

TCVN

TIÊU CHUẨN QUỐC GIA

TCVN 14191-1:2024

ISO/IEC 23264-1:2021

Xuất bản lần 1

**AN TOÀN THÔNG TIN – BIÊN TẬP LẠI DỮ LIỆU
XÁC THỰC - PHẦN 1: YÊU CẦU CHUNG**

Information security — Redaction of authentic data — Part 1: General

HÀ NỘI – 2024

Mục lục

Lời nói đầu.....	4
Giới thiệu	5
1 Phạm vi áp dụng.....	7
2 Tài liệu viện dẫn	7
3 Thuật ngữ và định nghĩa.....	7
4 Ký hiệu và quy ước.....	11
4.1 Các ký hiệu	11
4.2 Quy ước.....	12
5 Mô hình chung và các quá trình.....	12
5.1 Yêu cầu chung	12
5.2 Các bên và quá trình	12
5.3 Mô hình chung	12
5.4 Đặc điểm kỹ thuật của các quá trình	14
6 Thuộc tính mật mã của các lược đồ chứng thực có thể được biên tập lại.....	16
6.1 Các thuộc tính mật mã bắt buộc.....	16
6.2 Thuộc tính mật mã tùy chọn	16
Thư mục Tài liệu tham khảo	18

Lời nói đầu

TCVN 14191-1:2024 hoàn toàn tương đương với ISO/IEC 23264-1:2021.

TCVN 14191-1:2024 do Ban Cơ yếu Chính phủ biên soạn, Bộ Quốc phòng đề nghị, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Bộ tiêu chuẩn TCVN 14191 (ISO/IEC 23264) An toàn thông tin – Biên tập lại dữ liệu xác thực, gồm 02 phần:

- TCVN 14191-1:2024 (ISO/IEC 23264-1:2021): An toàn thông tin – Biên tập lại dữ liệu xác thực – Phần 1: Yêu cầu chung
- ISO/IEC 23264-2:2024: Information security – Redaction of authentic data – Part 2: Redactable signature schemes based on asymmetric mechanisms.

Giới thiệu

Các lược đồ chứng thực kỹ thuật số, cụ thể là các lược đồ chữ ký số hoặc mã xác thực thông điệp, có thể được sử dụng để cung cấp tính toàn vẹn của dữ liệu và xác thực nguồn gốc dữ liệu. Lược đồ chứng thực có thể được biên tập lại cho phép xác thực thông điệp bằng cách nhận biết một số phần nhất định của thông điệp chứng thực (được gọi là các trường) đã được biên tập lại (bị xóa, bỏ trống hoặc bị xóa vĩnh viễn) thì chứng thực của thông điệp đã được biên tập lại vẫn có thể được xác minh. Chính xác hơn, khi chứng thực một thông điệp, bên chứng thực biết khóa chứng thực bí mật có thể xác định những phần nào của thông điệp sau này đã được biên tập lại (theo nghĩa của ISO/IEC 27038) bởi bất kỳ thực thể nào chỉ biết thông điệp được chứng thực và khóa được biên tập lại của bên chứng thực. Bất kỳ sửa đổi nào khác của thông điệp đã được chứng thực (ví dụ: biên tập lại các phần thông điệp khác hoặc chèn/sửa đổi bất kỳ phần nào) sẽ làm mất hiệu lực chứng thực.

Các lược đồ chứng thực có thể được biên tập lại từ một khái cấu trúc cơ bản trong nhiều ứng dụng bảo vệ quyền riêng tư, chẳng hạn như chia sẻ hoặc xác thực dữ liệu bảo vệ quyền riêng tư, trong đó một thực thể có thể quyết định chỉ tiết lộ thông tin thực sự cần thiết để chuyển tiếp đến người nhận, trong khi ứng dụng này vẫn đảm bảo rằng thông tin nhận được đã được chứng thực trước đó, ví dụ: Cơ quan có thẩm quyền.

Mục tiêu của bộ tiêu chuẩn TCVN 14191 (ISO/IEC 23264) là khắc phục sự không tương thích hiện có hoặc các thuộc tính được xác định không nhất quán trong các thông số kỹ thuật hiện có của các lược đồ như vậy và để dễ dàng áp dụng công nghệ này trong thực tiễn. Cụ thể, mục tiêu của tiêu chuẩn này là tạo nền tảng cho các phần tiếp theo (ví dụ: tập trung vào các thuật toán cụ thể để biên tập lại tính xác thực của các định dạng tài liệu cụ thể như văn bản, hình ảnh, video, v.v.) bằng cách chỉ định và xác định các thuật ngữ và thuộc tính chung cho các chương trình như vậy.

Bộ tiêu chuẩn TCVN 14191 (ISO/IEC 23264) bổ sung cho tiêu chuẩn ISO/IEC 27038, quy định việc biên tập lại các tài liệu kỹ thuật số mà không đề cập đến tính xác thực của dữ liệu.

An toàn thông tin – Biên tập lại dữ liệu xác thực – Phần 1: Yêu cầu chung*Information security – Redaction of authentic data – Part 1: General***1 Phạm vi áp dụng**

Tiêu chuẩn này xác định các thuộc tính của cơ chế mật mã để biên tập lại dữ liệu xác thực. Đặc biệt, nó xác định các quá trình liên quan đến các cơ chế đó, các bên tham gia và các thuộc tính mật mã.

2 Tài liệu viện dẫn

Tiêu chuẩn này không sử dụng tài liệu viện dẫn.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các định nghĩa và thuật ngữ sau đây:

3.1**Những thay đổi có thể chấp nhận được (admissible changes)**

Mô tả về tất cả các sửa đổi có thể có của một thông điệp (mục 3.12) được chứng thực bằng lược đồ chứng thực có thể được biên tập lại (mục 3.16) có thể được áp dụng trong quá trình biên tập lại (mục 3.23) mà không làm mất hiệu lực của chứng thực đã được biên tập lại (mục 3.18).

CHÚ THÍCH 1: Tập hợp các thay đổi có thể chấp nhận được gọi là không đáng kể, nếu những thay đổi có thể chấp nhận cho phép ít nhất một sửa đổi của thông điệp gốc sẽ tạo ra thông điệp đã được biên tập lại khác với thông điệp ban đầu.

CHÚ THÍCH 2: Trong phạm vi của tiêu chuẩn này, các thay đổi có thể có của thông điệp được giới hạn ở việc loại bỏ một số trường của thông điệp.

3.2**Khóa chứng thực (attestation key)****Khóa chứng thực bí mật (private attestation key)**

Hạng mục dữ liệu bí mật được dành riêng cho bên chứng thực (mục 3.4) và chỉ thực thi này mới có thể sử dụng được trong quá trình chứng thực có thể được biên tập lại (mục 3.15).

CHÚ THÍCH 1: Thuật ngữ "Quá trình chứng thực có thể được biên tập lại" được sử dụng thay vì "quá trình ký số", định nghĩa này phù hợp với "khóa ký số" như được định nghĩa trong TCVN 12214-1:2018, 3.13.

3.3**Thông điệp đã được chứng thực (attested message)**

Tập hợp các mục dữ liệu bao gồm chứng thực có thể được biên tập lại (3.14), những thay đổi có thể chấp nhận được (3.1) và các trường (3.10) của thông điệp (3.12) được chứng thực.

CHÚ THÍCH 1: Tùy thuộc vào việc khởi tạo, nếu không phải tất cả các thay đổi có thể chấp nhận đều là một phần của thông điệp đã được chứng thực, thì ít nhất những thay đổi có thể chấp nhận đó có liên quan đến quá trình xác minh có thể được cấu trúc lại từ chứng thực có thể được biên tập lại kết hợp với các trường của thông điệp đã được chứng thực và khóa xác minh.

3.4**Bên chứng thực (attestor)**

Thực thi sử dụng khóa chứng thực bí mật (mục 3.2) để thực hiện quá trình chứng thực có thể được biên tập lại (mục 3.15), tạo ra một thông điệp (mục 3.3) đã được chứng thực.

3.5

Tính bí mật (confidentiality)

Tính chất không được cung cấp hoặc tiết lộ thông tin cho các cá nhân, thực thể hoặc quá trình trái phép.

[NGUỒN: 3.3.16, TCVN 9696-2:2013, được sửa đổi - Đã bị xóa.]

3.6

Toàn vẹn dữ liệu (data integrity)

Tính chất không bị thay đổi hoặc phá hủy dữ liệu theo cách trái phép.

[NGUỒN: 3.3.21, TCVN 9696-2:2013, được sửa đổi - Đã bị xóa.]

3.7

Chứng thực số (digital attestation)

Dữ liệu được nén thêm hoặc sự biến đổi mật mã của *thông điệp* (mục 3.12) cho phép người nhận dữ liệu xác minh nguồn gốc và tính *toàn vẹn dữ liệu* (mục 3.6) của *thông điệp* (mục 3.12).

3.8

Miền (domain)

Tập hợp các thực thể hoạt động theo một chính sách an toàn duy nhất.

Lưu ý 1: Trong phạm vi của tiêu chuẩn này, một miền chứa tất cả những bên chứng thực, bên biên tập lại và bên xác minh tham gia.

[NGUỒN: 3.4, TCVN 12214-1:2018, được sửa đổi - Chủ thích 1 đã được bổ sung.]

3.9

Tham số miền (domain parameter)

Phần dữ liệu phổ biến và được biết đến hoặc có thể truy cập được đổi với tất cả các thực thể trong *miền* (mục 3.8).

[NGUỒN: 3.5, TCVN 12214-1:2018, được sửa đổi - Đã bị xóa.]

3.10

Trường (field)

Chuỗi con có độ dài bất kỳ của *thông điệp* (mục 3.12).

3.11

Quá trình sinh khóa (key generation process)

Quá trình sinh khóa mật mã.

3.12

Thông điệp (message)

Chuỗi các bit có độ dài bất kỳ.

CHÚ THÍCH 1: Trong ngữ cảnh của tiêu chuẩn này, *thông điệp* luôn bao gồm một hoặc một số trường. Thành phần cấu thành và sự phân tách luôn có thể nhận được từ *thông điệp*.

[NGUỒN: 3.10, TCVN 12214-1:2018, được sửa đổi - Chủ thích 1 được bổ sung.]

3.13

Hướng dẫn sửa đổi (modification instruction)

Tiêu chuẩn này cung cấp mô tả việc *thông điệp* được biên tập lại, tức là cách một *thông điệp* (mục 3.12) đã được biên tập lại bởi *bên biên tập lại* (mục 3.24) trong một *quá trình biên tập lại* (mục 3.23).

CHÚ THÍCH 1: Hướng dẫn sửa đổi được gọi là không đáng kể nếu thông điệp đầu vào và thông điệp thu được bởi quá trình biên tập lại không giống nhau.

3.14

Chứng thực có thể được biên tập lại (redactable attestation)

Chứng thực số có thể được biên tập lại (redactable digital attestation)

Dữ liệu thu được từ quá trình chứng thực xử lý các dữ liệu bí mật được nối vào *thông điệp* (mục 3.12) cho phép người nhận dữ liệu này xác minh nguồn gốc và tính toàn vẹn của *thông điệp* (mục 3.12).

CHÚ THÍCH 1: Chuỗi bit này có thể có cấu trúc bên trong đặc trưng cho cơ chế chứng thực.

3.15

Quá trình chứng thực có thể được biên tập lại (redactable attestation process)

Quá trình nhận làm đầu vào *thông điệp* (mục 3.12), *khóa chứng thực bí mật* (mục 3.2), *các thay đổi có thể chấp nhận được* (mục 3.1) và *các tham số miền* (mục 3.9) và kết quả đầu ra *chứng thực xử lý các dữ liệu bí mật* (mục 3.14).

3.16

Lược đồ chứng thực có thể được biên tập lại (redactable attestation scheme)

Tập hợp các quá trình thực hiện *chứng thực số* (mục 3.7) và hỗ trợ việc tạo và xác minh các *Chứng thực số có thể được biên tập lại* (3.14) cùng với *quá trình biên tập lại* (mục 3.23).

3.17

Những thay đổi được chấp nhận đã được biên tập lại (redacted admissible changes)

Những thay đổi có thể chấp nhận được (mục 3.1) là đầu ra của *quá trình biên tập lại* (mục 3.23).

CHÚ THÍCH 1: Những thay đổi chấp nhận được đã được biên tập lại được phát sinh trong quá trình biên tập lại từ những thay đổi có thể chấp nhận được bằng cách áp dụng Hướng dẫn sửa đổi.

3.18

Chứng thực đã được biên tập lại (redacted attestation)

Chứng thực số đã được biên tập lại (redacted digital attestation)

Chứng thực do áp dụng *quá trình biên tập lại* (mục 3.23) ít nhất một lần với một số *Hướng dẫn sửa đổi* (mục 3.13).

CHÚ THÍCH 1: Chuỗi bit này có thể có cấu trúc bên trong cụ thể cho cơ chế chứng thực.

3.19

Thông điệp chứng thực đã được biên tập lại (redacted attested message)

Tập hợp các hạng mục dữ liệu là kết quả của *quá trình biên tập lại* (mục 3.23) bao gồm *chứng thực được biên tập lại* (mục 3.18), *những thay đổi chấp nhận được đã được biên tập lại* (mục 3.17) và *thông điệp được biên tập lại* (mục 3.20) được tạo từ các trường (mục 3.10) không chịu bất kỳ sự biên tập lại nào.

CHÚ THÍCH 1: Tùy thuộc vào việc khởi tạo, nếu không phải tất cả những thay đổi chấp nhận được đã được biên tập lại đều là một phần của thông điệp đã được biên tập lại, thì ít nhất những thay đổi chấp nhận được đã được biên tập lại đó có liên quan đến quá trình xác minh có thể được tạo lại từ chứng thực đã được biên tập lại kết hợp với thông điệp đã được biên tập lại và khóa xác minh.

3.20

Thông điệp đã được biên tập lại (redacted message)

Thông điệp (mục 3.12) là kết quả đầu ra từ *quá trình biên tập lại* (mục 3.23).

3.21

Biên tập lại (redaction)

Loại bỏ một *trường* (mục 3.10) dẫn đến việc xóa vĩnh viễn và không thể đảo ngược thông tin có trong trường đó khỏi *Thông điệp* (mục 3.12).

CHÚ THÍCH 1: Việc xóa một trường chỉ xóa thông tin có trong trường đó. Thông tin có thể được lấy từ các trường khác của thư hoặc từ các nguồn khác sẽ không bị xóa.

3.22

Khóa được biên tập lại (redaction key)

Tập hợp các hạng mục dữ liệu công khai có liên quan đến *khóa chứng thực bí mật* (mục 3.2) của *bên chứng thực* (mục 3.4) và được sử dụng bởi *bên biên tập lại* (mục 3.24) trong *quá trình biên tập lại* (mục 3.23).

CHÚ THÍCH 1: Tùy thuộc vào việc khởi tạo, khóa được biên tập lại có thể là bí mật hoặc công khai. Trong mọi trường hợp, kiến thức về hoạt động khóa được biên tập lại không đem kết quả về sự liên quan đến khóa chứng thực bí mật của bên chứng thực.

3.23

Quá trình biên tập lại (redaction process)

Quá trình lấy đầu vào là *Thông điệp đã được chứng thực* (mục 3.3), các *tham số miền* (mục 3.9), *khóa được biên tập lại* (mục 3.22), *Hướng dẫn sửa đổi* (mục 3.13) và xuất ra một *Thông điệp chứng thực đã được biên tập lại* (mục 3.19) bằng cách áp dụng *Hướng dẫn sửa đổi*.

CHÚ THÍCH 1: Đầu vào cho quá trình xử lý các dữ liệu bí mật có thể là một *Thông điệp đã được chứng thực* hoặc một *Thông điệp chứng thực đã được biên tập lại* do một (hoặc nhiều) ứng dụng trước đó của một quá trình *biên tập lại*.

CHÚ THÍCH 2: Những thay đổi có thể chấp nhận được cung cấp ngầm dưới dạng đầu vào như một phần của *Thông điệp đã được chứng thực*.

CHÚ THÍCH 3: Chỉ có thể tạo chứng thực đã được biên tập lại có thể xác minh được bằng cách sử dụng khóa xác minh của bên chứng thực, nếu một *Hướng dẫn sửa đổi* nhất định phù hợp với những thay đổi có thể chấp nhận do bên chứng thực chỉ định.

3.24

Bên biên tập lại (redactor)

Thực thể thực hiện *quá trình biên tập lại* (mục 3.23).

3.25

Khóa xác minh (verification key)

Tập hợp các hạng mục dữ liệu có liên quan đến *khóa chứng thực bí mật* (mục 3.2) của *bên chứng thực* và được *bên xác minh* (mục 3.27) sử dụng trong *quá trình xác minh* (mục 3.26).

CHÚ THÍCH 1: Tùy thuộc vào việc khởi tạo, khóa xác minh có thể là bí mật hoặc công khai. Trong trường hợp khóa xác minh công khai, không thể sử dụng kiến thức về khóa xác minh để suy ra thông tin về khóa chứng thực bí mật của bên chứng thực.

3.26

Quá trình xác minh (verification process)

Quá trình như sau:

- Lấy đầu vào là *thông điệp đã được chứng thực* (mục 3.13) (khả năng đã được biên tập lại), bao gồm: *thông điệp* (mục 3.12) (khả năng đã được biên tập lại), *những thay đổi có thể chấp nhận được* (mục 3.1) (khả năng đã được biên tập lại) và *chứng thực có thể được biên tập lại* (mục 3.14), *khóa xác minh* (mục 3.25) (khả năng đã được biên tập lại) và *các tham số miền* (mục 3.9);
- Kiểm tra xem chứng thực đã cho có phải là chứng thực hợp lệ cho thông điệp đã cho trong khóa xác minh nhất định hay không;
- Đưa ra kết quả của việc xác minh chứng thực: Hợp lệ hay không hợp lệ.

CHÚ THÍCH 1: Chỉ có thể xuất ra hợp lệ nếu Hướng dẫn sửa đổi đã được áp dụng trong một (hoặc nhiều) ứng dụng của quá trình xử lý lại phù hợp với các thay đổi có thể chấp nhận do bên chứng thực chỉ định.

CHÚ THÍCH 2: Tùy thuộc vào việc khởi tạo, nếu không phải tất cả các thay đổi có thể chấp nhận (khả năng đã được biên tập lại) là một phần của thông điệp đã được chứng thực (khả năng đã được biên tập lại), thì ít nhất những thay đổi có thể chấp nhận được (khả năng đã được biên tập lại) có liên quan đến quá trình xác minh có thể được tạo lại từ xác thực (khả năng đã được biên tập lại) kết hợp với thông điệp (khả năng đã được biên tập lại) và khóa xác minh.

3.27

Bên xác minh (verifier)

Thực thể thực hiện *quá trình xác minh* (mục 3.26).

4 Ký hiệu và quy ước

4.1 Các ký hiệu

<i>adm</i>	mô tả về những thay đổi chấp nhận được đã được biên tập lại hoặc những thay đổi ban đầu được chấp nhận
<i>adm'</i>	mô tả về những thay đổi chấp nhận được đã được biên tập lại
<i>ak</i>	khóa chứng thực
<i>att</i>	chứng thực có thể biên tập lại hoặc chứng thực đã được biên tập lại
<i>att'</i>	chứng thực đã được biên tập lại
<i>m</i>	thông điệp đã được biên tập lại hoặc thông điệp gốc
<i>m'</i>	thông điệp đã được biên tập lại
<i>m₁, ..., m_n</i>	các trường riêng lẻ của một thông điệp
<i>mod</i>	mô tả Hướng dẫn sửa đổi
<i>n</i>	số trường trong một thông điệp
<i>rk</i>	khóa được biên tập lại
<i>vk</i>	khóa xác minh
<i>Z</i>	tập hợp một hoặc nhiều tham số miền

4.2 Quy ước

Bộ ba thông điệp, chứng thực và danh sách những thay đổi có thể chấp nhận được ký hiệu là (m , att , adm). Theo cách tương tự, một bộ ba thông điệp đã được biên tập lại, chứng thực đã được biên tập lại và những thay đổi chấp nhận được đã được biên tập lại được biểu thị bằng (m' , att' , adm').

Các giá trị cụ thể của một biểu tượng (ví dụ: sym) được phân biệt bằng cách sử dụng chỉ số trên (ví dụ: sym^* , sym^{**} , v.v.)

5 Mô hình chung và các quá trình

5.1 Yêu cầu chung

Các lược đồ chứng thực kĩ thuật số như lược đồ chữ ký số hoặc mã xác thực thông điệp có thể được sử dụng để xác thực thực nguồn gốc dữ liệu và tính toàn vẹn của dữ liệu cho toàn bộ thông điệp. Đặc biệt, chúng không hỗ trợ bất kỳ sự thay đổi nào của một thông điệp mà không làm mất hiệu lực của chứng thực kĩ thuật số. Ngược lại, lược đồ chứng thực có thể được biên tập lại cho phép chứng thực thông điệp bằng cách cho phép biên tập lại (xóa hoặc xóa vĩnh viễn) sau các phần nhất định của thông điệp đã được chứng thực (được gọi là các trường), đồng thời bảo vệ chống lại bất kỳ sửa đổi nào khác. Thao tác lại này có thể được thực hiện bởi bất kỳ thực thể nào chỉ biết thông điệp chứng thực và khóa được biên tập lại của bên chứng thực, nhưng không phải khóa chứng thực bí mật.

5.2 Các bên và quá trình

Các bên tham gia vào một lược đồ chứng thực có thể được biên tập lại là:

- a) Một bên chứng thực;
- b) Một bên biên tập lại;
- c) Một bên xác minh.

Một lược đồ chứng thực có thể được biên tập lại được xác định bởi đặc điểm kỹ thuật của các quá trình sau:

- a) Một quá trình sinh khóa;
- b) Một quá trình chứng thực có thể được biên tập lại;
- c) Một quá trình biên tập lại;
- d) Một quá trình xác minh.

CHÚ THÍCH: Cơ chế được các bên liên quan sử dụng để đồng ý về một lược đồ chứng thực có thể được biên tập lại cụ thể nằm ngoài phạm vi của tiêu chuẩn này.

5.3 Mô hình chung

Các bên sau thực hiện các quy trình liên quan đến lược đồ chứng thực có thể được biên tập lại.

- a) Bên chứng thực phải:
 - 1) Lấy khóa chứng thực ak , các tham số miền Z và những thay đổi có thể chấp nhận được adm ;
 - 2) Sử dụng khóa chứng thực bí mật ak , các tham số miền Z và những thay đổi có thể chấp nhận được adm để chứng thực thông điệp m ;
 - 3) Chứng thực có thể được biên tập lại att có thể chứa một số thông tin về những thay đổi có thể chấp nhận được adm .

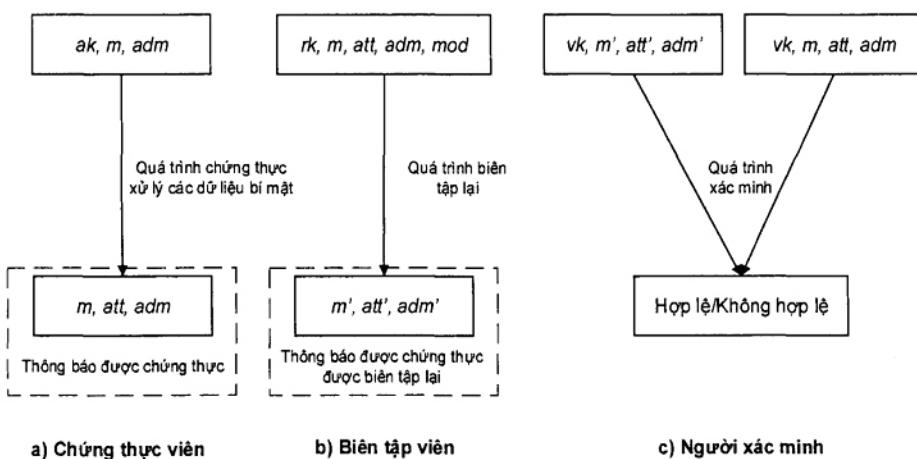
b) Bên biên tập lại phải:

- 1) Thu được khóa sau khi được biên tập lại rk của bên chứng thực, các tham số miền Z, thông điệp m (khả năng đã được biên tập lại), chứng thực có thể được biên tập lại att (khả năng đã được biên tập lại), những thay đổi có thể chấp nhận được adm và Hướng dẫn sửa đổi mod ;
- 2) Nếu không được cung cấp làm đầu vào, hãy sử dụng khóa được biên tập lại rk , các tham số miền Z, thông điệp m (khả năng đã được biên tập lại) và chứng thực có thể được biên tập lại (khả năng đã được biên tập lại) để tạo lại những thay đổi có thể chấp nhận adm (khả năng đã được biên tập lại);
- 3) Sử dụng hướng dẫn sửa đổi mod để biên tập thông điệp m , và điều chỉnh (nếu cần thiết) những thay đổi được chấp nhận adm ;
- 4) Sử dụng khóa được biên tập lại rk của bên chứng thực, các tham số miền Z, và Hướng dẫn sửa đổi để biên tập lại chứng thực có thể được biên tập lại att ;
- 5) Thông điệp đã biên tập lại m' thu được, những thay đổi chấp nhận được đã được biên tập lại adm' và chứng thực đã được biên tập lại att' .

c) Bên xác minh phải:

- 1) Thu được khóa xác minh vk của bên chứng thực, tham số miền Z, thông điệp m (khả năng đã được biên tập lại), chứng thực có thể được biên tập lại (khả năng đã được biên tập lại) và những thay đổi có thể chấp nhận được adm (khả năng đã được biên tập lại);
- 2) Nếu không được cung cấp đầu vào, hãy sử dụng khóa xác minh vk , thông số miền Z, thông điệp m (khả năng biên tập lại) và chứng thực có thể được biên tập lại (khả năng đã được biên tập lại) để tạo lại những thay đổi có thể chấp nhận adm (khả năng đã được biên tập lại);
- 3) Sử dụng khóa xác minh vk , các tham số miền Z, thông điệp m (khả năng đã được biên tập lại) và các thay đổi có thể chấp nhận được adm (khả năng đã được biên tập lại) để xác minh chứng thực có thể được biên tập lại att (khả năng đã được biên tập lại);
- 4) Thu được kết quả hợp lệ hoặc không hợp lệ.

Hình 1 cung cấp một cái nhìn tổng quan về các quá trình được thực hiện bởi các bên trong một lược đồ chứng thực có thể được biên tập lại. Ngắn gọn hơn, Hình 1 không hiển thị các tham số miền Z. Đầu vào cho quá trình biên tập lại cũng như quá trình xác minh có thể là thông điệp ban đầu (thông điệp gốc) (tức là thông điệp đã được chứng thực) hoặc thông điệp đã được biên tập lại (tức là đầu ra của quá trình biên tập lại trước đó).



Hình 1 - Tổng quan về các quá trình trong lược đồ chứng thực có thể được biên tập lại

5.4 Đặc điểm kỹ thuật của các quá trình

5.4.1 Quá trình sinh khóa

Quá trình sinh khóa của cơ chế chứng thực có thể được biên tập lại bao gồm hai quy trình sau:

- a) Tạo ra các tham số miền Z;
- b) Tạo khóa chứng thực ak , khóa được biên tập lại rk và khóa xác minh vk .

Thủ tục đầu tiên được thực hiện một lần khi miền được thiết lập. Các tham số miền kết quả là cần thiết trong các quá trình và chức năng tiếp theo. Thủ tục thứ hai được thực hiện cho mỗi chứng thực trong miền.

CHÚ THÍCH 1: Có thể yêu cầu xác thực các tham số miền và khóa. Tuy nhiên, làm thế nào điều này đạt được nằm ngoài phạm vi của tiêu chuẩn này.

CHÚ THÍCH 2: Phân phối khóa nằm ngoài phạm vi của tiêu chuẩn này.

5.4.2 Quá trình hưng thực có thể được biên tập lại

Trong quá trình chứng thực có thể được biên tập lại, bên chứng thực tính toán chứng thực có thể được biên tập lại cho một thông điệp nhất định và xác định rõ về các thay đổi có thể chấp nhận được dựa trên sự phân tích nhất định của thông điệp. Chứng thực có thể được biên tập lại (bao gồm thông tin cần thiết để xác minh và biên tập lại) được thêm vào thông điệp để tạo thành thông điệp đã được chứng thực.

Cụ thể, các mục dữ liệu sau là bắt buộc đối với quá trình chứng thực có thể được biên tập lại:

- Các tham số miền Z;
- Khóa chứng thực ak ;
- Thông điệp m ;
- Những thay đổi có thể chấp nhận được adm .

Quá trình tạo chứng thực có thể được biên tập lại liên kết thông điệp m với những thay đổi có thể chấp nhận được adm và với khóa xác minh vk tương ứng với khóa chứng thực ak .

5.4.3 Quá trình biên tập lại

Trong quá trình biên tập lại, bên biên tập lại tạo thủ tục chứng thực đã được biên tập lại của một thông điệp đã được chứng thực hoặc đã được biên tập lại theo Hướng dẫn sửa đổi nhất định. Đầu vào cho quá trình biên tập lại có thể là một thông điệp đã được chứng thực hoặc một thông điệp đã được biên tập lại. Đầu ra của quá trình biên tập lại là một thông điệp đã được biên tập lại và chứng thực đã được biên tập lại tương ứng bao gồm thông tin về những thay đổi chấp nhận được đã được biên tập lại. Điều này có nghĩa là một thông điệp đã được chứng thực đã được biên tập lại có thể có nhiều lần biên tập lại.

CHÚ THÍCH 1: Có hay không (các) ứng dụng trước đó của một quá trình biên tập lại có thể được phát hiện bởi bên xác minh hoặc bên biên tập lại sau đó phụ thuộc vào các thuộc tính an toàn của chương trình (xem 6.2.1).

Các mục dữ liệu sau đây là bắt buộc cho quá trình biên tập lại:

- Các tham số miền Z;
- Khóa được biên tập lại rk ;
- Thông điệp gốc hoặc thông điệp được biên tập lại m ;
- Chứng thực có thể được biên tập lại hoặc đã được biên tập lại;
- Những thay đổi có thể chấp nhận được ban đầu hoặc được biên tập lại;

- Hướng dẫn sửa đổi mod phù hợp với những thay đổi có thể chấp nhận được *adm*.

Nếu những thay đổi có thể chấp nhận được *adm* không được cung cấp trực tiếp dưới dạng đầu vào, thì trước tiên quá trình biên tập lại sẽ tạo lại chúng bằng cách sử dụng khóa được biên tập lại *rk*, các tham số miền *Z*, thông điệp *m* và chứng thực có thể được biên tập lại *att*.

Thủ tục của quá trình một tạo đầu ra chứng thực đã được biên tập lại tương ứng với thông điệp đã được biên tập lại *m'* thu được bằng cách áp dụng Hướng dẫn sửa đổi mod cho thông điệp đầu vào *m*. Nếu chứng thực đầu vào là hợp lệ trong khoảng trên *m* dưới *vk* và Hướng dẫn sửa đổi được áp dụng nằm trong giới hạn của những thay đổi có thể chấp nhận được của bên chứng thực ủy quyền *adm*, thì kết quả suy luận được (*m'*, *att*) sẽ tạo ra kết quả rõ ràng khi đầu vào cho quá trình cùng với khóa xác minh *vk* tương ứng với khóa chứng thực *ak* của bên chứng thực. Ngoài ra, thủ tục của quá trình tạo ra *adm'* như một phiên bản có khả năng được sửa đổi của *adm*.

Quá trình này không yêu cầu quyền truy cập vào khóa chứng thực *ak* hoặc khóa xác minh *vk* để hoạt động chính xác. Truy cập vào khóa được biên tập lại *rk* không mang lại thông tin về khóa chứng thực *ak* của bên chứng thực cũng như khóa xác minh *vk*.

CHÚ THÍCH 2: Để cho phép quá trình biên tập lại là một hoạt động công khai, khóa được biên tập lại *rk* của bên chứng thực có thể được công khai, ví dụ: bằng cách phân phối nó cùng với thông điệp đã được chứng thực. Điều này không ảnh hưởng đến tính an toàn của khóa chứng thực của bên chứng thực *ak* cũng như của khóa xác minh *vk*. Do đó, các lược đồ bảo mật với *rk* công khai hoặc rõ ràng vẫn đạt được chứng thực số của thông điệp được chứng thực.

5.4.4 Quá trình xác minh

Các mục dữ liệu sau là bắt buộc cho quá trình xác minh:

- Các tham số miền *Z*;
- Khóa xác minh *vk*;
- Thông điệp đã được biên tập lại hoặc thông điệp gốc *m*;
- Chứng thực có thể được biên tập lại hoặc đã được biên tập lại *att*;
- Những thay đổi chấp nhận được đã được biên tập lại hoặc những thay đổi ban đầu được chấp nhận *adm*.

Nếu những thay đổi có thể chấp nhận được *adm* không được cung cấp trực tiếp dưới dạng đầu vào, thì quá trình xác minh trước tiên sẽ cấu trúc lại chúng bằng cách sử dụng khóa xác minh *vk*, các tham số miền *Z*, thông điệp *m* và chứng thực có thể được biên tập lại (khả năng được biên tập lại).

Kết quả đầu ra của quá trình cho biết liệu chứng thực *att* có phải là chứng thực hợp lệ trên thông điệp *m* đối với các tham số miền *Z* đã cho, khóa xác minh *vk* và những thay đổi có thể chấp nhận được hay không. Nếu các đầu vào cho quá trình xác minh được tính toán phù hợp với các quá trình quy định trong mục 5.3, a) b) và có khả năng là c), thì đầu ra của quá trình xác minh phải cho biết là hợp lệ với xác suất áp đảo.

CHÚ THÍCH: Mặc dù, đối với hầu hết các chương trình, đầu ra của quá trình xác minh trên các đầu vào như được định nghĩa ở trên cho thấy hợp lệ với xác suất 1, một số chương trình không đạt được đặc tính mạnh này mà chỉ đạt được xác suất rất gần với 1 (ví dụ: xác suất 1 - 1/2³⁰). Mặc dù tác động thực tế của sự lỗi này là không đáng kể, xác suất 1 là không bắt buộc để không loại trừ các lược đồ này.

Để xác minh thành công, điều cần thiết là, trước quá trình xác minh, bên xác minh có thể liên kết khóa xác minh chính xác với chứng thực.

6 Thuộc tính mật mã của các lược đồ chứng thực có thể được biên tập lại

6.1 Các thuộc tính mật mã bắt buộc

6.1.1 Tính chính xác

Việc xác minh các thông điệp được chứng thực được tạo một cách đúng đắn bởi quá trình chứng thực có thể được biên tập lại phải thành công, tức là đưa ra đầu ra "hợp lệ" với xác suất áp đảo, giả sử khóa xác minh được sử dụng tương ứng với khóa chứng thực được sử dụng cho chứng thực.

Tương tự như vậy, việc xác minh các thông điệp đã xác thực đã được xử lý lại được tạo chính xác bởi quá trình xử lý lại phải thành công, tức là đưa ra đầu ra "hợp lệ" với xác suất áp đảo, giả sử các khóa xác thực được sử dụng tương ứng với khóa chứng thực cho mục đích chứng thực.

6.1.2 Tính chống thoái thác

Một thực thể không có quyền truy cập vào khóa chứng thực bí mật ak tương ứng với khóa xác minh vk , nhưng có quyền truy cập khóa được biên tập lại rk , có thể tạo ra một tập hợp phải là hợp lệ duy nhất (m^* , att^* , adm^*) của thông điệp, chứng thực và những thay đổi có thể chấp nhận được đối với vk này, nếu (m^* , att^* , adm^*) có thể được lấy từ đầu ra (m , att , adm) của quá trình chứng thực có thể được biên tập lại trên đầu vào ak , theo sau là không có hoặc nhiều ứng dụng tiếp theo của quá trình xử lý các dữ liệu bí mật bằng cách sử dụng Hướng dẫn sửa đổi phù hợp với những thay đổi có thể chấp nhận được adm .

CHÚ THÍCH: Đặc biệt, nếu khóa xác minh được công khai trong khi khóa chứng thực được giữ bí mật, thì tính không khả thi cho phép các lược đồ chứng thực có thể được biên tập lại như vậy được sử dụng để hỗ trợ các dịch vụ chống chối bỏ như được định nghĩa trong TCVN 11393-1.

6.1.3 Quyền riêng tư

Với chứng thực đã được biên tập lại att' , thông điệp đã được biên tập lại m' , khóa được biên tập lại rk và những thay đổi có thể chấp nhận được đã được biên tập lại adm' , là đầu ra của quá trình biên tập lại, cũng như khóa xác minh vk và các tham số miền Z, nó phải là không thể khôi phục về mặt tính toán bất kỳ thông tin nào về thông điệp m^* được sử dụng làm đầu vào trong quá trình xử lý lại vượt ra ngoài những gì được tiết lộ bởi m' .

CHÚ THÍCH: Rò rỉ thông tin qua nội dung ngữ nghĩa của thông điệp được biên tập lại nằm ngoài phạm vi của định nghĩa này.

6.2 Thuộc tính mật mã tùy chọn

6.2.1 Không thể phát hiện việc biên tập lại

Các kết quả đầu ra của quá trình chứng thực có thể được biên tập lại và của các quá trình biên tập lại phải không thể phân biệt được về mặt tính toán.

CHÚ THÍCH 1: Trong tài liệu học thuật, đặc tính này thường được gọi là tính minh bạch. Tuy nhiên, thuật ngữ này bị tránh trong tiêu chuẩn này vì có thể có sự không rõ ràng.

CHÚ THÍCH 2: Mọi lược đồ đáp ứng thuộc tính này cũng đạt được sự riêng tư như được định nghĩa trong 6.1.3.

6.2.2 Có thể phát hiện việc biên tập lại

Bất kỳ thực thể nào không yêu cầu quyền truy cập vào bất kỳ khóa bí mật nào đều có thể nhận biết có các trường hoặc không có các trường nào của thông điệp đã được biên tập lại hay và xác định các vị trí trong tài liệu mà việc biên tập lại đã được thực hiện. Khả năng phát hiện việc biên tập lại là thuộc tính đối lập với khả năng không thể phát hiện việc biên tập lại.

CHÚ THÍCH: Đây là rõ một khái niệm rõ ràng hơn trường hợp không thể có khả năng phát hiện việc biên tập lại, trong trường hợp đó việc biên tập lại một phần nào đó có thể được phát hiện trong khi việc biên tập lại khác thì không.

6.2.3 Tính không liên kết của việc biên tập lại

Không thực thể nào có thể quyết định xem hai đầu ra (m^*, att^*, adm^*) và $(m^{**}, att^{**}, adm^{**})$ với $m^* = m^{**}$ và $adm^* = adm^{**}$ nhưng $att^* \neq att^{**}$ của quá trình chứng thực có thể được biên tập lại hoặc được biên tập lại cho cùng một khóa xác minh vk được bắt nguồn từ các đầu vào giống nhau hoặc khác nhau.

6.2.4 Kiểm soát công khai

Bên chứng thực được phép xác định những thay đổi adm có thể chấp nhận được theo cách mà một hoặc nhiều trường m , không thể biên tập lại trong quá trình biên tập lại.

CHÚ THÍCH: Đối với các chương trình không hỗ trợ kiểm soát công khai, những thay đổi có thể chấp nhận được luôn cho phép biên tập lại bất kỳ trường nào trong thông điệp.

6.2.5 Kiểm soát biên tập lại liên tục

Bên chứng thực cho phép bên biên tập lại thực hiện loại bỏ các trường khỏi những thay đổi có thể chấp nhận và được xác định bởi bên chứng thực adm . Nếu thuộc tính được đưa ra, bên biên tập lại có thể chọn thuộc tính đó trong quá trình biên tập lại để lại trường m ; có khả năng được biên tập lại trong thông điệp m và chỉ loại bỏ khả năng việc trường m ; đó về sau có thể được biên tập lại một lần nữa, tức là loại bỏ trường m ; khỏi những thay đổi có thể chấp nhận được một lần nữa. Sau lần xử lý này, bên biên tập lại không thể biên tập lại trường m ; một cách liên tục được nữa.

6.2.6 Khả năng kết hợp

Để (m^*, att^*, adm^*) và $(m^{**}, att^{**}, adm^{**})$ là các thông điệp đã được biên tập lại, chứng thực đã được biên tập lại và những thay đổi chấp nhận được đã được biên tập lại:

- Mà quá trình xác minh với cùng một khóa xác minh vk cho kết quả hợp lệ;
- Cả hai đều được tạo từ cùng một đầu vào (m, att, adm) bằng cách áp dụng (có thể nhiều hơn một) quá trình biên tập lại với Hướng dẫn sửa đổi có thể khác nhau.

Sau đó, bất kỳ thực thể nào biết (m^*, att^*, adm^*) và $(m^{**}, att^{**}, adm^{**})$ đều có thể nhận được bộ ba $(m^{***}, att^{***}, adm^{***})$, trong đó m^{***} chứa tất cả các trường có trong m^* và m^{**} , mà quá trình xác minh với khóa xác minh vk cho kết quả hợp lệ.

Thư mục tài liệu tham khảo

- [1] Tiêu chuẩn quốc gia TCVN 9696-2:2013 (ISO/IEC 7498-2:1989) về Công nghệ thông tin – Liên kết hệ thống mở - Mô hình tham chiếu cơ sở - Phần 2: Kiến trúc an ninh.
 - [2] Tiêu chuẩn quốc gia TCVN 11393-1:2016 (ISO/IEC 13888-1:2009) về Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 1: Tổng quan.
 - [3] Tiêu chuẩn quốc gia TCVN 12214-1:2018 (ISO/IEC 14888-1:2008) về Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số kèm phụ lục – Phần 1: Tổng quan.
 - [4] ISO/IEC 27038:2014, Information technology — Security techniques — Specification for digital redaction.
-