Đối với bản ghi bằng chứng, việc tăng cường có thể được thực hiện bằng cách gia hạn dấu thời gian hoặc gia hạn cây băm theo IETF RFC 4998 hoặc IETF RFC 6283.

7.16 Gói xuất - nhập

7.16.1 [WST] PSP phải cho phép máy khách dịch vụ bảo quản hoặc dịch vụ bảo quản được ủy quyền khác yêu cầu một hoặc nhiều gói xuất - nhập. Gói xuất - nhập phải bao gồm dữ liệu được bảo quản, bằng chứng bảo quản và toàn bộ thông tin cần thiết để xác thực bằng chứng.

CHÚ THÍCH 1: Gói xuất - nhập có thể được sử dụng để chuyển dữ liệu được bảo quản từ dịch vụ bảo quản này sang dịch vụ bảo quản khác.

CHÚ THÍCH 2: Tiêu chuẩn này không quy định về định dạng cụ thể của gói xuất - nhập. Xem ETSI TS 119 512 để tham khảo một cấu trúc khả dĩ.

7.16.2 [WST] PSP nên sử dụng định dạng tiêu chuẩn cho (các) gói xuất - nhập.

VÍ DỤ 1: (Các) gói xuất - nhập theo mô tả tại ETSI TS 119 512.

VÍ DỤ 2: (Các) gói xuất - nhập theo TR-ESOR-M.3, điều 2.5.

7.16.3 [WST] (Các) gói xuất - nhập chỉ được cung cấp cho pháp nhân hoặc cá nhân đã được ủy quyền.

7.16.4 [WST] PSP phải lưu trữ hồ sơ về tất cả các gói xuất - nhập đã được cung cấp, bao gồm:

1) Thời điểm xảy ra sự kiện.

2) Các tiêu chí đã được sử dụng để lựa chọn tập hợp các đối tượng bảo quản được đưa vào gói xuất - nhập.

7.17 Chuỗi cung ứng

7.17.1 Áp dụng các yêu cầu quy định tại Điều 7.14 của ETSI EN 319 401.

8 Giao thức vận hành và thông báo

8.1 Giao thức bảo quản

8.1.1 Kênh truyền thông giữa máy khách dịch vụ bảo quản và PSP phải được bảo vệ; PSP phải cung cấp cơ chế để máy khách xác thực PSP và phải bảo đảm tính bí mật của dữ liệu trao đổi.

8.1.2 Nên sử dụng giao thức bảo quản được định nghĩa trong ETSI TS 119 512.

8.1.3 Các giao thức phải được bảo vệ để ngăn chặn việc sử dụng trái phép.

Trường hợp chung

8.1.4 Dịch vụ bảo quản phải cho phép truy xuất thông tin về các hồ sơ bảo quản hiện được hỗ trợ và đã từng được hỗ trợ.

VÍ DỤ 1: RetrieveInfo theo định nghĩa tại ETSI TS 119 512 để truy xuất thông tin về các hồ sơ bảo quản.

8.1.5 Dịch vụ bảo quản phải cho phép gửi một hoặc nhiều đối tượng dữ liệu gửi (SubDO) theo một hồ sơ bảo quản cụ thể và phải trả về định danh đối tượng bảo quản hoặc trả ngay bằng chứng bảo quản theo chế độ đồng bộ.

VÍ DỤ 2: Định danh đối tượng bảo quản có thể được sử dụng sau này để truy xuất (các) đối tượng bảo quản (PO), và/hoặc các dấu vết, hoặc để xóa (các) PO hoặc cập nhật các vùng chứa đối tượng bảo quản (chế độ bất đồng

bộ).

VÍ DỤ 3: PreservePO theo định nghĩa tại ETSI TS 119 512.

8.1.6 Dịch vụ bảo quản có thể cho phép truy xuất dấu vết của mọi hoạt động liên quan đến một định danh đối tượng bảo quản cụ thể.

VÍ DỤ 4: RetrieveTrace theo định nghĩa tại ETSI TS 119 512.

8.1.7 Dịch vụ bảo quản có thể cho phép tìm kiếm đối tượng bảo quản và truy xuất tập hợp định danh đối tượng bảo quản để sử dụng trong các thao tác khác, ví dụ 8.1.5.

VÍ DỤ 5: Search theo định nghĩa tại ETSI TS 119 512.

8.1.8 Dịch vụ bảo quản có thể cho phép gửi một bằng chứng bảo quản và chuỗi PO tương ứng để xác thực bằng chứng và nhận báo cáo xác thực bằng chứng bảo quản.

VÍ DỤ 6: ValidateEvidence theo định nghĩa tại ETSI TS 119 512.

8.1.9 [CÓ ĐIỀU KIỆN] Nếu cho phép tìm kiếm đối tượng bảo quản, dịch vụ bảo quản có thể cung cấp chức năng lọc theo tiêu chí mà đối tượng bảo quản hoặc định danh của đối tượng phải đáp ứng.

Dịch vụ bảo quản có lưu trữ

8.1.10 [WST] Dịch vụ bảo quản có lưu trữ phải cho phép truy xuất bằng chứng bảo quản và/hoặc các đối tượng bảo quản (PO).

CHÚ THÍCH 1: PO cũng có thể chứa các bằng chứng.

VÍ DỤ 7: RetrievePO theo định nghĩa tại ETSI TS 119 512.

8.1.11 [WST] Dịch vụ bảo quản có lưu trữ phải cho phép xóa các PO đã lưu trữ. Trong trường hợp xóa bằng chứng bảo quản thì SubDO tương ứng cũng phải bị xóa.

8.1.12 [WST] Dịch vụ bảo quản phải bảo đảm PO đã lưu trữ chỉ có thể bị xóa trước khi kết thúc thời hạn bảo quản khi yêu cầu xóa kèm theo lý do. Lý do phải được ghi nhật ký cùng thông tin của yêu cầu xóa.

VÍ DỤ 8: DeletePO theo định nghĩa tại ETSI TS 119 512.

8.1.13 [WST] Dịch vụ bảo quản có lưu trữ nên cho phép yêu cầu một tập hợp các định danh đối tượng bảo quản, các định danh này có thể được sử dụng để truy xuất hoặc xóa PO như quy định tại 8.1.10 và 8.1.11.

VÍ DỤ 9: Search theo định nghĩa tại ETSI TS 119 512.

8.1.14 [WST] Dịch vụ bảo quản có lưu trữ có thể cho phép cung cấp một phiên bản mới của một POC đã được gửi trước đó. Phiên bản mới có thể chỉ được xác định bằng phần khác biệt so với phiên bản trước.

VÍ DỤ 10: UpdatePOC theo định nghĩa tại ETSI TS 119 512.

CHÚ THÍCH 2: Chức năng cập nhật cho phép cung cấp một phiên bản mới của SubDO. Phiên bản này có thể thay thế hoàn toàn hoặc một phần phiên bản ban đầu. Tất cả các phiên bản đều được lưu trữ, nhưng một phiên bản sẽ được đánh dấu là phiên bản mới nhất.

Dịch vụ bảo quản có lưu trữ tạm thời

8.1.15 [WTS] Dịch vụ bảo quản có lưu trữ tạm thời phải cho phép truy xuất bằng chứng bảo quản được tạo theo chế độ bất đồng bộ.

CHÚ THÍCH 3: Do các bằng chứng được tạo ra theo chế độ bất đồng bộ và có thể áp dụng cho một số SubDO, nên chúng được cung cấp trong một khoảng thời gian theo quy định trong hồ sơ bảo quản.

VÍ DỤ 11: RetrievePO theo định nghĩa tại ETSI TS 119 512.

8.2 Giao thức thông báo

8.2.1 Dịch vụ bảo quản có thể xác định giao thức thông báo để gửi thông điệp hoặc thông tin tới thuê bao.

CHÚ THÍCH: Cách thức thực hiện thông báo không thuộc phạm vi của tiêu chuẩn này.

8.2.2 [CÓ ĐIỀU KIỆN] Khi dịch vụ bảo quản cung cấp giao thức thông báo và một chính sách bằng chứng bảo quản được viện dẫn trong hồ sơ bảo quản đang có hiệu lực được xem là trở nên không an toàn, dịch vụ bảo quản phải thông báo cho các thuê bao có khả năng đang sử dụng hồ sơ tương ứng về các quan ngại an toàn đặc thù đối với chính sách bằng chứng bảo quản đó.

8.2.3 [CÓ ĐIỀU KIỆN] Khi dịch vụ bảo quản cung cấp giao thức thông báo và có thay đổi đối với các thành phần được viện dẫn làm ảnh hưởng đến một hồ sơ bảo quản cụ thể, PSP phải thông báo cho các thuê bao có khả năng đang sử dụng hồ sơ đó.

9 Quy trình bảo quản

9.1 Lưu trữ dữ liệu và bằng chứng bảo quản

9.1.1 [WTS] [WOS] Dịch vụ bảo quản không lưu trữ hoặc có lưu trữ tạm thời không nên lưu trữ dữ liệu cần bảo quản sau khi bằng chứng đã được tạo.

9.1.2 [WOS] [WTS] [CÓ ĐIỀU KIỆN] Dịch vụ bảo quản không lưu trữ hoặc có lưu trữ tạm thời mà vẫn lưu trữ dữ liệu cần bảo quản sau khi bằng chứng đã được tạo nên nêu rõ lý do trong điều khoản và điều kiện của mình.

9.1.3 [WTS] Dịch vụ bảo quản có lưu trữ tạm thời không được lưu giữ bằng chứng bảo quản lâu hơn thời hạn quy định trong quy chế chứng thực dịch vụ bảo quản.

9.2 Bằng chứng bảo quản

9.2.1 [CÓ ĐIỀU KIỆN] Nếu dịch vụ bảo quản sử dụng thẻ dấu thời gian, thẻ dấu thời gian phải phù hợp với IETF RFC 3161, bao gồm bản cập nhật tại IETF RFC 5816.

9.2.2 [CÓ ĐIỀU KIỆN] Nếu dịch vụ bảo quản sử dụng thẻ dấu thời gian, thẻ dấu thời gian nên phù hợp với giao thức cấp dấu thời gian và các hồ sơ thẻ dấu thời gian quy định trong ETSI EN 319 422.

9.2.3 [CÓ ĐIỀU KIỆN] Nếu dịch vụ bảo quản sử dụng bản ghi bằng chứng, bản ghi phải phù hợp với IETF RFC 4998 hoặc IETF RFC 6283.

9.2.4 [CÓ ĐIỀU KIỆN] Nếu chính sách bằng chứng bảo quản không thể được xác định từ ngữ cảnh, thì chính sách bằng chứng bảo quản nên được bao gồm trực tiếp trong bằng chứng bảo quản.

CHÚ THÍCH: Chính sách bằng chứng bảo quản được tham chiếu bởi hồ sơ bảo quản. Nếu hồ sơ bảo quản đã được xác định từ ngữ cảnh, thì chính sách bằng chứng cũng được xác định tương ứng.

9.2.5 [CÓ ĐIỀU KIỆN] Nếu chính sách bằng chứng bảo quản được bao gồm trong bằng chứng bảo quản, thì chính sách này nên được bảo vệ bằng cơ chế mật mã.

9.3 Bảo quản chữ ký số

9.3.1 [PDS][PDS+PGD] [CÓ ĐIỀU KIỆN] Nếu máy khách dịch vụ bảo quản không cung cấp dữ liệu xác thực, dịch vụ bảo quản phải nỗ lực tối đa để thu thập và xác minh dữ liệu xác thực theo chính sách xác thực chữ ký số được hỗ trợ trong hồ sơ bảo quản (xem 6.6).

9.3.2 [PDS][PDS+PGD] [CÓ ĐIỀU KIỆN] Nếu máy khách dịch vụ bảo quản cung cấp dữ liệu xác thực, dịch vụ bảo quản nên xác minh dữ liệu đã cung cấp theo chính sách xác thực chữ ký số được hỗ trợ trong hồ sơ bảo quản (xem 6.6), đồng thời kiểm tra dữ liệu xác thực đó có phù hợp hay không; nếu không phù hợp, dịch vụ nên thu thập và xác minh dữ liệu xác thực phù hợp.

9.3.3 [PDS] Để kéo dài khả năng xác thực chữ ký số và duy trì trạng thái hiệu lực của chữ ký số, dịch vụ bảo quản tối thiểu phải cung cấp bằng chứng về sự tồn tại của chữ ký số và dữ liệu xác thực cần thiết để xác thực chữ ký số bằng các kỹ thuật chữ ký số (chữ ký số, dấu thời gian hoặc bản ghi bằng chứng).

CHÚ THÍCH 1: Bằng chứng về sự tồn tại của một chữ ký số tách rời cũng cung cấp bằng chứng về sự tồn tại của dữ liệu đã được ký số, với điều kiện các thuật toán (ví dụ: hàm băm được sử dụng trong chữ ký ban đầu) có khả năng chống lại các tấn công va chạm.

9.3.4 [PDS+PGD] Để kéo dài khả năng xác thực chữ ký số và duy trì trạng thái hiệu lực của chữ ký số, dịch vụ bảo quản phải cung cấp bằng chứng về sự tồn tại của chữ ký số, dữ liệu xác thực cần thiết và dữ liệu đã ký số.

CHÚ THÍCH 2: Tiêu chuẩn này không hạn chế cách thức dịch vụ bảo quản thu thập dữ liệu xác thực cần thiết để xác thực chữ ký số.

VÍ DỤ: Dịch vụ bảo quản có thể sử dụng dịch vụ xác thực nội bộ hoặc bên ngoài để thu thập dữ liệu xác thực cần thiết, hoặc có thể áp dụng dấu thời gian phù hợp và thực hiện xác thực đường dẫn chứng thư chữ ký số X.509 của người ký.

9.3.5 [PDS][PDS+PGD] [CÓ ĐIỀU KIỆN] Đối với chữ ký số tách rời, dịch vụ bảo quản có thể cho phép thuê bao chỉ cung cấp giá trị băm của dữ liệu đã ký số.

9.3.6 [PDS][PDS+PGD] [CÓ ĐIỀU KIỆN] Trong trường hợp chữ ký số tách rời và dịch vụ bảo quản cho phép thuê bao chỉ cung cấp giá trị băm của dữ liệu đã ký số, PSP phải quy định trong hồ sơ bảo quản các định danh của các hàm băm được phép sử dụng.

9.3.7 [PDS][PDS+PGD] [CÓ ĐIỀU KIỆN] Trong trường hợp chữ ký số tách rời và dịch vụ bảo quản cho phép thuê bao chỉ cung cấp giá trị băm của dữ liệu đã ký số, dịch vụ bảo quản phải xử lý giá trị băm, kèm theo định danh hàm băm, như dữ liệu tổng quát có liên kết với chữ ký số, vì dịch vụ không có cách xác định giá trị băm đó có thực sự tương ứng với dữ liệu đã ký số hay không.

CHÚ THÍCH 3: Trong trường hợp này, dịch vụ bảo quản chỉ chịu trách nhiệm bảo quản giá trị băm đã được cung cấp, kèm theo định danh hàm băm.

9.3.8 [PDS][PDS+PGD] [CÓ ĐIỀU KIỆN] Trong trường hợp chữ ký số tách rời và dịch vụ bảo quản cho phép thuê bao chỉ cung cấp giá trị băm của dữ liệu đã ký số, dịch vụ bảo quản phải xác minh rằng đối tượng bảo quản được gửi chứa các định danh hàm băm phù hợp với các định danh được liệt kê trong hồ sơ bảo quản và mỗi giá trị băm có độ dài phù hợp với định danh hàm băm tương ứng.

Thư mục tài liệu tham khảo

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

[2] ETSI TS 119 511 V1.2.1 (2025-10), Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques (Chữ ký điện tử và hạ tầng tin cậy (ESI) – Yêu cầu về chính sách và an toàn đối với tổ chức cung cấp dịch vụ tin cậy cung cấp dịch vụ bảo quản dài hạn chữ ký số hoặc dữ liệu tổng quát bằng kỹ thuật chữ ký số).

[3] ETSI TR 119 001, Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations (Chữ ký điện tử và hạ tầng tin cậy (ESI) – Khung tiêu chuẩn hóa chữ ký – Thuật ngữ, định nghĩa và chữ viết tắt).

[4] ETSI TS 119 312, Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites (Chữ ký điện tử và hạ tầng tin cậy (ESI) – Bộ thuật toán mật mã).

[5] ETSI TS 119 122-3, Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES (Chữ ký số CAdES – Phần 3: Tích hợp cơ chế cú pháp bản ghi bằng chứng (ERS) trong CAdES).

[6] ETSI EN 319 162-1, Electronic Signatures and Trust Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers (Chữ ký điện tử và hạ tầng tin cậy (ESI) – Vùng chứa chữ ký liên kết (ASiC) – Phần 1: Các thành phần cơ bản và vùng chứa ASiC cơ sở).

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

[8] ETSI EN 319 411-2, Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (Chữ ký điện tử và hạ tầng tin cậy (ESI) – Yêu cầu về chính sách và an toàn đối với tổ chức cung cấp dịch vụ tin cậy phát hành chứng thư chữ ký số – Phần 2: Yêu cầu đối với tổ chức cung cấp dịch vụ tin cậy phát hành chứng thư đủ điều kiện của Liên minh châu Âu).

[9] ETSI EN 319 421, Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (Chữ ký điện tử và hạ tầng tin cậy (ESI) – Yêu cầu về chính sách và an toàn đối với tổ chức cung cấp dịch vụ tin cậy cấp dấu thời gian).

[10] ETSI EN 319 422, Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles (Chữ ký điện tử và hạ tầng tin cậy (ESI) – Giao thức cấp dấu thời gian và hồ sơ thẻ dấu thời gian).

[11] ETSI TS 119 512, Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services (Chữ ký điện tử và hạ tầng tin cậy (ESI) – Giao thức dành cho tổ chức cung cấp dịch vụ tin cậy cung cấp dịch vụ bảo quản dữ liệu dài hạn).

[12] ISO/IEC 21320-1:2015, Information technology — Document Container File — Part 1: Core (Công nghệ thông tin – Tệp vùng chứa tài liệu – Phần 1: Thành phần cốt lõi).

[13] ISO 14641-1:2018, Electronic archiving — Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation (Lưu trữ điện tử – Phần 1: Yêu cầu kỹ thuật đối với việc thiết kế và vận hành hệ thống thông tin bảo quản thông tin điện tử).

[14] ISO 14721:2012, Space data and information transfer systems — Open archival information system (OAIS) — Reference model (Hệ thống truyền dữ liệu và thông tin không gian – Hệ thống thông tin lưu trữ mở (OAIS) – Mô hình tham chiếu).

[15] ISO 16363:2011, Space data and information transfer systems — Audit and certification of trustworthy digital repositories (Hệ thống truyền dữ liệu và thông tin không gian – Đánh giá và chứng nhận kho lưu trữ số tin cậy).

[16] IETF RFC 3986, Uniform Resource Identifier (URI): Generic Syntax (Định danh tài nguyên thống nhất (URI) – Cú pháp chung).

[17] IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (Hạ tầng khóa công khai X.509 trên Internet – Hồ sơ chứng thư chữ ký số và danh sách chứng thư chữ ký số bị thu hồi).

[18] IETF RFC 6960 (2013), X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (Hạ tầng khóa công khai X.509 trên Internet – Giao thức kiểm tra trực tuyến trạng thái chứng thư chữ ký số).

[19] W3C Recommendation 26 November 2008, Extensible Markup Language (XML) 1.0 (Fifth Edition) (Ngôn ngữ đánh dấu mở rộng (XML) phiên bản 1.0 – Ấn bản lần thứ năm).

[20] BSI TR-03125-F, Preservation of Evidence of Cryptographically Signed Documents; Formats (TR-ESOR-F) (Bảo quản bằng chứng của tài liệu được ký số – Các định dạng).

[21] BSI TR-03125-M.3, Preservation of Evidence of Cryptographically Signed Documents; Formats (TR-ESOR-M.3) (Bảo quản bằng chứng của tài liệu được ký số – Các định dạng).