TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 11393-3:2016
ISO/IEC 13888-3:2009

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - CHỐNG CHỐI BỎ - PHẦN 3: CÁC CƠ CHẾ SỬ DỤNG KỸ THUẬT PHI ĐỐI XỨNG

Information technology - Security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques

HÀ NỘI - 2016

Mục lục

Lời giới thiệu

Mục đích của một dịch vụ chống chối bỏ là tạo ra, thu thập, duy trì, sẵn sàng cung cấp và xác minh bằng chứng liên quan đến một sự kiện hay hành động đã yêu cầu nhằm giải quyết tranh chấp về sự xuất hiện hay không xuất hiện của sự kiện hay hành động.

Phần này của bộ tiêu chuẩn TCVN 11393 (ISO/IEC 13888) chỉ đề cập đến các dịch vụ chống chối bỏ sau đây:

- **Chống chối bỏ nguồn gốc;**
- **Chống chối bỏ việc chuyển phát;**
- **Chống chối bỏ việc đệ trình;**
- **Chống chối bỏ việc vận chuyển.**

Các cơ chế chống chối bỏ liên quan đến việc trao đổi các thẻ chống chối bỏ đặc trưng cho từng dịch vụ chống chối bỏ. Các cơ chế chống chối bỏ được định nghĩa trong tiêu chuẩn này bao gồm các chữ ký số và dữ liệu bổ sung. Các thẻ chống chối bỏ được lưu giữ như thông tin chống chối bỏ và được sử dụng tiếp đó trong sự kiện có tranh chấp.

Thông tin bổ sung được yêu cầu để hoàn thành thẻ chống chối bỏ. Tùy thuộc vào chính sách chống chối bỏ hiện hành cho một ứng dụng cụ thể và môi trường pháp lý, trong đó ứng dụng hoạt động, thông tin bổ sung cần có một trong hai dạng sau:

- **Thông tin được cung cấp bởi một tổ chức cấp tem thời gian, tổ chức này cung cấp sự bảo đảm rằng chữ ký của thẻ chống chối bỏ đã được tạo ra trước một thời điểm đã cho.**
- **Thông tin được cung cấp bởi một dịch vụ đánh dấu thời gian, dịch vụ đó cung cấp sự bảo đảm rằng chữ ký của thẻ chống chối bỏ đã được ghi lại trước một thời điểm đã cho.**

Chống chối bỏ chỉ có thể được cung cấp trong ngữ cảnh của một chính sách an toàn đã được định nghĩa rõ đối với một ứng dụng cụ thể và môi trường pháp lý của nó. Các chính sách chống chối bỏ được mô tả trong ISO/IEC 10181-4.

Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 3: Các cơ chế sử dụng kỹ thuật phi đối xứng

Information technology - Security techniques - Non-repudation - Part 3: Mechanisms using symmetric techniques

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các cơ chế cho việc cung cấp các dịch vụ chống chối bỏ cụ thể liên quan đến việc truyền thông, sử dụng các kỹ thuật mật mã phi đối xứng.

2 Tài liệu viện dẫn

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

TCVN 13888-1:2016 (ISO/IEC 13888-1:2010), Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 1: Tổng quan (*Information technology - Security techniques - Non-repudiation - Part 1: General).*

TCVN 7818-1 (ISO/IEC 18014-1), Công nghệ thông tin - Kỹ thuật mật mã - Dịch vụ tem thời gian - Phần 1: Khung tổng quát.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ, định nghĩa trong TCVN 11393-1:2016.

4 Ký hiệu và chữ viết tắt

A	Bên phát thông điệp được yêu cầu
B	Bên nhận thông điệp hoặc bên nhận thông điệp dự kiến
C	Định danh phân biệt của bên thứ ba tin cậy
CA	Tổ chức chứng thực (Certification Authority)
D_i	Định danh phân biệt của tổ chức chuyển phát thứ i, một bên thứ ba tin cậy ($i \in \{1, 2, ..., n\}$), trong đó *n* là số lượng tổ chức chuyển phát trong hệ thống)
f_i	Phần dữ liệu (cờ) biểu thị kiểu dịch vụ chống chối bỏ

	(i ∈ {nguồn gốc, chuyển phát, đệ trình, vận chuyển})
Imp(y)	Dấu vết của dữ liệu *y*, bao gồm hoặc *y* hoặc mã băm của *y* cùng với một định danh của hàm băm đang được sử dụng
M	Thông điệp được gửi từ thực thể A tới thực thể B tương ứng với dịch vụ chống chối bỏ được cung cấp
NR	Chống chối bỏ (non-repudiation)
NRD	Chống chối bỏ chuyển phát (non-repudiation of delivery)
NRDT	Thẻ chống chối bỏ chuyển phát (non-repudiation of delivery token)
NRO	Chống chối bỏ nguồn gốc (non-repudiation of origin)
NROT	Thẻ chống chối bỏ nguồn gốc (non-repudiation of origin token)
NRS	Chống chối bỏ việc đệ trình (non-repudiation of submission)
NRST	Thẻ chống chối bỏ việc đệ trình (non-repudiation of submission token)
NRT	Chống chối bỏ vận chuyển (non-repudiation of transport)
NRTT	Thẻ chống chối bỏ vận chuyển (non-repudiation of transport token)
Pol	Định danh phân biệt của chính sách chống chối bỏ (hoặc các chính sách) áp dụng cho bằng chứng.
Q	Dữ liệu tùy chọn có thể chứa thông tin bổ sung, ví dụ các định danh phân biệt của thông điệp *m*, cơ chế chữ ký, hoặc hàm băm
S	Phép toán ký được thực hiện với thuật toán chữ ký. Chữ ký của thông điệp m được tính bằng khóa bí mật của thực thể *X* ký hiệu là *S(X, m)*
T_i	Ngày giờ xảy ra kiểu thứ *i* của sự kiện hoặc hành động (i là chỉ số của sự kiện hoặc hành động), i ∈ {1, 2, 3, 4})
T_g	Ngày giờ bằng chứng được tạo ra.
$text_i$	Phần dữ liệu tùy chọn, có thể chứa thông tin bổ sung, ví dụ một định danh khóa và / hoặc định danh thông điệp (i ∈ {1, 2, 3, 4, 5, 6})
TSA	Tổ chức cấp tem thời gian (Time-Stamping Authority)
TST	Thẻ tem thời gian (Time-Stamp Token)
TTP	Bên thứ ba tin cậy (Trusted Third Party)
X,Y	Các biến sử dụng để biểu thị tên thực thể

$y \| z$ Kết quả của việc ghép nối y và z theo thứ tự đã cho. Khi ghép nối các phần dữ liệu, cần phải mã hóa phù hợp để các phần dữ liệu đơn lẻ có thể được khôi phục từ chuỗi ghép nối.

5 Các yêu cầu

Tùy thuộc vào cơ chế cơ bản dùng để tạo ra các thẻ chống chối bỏ và độc lập với dịch vụ chống chối bỏ được hỗ trợ bởi các cơ chế chống chối bỏ, các yêu cầu sau đây đặt ra cho các thực thể tham gia vào một trao đổi chống chối bỏ trong tiêu chuẩn này:

- Các thực thể thực hiện một trao đổi chống chối bỏ phải tin cậy cùng các bên thứ ba tin cậy (TTP).
- Khóa chữ ký thuộc về một thực thể phải được giữ bí mật bởi thực thể đó.
- Một hàm *Imp* chung phải được hỗ trợ bởi tất cả thực thể trong dịch vụ chống chối bỏ. Hàm *Imp* cần là hàm định danh hoặc một hàm băm chống xung đột như đã định nghĩa trong ISO/IEC 10118.
- Cơ chế chữ ký số sử dụng cần thỏa mãn các yêu cầu an toàn đã quy định bởi chính sách chống chối bỏ.
- Trước khi tạo bằng chứng, bên tạo bằng chứng phải biết bằng chứng cần được tạo ra tương ứng với các chính sách chống chối bỏ nào, kiểu bằng chứng cần được tạo ra và cơ chế cần sử dụng để xác minh bằng chứng.
- Các cơ chế để tạo ra và xác minh bằng chứng phải sẵn sàng cho các thực thể thực hiện trao đổi chống chối bỏ cụ thể hoặc một tổ chức tin cậy phải sẵn sàng để cung cấp các cơ chế.
- Bên tạo bằng chứng hoặc bên xác minh bằng chứng cần sử dụng dịch vụ cấp tem thời gian hoặc dịch vụ đánh dấu thời gian.

6 Sự tham gia của bên thứ ba tin cậy

Các bên thứ ba tin cậy được tham gia vào việc cung cấp các dịch vụ chống chối bỏ, vai trò chính xác của họ phụ thuộc vào các cơ chế được sử dụng và chính sách chống chối bỏ hiện hành. Một bên thứ ba tin cậy có thể hoạt động với một hoặc nhiều vai trò sau:

- Một tổ chức chuyển phát (DA) được tin cậy để chuyển phát thông điệp tới bên nhận dự kiến và để cung cấp thẻ chống chối bỏ việc đệ trình hoặc chống chối bỏ chuyển phát.
- Việc sử dụng các kỹ thuật mật mã phi đối xứng có thể yêu cầu sự tham gia của một bên thứ ba tin cậy để đảm bảo tính xác thực của các khóa xác minh công khai, như đã mô tả ví dụ trong ISO/IEC 9594-8.

- Chính sách chống chối bỏ hiện hành có thể yêu cầu bằng chứng được tạo ra từng phần hoặc toàn bộ bởi một bên thứ ba tin cậy.
- Một thẻ tem thời gian được phát hành bởi một tổ chức cấp tem thời gian (TSA) cũng có thể được sử dụng để đảm bảo rằng một thẻ chống chối bỏ vẫn còn hợp lệ.
- Một tổ chức cấp tem thời gian có thể được tham gia để cung cấp sự bảo đảm về việc chữ ký của thẻ chống chối bỏ đã cho đã được ghi lại trước thời điểm đã cho.
- Một tổ chức ghi bằng chứng có thể được tham gia để ghi bằng chứng để có thể được lấy ra sau này nếu có tranh chấp.

Bên thứ ba tin cậy có thể liên quan ở các mức độ khác nhau trong các giai đoạn khác nhau của việc cung cấp dịch vụ chống chối bỏ. Khi trao đổi bằng chứng, các bên phải biết hoặc đồng ý về chính sách chống chối bỏ nào được áp dụng đối với bằng chứng.

7 Chữ ký số

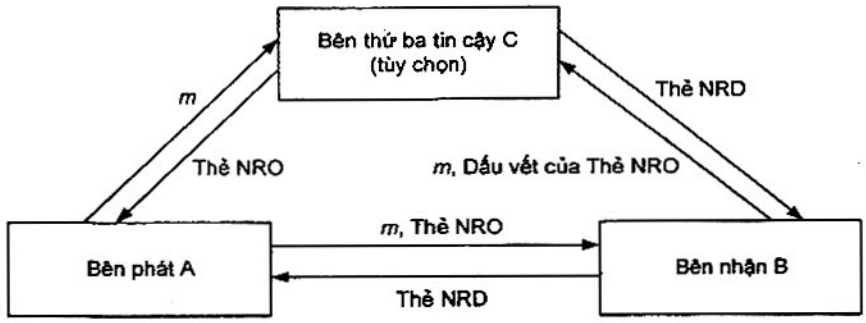
Đối với các cơ chế được quy định trong tiêu chuẩn này, các thẻ chống chối bỏ được tạo lập bằng việc sử dụng chữ ký số. Kỹ thuật chữ ký số được dùng để tạo ra các chữ ký số này phải phù hợp với ISO/IEC 9796 hoặc ISO/IEC 14888.

Khóa công khai cần sử dụng để xác minh chữ ký phải có trong chứng thư khóa công khai. Chứng thư này phải bao gồm khoảng thời gian biểu thị thời khoảng trong đó CA xử lý trạng thái thu hồi chứng thư.

Chữ ký từ một thẻ NR cần phải có tính chất xác minh được ít nhất trong thời gian hiệu lực của các chứng thư, được dùng để xác nhận khóa kiểm tra công khai được sử dụng để xác minh chữ ký, cũng như khi thời gian hợp lệ của các chứng thư này đã hết hạn. Để đạt được mục đích này, việc sử dụng hoặc là một dịch vụ cấp tem thời gian hoặc một dịch vụ đánh dấu thời gian là điều cần thiết (xem Điều 11). Các cơ chế mô tả trong Điều 11 phải được sử dụng để bảo đảm rằng thẻ chống chối bỏ vẫn còn hiệu lực một khi chứng thư cần được sử dụng để xác minh chữ ký của thẻ NR đã hết hạn hoặc khi chúng thư bị thu thồi.

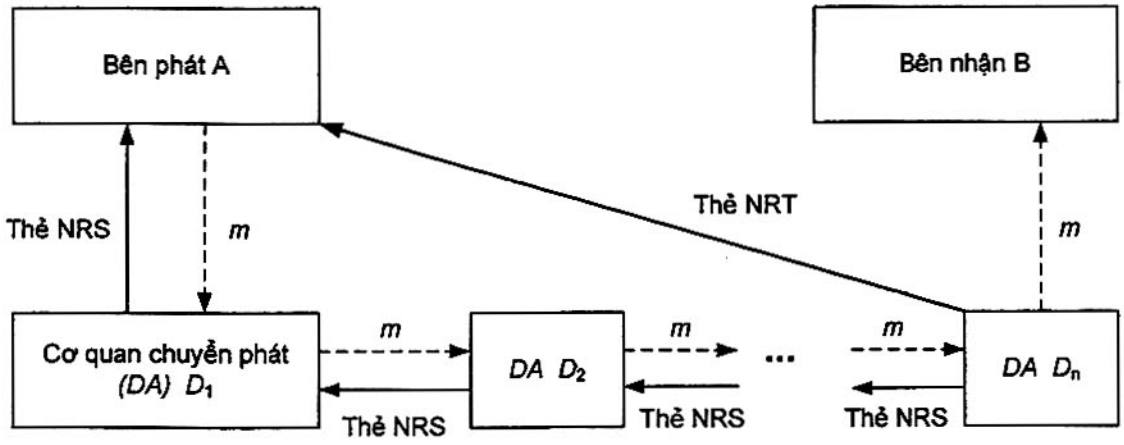
8 Sử dụng thẻ chống chối bỏ trong trường hợp có và không có tổ chức chuyển phát

Việc sử dụng các thẻ chống chối bỏ trong trường hợp các tổ chức chuyển phát (DA) không được sử dụng như thể hiện trong Hình 1. Các cơ chế tuân thủ mô hình này được quy định trong Điều 9. Bên thứ ba tin cậy *C* là bên tạo ra các thẻ NRO và NRD, là tùy chọn trong trường hợp cụ thể này của các dịch vụ chống chối bỏ.



Hình 1 - Sử dụng các thẻ chống chối bỏ không có tổ chức chuyển phát

Hình 2 minh họa việc sử dụng bốn kiểu thẻ chống chối bỏ trong trường hợp có bên thứ ba - Tổ chức chuyển phát (DA) được sử dụng. Các cơ chế trong mô hình này được quy định trong Điều 10.



Hình 2 - Sử dụng các thẻ chống chối bỏ với tổ chức chuyển phát

9 Bằng chứng tạo ra bởi các thực thể đầu cuối

9.1 Giới thiệu chung

Các cơ chế chống chối bỏ quy định trong Điều này cho phép việc tạo ra bằng chứng cho chống chối bỏ nguồn gốc (NRO) và chống chối bỏ chuyển phát (NRD) không có sự tham gia của bên thứ ba - Tổ chức chuyển phát (DA). Giả thiết rằng thực thể *A* muốn gửi thông điệp *m* tới thực thể *B*, và do đó là nguồn gốc của chống chối bỏ vận chuyển. Thực thể *B* là bên nhận.

Giả thiết rằng thực thể *A* biết chứng thư khóa công khai của nó và khóa riêng liên quan, thực thể *B* biết chứng thư khóa công khai của nó và một khóa riêng liên quan và các chứng thư khóa công khai có sẵn cho tất cả các thực thể có liên quan.

Nếu bên thứ ba tin cậy *C* được tham gia (tùy chọn), *C* phải giữ tất cả thẻ NRO đã được tạo ra và ghi lại việc mỗi thẻ NRO có được hay không được sử dụng để tạo ra thẻ NRD.

Hai cơ chế chống chối bỏ khác được mô tả trong phần dưới đây.

9.2 Chống chối bỏ nguồn gốc

9.2.1 Thẻ chống chối bỏ nguồn gốc (NRO)

Một thẻ NRO được sử dụng để cung cấp sự bảo vệ chống lại việc từ chối sai của bên phát đã phát đi thông điệp.

Thẻ NRO có đặc điểm:

- Được tạo ra bởi nguồn phát *A* của thông điệp *m* (hoặc bởi tổ chức *C*),
- Được gửi bởi *A* tới bên nhận *B*,
- Được lưu trữ bởi bên nhận *B* sau khi *B* đã xác minh thẻ NRO sử dụng chứng thư khóa công khai của *A*.

Cấu trúc của thẻ NRO như sau:

$$NROT = text_1 \,||\, z_1 \,||\, S(A, z_1),$$

trong đó:

$$z_1 = Pol \,||\, f_{origin} \,||\, A\,[||\, B]\,||\, C\,||\, T_g\,[||\, T_i]\,||\, Q\,||\, Imp(m).$$

Chuỗi dữ liệu z_1 trong thẻ NRO bao gồm các phần dữ liệu sau:

Pol Định danh phân biệt của chính sách (hoặc các chính sách) chống chối bỏ áp dụng cho bằng chứng,

f_{origin} Cờ biểu thị chống chối bỏ nguồn gốc,

A Định danh phân biệt của nguồn phát thông điệp *m*, ví dụ một địa chỉ email,

B (Các) định danh phân biệt của (các) bên nhận dự kiến của thông điệp *m* (tùy chọn), ví dụ một địa chỉ email,

C Định danh phân biệt của tổ chức tham gia (tùy chọn): Nếu như thẻ được tạo ra bởi tổ chức *C* thì phần dữ liệu này là bắt buộc và chữ ký $S(A, z_1)$ trong thẻ NRO, *NROT*, cần được thay thế bằng $S(C, z_1)$,

T_g Ngày giờ, tùy theo bên tạo thẻ, tại đó thẻ được tạo ra,

T_i Ngày giờ, tùy theo nguồn phát, tại đó thông điệp *m* được gửi đi (tùy chọn),

Q Một phần dữ liệu tùy chọn có thể chứa thông tin bổ sung, ví dụ các định danh phân biệt của thông điệp *m*, cơ chế chữ ký và / hoặc hàm băm và thông tin liên quan các chứng chỉ và hiệu lực của các khóa công khai,

Imp (m) Dấu vết của dữ liệu *m*, bao gồm hoặc *m* hoặc hàm băm của *m* cùng với định danh của hàm băm đang được sử dụng.

9.2.2 Cơ chế chống chối bỏ nguồn gốc

Thẻ chống chối bỏ nguồn gốc (NRO) được tạo ra bởi nguồn phát *A* của thông điệp và gửi tới bên nhận thông điệp *B*.

Giao dịch – từ thực thể *A* tới thực thể *B*

a) Nếu bên thứ ba tin cậy *C* được tham gia (tùy chọn),

1) *A* yêu cầu *C* tạo ra một thẻ NRO cho thông điệp *m*.

2) *C* nhận thông điệp *m* và kiểm tra tính hợp lệ của yêu cầu cho một thẻ NRO.

3) *C* tạo một thẻ NRO như quy định trong Điều 9.2.1.

4) *C* gửi thẻ NRO tới *A* và giữ nó.

5) *A* nhận thẻ NRO từ *C*.

Ngược lại, *A* sẽ hình thành một thẻ NRO như quy định trong Điều 9.2.1.

b) *A* gửi thẻ NRO (cùng với thông điệp *m*) tới *B*.

B kiểm tra tính hợp lệ của thẻ NRO và nội dung của nó bằng cách kiểm tra:

- kiểu và giá trị của các phần dữ liệu trong *NROT*, và
- Tính hợp lệ của chữ ký trong *NROT*.

Nếu chúng hợp lệ, thẻ *NRO* được lưu như bằng chứng cho chống chối bỏ nguồn gốc.

9.3 Chống chối bỏ chuyển phát

9.3.1 Thẻ chống chối bỏ chuyển phát (NRD)

Một thẻ NRD được sử dụng để cung cấp sự bảo vệ chống lại việc từ chối sai của bên nhận về việc đã nhận và chấp nhận nội dung của thông điệp *m*.

Thẻ NRD có đặc điểm:

- được tạo ra bởi bên nhận *B* (hoặc tổ chức *C*),
- được gửi bởi *B* tới một hoặc nhiều thực thể bao gồm nguồn phát thông điệp *A*, nếu biết trước,
- được lưu trữ bởi các thực thể sau khi *A* xác minh thẻ NRD bằng cách sử dụng chứng thư khóa công khai của *B* (hoặc thông qua tổ chức *C*).

Cấu trúc của thẻ NRD như sau:

$$NRDT = text_2 \,||\, z_2 \,||\, S(B, z_2),$$

trong đó:

$z_2 = Pol \| f_{delivery} [\| A] \| B [\| C] \| T_g [\| T_2] \| Q \| Imp(m)$.

chuỗi dữ liệu z_2 trong thẻ NRD bao gồm các phần dữ liệu sau:

Pol	Định danh phân biệt của chính sách (các chính sách) chống chối bỏ áp dụng cho bằng chứng,
$f_{delivery}$	Cờ biểu thị chống chối bỏ chuyển phát,
A	Định danh phân biệt của thực thể được tuyên bố bởi *B* là nguồn phát của thông điệp *m* (tùy chọn), ví dụ một địa chỉ email,
B	Định danh phân biệt của bên nhận thông điệp *m*, ví dụ một địa chỉ email,
C	Định danh phân biệt của tổ chức có liên quan (tùy chọn): Nếu thẻ được tạo ra bởi tổ chức *C* thì phần dữ liệu này là bắt buộc và chữ ký $S(B, z_2)$ trong thẻ NRO, NROT, cần được thay thế bằng $S(C, z_2)$,
T_g	Ngày giờ thẻ, tùy theo bên tạo thẻ, tại đó thẻ được tạo ra,
T_2	Ngày giờ, tùy theo bên nhận, tại đó thông điệp *m* đã được nhận (tùy chọn),
Q	Một phần dữ liệu tùy chọn có thể chứa thông tin bổ sung, ví dụ các định danh phân biệt của thông điệp *m*, cơ chế ký và / hoặc hàm băm, và thông tin liên quan đến các chứng thư tính hợp lệ của các khóa công khai,
Imp (m)	Dấu vết của dữ liệu *m*, bao gồm hoặc *m* hoặc hàm băm của *m* cùng với một định danh của hàm băm đang được sử dụng.

9.3.2 Cơ chế chống chối bỏ chuyển phát

Thẻ chống chối bỏ chuyển phát (NRDT) được tạo ra bởi bên nhận thông điệp *B* và được gửi tới nguồn phát thông điệp *A* sau khi B đã nhận thông điệp *m*.

Giao dịch 1 – Từ nguồn phát thông điệp *A* tới bên nhận thông điệp *B*

A gửi thông điệp *m* và một yêu cầu về một thẻ NRD tới *B*.

Giao dịch 2 – Từ thực thể B tới thực thể *A*

a) *B* nhận thông điệp *m* và kiểm tra tính hợp lệ của yêu cầu về thẻ NRD.

b) Nếu bên thứ ba tin cậy *C* được tham gia vào (tùy chọn), thì

1) *B* gửi hoặc *m* hoặc *m* || *Imp(NROT)* (nếu A gửi *NROT* với *m* và nếu *NROT* đã được tạo ra bởi *C*) tới *C* và yêu cầu *C* tạo ra một thẻ NRD cho thông điệp *m*.

2) *C* nhận *m* (và, tùy chọn, *Imp(NROT)*) và nếu có, nó sẽ kiểm tra xem thẻ NRO đã được tạo ra bởi *C* chưa và thẻ NRD tương ứng với dấu vết của thẻ NRO vẫn chưa được tạo ra. Nếu việc kiểm tra không đạt, *C* sẽ từ chối yêu cầu của thẻ NRD.

3) *C* hình thành một thẻ NRD như quy định trong Điều 9.3.1 và ghi lại việc thẻ *NROT* này đã được sử dụng để tạo thẻ NRD.

4) *C* gửi thẻ NRD tới *B*.

5) *B* nhận thẻ NRD từ *C*.

Ngược lại, *B* hình thành một thẻ NRD như quy định trong 9.3.1.

c) *B* gửi thẻ NRD tới *A*

A kiểm tra thẻ NRD và nội dung của nó bằng cách kiểm tra:

- kiểu và giá trị của các phần dữ liệu trong *NRDT*, và
- tính hợp lệ của chữ ký trong *NRDT*.

Nếu hợp lệ, thẻ NRD được lưu lại bởi *A* như bằng chứng thể hiện rằng *B* đã nhận được thông điệp *m*.

10 Bằng chứng tạo ra bởi một tổ chức chuyển phát

10.1 Tổng quan

Điều này quy định một số cơ chế bổ sung, trong đó bằng chứng được tạo ra bởi tổ chức chuyển phát tin cậy như một phần của quá trình chống chối bỏ. Cơ chế này có thể kết hợp chặt chẽ với các cơ chế cơ bản đã quy định trong Điều 9 để đáp ứng các yêu cầu đã định nghĩa bởi chính sách an toàn.

Các thuật ngữ việc đệ trình / vận chuyển được sử dụng tại nơi một tổ chức chuyển phát DA phát hành các thẻ chống chối bỏ (NRS/NRT) như sau:

- Một thẻ NRS cho phép nguồn phát hoặc tổ chức chuyển phát đứng trước đó nhận được bằng chứng về việc một thông điệp đã được đệ trình cho việc vận chuyển trong một hệ thống lưu trữ và chuyển tiếp.
- Một thẻ NRT cho phép nguồn phát lấy bằng chứng về việc một thông điệp đã được chuyển phát bởi tổ chức chuyển phát DA tới bên nhận dự kiến.

10.2 Chống chối bỏ việc đệ trình

10.2.1 Thẻ chống chối bỏ việc đệ trình (NRS)

Trong cơ chế này, một thẻ NRS được tạo lập bởi một tổ chức chuyển phát DA (Delivery Authority). Bên tạo bằng chứng trong trường hợp này là tổ chức chuyển phát DA. Khi nguồn phát hoặc một tổ chức chuyển phát đứng trước *X* (*A* hoặc D_i , i ∈ {1, 2, ..., *n* -1}) đã gửi đi thông điệp *m* tới tổ chức chuyển phát *Y* (D_1 hoặc D_{i+1} tương ứng) và sau khi tổ chức chuyển phát *Y* đã nhận được thông điệp *m*, *Y* sẽ

gửi thẻ NRS tới *X*. Điều này cung cấp bằng chứng về việc thông điệp đã được đệ trình cho chuyển phát tiếp.

Thẻ NRS có đặc điểm:

- được tạo ra bởi tổ chức chuyển phát *Y*,
- được gửi bởi *Y* tới *X* (nguồn phát thông điệp A hoặc một tổ chức chuyển phát định trước D_i) ,
- được lưu trữ bởi *X* sau khi *X* đã xác minh thẻ NRS sử dụng chứng thư khóa công khai của *Y*.

Cấu trúc của một thẻ NRS (NRST) được gửi từ D_{i+1} tới D_i là:

$$NRST = text_3 \,||\, z_3 \,||\, S\,(D_{i+1}, z_3),$$

trong đó:

$$z_3 = Pol \,||\, f_{submission} \,[||\, A] \,||\, B||\, D_1 \,||\, D_2 \,||\, \ldots \,||\, D_i \,||\, D_{i+1} \,||\, T_g \,||\, T_3 \,[||\, Q] \,||\, Imp(m).$$

Tiếp theo tên của bên nhận, các tên của các tổ chức chuyển phát liên quan được liệt kê theo thứ tự mà thông điệp *m* được chuyển phát. Chuỗi dữ liệu z_3 trong thẻ NRS bao gồm các phần dữ liệu sau:

Pol	Định danh phân biệt của chính sách (các chính sách) chống chối bỏ áp dụng cho bằng chứng,
$f_{submission}$	Cờ biểu thị chống chối bỏ việc đệ trình,
A	Định danh phân biệt của nguồn phát của thông điệp *m* (tùy chọn), trong đó tính hiệu lực của định danh A, ví dụ một địa chỉ email, có thể hoặc không được xác minh bởi C,
B	Định danh phân biệt của bên nhận dự kiến của thông điệp *m*, ví dụ một địa chỉ email,
D_i	Tổ chức chuyển phát, một bên thứ ba tin cậy ($i \in \{1, 2, \ldots, n\}$, với *n* là số lượng tổ chức chuyển phát trong hệ thống).
T_g	Ngày giờ, tùy theo bên tạo thẻ, tại đó thẻ được tạo ra,
T_3	Ngày giờ, tùy theo bên tạo thẻ, tại đó thông điệp *m* đã được đệ trình,
Q	Một phần dữ liệu tùy chọn có thể chứa thông tin bổ sung, ví dụ các định danh phân biệt của thông điệp *m*, cơ chế chữ ký và / hoặc hàm băm, và thông tin liên quan đến các chứng thư và tính hợp lệ của các khóa công khai,
Imp (m)	Dấu vết của dữ liệu *m*, bao gồm hoặc *m* hoặc hàm băm của *m* cùng với định danh của hàm băm đang được sử dụng.

10.2.2 Cơ chế chống chối bỏ việc đệ trình

Trong giao dịch đầu tiên của cơ chế này, thực thể bên gửi X (A hoặc D_i, i ∈ {1, 2, ... , n -1}) sẽ gửi một thông điệp tới một tổ chức chuyển phát Y (D_1 hoặc D_{i+1} tương ứng) để chuyển phát tiếp. Trong giao dịch thứ 2, thẻ NRD được gửi từ tổ chức chuyển phát Y tới thực thể X. Chống chối bỏ việc đệ trình được thiết lập trong giao dịch thứ 2.

Giao dịch 1 – Từ thực thể X tới tổ chức chuyển phát Y

X gửi thông điệp m và một yêu cầu thẻ NRS tới Y.

Giao dịch 2 – Từ tổ chức chuyển phát Y tới thực thể X

a) Y hình thành thẻ NRS như quy định trong Điều 10.2.1.

b) Y gửi thẻ NRS tới X.

Thực thể X kiểm tra thẻ NRS và nội dung của nó bằng cách kiểm tra:

- các kiểu và giá trị của các phần dữ liệu trong *NRST* và
- tính hợp lệ của chữ ký trong *NRST*.

Nếu hợp lệ, thẻ NRS được lưu lại bởi X như bằng chứng để chống chối bỏ việc đệ trình (nghĩa là thông điệp đã được đệ trình).

10.3 Chống chối bỏ vận chuyển

10.3.1 Thẻ chống chối bỏ vận chuyển (NRT)

Một thẻ *NRT* được sử dụng bởi nguồn phát thông điệp như bằng chứng về việc thông điệp m đã được gửi tới B bởi tổ chức chuyển phát cuối cùng trong chuỗi các tổ chức chuyển phát. Bên tạo bằng chứng trong trường hợp này là tổ chức chuyển phát (xem Hình 2). Khi nguồn phát hoặc một trong số các tổ chức chuyển phát định trước X (A hoặc D_i, i ∈ {1, 2, ..., n -1}) đã gửi đi một thông điệp m tới tổ chức chuyển phát Y (D_1 hoặc D_{i+1} tương ứng), và sau khi tổ chức chuyển phát cuối cùng D_n đã nhận được thông điệp m, D_n vận chuyển thông điệp m tới bên nhận B đồng thời cũng gửi thẻ NRT tới nguồn phát A của thông điệp m. Điều này cung cấp bằng chứng về việc thông điệp m đã được vận chuyển tới B.

Thẻ NRT có đặc điểm:

- được tạo bởi tổ chức chuyển phát D_n,
- được gửi bởi D_n tới nguồn phát thông điệp A,
- được lưu trữ bởi A sau khi A đã xác minh rằng thẻ NRT sử dụng chứng thư khóa công khai của D_n.

Cấu trúc của thẻ NRT (*NRTT*) được gửi từ D_n tới A là:

$$NRTT = text_4 \,||\, z_4 \,||\, S\,(D_n,\, z_4),$$

trong đó:

$z_4 = Pol \,||\, f_{transport}\, [\,||\, A] \,||\, B \,||\, D_1 \,||\, D_2 \,||\, \ldots \,||\, D_n \,||\, T_g \,||\, T_4\, [||\, Q] \,||\, Imp(m).$

Tiếp theo tên của bên nhận, các tên của các tổ chức chuyển phát liên quan được liệt kê theo thứ tự mà thông điệp *m* được chuyển phát. Chuỗi dữ liệu z_4 trong thẻ *NRT* bao gồm các phần dữ liệu sau:

Pol Định danh phân biệt của chính sách (các chính sách) chống chối bỏ áp dụng cho bằng chứng,

$f_{transport}$ Cờ biểu thị chống chối bỏ vận chuyển,

A Định danh phân biệt của nguồn phát của thông điệp *m* (tùy chọn), trong đó tính hiệu lực của định danh *A*, ví dụ một địa chỉ email, có thể không được xác minh bởi C,

B Định danh phân biệt của bên nhận dự kiến của thông điệp *m*, ví dụ một địa chỉ email,

D_i Tổ chức chuyển phát, một bên thứ ba tin cậy ($i \in \{1, 2, \ldots, n\}$, với *n* là số lượng tổ chức chuyển phát trong hệ thống).

T_g Ngày giờ, tùy theo bên tạo thẻ, tại đó thẻ được tạo ra,

T_4 Ngày giờ, tùy theo bên tạo thẻ, tại đó thông điệp *m* đã được chuyển phát,

Q Một phần dữ liệu tùy chọn có thể chứa thông tin bổ sung, ví dụ các định danh phân biệt của thông điệp *m*, cơ chế chữ ký và / hoặc hàm băm, và thông tin liên quan đến các chứng thư và tính hợp lệ của các khóa công khai,

Imp (m) Dấu vết của dữ liệu *m*, bao gồm hoặc *m* hoặc hàm băm của *m* cùng với định danh của hàm băm đang được sử dụng.

10.3.2 Cơ chế chống chối bỏ vận chuyển

Trong giao dịch đầu tiên của cơ chế này, thực thể bên gửi *X* (*A* hoặc D_i, $i \in \{1, 2, \ldots, n-1\}$) sẽ gửi một thông điệp *m* tới một tổ chức chuyển phát *Y* (D_1 hoặc D_{i+1} tương ứng) để chuyển phát tiếp. Trong giao dịch thứ 2, thông điệp *m* được gửi từ D_n tới bên nhận *B*. Trong giao dịch thứ ba, thẻ *NRT* được tạo bởi D_n và gửi tới thực thể *A*, nguồn của thông điệp *m*. Chống chối bỏ vận chuyển được thiết lập trong giao dịch thứ ba.

Giao dịch 1 – Từ thực thể *X* tới tổ chức chuyển phát *Y*

X gửi thông điệp *m* tới *Y*

Giao dịch 2 – Từ tổ chức chuyển phát D_n tới thực thể *B*

D_n gửi thông điệp m tới *B*.

Giao dịch 3 – Từ tổ chức chuyển phát D_n tới thực thể *A*

a) D_n hình thành thẻ NRT như quy định trong Điều 10.3.1.

b) D_n gửi thẻ NRT tới *A*.

A kiểm tra thẻ NRT và nội dung của nó bằng cách kiểm tra:

- các kiểu và giá trị của các phần dữ liệu trong *NRTT* và
- tính hợp lệ của chữ ký trong *NRTT*.

Nếu hợp lệ, thẻ NRT được lưu trữ bởi *A* như bằng chứng cho chống chối bỏ vận chuyển (nghĩa là thông điệp đã được chuyển phát tới bên nhận dự kiến *B*).

11 Các cơ chế đảm bảo thẻ NR được ký trước một thời điểm *t*

11.1 Giới thiệu chung

Mỗi thẻ NR đều được ký. Vì các tổ chức chứng thực không xử lý trạng thái thu hồi khi chứng thư hết hạn, nên cần thiết phải thể hiện rằng chữ ký của thẻ NR đã được thực hiện trong khoảng thời gian hiệu lực của chứng thư đã sử dụng để xác nhận chữ ký của thẻ NR.

Nếu chứng thư dùng để xác nhận chữ ký của thẻ NR bị thu hồi, thì cần thiết phải thể hiện rằng chữ ký đã được thực thi trước thời gian chứng thư bị thu hồi. Điều này có thể được thực hiện hoặc bằng cách hoặc áp dụng một thẻ tem thời gian trên chữ ký của thẻ NR hoặc sử dụng một dấu thời gian (Time-Mark), tức là một bản ghi trong một vết kiểm toán an toàn của chữ ký hoặc giá trị băm của nó cùng với định danh của thuật toán băm. Các cơ chế này cho phép một thực tế là chữ ký của thẻ chống chối bỏ đã được tạo ra trước một thời điểm đã cho cần phải được thiết lập.

Những cơ chế đó cho phép một thẻ NR được duy trì hiệu lực vô hạn:

a) Sau khi hết hạn chứng thư được sử dụng để xác minh chữ ký của thẻ NR hoặc

b) Nếu chứng thư bị thu hồi.

11.2 Cơ chế sử dụng dịch vụ cấp tem thời gian

Việc trao đổi giữa một thực thể (bên yêu cầu) và TSA khi yêu cầu một tem thời gian cần tuân theo các bước đã mô tả trong tiêu chuẩn TCVN 7818-1 (ISO/IEC 18014-1).

11.3 Cơ chế sử dụng dịch vụ đánh dấu thời gian

Thực thể *X* phải trao đổi với dịch vụ đánh dấu thời gian thông qua một kênh truyền thông an toàn cung cấp cả sự xác thực nguồn gốc dữ liệu và tính toàn vẹn.

Bên yêu cầu *X* tạo ra giá trị băm cho chữ ký của thẻ NR để được đánh dấu thời gian, và bổ sung thêm định danh của thuật toán băm; sự kết hợp này được xem như "dữ liệu y" trong phần sau đây.

Trong giao dịch đầu tiên của cơ chế này, thực thể yêu cầu *X* yêu cầu một dấu thời gian (Time-Mark) bằng cách gửi dữ liệu *y* mà nó muốn được đánh dấu thời gian.

Trong giao dịch thứ hai, dịch vụ đánh dấu thời gian đáp ứng bằng việc trả lại dữ liệu.

Giao dịch 1 – Từ thực thể *X* tới dịch vụ đánh dấu thời gian

a) Thực thể *X* hình thành yêu cầu *Req*:

$Req = text_5 \| y$.

$text_5$ có thể bao gồm:

- định danh phân biệt của tổ chức đánh dấu thời gian,
- chính sách được sử dụng để lấy dấu thời gian,
- tên của bên yêu cầu *X*.

b) Thực thể *X* gửi yêu cầu *Req* tới dịch vụ đánh dấu thời gian.

Giao dịch 2 – Từ dịch vụ đánh dấu thời gian tới thực thể *X*

a) Dịch vụ đánh dấu thời gian kiểm tra tính hợp lệ của yêu cầu và ghi lại *Req* cùng với ngày giờ từ một nguồn tin cậy.

b) Dịch vụ đánh dấu thời gian gửi dữ liệu *Resp* trở lại thực thể *X*:

$Resp = text_6 \| recording\ number$.

$text_6$ có thể bao gồm:

- dữ liệu *y*,
- ngày giờ của việc ghi hồ sơ,
- tất cả hoặc một phần của $text_5$,
- chính sách được sử dụng để cấp dấu thời gian.

Trong một trao đổi tiếp theo, thực thể *X* hoặc bất kỳ thực thể được phép nào có thể cung cấp số hiệu bản ghi và phải nhận lại:

- dữ liệu *y*,
- ngày giờ của việc ghi hồ sơ,
- tất cả hoặc một phần của $text_5$,
- chính sách được sử dụng để cấp dấu thời gian.

Thư mục tài liệu tham khảo

[1] TCVN 9696-2:2013 (*ISO 7498-2:1989)* Công nghệ thông tin - Liên kết hệ thống mở - Mô hình tham chiếu cơ sở - Phần 2: Kiến trúc an ninh.

[2] ISO/IEC 9594-8:2008, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks *(Công nghệ thông tin – Liên kết hệ thống mở – Danh bạ: các bộ khung cho khóa công khai và chứng chỉ thuộc tính).*

[3] ISO/IEC 9796 (all parts), Information technology – Security techniques – Digital signature scheme giving message recovery *(Công nghệ thông tin – Kỹ thuật an toàn – Lược đồ chữ ký số cho khôi phục thông điệp).*

[4] ISO/IEC 10118-2:2000/Cor.2: 2007, Information technology – Security techniques – Hashfunctions – Part 2: Hash-functions using an n-bit block cipher *(Công nghệ thông tin – Kỹ thuật an toàn – Các hàm băm – Phần 2: Các hàm băm sử dụng một khối mã n bit).*

[5] ISO/IEC 10118-3:2004/Amd.1:2006, Information technology – Security techniques – Hashfunctions – Part 3: Dedicated hash-functions *(Công nghệ thông tin – Kỹ thuật an toàn – Các hàm băm – Phần 3: Các hàm băm dùng riêng).*

[6] ISO/IEC 10118-4:1998, Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic *(Công nghệ thông tin – Kỹ thuật an toàn – Các hàm băm – Phần 4: Các hàm băm sử dụng tính toán số học theo khối).*

[7] ISO/IEC 10181-1:1996, Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview *(Công nghệ thông tin – Liên kết hệ thống mở – Bộ khung an toàn cho các hệ thống mở: Tổng quan).*

[8] ISO/IEC 10181-4:1997, Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 4: Non-repudiation framework *(Công nghệ thông tin – Liên kết hệ thống mở – Bộ khung an toàn cho các hệ thống mở – Phần 4: Bộ khung chống chối bỏ).*

[9] ISO/IEC TR 14516:2002, Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services *(Công nghệ thông tin – Các kỹ thuật an toàn – Hướng dẫn sử dụng và quản lý các dịch vụ bên thứ ba tin cậy).*

[10] ISO/IEC 14888 (all parts), Information technology – Security techniques – Digital signatures with appendix *(Công nghệ thông tin – Các kỹ thuật an toàn – Các chữ ký số với phụ lục).*

[11] ISO/IEC 15945:2002, Information technology – Security techniques – Specification of TTP services to support the application of digital signatures *(Công nghệ thông tin – Các kỹ thuật an toàn – Đặc tả của các dịch vụ TTP để hỗ trợ ứng dụng với chữ ký số).*

[12] ISO/IEC 15946-2:2002, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures *(Công nghệ thông tin – Các kỹ thuật an toàn – Các kỹ thuật mật mã dựa trên đường cong Elliptic – Phần 2: Chữ ký số).*

[13] TCVN 7818 (tất cả các phần) *(ISO/IEC 18014)*, Công nghệ thông tin – Kỹ thuật an toàn – Các dịch vụ cấp tem thời gian.