TCVN TIÊU CHUẨN QUỐC GIA

TCVN 7818 - 3:2010

ISO/IEC 18014 - 3:2009

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN - KỸ THUẬT AN NINH - DỊCH VỤ TEM THỜI GIAN - PHẦN 3: CƠ CHẾ TẠO THẺ LIÊN KẾT

Information technology – Security techniques – Time stamping services
Part 3: Mechanisms producing linked token

HÀ NỘI - 2010

Mục lục **Trang**

Lời nói đầu

TCVN 7818 – 3:2010 hoàn toàn tương đương với ISO/IEC 18014 – 3:2009.

TCVN 7818 – 3:2010 do Tiểu ban Kỹ thuật Tiêu chuẩn quốc gia TCVN/JTC1/SC27 "*Kỹ thuật mật mã*" biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ công bố.

Bộ tiêu chuẩn TCVN 7818 gồm 3 phần:

- TCVN 7818 – 1:2007 Công nghệ thông tin – Kỹ thuật mật mã – Dịch vụ cấp tem thời gian, phần 1: Khung tổng quát.
- TCVN 7818 – 2:2007 Công nghệ thông tin – Kỹ thuật mật mã – Dịch vụ cấp tem thời gian, phần 2: Cơ chế token độc lập.
- TCVN 7818 – 3:2010 Công nghệ thông tin – Kỹ thuật an ninh – Dịch vụ cấp tem thời gian, phần 3: Cơ chế tạo thẻ liên kết.

Công nghệ thông tin – Kỹ thuật an ninh – Dịch vụ cấp tem thời gian - Phần 3: Cơ chế tạo thẻ liên kết

Information technology – Security techniques – Time stamping services
Part 3: Mechanisms producing linked tokens

1 Phạm vi áp dụng

Tiêu chuẩn này:

- Mô tả mô hình chung cho các dịch vụ cấp tem thời gian tạo thẻ liên kết,
- Mô tả các thành phần cơ bản để xây dựng dịch vụ cấp tem thời gian tạo thẻ liên kết,
- Xác định cấu trúc dữ liệu tương tác với dịch vụ cấp tem thời gian tạo thẻ liên kết,
- Mô tả các trường hợp cụ thể của dịch vụ cấp tem thời gian tạo thẻ liên kết, và
- Xác định giao thức được sử dụng bởi dịch vụ cấp tem thời gian tạo thẻ liên kết nhằm mục đích gia hạn thẻ liên kết với các giá trị công bố.

2 Tài liệu viện dẫn

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

TCVN 7818-1:2007 Công nghệ thông tin – Kỹ thuật mật mã – Dịch vụ cấp tem thời gian - Phần 1: Khung tổng quát .

ISO/IEC 10118 (tất cả các phần), Information technology - Security techniques - Hash-functions *(Công nghệ thông tin – Kỹ thuật an ninh – Các hàm băm)*

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các định nghĩa sau:

3.1

Tổ hợp (aggregation)

Quá trình tạo mục dữ liệu đại diện cho một nhóm các mục dữ liệu được liên kết với nhau và tạo liên kết mật mã có thể xác minh giữa mỗi mục dữ liệu với các mục dữ liệu còn lại của nhóm đó.

3.2

Hàm băm kháng xung đột (collision-resistant hash-function)

Hàm băm thỏa mãn các đặc tính sau: không thể tính toán để tìm ra hai đầu vào khác nhau mà ánh xạ tới cùng một đầu ra.

[ISO/IEC 10118-1:2000, định nghĩa 3.2]

3.3

Biểu diễn mục dữ liệu (data item's representation)

Mục dữ liệu hoặc giá trị hàm băm tương ứng.

[TCVN 7818 - 1: 2007]

3.4

Hàm băm (hash-function)

Hàm ánh xạ các chuỗi bit thành các chuỗi bit có độ dài cố định, thỏa mãn hai đặc tính sau: với một đầu ra cho trước, không thể tính toán để tìm ra đầu vào tương ứng với đầu ra đó; và với một đầu vào cho trước, không thể tính toán để tìm ra đầu vào thứ hai có chung đầu ra với đầu vào đó.

[ISO/IEC 10118-1:2000, định nghĩa 3.5]

3.5

Giá trị băm (hash value)

Chuỗi các bit là đầu ra của hàm băm.

[ISO/IEC 10118-1:2000, định nghĩa 3.4]

3.6

Liên kết (link)

Mục dữ liệu chứng nhận sự tồn tại của ít nhất hai mục dữ liệu khác thông qua việc sử dụng các hàm băm kháng xung đột.

3.7

Tổ chức cấp tem thời gian (time-stamping authority)

TSA

Bên thứ ba tin cậy được chứng thực để cung cấp dịch vụ cấp tem thời gian.

[TCVN 7818 - 1: 2007, định ngĩa 3.17]

3.8

Dịch vụ cấp tem thời gian (time-stamping service)

TSS

Dịch vụ cung cấp bằng chứng rằng một mục dữ liệu đã tồn tại trước một thời điểm nào đó.

[TCVN 7818 - 1:2007, định nghĩa 3.18]

3.9

Thẻ tem thời gian (time-stamp token)

TST

Cấu trúc dữ liệu chứa ràng buộc mật mã có thể xác minh giữa biểu diễn của mục dữ liệu và một giá trị thời gian.

CHÚ THÍCH – Thẻ tem thời gian có thể bao gồm các mục dữ liệu bổ sung trong ràng buộc đó.

[TCVN 7818 – 1:2007, định nghĩa 3.15]

3.10

Bên thứ ba tin cậy (trusted third party)

TTP

Cơ quan về an ninh hoặc các đại diện của cơ quan đó được các thực thể khác tin cậy trong các hoạt động liên quan đến an ninh.

[ISO/IEC 10181 – 1:1996, định nghĩa 3.3.30]

4 Khái quát

Tiêu chuẩn này mô tả phương pháp và quá trình tạo thẻ tem thời gian có liên quan hoặc "được liên kết" với các thẻ tem thời gian khác được tạo bằng các phương pháp và quá trình được mô tả trong tiêu chuẩn này. Tổ chức cấp tem thời gian (TSA) sử dụng các phương pháp và quá trình này để cung cấp ràng buộc mật mã có thể xác minh và bảo mật giữa một thời điểm nào đó và các giá trị dữ liệu và để tăng cường an ninh của các thẻ tem thời gian thu được bằng cách giảm mức đảm bảo đòi hỏi trong các hoạt động của TSA. Tính tin cậy của thẻ tem thời gian được tính toán bằng phương pháp và quá trình này phụ thuộc vào tính toàn vẹn của kho do TSA duy trì để lưu trữ các kết quả tính toán thao tác liên kết trước đó. Tính toàn vẹn của kho các liên kết và các thao tác liên kết được thực hiện bởi TSA có thể xác minh bằng mật mã và không phụ thuộc vào tính tin cậy của hạ tầng khóa công khai (PKI) hoặc yêu cầu chứng thực rằng khóa riêng không bị hỏng.

Ngoài ra, tiêu chuẩn này:

- Mô tả các phương pháp và quá trình khi TSA tạo các thẻ liên kết có thể sử dụng để tạo ra các giá trị được dẫn xuất từ các thao tác liên kết của nó với mục đích phổ biến rộng rãi chúng trên các phương tiện trực tuyến hoặc ngoại tuyến, và
- Định nghĩa giao thức "yêu cầu - đáp ứng" cho phép thẻ tem thời gian cấp bởi TSA được gia hạn cho các mục dữ liệu dựa trên các giá trị do TSA công bố.

Các dịch vụ cấp tem thời gian tuân theo tiêu chuẩn này có thể liên tác thông qua việc sử dụng các thẻ, các thao tác và các định dạng dữ liệu chuẩn. Nói chung, TSA tạo thẻ liên kết sử dụng các đặc tính mật mã của hàm băm để "liên kết" một thẻ tem thời gian với các thẻ tem thời gian khác được tạo trước đó bởi TSA đó. Một phương pháp được khuyến cáo khi tính toán giá trị liên kết một sự kiện với các liên kết đã tạo trước là nên ghép nối biểu diễn dữ liệu của sự kiện với liên kết và sử dụng kết quả ghép nối này làm đầu vào của hàm băm. Giá trị băm thu được cung cấp liên kết mật mã có thể xác minh giữa sự kiện và các liên kết đã tạo trước. Hàm băm kháng xung đột được định nghĩa trong ISO/IEC 10118 thích hợp để định dạng thẻ liên kết: tính kháng nghịch ảnh giúp che giấu nội dung của mục dữ liệu gốc từ TSA, trong khi tính kháng xung đột đảm bảo rằng thẻ giả không thể được chèn vào tập hợp các thẻ liên kết đã có.

CHÚ THÍCH – Đối với xử lý đầy đủ của việc cấp tem thời gian với các thẻ liên kết, xem [HS91], [BHS93], [HS97], [BLLV98] và [BLS00]. Để chứng minh tính an toàn của kỹ thuật liên kết này, xem [HS97] Mục 3.1, Định lý 1.

5 Thao tác quy định cho TSA tạo thẻ liên kết

5.1 Thao tác liên kết

Thao tác liên kết là hình thành các ràng buộc có thể xác minh giữa thẻ tem thời gian và các liên kết đã được TSA tạo trước đó thông qua việc sử dụng hàm băm kháng xung đột. Giá trị được tạo gần đây nhất để liên kết cung cấp một tóm tắt mật mã về các thẻ tem thời gian như đã tham gia trong quá trình liên kết.

TSA phù hợp khi tạo các thẻ liên kết phải thực hiện các thao tác liên kết bằng một trong các phương pháp sau:

- Liên kết xích tuyến tính;
- Liên kết nhị phân chống đơn điệu;
- Liên kết cây phân luồng.

Liên kết xích tuyến tính tạo các liên kết theo cách sau: đầu tiên giá trị của liên kết mới tạo gần nhất phải ghép nối với giá trị băm của một biểu diễn sự kiện xảy ra gần nhất, sau đó áp dụng hàm băm kháng xung đột cho giá trị thu được trên.

Liên kết nhị phân chống đơn điệu tạo các liên kết theo cách sau: đầu tiên giá trị của hai liên kết đã có trước ghép nối với các giá trị băm của một biểu diễn sự kiện xảy ra gần nhất, sau đó hàm băm kháng xung đột áp dụng vào giá trị nhận được. Một trong hai liên kết đầu vào phải là liên kết mới được tạo gần nhất và định danh chính xác liên kết còn lại phải được xác định bởi cấu trúc dữ liệu, được TSA duy trì và có dạng đồ thị phi chu trình có hướng (xem Phụ lục B.2.3).

Liên kết cây phân luồng tạo các liên kết theo cách sau: đầu tiên các giá trị của một số các liên kết đã có trước phải ghép nối với các giá trị băm của một biểu diễn sự kiện xảy ra gần nhất, sau đó áp dụng hàm băm kháng xung đột vào giá trị thu được. Một trong các liên kết đầu vào phải là liên kết mới được tạo gần nhất và định danh chính xác của các liên kết còn lại được xác định bởi cấu trúc dữ liệu, được TSA duy trì và có dạng của cây phân luồng (xem Phụ lục B.2.4).

Trong tất cả các trường hợp, các mục dữ liệu khác có thể ghép nối với đầu vào của hàm băm kháng xung đột trước khi tạo ra liên kết mới (ví dụ: tham số biến thiên theo thời gian). Ngoài ra, nhiều hàm băm kháng xung đột được sử dụng đồng thời trên cùng đầu vào với mục đích sinh ra liên kết mới và trong trường hợp này, liên kết mới được tạo ra từ ghép nối các kết quả hàm băm với nhau.

Các giá trị của các liên kết trước đã sử dụng làm đầu vào của hàm băm kháng xung đột phải được gộp trong (các) thẻ tem thời gian gắn liền sự kiện xảy ra gần đây nhất và trả lại cho bên yêu cầu trong các trường "links" của cấu trúc 'BindingInfo' (xem Điều 7.4).

Nếu sử dụng hàm băm cho thao tác liên kết thì phải sử dụng các hàm quy định trong ISO/IEC 10118.

Phụ lục B.2 gồm thảo luận bổ sung về các thuật toán có thể sử dụng trong thao tác liên kết.

5.2 Thao tác tổ hợp

Thao tác tổ hợp là việc hình thành một ràng buộc có thể xác minh trong nhóm thẻ tem thời gian mà được gán cùng giá trị thời gian thông qua việc sử dụng hàm mật mã có cả hai tính chất kháng nghịch ảnh và kháng xung đột, chẳng hạn như hàm băm kháng xung đột. Lược đồ tổ hợp lấy một nhóm thẻ tem thời gian làm đầu vào và tạo một giá trị tổ hợp đơn, cũng như liên kết dữ liệu mật mã có thể xác minh của từng thẻ tem thời gian với phần còn lại của nhóm. Giá trị tổ hợp được kết hợp với thao tác tổ hợp được tiếp tục sử dụng làm đầu vào cho thao tác liên kết của TSA, theo cách tương tự với trường hợp thao tác liên kết cho một thẻ tem thời gian đơn. Một TSA phù hợp phải thực hiện các thao tác liên kết cho nhóm thẻ tem thời gian thay vì cho từng thẻ tem thời gian riêng lẻ, để nâng cao hiệu quả tính toán hoặc đạt được khả năng mở rộng dịch vụ cao hơn.

TSA phù hợp khi tạo các thẻ liên kết hỗ trợ tổ hợp phải thực hiện các thao tác tổ hợp, sử dụng một trong các phương pháp sau:

- Tổ hợp kiểu cây Merkle;
- Tổ hợp kiểu tích lũy một chiều.

Tất cả các dạng tổ hợp đều đòi hỏi áp dụng đầu tiên hàm băm kháng xung đột vào cấu trúc gói dữ liệu 'TSTInfo' của các thẻ tem thời gian cần tổ hợp. Ở đây đề cập tới các giá trị băm thu được là "các giá trị băm cần tổ hợp".

Tổ hợp kiểu cây Merkle đòi hỏi sắp xếp các giá trị băm để tổ hợp giống như lá trong cấu trúc cây (xem Phụ lục B.3.3). Một giá trị được gán cho một nút không lá của cây bằng cách ghép các giá trị băm đã gán cho các nút con của nó và sau đó áp dụng hàm băm kháng xung đột, tiếp tục cho đến khi tất cả các nút của cây đều đã được gán giá trị. Giá trị được gán cho nút gốc của cây là giá trị tổ hợp. Nhiều hàm băm kháng xung đột được áp dụng đồng thời trong quá trình này và trong trường hợp này giá trị bị gán cho nút không lá được tính bằng cách ghép nối các giá trị băm sinh ra từ từng hàm băm riêng lẻ.

Tổ hợp kiểu tích lũy một chiều đòi hỏi tính toán giá trị tổ hợp sao cho việc xác minh giá trị tổ hợp cho bất kỳ giá trị băm nào tham gia được thực hiện trong một khoảng thời gian không đổi bất kể số lượng giá trị băm được tổ hợp. Cách thức để thực hiện chính xác việc này nằm ngoài phạm vi của tiêu chuẩn này, ví dụ về một số kỹ thuật này được trình bày trong Phụ lục B.3.4.

Hàm băm được sử dụng trong thao tác tổ hợp phải sử dụng hàm được quy định trong ISO/IEC 10118.

Phụ lục B.3 gồm các thảo luận bổ sung về các thuật toán được sử dụng trong thao tác tổ hợp.

CHÚ THÍCH – Các dạng thường gặp của tổ hợp bao gồm cây băm Merkle [M80], tích lũy một chiều [BD93], hoặc các lược đồ liên kết nhị phân khác [BLLV98].

5.3 Thao tác công bố

Giá trị dẫn xuất từ các liên kết được tạo bởi TSA phù hợp, có thể được công bố theo cách làm cho thao tác liên kết được "chứng nhận rộng rãi". Điều này có thể thực hiện được bằng việc cho công bố định kỳ trên các phương tiện truyền thông rộng rãi sẵn có, ví dụ như trang web hoặc các ấn phẩm in. Giá trị được công bố phụ thuộc vào tất cả các thẻ tem thời gian đã được TSA tạo ra kể từ sự kiện công bố trước đó. Bằng cách liên kết các thẻ với các sự kiện "chứng nhận rộng rãi", trên thực tế TSA tạo ra các tuyên bố có thể xác minh về thời điểm mà mỗi thẻ tem thời gian được tạo ra từ hệ thống.

TSA phù hợp khi tạo các thẻ liên kết hỗ trợ việc công bố phải thực hiện các thao tác công bố, sử dụng một trong các phương pháp sau:

- Công bố liên kết đơn;
- Công bố cây Merkle.

Công bố liên kết đơn là việc công bố định kỳ một giá trị liên kết đơn. Giá trị liên kết đơn này cho phép xác minh tất cả các giá trị liên kết đã được tạo ra cho đến thời điểm mà tại đó nó được tạo ra. Để biết thêm chi tiết xem trong Phụ lục B.4.3.

Công bố cây Merkle là việc công bố định kỳ tổ hợp cây Merkle của tất cả các liên kết được tạo ra sau sự kiện công bố gần nhất. Để biết thêm chi tiết xem Phụ lục B.4.4.

Hàm băm được sử dụng trong thao tác tổ hợp phải sử dụng hàm được quy định trong ISO/IEC 10118.

Phụ lục B.4 gồm các thảo luận bổ sung về các thao tác công bố từ TSA phù hợp.

5.4 Thao tác mở rộng

Khi TSA phù hợp làm cho giá trị công bố khả dụng, thực thể đang sở hữu thẻ liên kết được phát hành từ TSA này có thể thực hiện một giao thức "yêu cầu - đáp ứng" với TSA hoặc các bên TTP có quyền truy cập vào liên kết của TSA với mục đích gia hạn thẻ tem thời gian đến một giá trị công bố, bằng cách sử dụng kênh bảo mật tính toàn vẹn và xác thực nguồn gốc dữ liệu. Giao thức này nên được thực hiện khi giá trị công bố tương ứng với thẻ tem thời gian này đã được TSA phát hành và trở thành khả dụng, kết quả là tạo ra thẻ tem thời gian mới chứa các thành phần giống với bản gốc, cũng như các mục dữ liệu bổ sung liên quan đến các giá trị công bố và ràng buộc với các thẻ liên kết. Các mục dữ liệu bổ sung cho phép tính toán giá trị công bố tương ứng, mà không cần yêu cầu truy cập vào liên kết của bên TSA. Định dạng thông điệp hỗ trợ thao tác mở rộng được mô tả tại các Điều 6.5 và 6.6.

6 Định dạng thông điệp

6.1 Yêu cầu tem thời gian

Yêu cầu tem thời gian là một thông điệp được gửi bởi bên yêu cầu tem thời gian tới TSA, nhằm yêu cầu TSA phát hành một thẻ tem thời gian cho các mục dữ liệu trong thông điệp đó. Theo định nghĩa trong TCVN 7818 - 1, yêu cầu tem thời gian chứa các trường dữ liệu liệt kê trong Bảng 1.

Bảng 1: Yêu cầu tem thời gian.

Trường dữ liệu	Mô tả
version	Số phiên bản của cấu trúc dữ liệu
messageImprint	Dấu thông điệp được TSA gắn với giá trị thời gian
reqPolicy	Chính sách dịch vụ được TSA yêu cầu (tùy chọn)
nonce	Định danh cho phép yêu cầu được phù hợp với với thẻ tem thời gian đã phát hành (tùy chọn)
certReq	Yêu cầu TSA cung cấp thông tin chứng chỉ (nếu có)
extensions	Các mục bổ sung để hoàn thành một cách đầy đủ yêu cầu của tem thời gian được yêu cầu (tùy chọn)

Phụ lục A đưa ra định nghĩa mô đun ASN.1 về yêu cầu tem thời gian: `TimeStampReq`.

6.2 Đáp ứng tem thời gian

Đáp ứng tem thời gian là thông điệp phản hồi được gửi từ TSA để đáp ứng lại yêu cầu tem thời gian. Theo định nghĩa trong TCVN 7818 – 1, đáp ứng tem thời gian chứa các trường dữ liệu liệt kê trong Bảng 2.

Bảng 2: Đáp ứng tem thời gian.

Trường dữ liệu	Mô tả
status	Trạng thái của thao tác tem thời gian
timeStampToken	Thẻ tem thời gian được phát hành, nếu các thao tác tem thời gian thực hiện thành công.

Phụ lục A đưa ra định nghĩa mô đun ASN.1 về đáp ứng tem thời gian: `TimeStampResp`.

6.3 Yêu cầu xác minh

Yêu cầu xác minh là thông điệp được gửi bởi bên xác minh tem thời gian tới TSA hoặc bên TTP có quyền truy cập vào liên kết của TSA để yêu cầu thực thể nhận thông điệp xác minh tính hợp lệ của thẻ tem thời gian chứa trong thông điệp. Theo định nghĩa trong TCVN 7818 - 1, yêu cầu xác minh chứa các trường dữ liệu liệt kê trong Bảng 3.

Bảng 3: Yêu cầu xác minh.

Trường dữ liệu	Mô tả
version	Số phiên bản của cấu trúc dữ liệu
tst	Thẻ tem thời gian đang được xác minh
requestID	Định danh yêu cầu (tùy chọn)

Phụ lục A đưa ra định nghĩa mô đun ASN.1 về yêu cầu xác minh: `VerifyReq`.

6.4 Đáp ứng xác minh

Đáp ứng xác minh là thông điệp phản hồi từ TSA hoặc bên TTP có quyền truy cập vào liên kết của TSA trong đáp ứng đối với yêu cầu xác minh. Theo định nghĩa trong TCVN 7818 - 1, đáp ứng xác minh chứa các trường dữ liệu liệt kê trong Bảng 4.

Bảng 4: Đáp ứng xác minh.

Trường dữ liệu	Mô tả
version	Số phiên bản của cấu trúc dữ liệu.
status	Trạng thái của thao tác xác minh.
tst	Thẻ tem thời gian được đệ trình.
requestID	Định danh đáp ứng, tương ứng với định danh yêu cầu (*tùy chọn*)

Phụ lục A đưa ra định nghĩa mô đun ASN.1 về đáp ứng xác minh: `VerifyResp`.

6.5 Yêu cầu mở rộng

Yêu cầu mở rộng là thông điệp được gửi từ thực thể sở hữu thẻ liên kết tới TSA hoặc bên TTP có quyền truy cập vào liên kết của TSA đó để yêu cầu thực thể nhận thông điệp mở rộng thẻ tem thời gian

chứa trong thông điệp đó với các mục dữ liệu bổ sung dựa vào giá trị công bố bởi TSA phát hành. Yêu cầu mở rộng có thể được đảm bảo một khi việc công bố đối với thẻ tem thời gian được thực hiện, nghĩa là sau khi TSA phát hành giá trị khoảng thời gian được công bố bao hàm giá trị thời gian trong thẻ tem thời gian. Yêu cầu mở rộng chứa các trường dữ liệu liệt kê trong Bảng 5.

Bảng 5: Yêu cầu mở rộng.

Trường dữ liệu	Mô tả
version	Số phiên bản của cấu trúc dữ liệu
tst	Thẻ tem thời gian đợi gia hạn với giá trị công bố.
requestID	Định danh yêu cầu (tùy chọn)

Đối với mục đích của tiêu chuẩn này, trường "version" được đặt giá trị là 1.

Trường "requestID" gắn kết yêu cầu mở rộng với đáp ứng mở rộng tương ứng.

Phụ lục A đưa ra định nghĩa mô đun ASN.1 về yêu cầu mở rộng: `ExtendReq`.

6.6 Đáp ứng mở rộng

Đáp ứng mở rộng là thông điệp phản hồi từ TSA hoặc bên TTP có quyền truy cập vào liên kết của TSA để đáp ứng lại yêu cầu mở rộng. Nếu yêu cầu được đáp ứng, thì một thẻ tem thời gian mới được gửi lại ở trong đáp ứng với các mục dữ liệu bổ sung dựa vào giá trị công bố của TSA. Đáp ứng mở rộng chứa các trường dữ liệu liệt kê trong Bảng 6.

Bảng 6: Đáp ứng mở rộng.

Trường dữ liệu	Mô tả
version	Số phiên bản của cấu trúc dữ liệu
status	Trạng thái của thao tác mở rộng.
tst	Thẻ tem thời gian đã cập nhật nếu yêu cầu mở rộng được đáp ứng; nếu không thì để nguyên thẻ tem thời gian gốc.
requestID	Định danh đáp ứng, tương ứng với định danh yêu cầu (tùy chọn)

Đối với mục đích của tiêu chuẩn này, trường "version" được đặt giá trị là 1.

Trường "status" cho biết kết quả của thao tác mở rộng được thực hiện bởi việc hoàn thành đáp ứng đó của TSA hoặc TTP khác để mở rộng thẻ tem thời gian được đệ trình đến giá trị được công bố.

Trường "tst" bao gồm thẻ tem thời gian tương ứng với thẻ tem thời gian đã gửi trong yêu cầu mở rộng tương ứng. Nếu yêu cầu mở rộng đó không được đáp ứng, thì thẻ tem thời gian trong trường "tst" chính là thẻ lấy từ yêu cầu mở rộng; Nếu yêu cầu mở rộng đó được đáp ứng, thì thẻ tem thời gian trong trường "tst" phù hợp với một trong tất cả các thành phần của yêu cầu mở rộng với trường hợp ngoại lệ có thể có của bất kỳ mục dữ liệu nào bên trong thành phần mở rộng đã công bố hiện có thuộc cấu trúc 'BindingInfo' của thẻ tem thời gian và các mục dữ liệu bổ sung dựa vào ít nhất một giá trị đã công bố. Các mục dữ liệu bổ sung có trong một hoặc nhiều cấu trúc 'PublicationInfo' được mô tả trong Điều 7.8. Trong trường hợp thẻ tem thời gian sử dụng gói "DigestedData" như mô tả trong Điều 8.2,

cấu trúc 'PublicationInfo' có tại phần mở rộng đã công bố bên trong trường "extensions" thuộc cấu trúc 'BindingInfo' của thẻ tem thời gian.

Trường "requestID" phải có mặt nếu định danh yêu cầu có trong yêu cầu mở rộng tương ứng; trong trường hợp này, nó phải có cùng giá trị với định danh yêu cầu trong yêu cầu mở rộng tương ứng.

Phụ lục A đưa ra định nghĩa mô đun ASN.1 về đáp ứng mở rộng: `ExtendResp`.

7 Kiểu dữ liệu

7.1 Định danh đối tượng

Trong tiêu chuẩn này việc định nghĩa cung định danh đối tượng gốc nhằm hỗ trợ cho việc cấp phát các định danh đối tượng tiếp theo. Trong Phụ lục A có Mô đun ASN.1 định nghĩa định danh đối tượng là `tsp-lt` và được mô phỏng như sau:

```
tsp-lt ::= OBJECT IDENTIFIER { iso(1) standard(0) time-stamp(18014) lt(3) }
```

Các định danh đối tượng tiếp theo được định nghĩa trong tiêu chuẩn này bắt nguồn từ định danh gốc này và được liệt kê trong Phụ lục A. Các định danh đối tượng bổ sung được quy định ở nơi khác và được sử dụng trong tiêu chuẩn này cũng được trình bày trong Phụ lục A.

7.2 TSTInfo

Kiểu dữ liệu 'TSTInfo' biểu diễn đối tượng được tạo bởi TSA trong quá trình phát hành thẻ tem thời gian. Theo định nghĩa trong TCVN 7818 - 1, kiểu dữ liệu 'TSTInfo' chứa các trường dữ liệu liệt kê trong Bảng 7.

Bảng 7: Kiểu dữ liệu TSTInfo.

Trường dữ liệu	Mô tả
version	Số phiên bản của cấu trúc dữ liệu
policy	Điều khoản dịch vụ của TSA
messageImprint	Dấu thông điệp được TSA gắn kết với giá trị thời gian
serialNumber	Số nguyên được gán bởi TSA
genTime	Thời gian được gán bởi TSA
accuracy	Độ chính xác của trường "genTime" so với UTC (tùy chọn)
ordering	Kiểu Boolean, mặc định là "false", nếu đặt là "true" thì cho phép sắp thứ tự các thẻ tem thời gian đã được phát hành từ TSA dựa trên một mình trường "genTime" (bỏ qua trường "accuracy")
nonce	Định danh phù hợp với trường "nonce" của yêu cầu tem thời gian (tùy chọn)
tsa	Tên của TSA (tùy chọn)
extensions	Các mục dữ liệu bổ sung (tùy chọn)

Với mục đích của tiêu chuẩn này, thì trường "version" có giá trị là 1.

Trường "serialNumber" có thể đặt giá trị bằng 0, nếu giá trị khác 0 thì giá trị của nó phải là một số nguyên được gán bởi TSA cho mỗi thẻ tem thời gian và phải là duy nhất đối với từng thẻ tem thời gian do TSA phát hành trong suốt thời gian thao tác tồn tại.

Trường "extensions" chứa các mục dữ liệu biểu diễn các thông tin bổ sung về các mục dữ liệu trong yêu cầu tem thời gian tương ứng. Điều 7.9.1 có định nghĩa về các kiểu dữ liệu có thể sử dụng trong trường "extensions" này.

Phụ lục A đưa ra định nghĩa mô đun ASN.1 về kiểu dữ liệu 'TSTInfo' : `TSTInfo`.

7.3 TimeStampToken

Kiểu dữ liệu 'TimeStampToken' biểu diễn cho thẻ tem thời gian được phát hành bởi TSA. Theo định nghĩa trong TCVN 7818 - 1, TSA tạo ra thẻ tem thời gian bằng cách:

- Tạo cấu trúc 'TSTInfo' theo các mục dữ liệu có trong yêu cầu tem thời gian,
- Thực hiện các thao tác theo cơ chế tem thời gian mà TSA sử dụng,
- Đóng gói cấu trúc 'TSTInfo' thu được và các mục dữ liệu khác theo kiểu gói nội dung phù hợp với cơ chế tem thời gian mà TSA sử dụng.

Đối với mục đích của tiêu chuẩn này thì chỉ có kiểu gói nội dung dạng "DigestedData" và "SignedData" mới được hỗ trợ.

Mô đun ASN.1 định nghĩa kiểu dữ liệu 'TimeStampToken' trong Phụ lục A là: `TimeStampToken`.

7.4 BindingInfo

Kiểu dữ liệu 'BindingInfo' biểu diễn các mục dữ liệu được tạo ra bởi TSA như là kết quả của việc liên kết gói cấu trúc 'TSTInfo' của một thẻ tem thời gian với các thẻ tem thời gian đã tạo trước đó. Kiểu dữ liệu 'BindingInfo' chứa các trường dữ liệu liệt kê trong Bảng 8.

Bảng 8: Kiểu dữ liệu 'BindingInfo'.

Trường dữ liệu	Mô tả
version	Số phiên bản của cấu trúc dữ liệu
msgImprints	Phân loại thông điệp được tính trên gói cấu trúc 'TSTInfo' của thẻ tem thời gian
aggregate	Dữ liệu xác thực tổ hợp trường "msgImprints" với các nhân tố khác của tập hợp (*tùy chọn*)
links	Mục dữ liệu kết hợp kết quả của trường "msgImprints" và trường "aggregate" với các kết quả ưu tiên của các thao tác liên kết.
publish	Dữ liệu xác thực kết quả của thao tác liên kết dựa vào giá trị công bố (*tùy chọn, không nên dùng*)
extensions	Các mục dữ liệu bổ sung (*tùy chọn*)

Đối với mục đích của tiêu chuẩn này, trường "version" có giá trị là 1.

Trường "msgImprints" được tính toán trên gói cấu trúc 'TSTInfo' của thẻ tem thời gian như trong mô tả ở Điều 8.1.

Trường "aggregate" chứa một hoặc nhiều phiên bản kiểu 'Chain' và xác nhận sự tham gia của trường "msgImprints" trong thao tác tổ hợp như mô tả ở Điều 8.1 (nếu có). Một phiên bản của kiểu 'Chain' chứa dữ liệu xác thực tham gia trong một thao tác tổ hợp đơn. Trường "aggregate" có thể chứa nhiều phiên bản của kiểu 'Chain' khi lược đồ tổ hợp đa tầng được hỗ trợ và giá trị của các trường hợp kiểu 'Chain' được tính toán tuần tự.

Trường "links" chứa một hoặc nhiều phiên bản kiểu 'Link'. Nó biểu diễn thao tác liên kết giá trị thời gian được gán vào gói 'TSTInfo' của thẻ tem thời gian tương ứng và chứa trong đó các thành phần kết quả của các thao tác liên kết từ những giá trị thời gian ưu tiên đang làm đầu vào hiện hành. Trường "links" luôn phải chứa bên trong các thành phần của nó kết quả của các thao tác liên kết với giá trị thời gian tức thời, nó biểu diễn tóm tắt hoạt động của các thao tác liên kết tích lũy cho đến hiện tại. Nếu có nhiều phiên bản kiểu 'Link' có mặt, thì giá trị của các trường hợp kiểu 'Link' được tính toán tuần tự.

Đối với cấu trúc 'BindingInfo' cho trước bên trong thẻ tem thời gian, kết quả của thao tác liên kết đối với giá trị thời gian trong gói cấu trúc 'TSTInfo' phải được tính toán như sau: nếu không tồn tại trường "aggregate", giá trị của trường "links" được tính toán lấy trong nội dung của trường "msgImprints"; mặt khác, giá trị đầu tiên của trường "aggregate" được tính toán lấy trong nội dung của trường "msgImprints" và sau đó giá trị của trường "links" được tính toán lấy trong kết quả tính toán trước đó của trường "aggregate".

Không nên sử dụng trường "publish", xem trong Điều 7.9.2.3 và 7.8 về thông tin bổ sung liên quan đến giá trị công bố và các kiểu dữ liệu có thể chuyển vào trường "extensions" của cấu trúc 'BindingInfo'.

Trường "extensions" chứa các mục dữ liệu biểu diễn thông tin bổ sung liên quan đến các thao tác tổ hợp, liên kết và công bố đối với giá trị thời gian có trong gói cấu trúc 'TSTInfo' của thẻ tem thời gian. Điều 7.9.2 định nghĩa các kiểu dữ liệu có thể được sử dụng trong trường "extensions".

Mô đun ASN.1 định nghĩa kiểu dữ liệu 'BindingInfo' trong phụ lục A là: `BindingInfo`.

7.5 Chain

Kiểu dữ liệu 'Chain' biểu diễn dãy các thao tác đại diện cho thao tác tổ hợp hoặc thao tác công bố. Kiểu dữ liệu 'Chain' chứa các trường dữ liệu liệt kê trong Bảng 9.

Bảng 9: Kiểu dữ liệu 'Chain'.

Trường dữ liệu	Mô tả
algorithm	Định danh đối tượng của thuật toán được sử dụng để tính toán giá trị của xích.
links	dãy các mục dữ liệu của kiểu 'Link'

Giá trị của một trường hợp kiểu 'Chain' được tính toán bằng cách thực hiện thuật toán được quy định trong trường "algorithm" qua trình tự các trường hợp kiểu 'Link' chứa trong trường "links". Ví dụ: một phiên bản kiểu 'Chain' có thể được xây dựng để biểu diễn kết quả tính toán cây băm Makle [M80]; trong trường hợp này, dãy các trường hợp kiểu 'Link' biểu diễn đường dẫn tính toán từ một nút lá đã xác định đến nút gốc chung. Phụ lục B.3 có chứa thảo luận bổ sung về các thuật toán có thể sử dụng trong các thao tác tổ hợp.

Mô đun ASN.1 định nghĩa kiểu dữ liệu 'Chain' trong phụ lục A là: `Chain`.

7.6 Link

Kiểu dữ liệu 'Link' biểu diễn một thao tác liên kết đơn hoặc một bước đơn của thao tác tổ hợp hoặc công bố. Kiểu dữ liệu 'Link' chứa các trường dữ liệu liệt kê trong Bảng 10.

Bảng 10: Kiểu dữ liệu 'Link'.

Trường dữ liệu	Mô tả
algorithm	Định danh đối tượng của thuật toán được sử dụng để tính toán giá trị liên kết (*tùy chọn*)
identifier	Định danh liên kết cục bộ, trong khi liên kết được chỉ đến bởi các liên kết khác (*tùy chọn*)
members	Dãy các mục dữ liệu của kiểu cấu trúc 'Node' được liên kết.

Giá trị của phiên bản của kiểu 'Link' được tính toán bằng cách thực hiện thuật toán được quy định trong trường "algorithm" trên dãy các phiên bản của kiểu 'Node' có chứa trong trường "members". Nếu kết quả của việc tính toán này được sử dụng làm đầu vào của các thao tác khác, chúng được định danh bởi định danh cục bộ lưu trữ trong trường "identifier" trên phiên bản kiểu 'Link'. Nếu trường "algorithm" không có mặt, thì thuật toán được sử dụng để tính toán giá trị của phiên bản kiểu 'Link' được xác định bởi ngữ cảnh. Trong trường hợp mà phiên bản kiểu 'Chain' chứa một dãy các trường hợp kiểu 'Link', thì thuật toán được sử dụng để tính toán giá trị của bất kỳ phiên bản kiểu 'Link' không có trường "algorithm" phải là thuật toán được quy định trong trường "algorithm" của phiên bản kiểu 'Chain'. Phụ lục B.2 có chứa thảo luận bổ sung về các thuật toán có thể được sử dụng trong các thao tác liên kết.

Mô đun ASN.1 định nghĩa kiểu dữ liệu 'Link' trong phụ lục A là: `Link`.

7.7 Node

Kiểu dữ liệu 'Node' biểu diễn một phần tử đầu vào đơn cho thao tác liên kết hoặc cho một bước của thao tác tổ hợp hoặc công bố. Kiểu dữ liệu 'Node' chứa các trường dữ liệu liệt kê trong Bảng 11.

Bảng 11: Kiểu dữ liệu 'Node'.

Trường dữ liệu	Mô tả
imprints	Các mục dữ liệu đầu vào
reference	Định danh cục bộ của phiên bản kiểu 'Link' mà từ đó thu được các mục dữ liệu đầu vào

Nếu trường "imprints" có mặt, thì phiên bản kiểu 'Node' chứa các mục dữ liệu hiện thời và giá trị của chúng phải được sử dụng như là một phần của các thao tác tiếp theo bao gồm cả phiên bản kiểu 'Node' này.

Nếu trường "reference" có mặt và giá trị của nó khác 0, thì phiên bản kiểu 'Node' cho biết có một phiên bản kiểu 'Link' trong ngữ cảnh. Trong trường hợp phiên bản kiểu 'Chain' có chứa một dãy các trường hợp kiểu 'Link' và cho một phiên bản kiểu 'Link' cụ thể có chứa một dãy các trường hợp kiểu 'Node', sự hiện diện của trường "reference" với giá trị khác 0 bên trong một phiên bản kiểu 'Node' ghép nối tới phiên bản kiểu 'Node' này thì cho phép định danh phiên bản kiểu 'Link' bằng giá trị số nguyên trong trường "identifier" của nó chứa bên trong phiên bản kiểu 'Chain'. Giá trị của phiên bản kiểu 'Node' phải là giá trị tham khảo của phiên bản kiểu 'Link'.

Nếu trường "reference" có mặt và giá trị của nó bằng 0, thì giá trị của phiên bản kiểu 'Node' thu được từ một nguồn ngoại vi mà tính toàn vẹn phụ thuộc vào ngữ cảnh. Trong trường hợp từng phiên bản của dãy các trường hợp kiểu 'Chain' chứa một dãy các trường hợp kiểu 'Link' và cho trường hợp phiên bản kiểu 'Link' cụ thể chứa một dãy các trường hợp kiểu 'Node', tại đó giá trị của một phiên bản kiểu 'Node' chứa đựng trường "reference" có giá trị 0 phải bằng giá trị phiên bản kiểu 'Chain' ngay trước phiên bản kiểu 'Chain' chứa phiên bản kiểu 'Node' đã nói ở trên.

Mô đun ASN.1 định nghĩa kiểu dữ liệu 'Node' trong phụ lục A là: `Node`.

7.8 PublicationInfo

Kiểu dữ liệu 'PublicationInfo' biểu diễn thông tin xác thực kết quả của thao tác liên kết được thực hiện bởi TSA dựa vào giá trị công bố (do TSA phát hành) và nó cung cấp các mục dữ liệu được yêu cầu cho việc nhận diện và tính toán giá trị công bố đó. Kiểu dữ liệu 'PublicationInfo' chứa các trường dữ liệu liệt kê trong Bảng 12.

Bảng 12: Kiểu dữ liệu 'PublicationInfo'.

Trường dữ liệu	Mô tả
pubTime	Giá trị thời gian gán vào sự kiện công bố (tùy chọn)
pubId	Định danh của giá trị công bố (tùy chọn)
pubChains	Dữ liệu xác thực sự tham gia của kết quả của thao tác liên kết trong sự kiện công bố (tùy chọn)
sourceId	Định danh của nguồn dữ liệu tham gia trong việc tạo giá trị công bố (tùy chọn)

Trường "pubTime" (nếu có) xác định giá trị thời gian gán vào sự kiện công bố đối với giá trị công bố được quan tâm. Ví dụ: trong trường hợp mà trường "pubId" nhận diện một sự công bố bằng phương tiện in hàng loạt, khi đó trường "pubTime" phải xác định thời gian công bố cho chuỗi các vấn đề có chứa giá trị công bố được quan tâm.

Trường "pubId" (nếu có) nhận diện vị trí của giá trị công bố được quan tâm. Ví dụ: trường "pubId" có thể là tên thư mục hoặc một URI cho biết vị trí của giá trị công bố được quan tâm.

Trường "pubChains" (nếu có) là một dãy phiên bản kiểu 'Chain'. Đối với thao tác liên kết cho trước được thực hiện bởi TSA, trường này được định nghĩa theo thao tác công bố được thực hiện bởi TSA đối với khoảng thời gian thực chứa giá trị thời gian của thao tác liên kết đã nói ở trên.

Trường "sourceId" (nếu có) xác định dữ liệu nguồn cho giá trị công bố, như vậy kết quả của các thao tác liên kết được tạo ra và duy trì bởi TSA cũng được sử dụng để tạo ra giá trị công bố, cũng như các đặc tính bổ sung bên trong của sự kiện công bố (ví dụ: tần suất công bố, khoảng thời gian được chứa trong kho các liên kết được duy trì bởi TSA,...).

Mô đun ASN.1 định nghĩa kiểu dữ liệu 'PublicationInfo' trong Phụ lục A là: `PublicationInfo`.

7.9 Mở rộng

7.9.1 Mở rộng yêu cầu tem thời gian

7.9.1.1 Mở rộng giá trị băm

Bên yêu cầu tem thời gian muốn đệ trình việc cấp tem thời gian với nhiều hơn một giá trị băm được dẫn xuất từ một mục dữ liệu đơn. Mở rộng giá trị băm được định nghĩa để cho phép đệ trình nhiều giá trị băm. Mở rộng này được chứa cả trong trường "extensions" của yêu cầu tem thời gian gửi bởi bên yêu cầu tới TSA và trong trường "extensions" của cấu trúc 'TSTInfo' thu được tạo bởi TSA và gửi lại bên yêu cầu trong thẻ tem thời gian.

Nếu mở rộng này hiện diện trong yêu cầu tem thời gian và TSA có thể xử lý nó, thì sau đó TSA phải ràng buộc mã hóa cả hai giá trị băm trong thông điệp yêu cầu tem thời gian xác định tại trường "messageImprints" của yêu cầu tem thời gian và trong mở rộng này với giá trị thời gian gán cho cấu trúc 'TSTInfo' trong thẻ tem thời gian thu được và phải tái tạo các nội dung của mở rộng này lúc chưa sửa đổi trong cấu trúc 'TSTInfo' nói trên.

Mô đun ASN.1 định nghĩa mở rộng giá trị băm trong Phụ lục A là: `extHash`.

7.9.1.2 Mở rộng phương pháp

Bên yêu cầu tem thời gian có thể chỉ ra TSA cụ thể sử dụng phương pháp cấp tem thời gian khi tạo nên thẻ tem thời gian cuối cùng. Mở rộng phương pháp được quy định để cho phép bên yêu cầu chỉ ra TSA cụ thể sử dụng phương pháp tem thời gian khi tạo thẻ tem thời gian thu được. Mở rộng này chứa trong trường "extensions" của yêu cầu tem thời gian gửi bởi bên yêu cầu đến TSA và trong trường "extensions" của cấu trúc 'TSTInfo' thu được từ TSA và gửi trả trong thẻ tem thời gian tới bên yêu cầu.

Nếu mở rộng này hiện diện trong yêu cầu tem thời gian và TSA có thể xử lý nó, thì sau đó TSA phải cố gắng thực hiện các yêu cầu bằng phương pháp cụ thể, hoặc báo lại lỗi cho biết phương pháp là không tồn tại. Nếu bên yêu cầu xác định nhiều hơn một phương pháp, thì TSA phải chọn một trong các phương pháp được đề xuất đó để tạo thẻ tem thời gian. Nếu mở rộng này không có mặt, thì TSA phải sử dụng cơ chế tem thời gian mặc định.

Mô đun ASN.1 định nghĩa mở rộng phương pháp trong Phụ lục A là: `extMethod`.

7.9.1.3 Mở rộng việc gia hạn

Bên yêu cầu tem thời gian có thể báo cho TSA biết rằng yêu cầu tem thời gian hiện thời là tem thời gian được gia hạn dựa trên dữ liệu của tem thời gian đã có trong quá khứ sao cho thời hạn hiệu lực của thẻ tem thời gian đã có được kéo dài thêm (ví dụ: khi hàm băm có trong thẻ tem thời gian gần bị phá bằng các tác động mới hoặc tác nhân tính toán có sẵn). Mở rộng việc gia hạn được quy định để cho phép đệ trình các yêu cầu gia hạn tem thời gian cho một thẻ tem thời gian sẵn có. Mở rộng này được đưa vào trong trường "extensions" của yêu cầu tem thời gian gửi bởi bên yêu cầu đến TSA và trong trường "extensions" của cấu trúc 'TSTInfo' thu được từ TSA và gửi trả lại cho bên yêu cầu.

Nếu mở rộng này có mặt trong yêu cầu tem thời gian và TSA có thể xử lý nó, thì sau đó TSA phải tái tạo lại dữ liệu của mở rộng này khi chưa chỉnh sửa trong cấu trúc 'TSTInfo' của thẻ tem thời gian thu được.

Mục ASN.1 định nghĩa mở rộng việc gia hạn trong Phụ lục A là: `extRenewal`.

7.9.2 Mở rộng 'BindingInfo'

7.9.2.1 Mở rộng tên

TSA khi tạo thẻ liên kết có thể nhận diện từng bước của toàn bộ quá trình cấp tem thời gian bằng tên riêng với mục đích kiểm tra và lưu trữ bản ghi. Mở rộng tên được quy định để cho phép nhận diện các bước bên trong cấu trúc 'BindingInfo'. Ví dụ: TSA phải có mở rộng này khi toàn bộ quá trình cấp tem thời gian được kết hợp bởi tập thao tác của các quá trình riêng lẻ.

Mô đun ASN.1 định nghĩa mở rộng tên trong Phụ lục A là: `extName`.

7.9.2.2 Mở rộng thời gian

TSA khi tạo thẻ liên kết có thể ghi lại giá trị thời gian tại mỗi bước của toàn bộ quá trình cấp tem thời gian với mục đích kiểm tra và lưu trữ bản ghi. Mở rộng thời gian được quy định để cho phép ghi lại các giá trị thời gian bên trong cấu trúc 'BindingInfo'. Ví dụ: TSA phải có mở rộng này khi toàn bộ quá trình cấp tem thời gian được kết hợp bởi tập thao tác của các quá trình riêng lẻ.

Mô đun ASN.1 định nghĩa mở rộng thời gian trong Phụ lục A là: `extTime`.

7.9.2.3 Mở rộng công bố

Bên yêu cầu các dịch vụ cấp tem thời gian phải có giao thức "yêu cầu – đáp ứng" với TSA hoặc bên TTP có quyền truy cập vào liên kết do TSA phát hành, để gia hạn thẻ tem thời gian sẵn có đến giá trị công bố. Mở rộng công bố được quy định để cho phép ghi lại dữ liệu gia hạn thẻ tem thời gian đến giá trị công bố bên trong cấu trúc 'BindingInfo'.

Các mục dữ liệu của mở rộng này có thể được sử dụng để xác minh tính hợp lệ của thẻ tem thời gian dựa vào giá trị công bố do TSA phát hành và dựa vào sự kiện do TSA công bố tương ứng. Nếu giá trị công bố từ TSA đã được xác thực từ các nguồn được chứng nhận rộng rãi, việc xác minh thẻ tem thời gian dựa vào giá trị công bố và giá trị thời gian của sự kiện công bố liên quan có thể được xác định độc lập với TSA đã tạo ra thẻ tem thời gian. Chú ý rằng các giá trị tem thời gian liên quan đến các sự kiện TSA công bố tiêu biểu cho thang thời gian "thô" hơn là thang thời gian được xác định bởi các giá trị thời gian gán cho trường "genTime" trong gói cấu trúc 'TSTInfo' của các thẻ tem thời gian.

Mở rộng công bố cho phép có mặt nhiều trường dữ liệu trong kiểu 'PublicationInfo' để cung cấp các giá trị công bố tại các khoảng thời gian khác nhau với độ chi tiết thời gian khác nhau, ví dụ: hàng ngày, hàng tuần.

Mô đun ASN.1 định nghĩa mở rộng công bố trong Phụ lục A là: `extPublication`.

CHÚ THÍCH – Kiểu dữ liệu 'BindingInfo' chứa trường "publish" có thể được sử dụng để hỗ trợ hạn chế các giá trị công bố bởi bên TSA tạo ra thẻ liên kết. Kiểu dữ liệu 'PublicationInfo' khi được sử dụng bên trong mở rộng công bố hỗ trợ tập đặc điểm lớn và được thiết đặt dùng trường "publish" bên trong kiểu dữ liệu 'BindingInfo'.

8 Tạo ra thẻ tem thời gian

8.1 Khái quát

Để thu được thẻ tem thời gian trên dữ liệu đã cho, bên yêu cầu tem thời gian phải gửi yêu cầu tem thời gian tới TSA, như đã mô tả trong Điều 6.1. Bên yêu cầu có thể quy định mở rộng phương pháp với định danh đối tượng *tsp-req-link* như đã xác định trong Phụ lục A tại trường "extensions" với mục đích yêu cầu được thẻ tem thời gian sử dụng gói "DigestedData". Hoặc bên yêu cầu có thể quy định mở rộng phương pháp với định danh đối tượng *tsp-req-link-ds* như định nghĩa trong Phụ lục A tại trường "extensions" với mục đích yêu cầu được thẻ tem thời gian sử dụng gói "SignedData".

Nếu mở rộng phương pháp được quy định trong trường "extensions" của yêu cầu tem thời gian và mở rộng phương pháp có chứa một hoặc nhiều định danh phương pháp tương ứng với các phương pháp được hỗ trợ từ TSA, thì TSA khi tạo thẻ liên kết phải đáp ứng yêu cầu sử dụng cụ thể một trong những phương pháp đó. Nếu không có mở rộng phương pháp trong trường "extensions" của yêu cầu tem thời gian, thì TSA khi tạo thẻ liên kết phải sử dụng gói "DigestedData" hoặc gói "SignedData" để tạo ra thẻ theo điều khoản dịch vụ.

Đáp ứng tem thời gian được gửi trả từ TSA phù hợp có thể chứa cấu trúc 'TimeStampToken' khi yêu cầu được chấp thuận. Một TSA phù hợp tạo thẻ tem thời gian liên kết phải tuân theo các bước được mô tả dưới đây.

TSA tạo ra đầu tiên thông tin tem thời gian theo cấu trúc 'TSTInfo' được định nghĩa tại Điều 7.2. Cấu trúc này bao gồm thông điệp tóm tắt của dữ liệu dành cho tem thời gian, giá trị thời gian được gán bởi TSA và các thông tin liên quan. Trường "tsa" của cấu trúc 'TSTInfo' phải có mặt, trường "tsa" được yêu cầu để xác minh tem thời gian. Trường "extensions" trong cấu trúc 'TSTInfo' phải có mặt nếu yêu cầu tem thời gian tương ứng chứa các mục dữ liệu có trong trường "extensions".

Kế tiếp, TSA phải mã hóa cấu trúc 'TSTInfo' vừa tạo với quy tắc mã hóa DER và lưu giữ các chuỗi octet thu được trong trường "eContent" của cấu trúc "EncapsulatedContentInfo".

Sau đó, TSA phải tính toán một hoặc nhiều giá trị băm trên trường "eContent" này bằng một hoặc nhiều hàm băm. Giá trị băm thu được gắn vào trường "msgImprints" trong cấu trúc 'BindingInfo' được định nghĩa tại Điều 7.4.

TSA phải sử dụng nội dung của trường "msgImprints" trong thao tác liên kết kết hợp với các liên kết từ các thao tác liên kết có trước, có thể trong tổ hợp với trường "msgImprints" từ các yêu cầu tem thời gian đồng thời khác (nghĩa là các yêu cầu tem thời gian nhận được cùng giá trị thời gian như trong kết quả cấu trúc 'TSTInfo') và phải có trong trường "links" và trường "aggregate" của cấu trúc 'BindingInfo' tương ứng.

Cuối cùng, TSA phải tạo thẻ tem thời gian bằng cách đóng gói cấu trúc 'TSTInfo' và tương ứng với cấu trúc 'BindingInfo' trong cấu trúc 'TimeStampToken'. TSA có thể thực hiện một trong hai kiểu gói sau:

- Gói "DigestedData" là trường hợp mà trường "contentType" chứa giá trị *id-digestedData* và trường "content" chứa giá trị kiểu "DigestedData". Kiểu gói này được sử dụng khi yêu cầu tem thời gian chứa mở rộng phương pháp trong trường "extensions" với giá trị định danh đối tượng là: *tsp-req-link*.
- Gói "SignedData" là trường hợp mà trường "contentType" chứa giá trị *id-signedData* và trường "content" chứa giá trị kiểu "SignedData". Kiểu gói này được sử dụng khi yêu cầu tem thời gian chứa mở rộng phương pháp trong trường "extensions" với giá trị định danh đối tượng là: *tsp-req-link-ds*.

8.2 Gói DigestedData

TSA khi tạo thẻ tem thời gian sử dụng phương pháp gói "DigestedData" phải thực hiện đầu tiên các bước đã mô tả trong Điều 8.1 và đặt cấu trúc "EncapsulatedContentInfo" thu được vào trong trường "encapContentInfo" của cấu trúc "DigestedData" (xem trong Phụ lục A). Khi tất cả các trường trong cấu trúc 'BindingInfo' được đưa vào, TSA phải mã hóa trường "BindingInfo" với quy tắc mã hóa DER và lưu giữ chuỗi octet thu được trong trường "digest" của cấu trúc "DigestedData".

Cuối cùng, TSA phải gắn định danh đối tượng `tsp-digestedData` tương ứng với phép đóng gói này (xem trong Phụ lục A) vào trong trường "digestAlgorithm" của cấu trúc "DigestedData".

8.3 Gói SignedData

TSA có thể tích hợp chữ ký số với hệ thống tem thời gian tạo thẻ liên kết. Bằng cách liên kết các thẻ đã ký độc lập với nhau, TSA có thể xác minh rõ ràng thứ tự của từng thẻ đã ký được phát hành.

Định danh đối tượng nhận diện dữ liệu ký có nội dung dạng:

```
id-signedData OBJECT IDENTIFIER :: = {
      iso(1) member-body(2) us(840)  rsadsi(113549)  pkcs(1) pkcs7(7) 2 }
```

Cấu trúc "SignedData" chứa một hoặc nhiều cấu trúc "SignerInfo", nói cách khác có thể gồm các đặc tính bổ sung ký hoặc bổ sung không ký và được định nghĩa trong Phụ lục A của TCVN 7818 - 1 như sau:

```
SignedData :: = SEQUENCE {
 version     CMSVersion,
 digestAlgorithms    DigestAlgorithmIdentifiers,
 encapContentInfo    EncapsulatedContentInfo,
 certificates    [0] IMPLICIT CertificateSet OPTIONAL,
 crls     [1] IMPLICITCertificateRevocationLists OPTIONAL,
 signerInfos    SignerInfos  }
SignerInfos ::= SET OF SignerInfo
SignerInfo ::= SEQUENCE {
 version     CMSVersion,
 sid     SignerIdentifier,
 digestAlgorithm  DigestAlgorithmIdentifier,
 signedAttrs    [0] IMPLICIT SignedAttributes OPTIONAL,
 signatureAlgorithm SignatureAlgorithmIdentifier,
 signature     SignatureValue,
 unsignedAttrs    [1] IMPLICIT UnsignedAttributes OPTIONAL }
SignedAttributes ::= SET SIZE (1..MAX) OF Attribute
UnsignedAttributes ::= SET SIZE (1..MAX) OF Attribute
Attribute ::= SEQUENCE {
 attrType     OBJECT IDENTIFIER,
 attrValues    SET OF AttributeValue }
AttributeValue  ::= ANY
```

TSA khi tạo thẻ tem thời gian sử dụng phương pháp gói "SignedData" phải sử dụng cấu trúc "SignedData" để đóng gói cả dữ liệu ký và dữ liệu liên kết. Đầu tiên TSA phải thực hiện các bước đã mô tả trong Điều 8.1 và sau đó đặt cấu trúc 'EncapsulatedContentInfo' thu được vào trường "encapContentInfo" của cấu trúc "SignedData". Một khi tất cả các trường của cấu trúc 'BindingInfo' được đưa vào, TSA phải mã hóa cấu trúc 'BindingInfo' như chuỗi octet với quy tắc mã hóa DER và chèn nó vào như là một phần tử của trường "attrValues" trong cấu trúc "Attribute". Dĩ nhiên TSA cũng phải chèn định danh đối tượng *tsp-signedData* (theo định nghĩa trong Phụ lục A) tương ứng với phương pháp đóng gói này vào trong trường "attrType" của cấu trúc "Attribute". Sau đó TSA phải chèn cấu trúc "Attribute" thu được vào trong trường "signedAttrs" của cấu trúc "SignerInfo" và hoàn thành quá trình ký tùy thuộc vào phương pháp ký được định nghĩa trong [CMS].

Chèn cấu trúc 'BindingInfo' như là một thuộc tính ký bên trong thẻ tem thời gian để giữ được tính hợp lệ của gói cấu trúc 'TSTInfo' lâu hơn thời gian tồn tại của chứng chỉ số đã sử dụng để hình thành chữ ký số. Thêm vào đó, thẻ tem thời gian này có thể chuyển dễ dàng vào trong thẻ tem thời gian sử dụng gói "DigestedData" và chứa cấu trúc 'TSTInfo' và 'BindingInfo' nhận diện trong thẻ tem thời gian gốc. Thẻ tem thời gian dạng mới này phải chứa dữ liệu liên kết giống như thẻ tem thời gian gốc và bỏ qua phần chữ ký số.

8.4 Xem xét về an ninh

TSA phù hợp khi tạo thẻ liên kết phải sử dụng mã hóa mạnh nguyên thủy trong các thao tác liên quan đến việc tạo ra thẻ tem thời gian, các liên kết và các mục dữ liệu có liên quan trong suốt quá trình thao tác tổ hợp, kết nối và công bố và phải thay thế cùng nâng cấp mật mã nguyên thủy trước khi chúng trở thành không đủ mạnh để đáp ứng các yêu cầu bảo mật cần thiết của dịch vụ.

TSA phù hợp khi tạo thẻ liên kết nên sử dụng đồng thời nhiều hàm băm trong khi tính toán trường "msgImprints" ở cấu trúc 'BindingInfo' của thẻ tem thời gian, trong quá trình tổ hợp và trong quá trình liên kết sao cho thẻ tem thời gian thu được và liên kết được tạo bởi TSA là được tách biệt với lỗi mật mã của mọi hàm băm đơn.

9 Xác minh thẻ tem thời gian

9.1 Khái quát

Tính hợp lệ của thẻ tem thời gian phải được xác minh bằng cách kiểm tra nó có thỏa mãn:

- Thẻ tem thời gian được thiết lập cú pháp tốt.
- Giá trị của trường "messageImprint" trong gói cấu trúc 'TSTInfo' phù hợp giá trị dấu thông điệp được đánh giá trên chủ đề tài liệu để giám sát.
- Giá trị của tất cả các trường "messageImprint" bên trong mở rộng giá trị băm trong trường "extensions" của gói cấu trúc 'TSTInfo' (nếu có) phù hợp với giá trị dấu thông điệp được đánh giá trên chủ đề tài liệu để giám sát.
- Cách giải quyết theo đó thẻ được phát hành là chấp nhận được đối với việc sử dụng dự tính và bằng cách thực hiện các bước xác minh bổ sung thích hợp cho phương pháp đóng gói được quy định trong thẻ tem thời gian.

9.2 Gói DigestedData

Trong trường hợp thẻ tem thời gian sử dụng gói "DigestedData", bên xác minh phải gửi yêu cầu xác minh tới TSA hoặc bên TTP có quyền truy cập vào các liên kết của TSA, như đã mô tả tại Điều 6.3, sử dụng kênh bảo mật tính toàn vẹn dữ liệu và xác thực nguồn gốc dữ liệu. Nếu trong kho của TSA hoặc

TTP không tồn tại liên kết nào liên quan đến giá trị thời gian bằng giá trị thời gian trong gói cấu trúc 'TSTInfo' của thẻ tem thời gian được xem xét thì việc xác minh thất bại. Mặt khác, TSA hoặc bên TTP đáp ứng yêu cầu phải thực hiện việc xác minh trường "msgImprints" trong cấu trúc 'BindingInfo' của thẻ tem thời gian phù hợp giá trị băm được tính toán trên gói cấu trúc 'TSTInfo'. Nếu không thì việc xác minh bị thất bại, mặt khác nếu trường "aggregate" có mặt trong cấu trúc 'BindingInfo', TSA hoặc bên TTP đáp ứng yêu cầu phải thực hiện việc tính toán giá trị trường "aggregate" (giả sử rằng giá trị trường "reference" là 0 bên trong một phiên bản cấu trúc 'Node' và dựa vào trường "msgImprints" của cấu trúc 'BindingInfo') và áp dụng thuật toán liên kết trên kết quả này và trường "links" để xác minh kết quả có phù hợp giá trị liên kết đã lưu trữ đối với giá trị thời gian trong gói cấu trúc 'TSTInfo' của thẻ tem thời gian; Nếu không tồn tại trường "aggregate", TSA hoặc bên TTP đáp ứng yêu cầu phải áp dụng thuận toán liên kết trên trường "msgImprints" và trường "links" của cấu trúc 'BindingInfo' theo cùng cách như nhau và thực hiện cùng các bước xác minh trên giá trị nhận được. Trong bất kỳ sự kiện nào, trường "status" thích hợp được bao gồm trong đáp ứng xác minh và đưa ra thẻ tem thời gian được tái tạo như lúc chưa chỉnh sửa, giống như mô tả trong Điều 6.4.

9.3 Gói "SignedData"

Trong trường hợp thẻ tem thời gian sử dụng gói "SignedData", bên xác minh tem thời gian phải:

- Hoặc thực hiện các bước xác minh bổ sung giống như cho thẻ tem thời gian được tạo ra bằng cách sử dụng gói "DigestedData", cụ thể là gửi một yêu cầu xác minh tới TSA hoặc bên TTP có quyền truy cập vào các liên kết của TSA như đã mô tả tại Điều 6.3, sử dụng kênh bảo mật tính toàn vẹn dữ liệu và xác thực nguồn gốc dữ liệu và trong trường hợp này TSA hoặc bên TTP đáp ứng yêu cầu phải truy cập các thành phần của thẻ tem thời gian và thực hiện các bước xác minh giống như cho thẻ tem thời gian sử dụng gói "DigestedData" trong Điều 9.2;

- Hoặc xử lý thẻ tem thời gian như một thẻ độc lập và thực hiện các bước xác minh bổ sung theo cách thức giống như cho thẻ tem thời gian với chữ ký số được mô tả trong TCVN 7818 – 2.

9.4 Xem xét về an ninh

Đối với mục đích hỗ trợ yêu cầu xác minh dựa vào các liên kết được duy trì từ TSA hoặc bên TTP, thì TSA hoặc bên TTP đáp ứng yêu cầu nên cố định trong khoảng thời gian liên kết và dữ liệu có liên quan cần thiết cho mục đích xác minh tem thời gian và kiểm soát, trước khi mật mã nguyên thủy đã sử dụng cho các thao tác liên kết, tổ hợp và công bố và đã được sử dụng để tạo ra các liên kết và dữ liệu có liên quan đã bị coi là yếu. Ví dụ: điều này có thể thực hiện bằng cách cấp tem thời gian với các giá trị của các liên kết và dữ liệu có liên quan được quan tâm và bằng cách gia hạn các thẻ tem thời gian thu được nếu cần, như mô tả trong Điều 11.

10 Mở rộng thẻ tem thời gian

Đối với mục đích mở rộng thẻ tem thời gian đến giá trị công bố, thực thể sở hữu thẻ tem thời gian có thể gửi yêu cầu mở rộng tới TSA hoặc bên TTP có quyền truy cập vào liên kết của TSA, như đã mô tả ở Điều 6.5, sử dụng kênh bảo mật tính toàn vẹn dữ liệu và xác thực nguồn gốc dữ liệu. Nếu TSA hoặc bên TTP đáp ứng yêu cầu hỗ trợ thao tác mở rộng thì phải thực hiện các bước xác minh trên thẻ tem thời gian phù hợp với gói "DigestedData" như đã mô tả tại Điều 9.2. Nếu tính hợp lệ của thẻ đã được xác minh, TSA hoặc bên TTP đáp ứng yêu cầu phải tiến hành kiểm tra xem sự tồn tại của giá trị công bố, mà có thể được gọi bởi thẻ tem thời gian đang xem xét; trong trường hợp này, TSA hoặc bên TTP đáp ứng yêu cầu phải đưa vào cấu trúc 'PublicationInfo' với các mục dữ liệu để xác thực thẻ tem thời gian dựa vào giá trị công bố theo Điều 7.9.2.3 và phải gửi lại bản nâng cấp thẻ tem thời gian đến bên đệ trình bên trong một đáp ứng mở rộng như đã mô tả tại Điều 6.6. Nếu không thực hiện thao tác mở rộng, nếu thẻ tem thời gian đang xem xét bỏ qua các bước xác minh, hoặc nếu giá trị công bố không tồn tại đối với thẻ tem thời gian đang xem xét, thì yêu cầu mở rộng không được đáp ứng, khi đó trường "status" thích hợp được đưa vào trong đáp ứng mở rộng và thẻ tem thời gian đã xem xét được đặt lại như lúc chưa chỉnh sửa, như mô tả trong Điều 6.6.

11 Gia hạn thẻ tem thời gian

11.1 Khái quát

Như định nghĩa ở TCVN 7818 - 1, "gia hạn" là một biến của thao tác cấp tem thời gian cơ bản trong đó tồn tại thẻ tem thời gian có các mục dữ liệu tem thời gian trước đó được hợp nhất công khai như lúc dữ liệu liên kết với thẻ tem thời gian mới tạo trên các mục dữ liệu giống nhau với giá trị thời gian mới (hiện hành). Bằng cách kết hợp thẻ tem thời gian tồn tại trước đó trong khi tạo ra thẻ tem thời gian mới và giả định rằng các xem xét về an ninh được đáp ứng thích hợp, thời hạn hiệu lực của thẻ tem thời gian sớm hơn trên các mục dữ liệu tem thời gian được mở rộng theo phạm vi của thẻ tem thời gian mới.

Với các thẻ liên kết, "gia hạn" có thể cần thiết khi hàm mã hóa được sử dụng để ghép nối giá trị thời gian với dữ liệu vẫn được tin tưởng, nhưng có bằng chứng mạnh mẽ cho rằng nó có khả năng dễ bị tấn công trong tương lai gần (ví dụ: khi hàm băm gần bị hỏng bởi các kiểu tấn công mới hoặc khả năng tính toán sẵn có). Gia hạn cần phải được thực hiện trước khi điều kiện như vậy làm thẻ tem thời gian ban đầu không còn giá trị.

Đối với mục đích gia hạn thẻ tem thời gian trên dữ liệu đã có, bên yêu cầu phải gửi một yêu cầu tem thời gian tới TSA như đã mô tả trong Điều 6.1 và có chứa thẻ tem thời gian sẵn có trong mở rộng việc gia hạn bên trong trường "extensions" của yêu cầu tem thời gian tuân theo Điều 7.9.1.3. Và TSA phải gửi trả đáp ứng tem thời gian tuân theo Điều 7.9.1.3.

11.2 Gia hạn và thao tác xác minh

Như đã mô tả trong TCVN 7818 - 1, việc xác minh thẻ tem thời gian đã được gia hạn là thực hiện theo cách mà các thẻ tem thời gian ngoài cùng (vừa được phát hành gần đây nhất) được xác minh tại thời điểm hiện hành, trong khi các thẻ tem thời gian kèm theo (đã phát hành trước đây) được xác minh với thời điểm phát hành của thẻ tem thời gian kèm theo. Trong trường hợp có nhiều "gia hạn" lồng nhau, mỗi thẻ tem thời gian lồng nhau được xác minh tại thời điểm mà thẻ tem thời gian gia hạn tiếp theo (kèm theo) cho đến khi thẻ tem thời gian ngoài cùng được xác minh tại thời điểm hiện hành. Trong trường hợp tất cả các thẻ tem thời gian đều được tạo bởi TSA phù hợp với tiêu chuẩn này, thì thẻ tem thời gian trong cùng (cũ nhất) được xác minh tại thời điểm hiện hành nếu thực hiện đúng theo các bước sau:

- Các thẻ tem thời gian ngoài cùng và lồng nhau được xác minh theo các bước xác minh cho gói "DigestedData" theo Điều 9,
- Các hàm mã hóa được liệt kê trong từng thẻ tem thời gian kèm theo là đáng tin cậy tại thời điểm phát hành thẻ tem thời gian gia hạn bao quanh tức thời,
- Kho chứa các liên kết được duy trì từ TSA mà đang phát hành thẻ tem thời gian gia hạn là đáng tin cậy với khoảng thời gian tồn tại trước bất kỳ thời điểm nào khi mật mã nguyên thủy được yêu cầu cho xác minh thuật toán của chúng có thể bị coi là yếu.

11.3 Gia hạn và thao tác mở rộng

Lưu ý gia hạn cũng có ảnh hưởng đến các thẻ tem thời gian được gia hạn đến giá trị công bố. Trong khi đó các thẻ tem thời gian có thể được xác minh dựa vào giá trị công bố độc lập với các liên kết của TSA, miễn là giá trị công bố có sẵn cách xác thực từ các nguồn được chứng nhận rộng rãi, quá trình xác minh này đưa ra xem xét về an ninh liên quan đến độ mạnh của mật mã nguyên thủy đã được sử dụng trong quá trình. Gia hạn thẻ tem thời gian đến giá trị công bố, tuân theo thao tác gia hạn và thao tác mở rộng tiếp theo đến một giá trị công bố mới trên thẻ tem thời gian gia hạn, giữ lại được khả năng khẳng định tính hợp lệ của thẻ tem thời gian ban đầu độc lập với các liên kết của TSA. Ví dụ: thẻ tem thời gian t_1 là được gia hạn đến giá trị công bố v_1 tương ứng với sự kiện do TSA công bố tại thời điểm p_1, kết quả là thẻ tem thời gian t_{1e}; sau đó thẻ tem thời gian t_{1e} được gia hạn và cho kết quả là thẻ tem thời gian gia hạn t_2 và tem thời gian gia hạn t_2 này được tiếp tục gia hạn đến giá trị công bố v_2 tương ứng với sự kiện do TSA công bố tại thời điểm p_2, kết quả là thẻ tem thời gian đã gia hạn t_{2e}; nếu theo các bước sau đây:

- Thẻ tem thời gian t_{1e} được xác minh dựa vào giá trị công bố v_1;
- Thẻ khôi phục t_{2e} được xác minh dựa vào giá trị công bố v_2;
- Mật mã nguyên thủy liên quan đến việc xác minh t_{1e} không bị coi là yếu tại thời điểm p_2;
- Mật mã nguyên thủy liên quan đến việc xác minh t_{2e} không bị coi là yếu tại thời điểm hiện hành.

Sau đó tính hợp lệ của câu lệnh mà thẻ t_{1e} còn là hợp lệ tại thời điểm p_1 đã xác nhận có thể được gia hạn thêm thời gian hiện hành, mà không yêu cầu bất kỳ sự bổ sung nào đến từ các liên kết được duy trì bởi TSA, ngay cả khi mật mã nguyên thủy liên quan đến việc xác minh t_{1e} dựa vào giá trị công bố v_1 bị coi là yếu trong thời điểm hiện hành.

Phụ lục A

(quy định)

Mô đun ASN.1 cho tem thời gian

Đây là mô đun ASN.1 dựa theo chuẩn ASN.1 hiện hành:

```
TimeStampProtocol-3 {
iso(1) standard(0) time-stamp(18014) modules(0) part3(3)
}
 DEFINITIONS IMPLICIT TAGS ::= BEGIN
                                -- EXPORTS All; --
IMPORTS
          -- ISO/IEC 9594-8 | ITU-T Rec. X.509 AuthenticationFramework --
 EXTENSION, Extensions
           FROM AuthenticationFramework {
               joint-iso-itu-t ds(5) module(1) authenticationFramework(7) 4 }
           -- ISO/IEC 9594-8 | ITU-T Rec. X.509 CertificateExtensions --
 GeneralName
            FROM CertificateExtensions {
               joint-iso-itu-t ds(5) module(1) certificateExtensions(26) 4 }
 SignedData
            FROM CryptographicMessageSyntax {
                iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
                smime(16) modules(0) cms(1) };
                          -- Supporting Definitions --
AlgorithmIdentifier { ALGORITHM:IOSet } ::= SEQUENCE {
       algorithm     ALGORITHM.&id({IOSet}),
       parameters    ALGORITHM.&Type({IOSet}{@algorithm})  OPTIONAL
}
ALGORITHM ::= CLASS {
       &id           OBJECT IDENTIFIER  UNIQUE,
       &Type         OPTIONAL
}
WITH SYNTAX { OID &id [PARMS &Type] }
CONTENT ::= TYPE-IDENTIFIER  -- ISO/IEC 8824-2, Phụ lục A
OIDS ::= CLASS {
      &id     OBJECT IDENTIFIER  UNIQUE
}
WITH SYNTAX { OID &id }
POLICY ::= OIDS  -- Các điều khoản mà TSA hỗ trợ
METHOD ::= OIDS  -- Các phương pháp của TSA
                          -- Yêu cầu tem thời gian --
TimeStampReq ::= SEQUENCE {
 version          Version,
 messageImprint   MessageImprint,
 reqPolicy        TSAPolicyId OPTIONAL,
 nonce            Nonce OPTIONAL,
 certReq          BOOLEAN DEFAULT FALSE,
 extensions       [0] Extensions OPTIONAL
}
Version ::= INTEGER { v1(1) }
MessageImprint ::= SEQUENCE  {
 hashAlgorithm    DigestAlgorithmIdentifier,
 hashedMessage    OCTET STRING
```

```
}
MessageImprints ::= SEQUENCE SIZE (1..MAX) OF MessageImprint
DigestAlgorithmIdentifier ::= AlgorithmIdentifier {{ DigestAlgorithms }}
DigestAlgorithms ALGORITHM ::= {
    { OID id-ripemd160  PARMS NULL } |
    { OID id-sha1 PARMS NULL } |
    { OID id-sha256 PARMS NULL } |
    { OID id-sha224 PARMS NULL } |
    { OID id-sha384 PARMS NULL } |
    { OID id-sha512 PARMS NULL } ,
      ...
                -- Các thuật toán phần loại bổ sung mong đợi --
}
TSAPolicyId ::= POLICY.&id({TSAPolicies})
TSAPolicies POLICY ::= {
           ...
                    -- Bất kỳ điều khoản được hỗ trợ từ TSA --
}
Nonce ::= INTEGER  -- Giá trị lớn mong đợi
                          -- Yêu cầu tem thời gian --
TimeStampResp ::= SEQUENCE {
 status            PKIStatusInfo,
 timeStampToken    TimeStampToken OPTIONAL
}
PKIStatusInfo ::=  SEQUENCE {
 status            PKIStatus,
 statusString      PKIFreeText OPTIONAL,
 failInfo          PKIFailureInfo OPTIONAL
}
PKIStatus ::=  INTEGER {
granted          (0),-- yêu cầu đã được đáp ứng hoàn toàn
grantWithMods    (1),-- các sửa đổi cần thiết, bên yêu cầu
                     -- có trách nhiệm xác nhận các khác biệt
rejection        (2),-- yêu cầu không thể thỏa mãn
                     -- mã lỗi không cung cấp thông tin bổ sung
waiting          (3),-- yêu cầu chưa được xử lý
                     -- bên yêu cầu nhận được thông báo rằng
                     -- yêu cầu đã đến đích
revocationWarning       (4), -- sự hủy bỏ sắp tiến hành
revocationNotification  (5)  -- thông báo có sự hủy bỏ
                             -- đã sảy ra
}
PKIFreeText ::= SEQUENCE SIZE(1..MAX) OF UTF8String
PKIFailureInfo ::= BIT STRING {
 badAlg               (0), -- định danh thuật toán không được công nhận hoặc hỗ trợ
 badRequest           (2), -- giao dịch không được phép hoặc không được hỗ trợ
 badDataFormat        (5), -- dữ liệu đã gửi bị định dạng sai
 timeNotAvailable    (14), -- Dịch vụ không tồn tại từ TSA
 unacceptedPolicy    (15), -- Các điều khoản được yêu cầu mà TSA không hỗ trợ
 unacceptedExtension (16), -- Các mở rộng được yêu cầu mà TSA không hỗ trợ
 addInfoNotAvailable (17), -- các thông tin bổ sung được yêu cầu
                           -- không thể hiểu hoặc không tồn tại
 systemNotAvailable  (24), -- hệ thống không tồn tại
 systemFailure       (25), -- hệ thống bị lỗi
 verificationFailure (27)  -- việc xác minh tem thời gian bị lỗi
}
                              -- Yêu cầu xác minh --
VerifyReq ::=  SEQUENCE {
 version       Version,
 tst           TimeStampToken,
 requestID     [0] OCTET STRING OPTIONAL
}
                              -- Đáp ứng xác minh --
VerifyResp ::= SEQUENCE {
```

```
 version        Version,
 status         PKIStatusInfo,
 tst            TimeStampToken,
 requestID      [0] OCTET STRING OPTIONAL
}
                                    -- Yêu cầu mở rộng --
ExtendReq ::=  SEQUENCE {
 version        Version,
 tst             TimeStampToken,
 requestID       [0] OCTET STRING OPTIONAL
}
                                    -- Đáp ứng mở rộng --
ExtendResp ::=  SEQUENCE {
 version        Version,
 status         PKIStatusInfo,
 tst            TimeStampToken,
 requestID      [0] OCTET STRING OPTIONAL
}
                              -- Các định danh đối tượng ---
                                      -- TCVN 7818-3--
tsp-lt  OBJECT IDENTIFIER ::= { iso(1) standard(0) time-stamp(18014) lt(3) }
tsp-req-link OBJECT IDENTIFIER ::= {tsp-lt link(1)}
tsp-req-link-ds OBJECT IDENTIFIER ::= {tsp-lt link-ds(2)}
tsp-ext-name OBJECT IDENTIFIER ::= { tsp-lt name(5) }
tsp-ext-time OBJECT IDENTIFIER ::= { tsp-lt time(6) }
tsp-ext-publication OBJECT IDENTIFIER ::= {tsp-lt publication(7) }
tsp-digestedData OBJECT IDENTIFIER ::= { tsp-lt digestedData(8) }
tsp-signedData OBJECT IDENTIFIER ::= { tsp-lt signedData(9) }
                                     -- TCVN 7818-1--
tsp-ext OBJECT IDENTIFIER ::= { iso(1) standard(0) time-stamp(18014) ext(1) }
tsp-ext-hash OBJECT IDENTIFIER ::= { tsp-ext hash(1) }
tsp-ext-meth OBJECT IDENTIFIER ::= { tsp-ext meth(2) }
tsp-ext-renewal OBJECT IDENTIFIER ::= { tsp-ext renewal(3) }
                                       -- khác --
der OBJECT IDENTIFIER ::= {
 joint-iso-itu-t asn1(1) ber-derived(2) distinguished-encoding(1) }
id-ct-TSTInfo OBJECT IDENTIFIER ::= {
 iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
 smime(16) ct(1) 4 }
id-digestedData OBJECT IDENTIFIER ::= {
 iso(1) member-body(2) us(840)  rsadsi(113549) pkcs(1) pkcs7(7) 5 }
id-ripemd160  OBJECT IDENTIFIER ::= {
 iso(1) identified-organization(3) teletrust(36) algorithm(3)
 hashAlgorithm(2) ripemd160(1)}
id-sha1 OBJECT IDENTIFIER ::= {
 iso(1) identified-organization(3) oiw(14) secsig(3) 2 26 }
id-sha256 OBJECT IDENTIFIER ::= {
 joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3)
 nistalgorithm(4) hashalgs(2) 1 }
id-sha384 OBJECT IDENTIFIER ::= {
 joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3)
 nistalgorithm(4) hashalgs(2) 2 }
id-sha512 OBJECT IDENTIFIER ::= {
 joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3)
 nistalgorithm(4) hashalgs(2) 3 }
id-signedData OBJECT IDENTIFIER ::= {
 iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) signedData(2) }
                                       -- TSTInfo --
TSTInfo ::=  SEQUENCE {
 version          Version,
 policy           TSAPolicyId,
 messageImprint   MessageImprint,
 serialNumber     SerialNumber,
```

```
 genTime          GeneralizedTime,
 accuracy         Accuracy OPTIONAL,
 ordering         BOOLEAN DEFAULT FALSE,
 nonce            Nonce OPTIONAL,
 tsa              [0] EXPLICIT GeneralName OPTIONAL,
 extensions       [1] Extensions OPTIONAL
}
SerialNumber ::= INTEGER  -- Giá trị lớn mong đợi
Accuracy ::= SEQUENCE {
   seconds    INTEGER  OPTIONAL,
   millis     [0] INTEGER(1..999)  OPTIONAL,
   micros     [1] INTEGER(1..999)  OPTIONAL
}
 (ALL EXCEPT({ -- không có thành phần nào có mặt -- }))
                              -- Thẻ tem thời gian --
TimeStampToken ::= SEQUENCE {
 contentType       CONTENT.&id({Contents}),
 content           [0] EXPLICIT CONTENT.&Type({Contents}{@contentType})
}
Contents CONTENT ::= {
{ DigestedData        IDENTIFIED BY id-digestedData } |
{ SignedData          IDENTIFIED BY id-signedData },
...
                      -- gói tem thời gian bổ sung mong đợi --
}
DigestedData ::= SEQUENCE {
 version            CMSVersion,
 digestAlgorithm    DigestAlgorithmIdentifier,
 encapContentInfo   EncapsulatedContentInfo,
 digest             Digest
}
EncapsulatedContentInfo::= SEQUENCE {
 eContentType              CONTENT.&id({EContents}),
 eContent                  [0] EXPLICIT CONTENT.&Type({EContents}{@eContentType})
}
EContents CONTENT ::= {
 { ETSTInfo IDENTIFIED BY id-ct-TSTInfo },
...
                       -- các kiểu dữ liệu bổ sung mong đợi --
}
ETSTInfo ::= OCTET STRING (CONTAINING TSTInfo ENCODED BY der)
Digest ::= OCTET STRING -- (CONTAINING BindingInfo ENCODED BY der)
                                -- Binding Info --
BindingInfo ::= SEQUENCE {
 version        Version,
 msgImprints    MessageImprints,
 aggregate      [0] Chains OPTIONAL,
 links          Links,
 publish        [1] Chains OPTIONAL,
 extensions     [2] Extensions OPTIONAL
}
                                        -- Chain --
Chain ::= SEQUENCE {
 algorithm      ChainAlgorithmIdentifier,
 links          Links
}
Chains ::= SEQUENCE SIZE (1..MAX) OF Chain
ChainAlgorithmIdentifier ::= AlgorithmIdentifier {{ ChainAlgorithms }}
ChainAlgorithms ALGORITHM ::= {
...
                      -- các thuật toán xích bổ sung mong đợi--
}
                                        -- Link --
Link ::= SEQUENCE {
```

```
 algorithm          [0] LinkAlgorithmIdentifier OPTIONAL,
 identifier         [1] INTEGER OPTIONAL,
 members            Nodes
}
Links ::= SEQUENCE SIZE (1..MAX) OF Link
LinkAlgorithmIdentifier ::= AlgorithmIdentifier {{ LinkAlgorithms }}
LinkAlgorithms ALGORITHM ::= {
...
                    -- các thuật toán liên kết bổ sung mong đợi --
}
                                        -- Node --
Node ::= CHOICE {
 imprints         [0] Imprints,
 reference        [1] INTEGER
}
Nodes ::= SEQUENCE SIZE (1..MAX) OF Node
Imprint ::= OCTET STRING
Imprints ::=  SEQUENCE SIZE (1..MAX) OF Imprint
                                    -- Publication Info --
PublicationInfo ::= SEQUENCE {
    pubTime     GeneralizedTime OPTIONAL,
    pubId       [0] GeneralName OPTIONAL,
    pubChains   [1] Chains      OPTIONAL,
    sourceId    [2] GeneralName OPTIONAL
}
                            -- Mở rộng yêu cầu tem thời gian --
TSExtensions EXTENSION ::= {
 extHash     |
 extMethod   |
 extRenewal,
 ...
                            -- các mở rộng bổ sung mong đợi --
}
extHash EXTENSION ::= {SYNTAX ExtHash IDENTIFIED BY tsp-ext-hash}
ExtHash ::= SEQUENCE SIZE(1..MAX) OF MessageImprint
extMethod EXTENSION ::= {SYNTAX ExtMethod IDENTIFIED BY tsp-ext-meth}
ExtMethod ::= SEQUENCE SIZE(1..MAX) OF Method
Method ::= METHOD.&id({Methods})
Methods METHOD ::= {
    tsp-digestedData |
    tsp-signedData,
...
                        -- bất kỳ phương pháp cấp tem thời gian--
}
extRenewal EXTENSION ::= {SYNTAX ExtRenewal IDENTIFIED BY tsp-ext-renewal}
ExtRenewal ::= TimeStampToken
                                    -- Mở rộng BindingInfo --
BExtensions EXTENSION ::= {
 extName     |
 extTime     |
 extPublication,
  ...
                            -- các mở rộng bổ sung mong đợi --
}
extName EXTENSION ::= { SYNTAX ExtName IDENTIFIED BY tsp-ext-name }
ExtName ::= GeneralName
extTime EXTENSION ::= { SYNTAX ExtTime IDENTIFIED BY tsp-ext-time }
ExtTime ::= GeneralizedTime
extPublication EXTENSION ::= {
 SYNTAX ExtPublication IDENTIFIED BY tsp-ext-publication
}
ExtPublication ::= SEQUENCE SIZE (1..MAX) OF PublicationInfo
 END  -- TimeStampProtocol 3 --
```

Phụ lục B

(tham khảo)

Thảo luận bổ sung

B.1 Giới thiệu

Các giải thích bổ sung khi lựa chọn các quá trình và kỹ thuật cụ thể cho các thao tác liên kết, tổ hợp và công bố.

B.2 Liên kết

B.2.1 Khái quát

Liên kết là cách mà nhờ đó giá trị băm được liên kết bằng mật mã với các biểu diễn giá trị băm khác, để thiết lập trật tự qua lại của các sự kiện tem thời gian và phục vụ như là bằng chứng cho tất cả các sự kiện liên kết trước đó. Các hàm liên kết phải là hàm mật mã mạnh, nghĩa là một khi giá trị băm mới được tính toán bởi thao tác liên kết thì nó không thể bị thay đổi hay bị xóa mà không bị phát hiện. Các giá trị băm liên kết lần lượt với nhau biểu diễn thành chuỗi theo đó chúng được tạo ra, như là một cách để xác minh việc áp dụng chính xác giá trị thời gian. Quá trình liên kết cũng dùng để tạo ra từng bằng chứng giá trị băm mới cho toàn bộ giá trị băm đã có trước đó, nghĩa là các giá trị băm đã có trước đó không thể thay đổi mà không làm ảnh hưởng các lượt tính toán kế tiếp. Mỗi giá trị băm cho biết một sự kiện mà khi được chứng nhận rộng rãi thì có thể được sử dụng để xác minh sự đúng đắn của tất cả các sự kiện đã gửi đi trước đó.

Trong thực tế, TSA tạo ra một biểu diễn giá trị băm hoặc một gói cấu trúc 'TSTInfo' đơn hoặc một tổ hợp của nhiều gói cấu trúc 'TSTInfo' có chứa cùng giá trị thời gian và thực hiện thao tác liên kết với nhau với các mục dữ liệu biểu diễn giá trị băm của các liên kết trước đó, sao cho giá trị băm mới tạo bởi thao tác liên kết tạo ra bản tổng kết hoạt động từ tất cả giá trị băm của các liên kết trước đó. TSA duy trì kho lưu trữ các giá trị được tạo ra bởi quá trình liên kết, gọi tắt là các liên kết, để hỗ trợ trong tương lai các yêu cầu xác minh và gia hạn, cũng như các thao tác công bố và kiểm soát.

Khuyến cáo nên sử dụng nhiều hàm băm đồng thời trong quá trình liên kết sao cho việc tính toán các liên kết không dính dáng tới lỗi mật mã của bất kỳ hàm băm riêng lẻ nào. Ví dụ TSA có thể thực hiện thao tác liên kết bằng cách: đầu tiên tính giá trị băm SHA256 trên dữ liệu ghép nối đầu vào của thao tác liên kết, sau đó tính toán giá trị băm RIPEMD trên cùng dữ liệu đầu vào và cuối cùng ghép nối hai giá trị băm đã tính toán để tạo ra giá trị của liên kết chính là kết quả của thao tác liên kết. Trong các điều khoản tiếp theo, người ta cho rằng bất cứ khi nào đề cập đến một giá trị băm đơn biểu diễn một số mục dữ liệu, TSA thay vì sử dụng nhiều giá trị hàm băm trên cùng mục dữ liệu, thì có thể tính toán riêng biệt từng hàm băm.

B.2.2 Liên kết xích tuyến tính

Khi sử dụng phương pháp liên kết này, mỗi liên kết trong xích tuyến tính được hình thành bởi các giá trị ghép nối từ liên kết sinh ra gần nhất trong xích tuyến tính với giá trị băm đang liên kết hiện thời và chuỗi bít thu được làm đầu vào của hàm băm. Đầu ra của hàm băm là giá trị của liên kết mới và là tóm tắt hoạt động của tất cả thao tác liên kết từ trước đến nay và nó được lưu trữ trong kho liên kết được duy trì bởi TSA; giá trị của liên kết trước đó làm đầu vào cho thao tác liên kết đã được gửi trả cho bên yêu cầu trong trường "links" của cấu trúc 'BindingInfo' tương ứng.

B.2.3 Liên kết nhị phân chống đơn điệu

Khi sử dụng phương pháp liên kết này, kho liên kết được duy trì bởi TSA được biểu diễn bằng đồ thị có hướng phi chu trình chống đơn điệu với mỗi đỉnh có số đo độ bằng 2 [BLS00]. Từng liên kết trong đồ thị có hướng chống đơn điệu được hình thành bởi ghép nối các giá trị của hai liên kết trước đó trong đồ thị có hướng được duy trì bởi TSA (một trong số chúng là liên kết được tạo gần đây nhất trong đồ thị có hướng) với giá trị băm đang được liên kết hiện thời, và chuỗi bit thu được sử dụng làm đầu vào của hàm băm. Đầu ra của hàm băm là giá trị của liên kết mới và là tóm tắt hoạt động của tất cả thao tác liên kết từ trước đến nay và nó được lưu trữ trong kho liên kết được duy trì bởi TSA; giá trị của hai liên kết trước đó được sử dụng làm đầu vào cho thao tác liên kết đã được gửi trả về bên yêu cầu trong trường "links" của cấu trúc 'BindingInfo' tương ứng.

B.2.4 Liên kết cây phân luồng

Phương pháp liên kết này sử dụng cây xác thực phân luồng tương tự như cây băm Merkle [M80] và được tăng cường bằng cách bổ sung các cạnh giữa các đỉnh [BLS00]. Từng liên kết của cây phân luồng được hình thành bởi ghép nối các giá trị của một số lượng thích hợp các liên kết trước đó trong đồ thị có hướng được duy trì từ TSA (một trong số chúng là liên kết tạo ra gần đây nhất trong đồ thị có hướng) với giá trị băm đang được liên kết hiện thời, và sử dụng chuỗi bit thu được làm đầu vào cho hàm băm. Đầu ra của hàm băm là giá trị của liên kết mới và là tóm tắt hoạt động của tất cả các thao tác liên kết từ trước đến nay và nó được lưu trữ trong kho liên kết được duy trì bởi TSA; giá trị của các liên kết trước đó được sử dụng làm đầu vào cho thao tác liên kết đã được gửi trả về bên yêu cầu trong trường "links" của cấu trúc 'BindingInfo' tương ứng.

B.3 Tổ hợp

B.3.1 Khái quát

Tổ hợp là phương pháp sử dụng một nhóm các giá trị băm để tính toán giá trị đầu ra đơn mà có thể làm đại diện trực tiếp cho các giá trị băm gốc. Quá trình tổ hợp kết hợp các giá trị băm thành một giá trị tổ hợp đơn, trong đó từng giá trị băm đầu vào đóng góp theo một cách nào đó vào nội dung của giá trị tổ hợp. Quá trình tổ hợp cũng tạo ra các dữ liệu bổ sung cần thiết để xác thực quan hệ thành viên của từng giá trị băm trong nhóm giá trị băm đã được dùng để tạo nên giá trị tổ hợp. Các kỹ thuật được sử

dụng để kết hợp nhiều giá trị băm thành một giá trị tổ hợp đơn dựa vào các đặc tính mật mã của các hàm băm một chiều hoặc các thuật toán chồng chất khác.

Trong thực tế, TSA tạo ra các giá trị băm biểu diễn các gói cấu trúc 'TSTInfo' có cùng giá trị thời gian, và sử dụng giá trị tổ hợp thu được làm đại diện cho tất cả các cấu trúc 'TSTInfo' trong thao tác liên kết tiếp theo. Dữ liệu xác thực tính thành viên trong tổ hợp được chèn vào trong trường "aggregate" của cấu trúc 'BindingInfo' tương ứng.

B.3.2 Tổ hợp đơn nhất

Hình thức đơn giản nhất của tổ hợp là không tổ hợp tất cả. Nghĩa là trong khi các thao tác quan trọng và bảo mật giúp ích cho việc tổ hợp các giá trị băm với nhau, không cần thiết có quá trình cấp tem thời gian để tổ hợp chúng. Các gói cấu trúc 'TSTInfo' riêng lẻ có thể tạo ra các giá trị băm bằng cách đơn giản là đưa trực tiếp vào quá trình liên kết mà không tổ hợp bất kỳ giá trị băm nào khác. Trong khi phương pháp này đơn giản hóa quá trình cấp tem thời gian, nó cũng làm tăng lên đáng kể việc tải quá trình liên kết. Thẻ tem thời gian được tạo ra mà không tổ hợp cũng không được hưởng lợi từ tính bảo mật bổ sung được cung cấp từ mỗi thành viên trong nhóm tổ hợp để làm bằng chứng trực tiếp sự kiện cấp tem thời gian cho tất cả các thành viên khác trong nhóm. Xác minh tính hợp lệ của thẻ tem thời gian được tạo ra từ tổ hợp đơn nhất không đòi hỏi công việc bổ sung nào ngoại trừ việc xác minh các bước liên kết liên quan.

B.3.3 Tổ hợp cây Merkle

Các biểu diễn giá trị băm có thể tổ hợp bằng cách sử dụng cây xác thực được đề xuất bởi Merkle [M80] để sử dụng trong việc hình thành các thư mục của các khóa mật mã. Trong ứng dụng này, cây nhị phân xây dựng từ [M80] được sử dụng để tổ hợp các giá trị băm nhiều hơn các khóa mật mã. Quá trình tổ hợp này được bổ sung bằng cách chọn nhóm gói cấu trúc 'TSTInfo' để tổ hợp và tính toán các biểu diễn giá trị băm của chúng. Xử lý các giá trị băm thu được như là các lá của cây nhị phân. Tính toán từng nút trung gian của cây bằng cách ghép nối các giá trị băm con của nút đó và xử lý ghép nối như là đầu vào của hàm băm. Đầu ra của phép tính băm trở thành giá trị của nút đó. Thực hiện các tính toán theo cách này có thể tính toán ra được các nút ở các bậc cao hơn của cây, cho đến khi giá trị băm gốc đơn cũng được tính toán. Bởi vì tất cả các giá trị lá góp phần vào việc tính toán cuối cùng tại giá trị gốc nên giá trị gốc đó có thể được sử dụng làm đại diện trực tiếp cho tất cả các giá trị lá.

Khi việc xây dựng cây nhị phân này được sử dụng để tổ hợp các biểu diễn giá trị băm của gói cấu trúc 'TSTInfo', TSA trả về trong trường "aggregate" của cấu trúc 'BindingInfo' tương ứng với mỗi gói cấu trúc 'TSTInfo', các giá trị băm trung gian được yêu cầu để tính toán đường đi từ giá trị băm lá ban đầu đến giá trị băm gốc. Đối với tổ hợp của N gói cấu trúc 'TSTInfo', chỉ có $log_2 N$ các giá trị băm trung gian là được yêu cầu để tính toán đường đi từ giá trị băm lá đến giá trị băm gốc. Tính toán giá trị của trường "aggregate" của cấu trúc 'BindingInfo' tương ứng thì cần yêu cầu $log_2 N$ phép tính băm nhằm xác thực giá trị băm lá dựa vào giá trị tổ hợp đã tạo.

B.3.4 Tổ hợp tích lũy một chiều

Một dạng khác của tổ hợp là thông qua ứng dụng tích lũy một chiều. Dạng tổ hợp này tìm cách tính toán tổ hợp sao cho việc xác minh thành viên trong tổ hợp đòi hỏi có tính toán hằng số thời gian đơn, không tính đến số lượng các giá trị trong tổ hợp. Một kỹ thuật tích lũy kiểu như thế này được đề xuất bởi Benaloh và De Mare trong [BD93], trong đó sử dụng mô đun số mũ RSA của thừa số chưa biết để tính toán giá trị tích lũy đơn từ nhiều giá trị đầu vào. Kỹ thuật này cũng được sử dụng để tính toán các tuyên bố có thể xác minh cho từng giá trị đầu vào mà biểu thị tính thành viên của giá trị đầu vào trong giá trị tổ hợp.

Đối với tập hợp các giá trị băm Y = (y_1, y_2 ,..., y_N) biểu diễn cho N gói cấu trúc 'TSTInfo', mô đun RSA $n=pq$ (trong đó p và q là số nguyên tố) và điểm bắt đầu (mô đun số n) ký hiệu là x, thuật toán tích lũy tính như sau:

$$A(Y) = x^{y_1 y_2 \cdots y_N} \bmod n$$

Thuật toán tạo dựng bằng chứng P xây dựng bằng chứng cho thành phần y_i như một phần của tổ hợp có giá trị:

$$P(y_i, Y) = x^{y_1 y_2 \cdots y_{i-1} y_{i+1} \cdots y_N} \bmod n$$

và chèn nó vào trường "aggregate" trong cấu trúc 'BindingInfo' tương ứng, được gói trong cấu trúc 'Chain'.

Xác minh các bước tổ hợp có nghĩa là kiểm tra:

$$P(y_i, Y)^{y_i} = A(Y)$$

Như vậy việc xác minh các bước tổ hợp cho bất kỳ giá trị băm nào tham gia yêu cầu phải tính toán giá trị thời gian độc lập trong N.

B.4 Công bố

B.4.1 Khái quát

Sự kiện được nhiều bên quan sát độc lập chứng kiến thì không được phủ nhận ảnh hưởng. Khi phơi bày sự kiện cho nhiều bên quan sát và họ có duy trì đầy đủ hồ sơ về sự kiện này thì việc sửa đổi tất cả hồ sơ về sự kiện hoặc cấu kết với tất cả bên quan sát để sửa đổi hồ sơ sự kiện là điều không thể xảy ra trên thực tế. Chứng kiến có thể có nhiều cấp độ để cung cấp nhiều lớp bảo đảm. Chứng kiến có phương pháp chung là các liên kết được tạo bởi TSA được thể hiện rộng rãi, để cho bất kỳ thay đổi nào trong các liên kết này là không thể thực hiện được. Tập các sự kiện được chứng kiến có thể được kiểm tra bởi các bên tham gia khác bên ngoài TSA nhằm cung cấp sự đảm bảo tính toàn vẹn.

Công bố là cách mà trong đó bản thân quá trình liên kết có thể trở thành sự kiện được "chứng nhận rộng rãi". Cách này thường được sử dụng để đảm bảo quá trình liên kết tạo ra các sự kiện "chứng nhận rộng rãi" thông qua việc công bố định kỳ các giá trị băm từ quá trình liên kết bằng các phương tiện truyền thông được nhiều người biết đến. Ví dụ: quá trình công bố có thể chèn định kỳ các giá trị băm từ quá trình liên kết vào trang web, ở đó các giá trị băm được phổ biến rộng rãi trên Internet thông

qua bộ đệm web và các trạm chỉ mục. Quá trình công bố có thể lựa chọn công bố các giá trị băm từ quá trình liên kết trên các phương tiện truyền thông ngoại tuyến, chẳng hạn quảng cáo trên các báo chí phổ biến toàn cầu. Các quá trình khác có thể chèn các giá trị băm từ quá trình liên kết vào thông điệp thư điện tử hoặc nhóm tin trực tuyến và dựa vào các phương tiện để truyền bá thông tin.

B.4.2 Không công bố

Quá trình cấp tem thời gian có thể lựa chọn phương án bỏ qua công bố, ví dụ trên thực tế, nếu các tình huống vận hành ngăn cản việc sử dụng quá trình công bố. Tuy nhiên các hệ thống như vậy không thể tuyên bố là được "chứng nhận rộng rãi".

B.4.3 Công bố liên kết đơn

Quá trình công bố này lựa chọn định kỳ giá trị của liên kết đơn để công bố. Các giá trị công bố lần lượt quy định một khoảng thời gian, sao cho tất cả các liên kết tạo ra bởi quá trình liên kết trong khoảng thời gian đó có thể được sắp đặt trên chuỗi tuyến tính và có thể tham khảo giá trị công bố đơn đánh dấu điểm kết thúc của khoảng thời gian. Việc xác minh tính đúng đắn của liên kết dưới quá trình công bố này đòi hỏi có sẵn giá trị băm (hoặc giá trị băm tổ hợp) được sử dụng làm đầu vào cho các thao tác liên kết được tạo ra tất cả các liên kết tiếp theo, cho đến khi liên kết tương ứng với giá trị công bố. Số lượng các giá trị băm được yêu cầu bên trong thành phần của trường "pubChains" của phiên bản kiểu "ExtPublication" tăng như sau:

- Nếu là trường hợp liên kết xích tuyến tính, tăng một cách tuyến tính theo số lượng các liên kết được tạo ra trong khoảng thời gian lựa chọn.
- Nếu là trường hợp liên kết cây phân luồng, tăng theo hàm logarit theo số lượng các liên kết được tạo ra trong khoảng thời gian lựa chọn.

B.4.4 Công bố cây Merkle

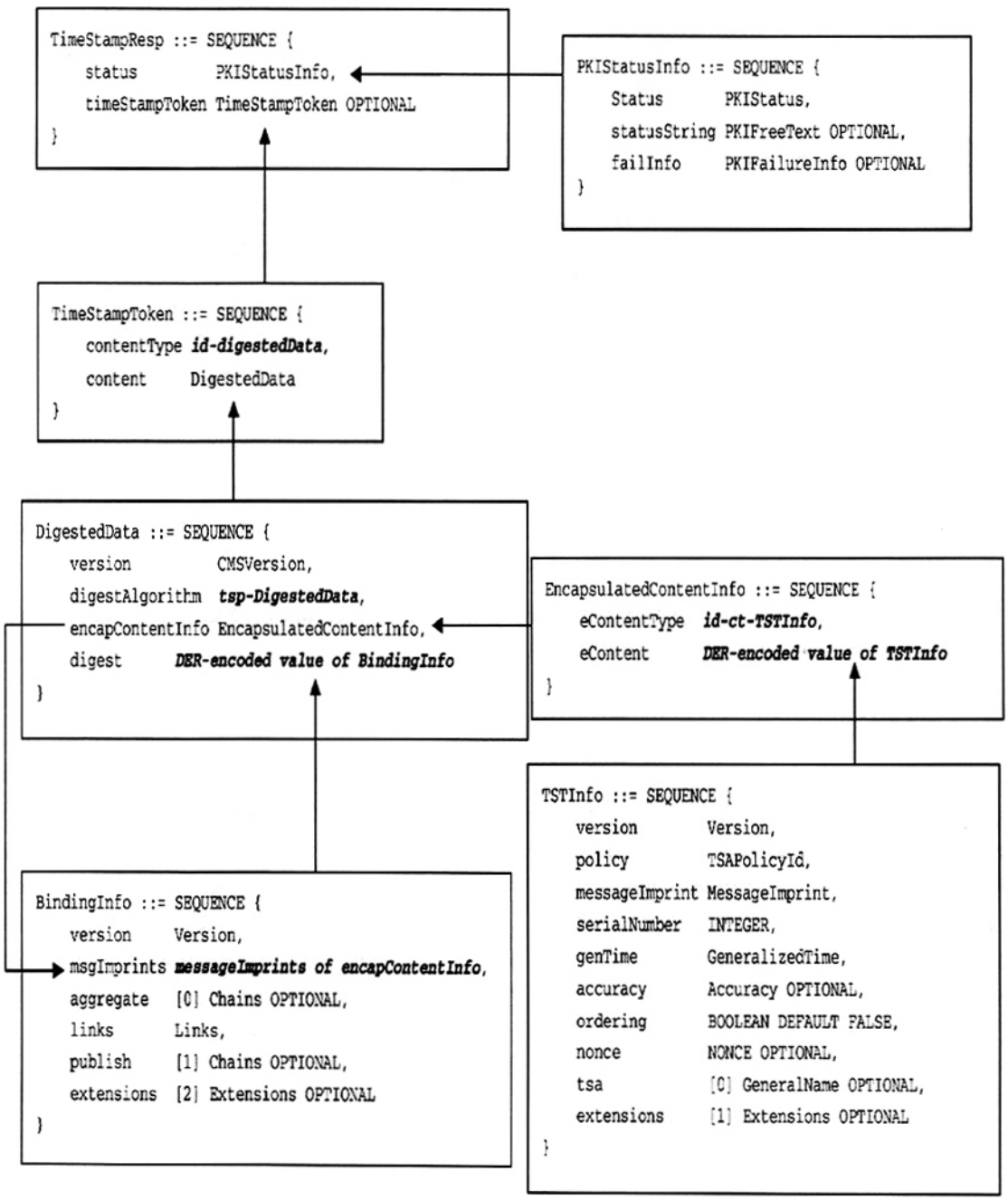
Một kiểu thao tác công bố khác bao gồm việc tích lũy một nhóm liên kết với nhau bằng phương pháp tính cây băm Merkle [*M80*]. Trong trường hợp này, các liên kết của một số khoảng thời gian đã chọn được tổ hợp với nhau và giá trị tổ hợp sau đó được công bố. Như quá trình tổ hợp để đóng gói cấu trúc *'TSTInfo'* đã được mô tả ở trên, mỗi liên kết lá trong cây công bố Merkle đều góp phần vào việc tính toán giá trị gốc, vì thế mà giá trị gốc có thể được sử dụng như đại diện trực tiếp tới tất cả các giá trị lá. Việc sử dụng cây nhị phân để tính toán các giá trị công bố đảm bảo rằng số lượng các giá trị băm được yêu cầu bên trong thành phần thuộc trường "pubChains" của phiên bản kiểu "ExtPublication" là $log_2 N$, trong đó N là số lượng liên kết được tạo ra trong khoảng thời gian đã chọn.

Phụ lục C

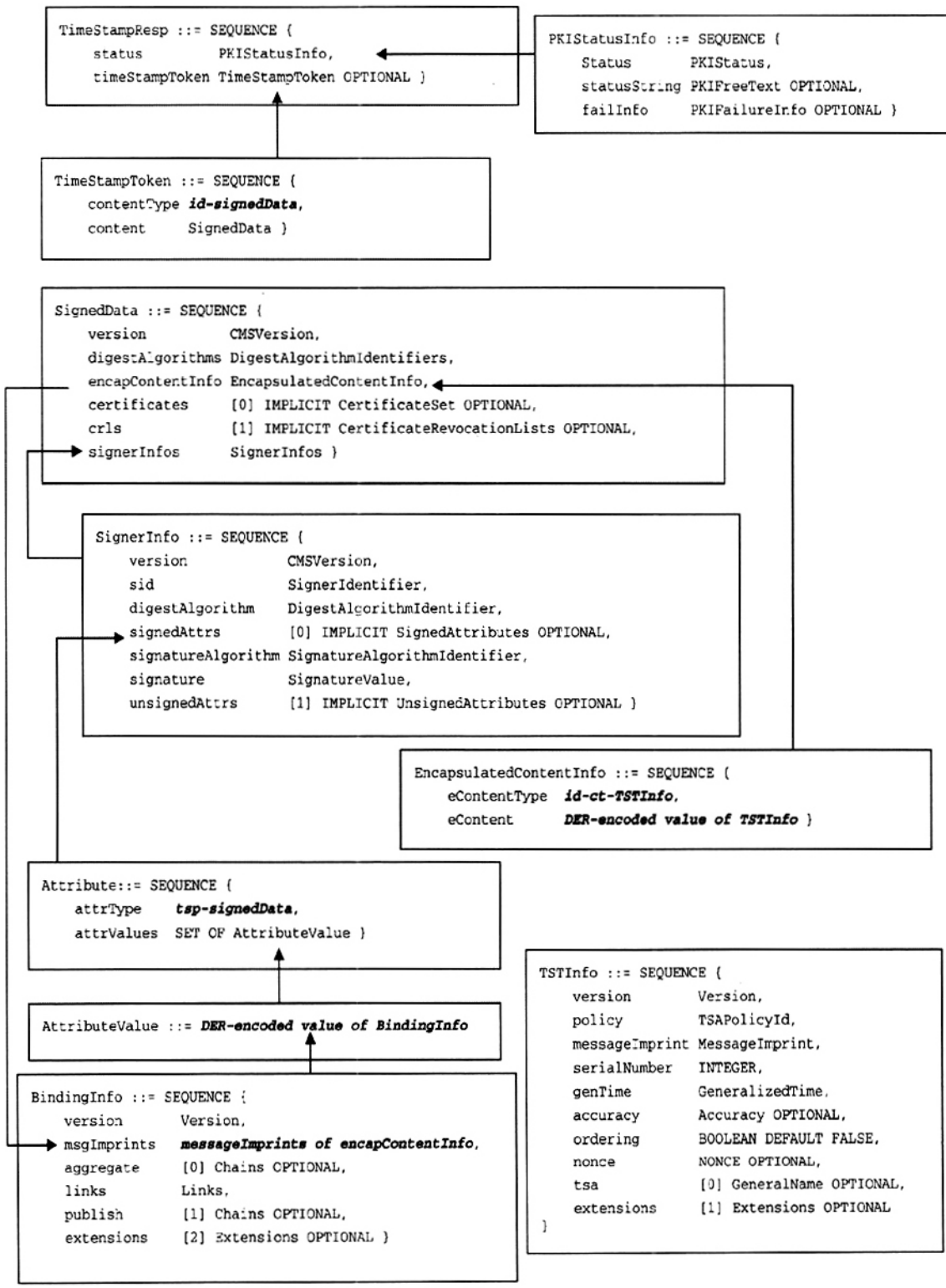
(tham khảo)

Cấu trúc dữ liệu

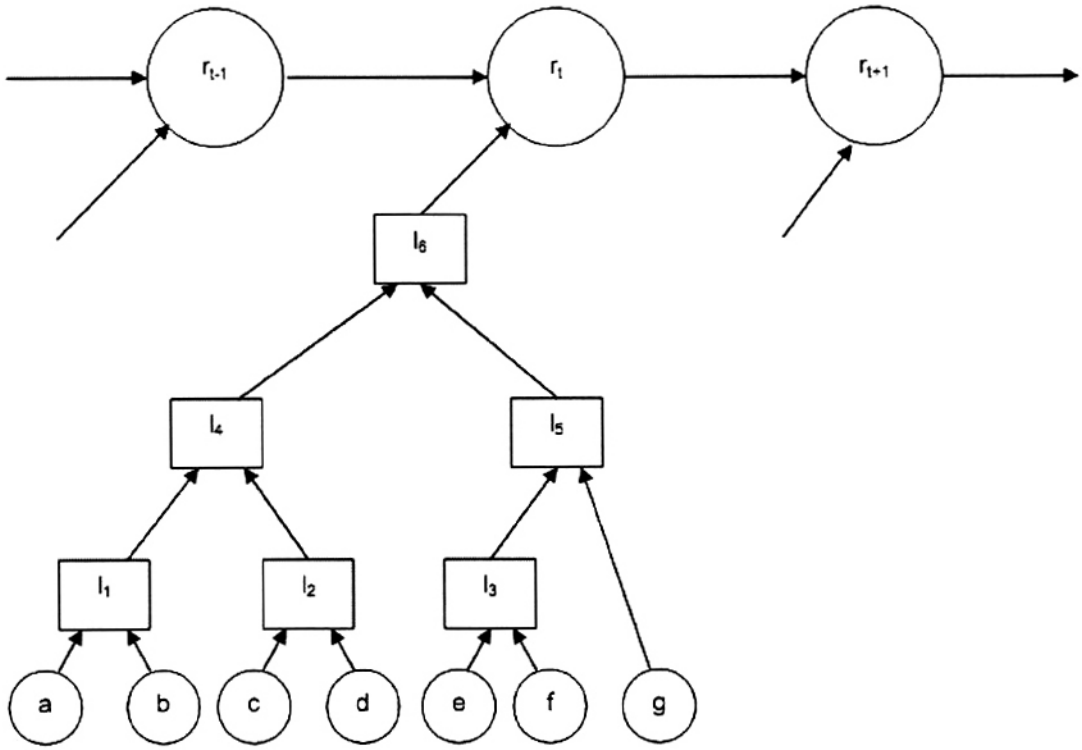
C.1 Thẻ tem thời gian sử dụng gói "DigestedData"



C.2 Thẻ tem thời gian sử dụng gói "SignedData"



C.3 Liên kết xích tuyến tính với tổ hợp cây Merkle



Biểu đồ thể hiện một ví dụ về tổ hợp cây Merkle tiếp theo thao tác liên kết xích tuyến tính. Giá trị đầu vào tại thời điểm *t* là: a, b, c, d, e, f, g. Trong nội dung của Điều 8.1, các giá trị này biểu diễn các octet của các dấu thông điệp trong trường "msgImprints" của cấu trúc 'BindingInfo' được tạo ra cho từng thẻ tem thời gian tham gia mà đã được gán cùng giá trị thời gian bên trong cấu trúc '*TSTInfo*'.

Tại thời điểm *t* của bước tổ hợp của cây *Merkle* tạo ra các giá trị trung gian l_1, l_2, l_3, l_4, l_5 và giá trị gốc l_6. Giá trị liên kết trong xích tuyến tính các liên kết tại thời điểm $t - 1$ là r_{t-1}. Giá trị của liên kết vừa được tính trên xích tuyến tính tại thời điểm *t* là r_t .

Gọi H là thuật toán được sử dụng tại mỗi bước tổ hợp của cây *Merkle* (ví dụ: hàm băm được áp dụng trên các chuỗi giá trị của đối số). Tiến hành như sau:

$l_1 = H(a, b)$ $l_2 = H(c, d)$ $l_3 = H(e, f)$

$l_4 = H(l_1, l_2)$ $l_5 = H(l_3, g)$

$l_6 = H(l_4, l_5)$

Mỗi giá trị đầu vào được xử lý tại thời điểm t có thể được coi như đường dẫn tới gốc cây Merkle (điểm l_6 trong biểu đồ) và có thể được sử dụng để tính toán gốc cây Merkle, do đó xác nhận sự có mặt của

giá trị đầu vào trong việc tính toán gốc cây Merkle. Các đường dẫn cho từng giá trị đầu vào có thể được thể hiện dưới dạng kiểu dữ liệu 'Chain' như định nghĩa tại Điều 7.5. Trong các định nghĩa sau đây, tham chiếu số 0 chỉ ra giá trị đầu vào của dây xích đang được định nghĩa và "Hàm(H)" biểu thị thuật toán tham số hóa được áp dụng trên dãy các trường hợp kiểu 'Link'. Để tham chiếu dễ dàng, định danh *j* chọn cho mỗi phiên bản kiểu 'Link' phù hợp với các ký hiệu được sử dụng cho các giá trị l_j tương ứng trong biểu đồ:

chuỗi (a) = (Hàm(H), ((1, (0, b)), (4, (1, l_2)), (6, (4, l_5))))
chuỗi (b) = (Hàm(H), ((1, (a, 0)), (4, (1, l_2)), (6, (4, l_5))))
chuỗi (c) = (Hàm(H), ((2, (0, d)), (4, (l_1, 2)), (6, (4, l_5))))
chuỗi (d) = (Hàm(H), ((2, (c, 0)), (4, (l_1, 2)), (6, (4, l_5))))
chuỗi (e) = (Hàm(H), ((3, (0, f)), (5, (3,g)), (6, (l_4, 5))))
chuỗi (f) = (Hàm(H), ((3, (e, 0)), (5, (3,g)), (6, (l_4, 5))))
chuỗi (g) = (Hàm(H), ((5, (l_3, 0)), (6, (l_4, 5))))

Tất cả các chuỗi tổ hợp cho các mục đầu vào được liệt kê trên đây đều tạo ra cùng giá trị l_6 trong khi giá trị của chuỗi được tính toán bằng cách áp dụng thuật toán H liên tục trên dãy các phần tử con của chuỗi cho đến khi còn lại một giá trị duy nhất. Ví dụ:

giá trị (chuỗi (d)) = giá trị ((Hàm(H), ((2, (c, d)), (4, (l_1, 2)), (6, (4, l_5)))))
= giá trị ((Hàm(H), ((4, (l_1, l_2)), (6, (4, l_5)))))
= giá trị ((Hàm(H), ((6, (l_4, l_5)))))
= l_6

Gọi G là thuật toán được sử dụng tại các thao tác liên kết tuyến tính (ví dụ: hàm băm áp dụng trên các giá trị ghép nối của đối số). Thuật toán này lấy giá trị đối số của liên kết trước đó trong kho (tức là được tạo ra bởi thao tác liên kết trước đó) và gốc cây Merkle được tính trên các giá trị đầu vào đã được cung cấp, theo cách sau:

$$r_t = G(r_{t-1}, l_6).$$

Thao tác liên kết cho tất cả các giá trị đầu vào tham gia trong cây Merkle với giá trị gốc l_6 có thể biểu thị dưới dạng phiên bản kiểu 'Link' đơn như đã định nghĩa ở Điều 7.6, sử dụng "Hàm(G)" để biểu thị thuật toán tham số hóa được áp dụng trên các thành viên của phiên bản kiểu 'Link', ví dụ:

liên kết (a, chuỗi (a)) = (Hàm(G), (r_{t-1}, 0))

Tham chiếu số 0 ở trên cho biết giá trị được tính toán trên chuỗi (a). Giá trị của mục dữ liệu này biểu diễn kết quả của thao tác liên kết được tính bằng cách áp dụng thuật toán G trên giá trị của liên kết trước đó và giá trị của chuỗi là:

giá trị (liên kết(a, chuỗi (a)) = giá trị ((Hàm(G), (r_{t-1}, giá trị (chuỗi (a))))
= giá trị ((Hàm(G), (r_{t-1}, l_6)))
= r_t

Như đã đề cập ở trên, thuật toán tham số hóa đơn ("Hàm(H)" hoặc "Hàm(G)") có thể được dùng để biểu thị các thuận toán liên kết và tổ hợp đã được sử dụng để tính toán các giá trị của mục dữ liệu phản hồi. Trong mô đun ASN X9.95-2005 "Tem thời gian đáng tin cậy, Quản lý và Bảo mật" *(Trusted Time Stamp, Management and Security)* và các định nghĩa của ASN.1 sau đây được cung cấp để xác định kiểu thuật toán tham số hóa:

```
merkle-chain ALGORITHM ::= {
```

```
       OBJECT IDENTIFIER id-merkle-chain PARMS MerkleChainParms }
id-merkle-chain OBJECT IDENTIFIER ::= {
      iso(1) identified-organization(3) tc68(133) country(16) x9(840)
      x9Standards(9) x9-95(95) ids(1) merkle-chain(1) }
MerkleChainParms ::= SEQUENCE SIZE(1..MAX) OF HashFunction
HashFunction ::= AlgorithmIdentifier {{ HashAlgorithms }}
HashAlgorithms ALGORITHM ::= {
    { OID sha1 PARMS NULL } |
    { OID id-sha256 PARMS NULL } |
    { OID id-sha224 PARMS NULL } |
    { OID id-sha384 PARMS NULL } |
    { OID id-sha512 PARMS NULL } ,
    ... -- expect additional algorithms --
}
```

Đối với thuật toán tham số hóa cho trước như trên, thì việc áp dụng thuật toán này ở phiên bản kiểu 'Link' đòi hỏi áp dụng từng hàm băm trong danh sách tham số để ghép nối các giá trị của các mục trong phiên bản kiểu 'Link', nhờ đó các hàm băm được liệt kê trong danh sách tham số. Các giá trị băm thu được sau đó được ghép nối vào một chuỗi octet biểu diễn giá trị của phiên bản kiểu 'Link'. Thuật toán tham số hóa được áp dụng trên các trường hợp kiểu 'Link' kế tiếp cho đến khi giá trị đơn được tính toán.

Tài liệu tham khảo

[1] [BD91] J. Benaloh, M. de Mare, "*Efficient Broadcast Time-Stamping*," TR 91-1, Clarkson University Department of Mathematics and Computer Science, 1991. (*Cấp tem thời gian quảng bá*).

[2] [BD93] J. Benaloh, M. de Mare, "*One-Way accumulators: A Decentralized Alternative to Digital Signatures*," Advances in Cryptology — EUROCRYPT 1993, Lecture Notes in Computer Science, vol.765, pp. 274-285, Springer-Verlag, 1994.(*Bộ tích lũy một chiều: khả năng phân quyền: chữ ký số*).

[3] [BHS93] D. Bayer, S. Haber, W. Stornetta, "*Improving the Efficiency and Reliability of Digital Time-Stamping*," Sequences II: Methods in Communication, Security and Computer Science, pp. 329-334, Springer-Verlag, 1993. (*Tăng cường hiệu quả và tính tin cậy của cấp tem thời gian số*).

[4] [BLLV98] A. Buldas, P. Laud, H. Lipmaa, J. Villemson, "*Time-Stamping with Binary Linking Schemes*," Advances in Cryptology — CRYPTO 1998, Lecture Notes in Computer Science, vol. 1462, pp. 486-501, Springer-Verlag, 1998. (*Cấp tem thời gian với lược đồ liên kết nhị phân*).

[5] [BLS00] A. Buldas, H. Lipmaa, B. Schoenmakers, "*Optimally Efficient Accountable Time-Stamping*," Public Key Cryptography 2000, pp. 293-305, Springer-Verlag, January 2000. (*Cấp tem thời gian tối ưu*).

[6] [HS91] S. Haber, W. Stornetta, "*How to Time-Stamp a Digital Document*," Journal of Cryptology, Vol. 3, No. 2, pp. 99-111, 1991. (*Phương phép cấp tem thời gian cho tài liệu số*)

[7] [HS97] S. Haber, W. Stornetta, "*Secure Names for Bit-Strings*," Proceedings of the 4th ACM Conference on Computer and Communication Security, pp. 28-35, ACM Press, 1997.(*Tên đảm bảo cho các chuỗi bit*).

[8] [J98] M. Just, "*Some Timestamping Protocol Failures*", Proceedings of the Internet Society Symposium on Network and Distributed System Security, p. 5, Internet Society, 1998. (*Một số lỗi giao thức cấp tem thời gian*).

[9] [M80] R. Merkle, "*Protocols for Public Key Cryptosystems*," Proceedings of the IEEE Symposium on Security and Privacy, pp. 122-133, IEEE Computer Society, 1980. (*Các giao thức cho các hệ thống mật mã khóa công khai*).

[10] [PKIXCP] R. Housley, W. Ford, W. Polk, D. Solo, "*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*" IETF RFC 3280, 2002. (*Hồ sơ CRL và chứng thư hạ tầng khóa*

công khai Internet X.509).

[11] [CMS] R. Housley, "*Cryptographic Message Syntax*", IETF RFC 3852, 2004. (*Cú pháp thông điệp mật mã hóa*).

[12] ISO/IEC 10181-1:1996, Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview (*Công nghệ thông tin – Liên kết nối hệ thông mở - Cơ cấu an ninh đối với các hệ thống mở: Tổng quan*).