TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 11393-2:2016
ISO/IEC 13888-2:2010

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - CHỐNG CHỐI BỎ - PHẦN 2: CÁC CƠ CHẾ SỬ DỤNG KỸ THUẬT ĐỐI XỨNG

Information technology -- Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques

HÀ NỘI - 2016

Mục lục

Lời nói đầu

TCVN 11393-2:2016 hoàn toàn tương đương tiêu chuẩn ISO/IEC 13888-2:2010.

TCVN 11393-2:2016 do Trung tâm Ứng cứu Khẩn cấp máy tính Việt Nam và Học viện Công nghệ Bưu chính Viễn thông biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Bộ tiêu chuẩn TCVN 11393 gồm 03 phần:

- TCVN 11393-1:2016 Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 1: Tổng quan
- TCVN 11393-2:2016 Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 2: Các cơ chế sử dụng kỹ thuật đối xứng
- TCVN 11393-3:2016 Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 3: Các cơ chế sử dụng kỹ thuật phi đối xứng.

Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 2: Các cơ chế sử dụng kỹ thuật đối xứng

Information technology - Security techniques - Non-repudation - Part 2: Mechanisms using symmetric techniques

1 Phạm vi áp dụng

Mục đích của dịch vụ chống chối bỏ là để tạo ra, thu thập, duy trì, sẵn sàng cung cấp và xác nhận bằng chứng liên quan đến một sự kiện hoặc hành động được yêu cầu để giải quyết tranh chấp về việc xảy ra hay không xảy ra sự kiện hoặc hành động. Tiêu chuẩn này cung cấp các mô tả về cấu trúc chung có thể được sử dụng cho các dịch vụ chống chối bỏ, và một số cơ chế liên quan đến trao đổi cụ thể có thể được sử dụng để cung cấp chống chối bỏ nguồn gốc (NRO) và chống chối bỏ việc chuyển phát (NRD). Các dịch vụ chống chối bỏ khác cũng có thể được xây dựng bằng các cấu trúc chung đã được mô tả trong tiêu chuẩn này để đáp ứng các yêu cầu được xác định bởi chính sách an toàn.

Tiêu chuẩn này dựa trên sự tồn tại của bên thứ ba tin cậy để ngăn chặn việc chối bỏ hoặc cáo buộc không trung thực. Thông thường cần có một TTP trực tuyến.

Chống chối bỏ chỉ có thể được cung cấp trong ngữ cảnh một chính sách an toàn được xác định rõ ràng cho một ứng dụng cụ thể và môi trường pháp lý của nó. Các chính sách chống chối bỏ được xác định trong tiêu chuẩn ISO/IEC 10181-4.

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).

ISO/IEC 9798-1:1997, Information technology - Security techniques - Entity authentication - Part 1: General *(ISO/IEC 9798-1:1997, Công nghệ thông tin - Các kỹ thuật an toàn - Xác thực cho thực thể - Phần 1: Giới thiệu chung).*

ISO/IEC 10118 (all parts), Information technology - Security techniques - Hash-functions *(ISO/IEC 10118 (toàn tập), Công nghệ thông tin - Các kỹ thuật an toàn - Các hàm băm).*

TCVN 11393-1 (ISO/IEC 13888-1), *Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 1: Tổng quan.*

3 Thuật ngữ và định nghĩa

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

3.1

Hàm kiểm tra mật mã (cryptographic check function)

Phép biến đổi mật mã nhận đầu vào là một khoá bí mật và một chuỗi tuỳ ý, cho đầu ra là một giá trị kiểm tra mật mã.

[ISO 9798-1]

3.2

Tính toàn vẹn dữ liệu (data integrity)

Thuộc tính biểu thị dữ liệu không bị thay đổi hoặc bị phá hủy một cách trái phép.

[TCVN 9696-2:2013 (ISO 7498-2:1989)]

3.3

Bên tạo bằng chứng (evidence generator)

Thực thể tạo ra bằng chứng chống chối bỏ.

[ISO/IEC 10181-4]

3.4

Hàm băm (hash-function)

Hàm thực hiện việc ánh xạ các chuỗi bít thành các chuỗi bit có chiều dài cố định, thỏa mãn hai thuộc tính sau:

- Đối với một đầu ra cho trước, không thể tính toán để tìm ra một đầu vào có ánh xạ đến đầu ra đó.
- Đối với một đầu vào cho trước, không thể tính toán để tìm ra một đầu vào thứ hai có ánh xạ đến cùng đầu ra.

[ISO/IEC 10118-1]

3.5

Khóa (key)

Dãy các ký hiệu dùng cho kiểm soát hoạt động biến đổi mật mã (ví dụ phép mật mã hóa, giải mật mã, tính toán hàm kiểm tra mật mã, tính toán chữ ký, hoặc xác minh chữ ký).

[TCVN 7817-1 ([ISO/IEC 11770-1)]

3.6

Thuật toán mã xác thực thông điệp (Message Authentication Code algorithm - MAC algorithm)

Thuật toán để tính toán hàm ánh xạ các chuỗi bit và một khóa bí mật vào các chuỗi bit có chiều dài cố định, thỏa mãn hai thuộc tính sau:

- Cho một khóa bất kỳ và chuỗi đầu vào bất kỳ, hàm có thể tính toán một cách hiệu quả.
- Cho bất kỳ một khóa cố định, khi không biết trước về khóa, không thể tính toán giá trị hàm trên cho bất kỳ chuỗi đầu vào mới nào, ngay cả khi biết về tập các chuỗi đầu vào và các giá trị hàm tương ứng, trong đó giá trị chuỗi đầu vào thứ i có thể đã được chọn sau khi quan sát giá trị của các giá trị hàm thứ i - 1 đầu tiên.

[ISO/IEC 9797-1]

3.7

Mã xác thực thông điệp (Message Authentication Code - MAC)

Chuỗi bit đầu ra của thuật toán MAC.

[ISO/IEC 9797-1]

CHÚ THÍCH: Một MAC đôi khi còn được gọi là một giá trị kiểm tra mật mã (xem ví dụ TCVN 9696-2:2013).

3.8

Khóa bí mật (secret key)

Khóa được sử dụng với kỹ thật mật mã đối xứng, và chỉ có thể sử dụng được bởi một tập các thực thể xác định trước.

[TCVN 7817-1 (ISO/IEC 11770-1)]

3.9

Chính sách an toàn (security policy)

Tập các tiêu chí dùng cho việc cung cấp dịch vụ an toàn.

[TCVN 9696-2:2013 (ISO 7498-2:1989)]

3.10

Tem thời gian (time-stamp)

Tham số biến đổi theo thời gian biểu thị một thời điểm liên quan đến một tham chiếu thời gian chung.

[TCVN 7818-1 (ISO/IEC 1014-1)]

3.11

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

Bên thứ ba tin cậy cung cấp dịch vụ cấp tem thời gian.

[TCVN 7818-1 (ISO/IEC 1014-1)]

4 Ký hiệu và chữ viết tắt

DA	Tổ chức chuyển phát
GNRT	Thẻ chống chối bỏ chung
MAC	Hàm kiểm tra mật mã của mã xác thực thông điệp
MAC	Giá trị kiểm tra mật mã của mã xác thực thông điệp
NRD	Chống chối bỏ chuyển phát
NRDT	Thẻ chống chối bỏ chuyển phát
NRO	Chống chối bỏ nguồn gốc
NROT	Thẻ chống chối bỏ nguồn gốc
PoI	Chính sách (hoặc các chính sách) chống chối bỏ áp dụng cho bằng chứng
PoI	Định danh phân biệt của chính sách (hoặc các chính sách) chống chối bỏ áp dụng cho bằng chứng
PON	đúng hoặc sai, kết quả của một quá trình xác minh
SENV	Hàm tạo ra vỏ bọc bảo vệ
SENV	Vỏ bọc bảo vệ
TSA	Tổ chức cấp tem thời gian tin cậy
TSA	Định danh phân biệt của tổ chức cấp tem thời gian tin cậy
TST	Thẻ tem thời gian được sinh ra bởi TSA
TTP	Bên thứ ba tin cậy
TTP	Định danh phân biệt của bên thứ ba tin cậy

CHÚ THÍCH: Trong mỗi phép ghép nối, cần phải thực hiện mã hóa dữ liệu thích hợp vì sau đó cần thiết phải chọn ra dữ liệu đã ghép nối một cách chính xác.

5 Ký hiệu

5.1 Ký hiệu từ tiêu chuẩn TCVN 11393-1:2016

Các ký hiệu sau được lấy từ tiêu chuẩn TCVN 11393-1:2016 dùng cho mục đích của tiêu chuẩn này:

A	Định danh phân biệt của thực thể A
B	Định danh phân biệt của thực thể B
C	Định danh phân biệt của bên tạo bằng chứng
D	Định danh phân biệt của quan sát viên, nếu một quan sát viên độc lập tham gia
E	Định danh phân biệt của các thực thể khác liên quan tới hành động
f, f_i	Phần dữ liệu (cờ) chỉ ra kiểu dịch vụ chống chối bỏ hiện hành
Q	Dữ liệu tùy chọn cần được bảo vệ
Imp	Hàm định danh hoặc một hàm băm
Imp(y)	Dấu vết của chuỗi dữ liệu y, là (1) mã băm của chuỗi dữ liệu *y*, hoặc (2) chuỗi dữ liệu *y*
m	Một thông điệp mà bằng chứng được tạo ra cho nó
$SENV_X(y)$	Vỏ bọc bảo vệ được tính trên dữ liệu y sử dụng khóa bí mật của thực thể *X*
text	Phần dữ liệu tạo nên một phần của thẻ có thể chứa thông tin bổ sung, ví dụ một định danh khóa và / hoặc định danh thông điệp
TG	Ngày giờ bằng chứng được tạo ra
T_i	Ngày giờ sự kiện hoặc hành động xảy ra

5.1 Ký hiệu duy nhất dùng cho mục đích của tiêu chuẩn này

Các ký hiệu duy nhất sau đây được dùng cho mục đích của tiêu chuẩn này:

a	Một khóa bí mật được biết chỉ cho thực thể A và một TTP
b	Một khóa bí mật được biết chỉ cho thực thể B và một TTP
da	Khóa bí mật của tổ chức chuyển phát DA
$MAC_X(y)$	Giá trị kiểm tra mật mã được tính trên dữ liệu y sử dụng khóa bí mật của thực thể *X*
ttp	Một khóa bí mật được biết chỉ cho TTP để tạo các thẻ chống chối bỏ
(y,z)	Cặp thứ tự chứa *y* và *z* theo thứ tự này
z_1	Một trường dữ liệu gồm các trường dữ liệu liên quan đến việc cung cấp thẻ NRO

z_2 Một trường dữ liệu gồm các trường dữ liệu liên quan đến việc cung cấp thẻ NRD

6 Các yêu cầu

Các cơ chế được chỉ ra trong tiêu chuẩn này có các yêu cầu sau:

- Mỗi một trong hai thực thể tham gia có thể trao đổi riêng biệt với DA, TSA hoặc TTP.
- Hai thực thể có nhu cầu sử dụng một trong các cơ chế cụ thể trong tiêu chuẩn này đều phải tin cậy cùng một bên thứ ba.
- Trước khi sử dụng các cơ chế này, giả thiết rằng mỗi thực thể chia sẻ một khóa bí mật với DA, TSA hay TTP. Mỗi DA, TSA và TTP cũng giữ một khóa duy nhất chỉ nó biết.

  CHÚ THÍCH: Việc quản lý khóa, tạo khóa và các cơ chế thiết lập khóa được xác định trong TCVN 1817 (ISO/IEC 11770).
- Một hàm Imp chung được chia sẻ bởi tất cả các thực thể trong dịch vụ chống chối bỏ.
- Một hàm MAC đã chọn để tạo vỏ bọc (*SENV*) phải được giữ bởi tất cả các bên tham gia dịch vụ chống chối bỏ.
- TTP tạo các thẻ chống chối bỏ có thể truy cập thời gian và ngày tháng.

Độ mạnh của các cơ chế quy định trong tiêu chuẩn này phụ thuộc vào mức độ an toàn và độ mạnh của các cơ chế mật mã và các thông số được sử dụng.

7 Vỏ bọc bảo vệ

Hai thực thể chia sẻ khóa bí mật (chỉ hai thực thể này biết) có thể gửi thông điệp tới một thực thể khác bằng một hàm cho tính toàn vẹn dữ liệu gọi là SENV. *SENV* được tạo thành bằng việc bảo vệ các thành phần dữ liệu đầu vào sử dụng một khóa bí mật. Một SENV cũng có thể được sử dụng bởi một TTP để tạo ra và xác minh bằng chứng, sử dụng một khóa bí mật được chia sẻ và chỉ được giữ bởi TTP.

Hàm SENV tạo ra vỏ bọc bảo vệ *SENV* sử dụng các kỹ thuật toàn vẹn đối xứng. Khóa bí mật x của thực thể X được sử dụng để tính giá trị kiểm tra mật mã $MAC_X(y)$ được gắn thêm vào dữ y như sau:

$$SENV_x(y) = (y, MAC_x(y)).$$

8 Tạo ra và xác minh các thẻ chống chối bỏ

8.1 Tạo lập các thẻ bởi bên thứ ba tin cậy

Trong các cơ chế chống chối bỏ được mô tả ở Điều 8 này, TTP hoạt động như một tổ chức tạo ra bằng chứng và xác minh bằng chứng. Nó được tin cậy để duy trì tính toàn vẹn của các hồ sơ nào đó và trực tiếp tham gia trong việc giải quyết tranh chấp bất kỳ.

TTP phát hành các "thẻ" nhằm kết hợp với một thông điệp *m*. Một thẻ bao gồm một vỏ bọc bảo vệ được tạo thành bởi TTP sử dụng khóa bí mật của nó trên dữ liệu cụ thể cho một thông điệp. Vì không

có thực thể nào biết khóa bí mật *ttp*, chỉ duy nhất TTP mới có thể tạo lập hoặc xác minh thẻ. Tiêu chuẩn TCVN 11393-1:2016 định nghĩa *thẻ chống chối bỏ chung (GNRT)* như sau:

$$GNRT = (text, SENV_X(y)).$$

Trong trường hợp này thì:

$$GNRT = (text, SENV_{TTP}(y)).$$

TTP cũng phải kiểm tra các phần dữ liệu có trong yêu cầu bằng chứng trước khi phát hành thẻ.

CHÚ THÍCH: thông điệp *m* có thể ở dạng văn bản rõ hoặc văn bản mã hóa.

8.2 Các thành phần dữ liệu dùng trong cơ chế chống chối bỏ

8.2.1 Thành phần dữ liệu trong vỏ bọc bảo vệ

Trường dữ liệu z sau đây tạo thành nội dung của vỏ bọc bảo vệ:

$$SENV_X(z) = (z, MAC_X(z))$$

để được trao đổi trong các cơ chế chống chối bỏ mô tả trong tiêu chuẩn này:

$$z = (Pol, f_i, A, B, C, D, E, TG, T_i, Q, Imp(m)).$$

Trường dữ liệu z bao gồm các phần dữ liệu sau:

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

f_i Kiểu dịch vụ chống chối bỏ đang được cung cấp,

A Định danh phân biệt của thực thể nguồn phát,

B Định danh phân biệt của thực thể tương tác với thực thể nguồn phát,

C Định danh phân biệt của bên tạo bằng chứng,

D Định danh phân biệt của bên yêu cầu bằng chứng, nếu bên yêu cầu bằng chứng khác với thực thể nguồn phát,

E Định danh phân biệt của các thực thể khác liên quan tới hành động (tùy thuộc vào dịch vụ),

TG Ngày giờ bằng chứng được tạo ra (tùy thuộc vào dịch vụ)

T_i Ngày giờ sự kiện hoặc hành động diễn ra

Q Dữ liệu tùy chọn cần được bảo vệ

Imp(m) Dấu vết của thông điệp *m*, là (1) mã băm của thông điệp *m*, hoặc là (2) thông điệp *m*.

CHÚ THÍCH: Tùy thuộc vào dịch vụ chống chối bỏ, chỉ số *i* có giá trị là *i* = 1 hoặc 2.

8.2.2 Các thành phần dữ liệu trong thẻ chống chối bỏ

Các thẻ chống chối bỏ bao gồm một trường văn bản và một vỏ bọc bảo vệ có cấu trúc như sau:

$$Non\text{-}repudiation\ token = (text, SENV_{TTP}(z))$$

CHÚ THÍCH: Văn bản bao gồm dữ liệu thêm vào (ví dụ một định danh thông điệp hoặc định danh khóa) không cần phải bảo vệ bằng mật mã, nhưng cần thiết để định danh thông điệp và khóa được sử dụng trong tính toán giá trị kiểm tra MAC bên trong phép tính toán SENV. Thông tin này phụ thuộc vào kỹ thuật được sử dụng.

8.3 Thẻ chống chối bỏ

8.3.1 Cung cấp bằng chứng

Bằng chứng được cung cấp bởi các thẻ chống chối bỏ và nếu chính sách yêu cầu, bởi các thẻ bổ sung ví dụ như thẻ tem thời gian (*TST*), hoặc một thẻ được cung cấp bởi bên thứ tư tin cậy (ví dụ một công chứng viên) để đảm bảo bổ sung về một sự kiện, hành động hoặc sự tồn tại của một thông điệp.

Nếu bên thứ ba tin cậy có thể tự tạo ra tem thời gian tin cậy cho chính nó, thì việc bổ sung một thẻ tem thời gian (*TST*) như bằng chứng là không cần thiết.

CHÚ THÍCH 1: Thời gian có trong các thẻ chống chối bỏ (*NROT* và *NRDT*) được cung cấp bởi bên thứ ba tin cậy, nghĩa là nó được coi là an toàn.

CHÚ THÍCH 2: Nếu các bên thứ ba tin cậy (TTP, DA) không thể cung cấp tem thời gian tin cậy, khi đó thẻ tem thời gian (*TST*) được cung cấp bởi tổ chức cấp tem thời gian (TSA) sẽ được bổ sung thêm vào tập thông tin chống chối bỏ để hoàn thiện bằng chứng. Tổ chức cấp tem thời gian tin cậy là một ví dụ về sự tin cậy trong việc cung cấp một tem thời gian tin cậy.

8.3.2 Thẻ chống chối bỏ nguồn phát

Thẻ chống chối bỏ nguồn phát (*NROT*) được tạo lập bởi TTP theo yêu cầu của nguồn phát.

$$NROT = (text, z_1, MAC_{TTP}(z1))$$

với: $z_1 = (Pol, f_1, A, B, C, D, TG, T_1, Q, Imp(m))$.

Thông tin z_1 cần thiết với *NROT*, 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_1 Cờ biểu thị dịch vụ chống chối bỏ nguồn phát,

A Định danh phân biệt của bên phát,

B Định danh phân biệt của bên nhận dự kiến,

C Định danh phân biệt của *TTP* tạo ra bằng chứng,

D Định danh phân biệt của quan sát viên, nếu có một quan sát viên độc lập tham gia,

TG Ngày giờ bằng chứng đã được tạo,

T_1 Ngày giờ thông điệp được khởi phát,

Q Dữ liệu tùy chọn cần được bảo vệ,

Imp(m) Dấu vết của thông điệp *m*, là (1) mã băm của thông điệp *m*, hoặc là (2) thông điệp *m*.

8.3.3 Thẻ chống chối bỏ chuyển phát

Thẻ chống chối bỏ chuyển phát (*NRDT*) được tạo bởi TTP theo yêu cầu của bên nhận.

$NRDT = (text, z_2, MAC_{TTP}(z_2))$,

với: $z_2 = (Pol, f_2, A, B, C, D, TG, T_2, Q, Imp(m))$.

Thông tin z_2 cần thiết cho *NRDT*, nó 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_2 Cờ biểu thị dịch vụ chống chối bỏ chuyển phát,

A Định danh phân biệt của nguồn phát,

B Định danh phân biệt của bên nhận,

C Định danh phân biệt của bên thứ ba tin cậy,

D Định danh phân biệt của quan sát viên, nếu có một bên quan sát viên độc lập tham gia.

TG Ngày giờ được tạo ra,

T_2 Ngày giờ thông điệp được chuyển phát,

Q Dữ liệu tùy chọn cần được bảo vệ,

Imp(m) Dấu vết của thông điệp *m*, hoặc là (1) mã băm của thông điệp *m*, hoặc là (2) thông điệp *m*.

8.3.4 Thẻ tem thời gian

Thẻ tem thời gian (*TST*) được cung cấp bởi tổ chức cấp tem thời gian (TSA), có thể được tạo lập bằng bất kỳ cách nào từ chuẩn TCVN 7818-1 (ISO/IEC 18014-1).

8.4 Xác minh các thẻ bởi TTP

8.4.1 Quá trình xác minh

Ở một thời điểm nào đó trong quá trình trao đổi chống chối bỏ, việc cần thiết cho TTP là phải xác minh thẻ (như được định nghĩa ở trên) đã nhận từ một thực thể. Một việc cũng cần thiết là phải xác minh lại thẻ sau khi trao đổi đã hoàn thành, hoặc cần cung cấp bằng chứng ứng với uy tín của họ cho bên thứ tư nào đó.

Quá trình xác minh không chỉ bao gồm việc kiểm tra thẻ đã tạo ra bởi TTP, mà cả việc thẻ phải phù hợp với trường dữ liệu của thông điệp mà thẻ đã tạo cho nó, cũng như tính thời sự của tem thời gian. Để kiểm tra về một thẻ đã tạo ra cho một thông điệp đã biết, một thực thể cần xác minh thông điệp bằng cách so sánh *Imp(m)* được tính từ thông điệp và *Imp(m)* chứa trong trường dữ liệu z, tiếp đó yêu cầu TTP xác minh thẻ cùng với trường dữ liệu của nó.

Để xác minh vỏ bọc bảo vệ đã được tạo ra bằng cách sử dụng các kỹ thuật toàn vẹn đối xứng, phép toán xác minh bao hàm việc tính toán lại giá trị kiểm tra mật mã $MAC_X(y)$ sử dụng khóa bí mật *x* phù hợp của thực thể X và dữ liệu *y* chứa trong vỏ bọc bảo vệ, và so sánh giá trị này với giá trị đã đưa ra.

TTP cần xác minh thẻ sử dụng một trong hai phương pháp đã chỉ ra trong 8.4.2 và 8.4.3.

8.4.2 Xác minh thẻ trực tuyến

Đối với phương pháp xác minh này, TTP sử dụng một mô-đun bảo mật chứa khóa bí mật *ttp* để xác minh thẻ. Mô-đun bảo mật so sánh thẻ với một giá trị được tái tạo cục bộ sử dụng phần dữ liệu z_i và khóa bí mật *ttp*, trả lại kết quả so sánh bằng việc xác định xem thẻ có hợp lệ hay không. Vì khóa *ttp* không thể ai khác biết ngoài TTP, nên thẻ đã được đưa ra để xác minh được coi là xác thực, nếu như mô-đun bảo mật trả lại một giá trị cho biết thẻ là hợp lệ.

8.4.3 Bảng các thẻ

Đối với phương pháp xác minh này, một bảng chứa tất cả các thẻ đã phát hành bởi TTP được lưu trữ. Với mỗi thẻ đã tạo ra, TTP ghi lại thẻ cùng với trường dữ liệu (z_i) tương ứng của nó và định danh khóa của khóa bí mật *ttp*. Để xác minh thẻ, TTP sử dụng thẻ như một chỉ mục vào bảng để tìm kiếm nó. Nếu thẻ đã được đưa ra để xác minh được tìm thấy trong bảng và trường dữ liệu đã được đưa ra cùng với thẻ (hoặc một phần của thẻ) tương ứng với trường dữ liệu kết hợp với nó trong bảng, thì khi đó thẻ được coi là xác thực.

9 Các cơ chế chống chối bỏ cụ thể

9.1 Cơ chế chống chối bỏ

Các cơ chế chống chối bỏ trong Điều 9 này cho phép tạo ra bằng chứng chối chối bỏ nguồn gốc (NRO) và chống chối bỏ chuyển phát (NRD). Ngoài ra, cơ chế để tạo tem thời gian được xác định. Thực thể A muốn gửi thông điệp m tới thực thể B và do đó Thực thể A sẽ là nguồn phát của truyền tải chống chối bỏ. Thực thể B sẽ là bên nhận.

Trong một số cơ chế đã được mô tả ở Điều 8, trường dữ liệu z_i được sử dụng. Trường dữ liệu này tương tự trường z_i trong thẻ chống chối bỏ, ngoại trừ nó không chứa thông tin về thời điểm bằng chứng được tạo ra. Thông tin thời gian này sẽ được cung cấp bởi TTP (hoặc DA) hoặc bởi tổ chức cấp tem thời gian TSA theo yêu cầu của TTP (hoặc DA).

CHÚ THÍCH: Trong trường hợp *Imp(m)* là thông điệp *m*, thì không cần thiết phải gửi thông điệp *m* cùng với thẻ, và các bước cho xác minh *Imp(m)* cũng được bỏ qua.

9.2 Cơ chế chống chối bỏ nguồn phát

9.2.1 Các giao dịch và cơ chế

Nguồn phát tạo ra thông điệp để gửi tới bên nhận cụ thể. Bên nhận có thể kiểm tra thông điệp có đúng là đến từ người gửi đã tuyên bố hay không bằng cách sử dụng TTP để xác minh thẻ chống chối bỏ nguồn gốc liên quan.

Trong giao dịch đầu tiên của cơ chế này, bên nguồn phát hình thành dữ liệu và truyền nó đi trong một *SENV* tới TTP. TTP tạo ra thẻ chống chối bỏ nguồn gốc (*NROT*) và trả lại nó cho nguồn phát A. Trong giao dịch thứ hai, *NROT* được gắn vào thông điệp *m* và được gửi đi từ nguồn phát A đến bên nhận B. Trong giao dịch thứ ba, bên nhận B gửi *NROT* đóng gói trong một vỏ bọc bảo vệ gửi tới TTP để xác minh. Chống chối bỏ nguồn gốc được thiết lập trong giao dịch thứ ba.

9.2.2 Sinh thẻ

9.2.2.1 Giao dịch 1 - giữa nguồn phát A và TTP

a. Thực thể A tạo ra vỏ bọc bảo vệ $SENV_A(z'_1)$ sử dụng khóa *a*, với z'_1 là z_1 được xác định trong 8.3.2 với phần dữ liệu *TG* là rỗng. Sau đó thực thể *A* yêu cầu một *NROT* bằng cách gửi vỏ bọc bảo vệ tới TTP.

b. TTP xác minh rằng vỏ bọc bảo vệ đến từ thực thể A và A là một thực thể với định danh phân biệt *A*. Nếu việc xác minh thành công, TTP hoàn tất z_1 bằng cách chèn phần dữ liệu *TG* và tính toán:

$NROT = (text, z_1, MAC_{TTP}(z_1))$

sử dụng khóa *ttp* và trả lại giá trị $SENV_A(NROT)$ tới A.

c. Thực thể A xác minh rằng $SENV_A(NROT)$ đến từ TTP và z_1 trong *NROT* tương ứng với z'_1 trong yêu cầu ban đầu.

9.2.2.2 Giao dịch 2 - từ nguồn phát A tới bên nhận B

Thực thể A gửi tới B: $(m, NROT)$

9.2.2.3 Giao dịch 3 - giữa bên nhận B và TTP

a. Thực thể B xác minh chính sách *Pol* trong z_1 phù hợp với các yêu cầu an toàn của nó, xác minh cờ f_1 trong z_1 biểu thị một thẻ chống chối bỏ nguồn phát, xác minh định danh của A, B và C trong z_1, xác minh định danh của D trong z_1, nếu như một quan sát viên độc lập có mặt, xác minh các trường thời gian *TG* và T_1 là đúng, xác minh giá trị *Imp(m)* chứa trong z_1 là đúng.

b. Thực thể B tạo ra $SENV_B(NROT)$ sử dụng khóa *b* và gửi nó tới TTP để yêu cầu xác minh *NROT* đã nhận được từ A.

c. TTP xác minh rằng $SENV_B(NROT)$ nhận từ B và cũng xác minh rằng *NROT* là xác thực. Nếu $SENV_B(NROT)$ là hợp lệ, TTP gửi $SENV_B(PON, NROT)$ tới B, trong đó *PON* là đúng nếu *NROT* là xác thực, là sai nếu *NROT* là không xác thực.

d. Thực thể B xác minh rằng $SENV_B(PON, NROT)$ nhận từ TTP. Nếu nó là hợp lệ thì xác minh là đúng, chống chối bỏ nguồn gốc (nghĩa là thông điệp đã đến từ A) được thiết lập.

e. *NROT* được lưu giữ cho chống chối bỏ nguồn gốc sau này.

9.2.3 Xác minh thẻ

Nếu người dùng bằng chứng B muốn xác minh, vào một thời điểm trong tương lai, tính xác thực của *NROT*, thì khi đó việc xác minh sẽ được thực hiện như đã chỉ ra trong giao dịch 3 của 9.2.2.3.

9.3 Cơ chế chống chối bỏ chuyển phát

9.3.1 Các giao dịch và cơ chế

Sau khi nhận thông điệp *m*, thực thể B gửi trong giao dịch đầu tiên của cơ chế này một yêu cầu tạo thẻ chống chối bỏ chuyển phát tới TTP đóng trong một vỏ bọc bảo vệ. TTP tạo thẻ chống chối bỏ chuyển phát (*NRDT*) và gửi lại cho bên nhận B. Trong giao dịch thứ 2, *NRDT* được gửi bởi bên nhận B tới nguồn phát A. Trong giao dịch thứ 3, nguồn phát gửi *NRDT* đóng trong vỏ bọc bảo vệ tới TTP để xác minh. Chống chối bỏ chuyển phát được thiết lập trong giao dịch thứ 3.

9.3.2 Sinh thẻ

9.3.2.1 Giao dịch 1 - giữa bên nhận B và TTP

a. Thực thể B tạo ra một vỏ bọc bảo vệ $SENV_B(z'_2)$ sử dụng khóa *b*, trong đó z'_2 là z_2 đã xác định trong 8.3.3 với phần dữ liệu *TG* là rỗng. Sau đó thực thể B yêu cầu một *NRDT* bằng cách gửi vỏ bọc bảo vệ tới TTP.

b. TTP xác minh vỏ bọc bảo vệ $SENV_B(z'_2)$ đến từ thực thể B. Nếu là đúng như vậy, TTP hoàn thành z_2 bằng cách chèn thêm phần dữ liệu *TG* và tính toán:

$$NRDT = (text\ ,\ z_2\ ,\ MAC_{TTP}(z_2))$$

sử dụng khóa *ttp* và trả lại $SENV_B(NRDT)$ cho B.

c. Thực thể B xác minh rằng $SENV_B(NRDT)$ đến từ TTP và z_2 chứa trong thẻ tương ứng với z'_2 đã được gửi trong bước *a*.

9.3.2.2 Giao dịch 2 - từ bên nhận B tới nguồn phát A

Thực thể B gửi tới A: *NRDT*.

9.3.2.3 Giao dịch 3 - giữa nguồn phát A và TTP

a. Thực thể A xác minh chính sách *Pol* trong z_2 phù hợp với các yêu cầu bảo mật của nó, xác minh cờ f_2 trong z_2 biểu thị một thẻ chống chối bỏ chuyển phát; xác minh định danh của A, B và C trong z_2;

xác minh định danh của D trong z_2 nếu có mặt một quan sát viên độc lập; xác minh trường thời gian *TG* và T_2 là đúng; xác minh giá trị của *Imp(m)* chứa trong z_2 là đúng.

b. Thực thể A tạo $SENV_A(NRDT)$ sử dụng khóa a và gửi nó tới *TTP* để yêu cầu xác minh *NRDT* đã nhận được từ B.

c. TTP xác minh $SENV_A(NRDT)$ đến từ A và cũng xác minh *NRDT* là xác thực. Nếu $SENV_A(NRDT)$ hợp lệ, *TTP* gửi $SENV_A(PON, NRDT)$ tới A, trong đó *PON* là đúng nếu *NRDT* được xác thực, là sai nếu *NRDT* không được xác thực.

d. Thực thể A xác minh $SENV_A((PON, NRDT))$ đến từ TTP. Nếu hợp lệ thì xác minh là đúng, chống chối bỏ chuyển phát được thiết lập.

e. *NRDT* được lưu trữ để chống chối bỏ chuyển phát sau này.

9.3.3 Xác minh thẻ

Nếu người dùng bằng chứng A muốn xác minh, ở một thời điểm trong tương lai, tính xác thực của một *NRDT*, thì khi đó việc xác minh sẽ được thực hiện như đã chỉ ra trong giao dịch 3 của 9.3.2.3.

9.4 Cơ chế lấy thẻ tem thời gian

Khi một tham chiếu thời gian tin cậy được yêu cầu và khi không thể tin cậy đồng hồ được cung cấp bởi bên tạo ra thẻ, thì cần phải dựa vào một bên thứ ba tin cậy là tổ chức cấp tem thời gian (TSA - Time-Stamping Authority).

Trao đổi giữa thực thể X (bên yêu cầu) và TSA khi yêu cầu một tem thời gian được mô tả trong chuẩn TCVN 7818-1 (ISO/IEC 18014-1).

Phụ lục A

(Tham khảo)

Ví dụ về các cơ chế chống chối bỏ cụ thể

A.1 Ví dụ về các cơ chế chống chối bỏ nguồn phát và chuyển phát

Các cơ chế chống chối bỏ trong Phụ lục này cung cấp chống chối bỏ nguồn phát và chống chối bỏ chuyển phát giữa hai thực thể A và B. Thực thể A muốn gửi một thông điệp tới thực thể B và là nguồn phát của trao đổi chống chối bỏ. Thực thể B là bên nhận thông điệp, gọi là bên nhận. Trước khi mô tả cơ chế, giả thiết rằng các khóa *a* và *b* có mặt tại vị trí thực thể A và B tương ứng, và TTP sở hữu các khóa *a* và *b* ngoài khóa *ttp* của bản thân nó.

Ba cơ chế chống chối bỏ khác nhau (M1, M2 và M3) sử dụng một TTP trực tuyến được cung cấp.

CHÚ THÍCH 1: Bằng cách sử dụng tem thời gian trong dữ liệu của *SENV* có thể đạt được việc bảo vệ chống lại sự gây trễ trái phép hoặc phát lại trái phép thông điệp. Bằng cách sử dụng đặt *NROT* và *NRDT* chứa tem thời gian, có thể đạt được việc xác minh sau này cho các tem thời gian tại thời điểm thông điệp được truyền.

CHÚ THÍCH 2: Trong trường hợp *Imp(m)* là thông điệp *m* thì không cần thiết phải gửi *m* cùng với thẻ, và các bước xác minh *Imp(m)* cũng được bỏ qua.

A.2 Cơ chế M1: NRO bắt buộc, NRD tùy chọn

A.2.1 Năm giao dịch của cơ chế M1

Chống chối bỏ nguồn phát được thiết lập trong ba giao dịch giữa các thực thể và TTP. Nếu các bước NRD tùy chọn được tiếp tục (do đặc quyền của bên nhận), chống chối bỏ chuyển phát được thiết lập trong hai giao dịch tiếp theo (xem Hình A.1).

CHÚ THÍCH 1: Trong khi tùy theo bên nhận để tiếp tục các bước cần thiết cho chống chối bỏ chuyển phát, cần hết sức lưu ý là chống chối bỏ chuyển phát tùy chọn này là bắt buộc hoàn toàn một khi nó được thiết lập.

CHÚ THÍCH 2: Cơ chế này cung cấp chống chối bỏ nguồn gốc và có thể được dùng theo tùy chọn để cung cấp chống chối bỏ chuyển phát. Việc sử dụng thủ tục (nghĩa là nó có được sử dụng để cung cấp chống chối bỏ nguồn phát hoặc cả chống chối bỏ nguồn phát và chống chối bỏ chuyển phát hay không) sẽ được quyết định giữa nguồn phát A, bên nhận B và bên thứ ba tin cậy TTP trước khi bắt đầu thực hiện một thủ tục cụ thể.

A.2.2 Giao dịch 1- giữa nguồn phát A và TTP

Các giao dịch của cơ chế M1 (Hình A.1) được thiết kế như sau:

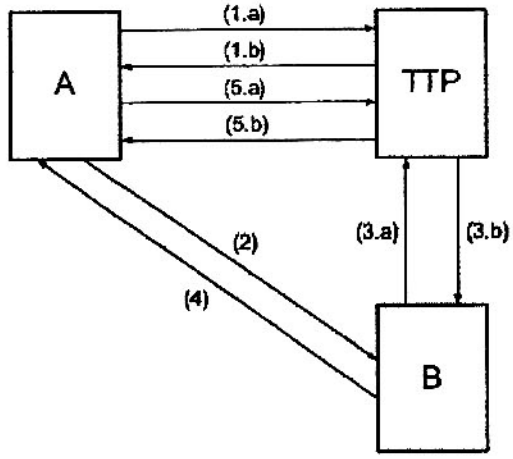
a. Thực thể A tạo ra một vỏ bọc bảo vệ $SENV_A(z'_1)$ sử dụng khóa a, trong đó z'_1 là z_1 như đã xác định trong 8.3.2 với phần dữ liệu *TG* là rỗng. Sau đó thực thể A yêu cầu một *NROT* bằng cách gửi vỏ bọc bảo vệ tới TTP.

b. TTP xác minh rằng vỏ bọc bảo vệ đến từ thực thể A, và A là một thực thể với định danh phân biệt *A*. Nếu đúng như vậy, TTP hoàn thành z_1 bằng cách chèn thêm phần dữ liệu *TG* và tính toán:

NROT = (text, z_1, $MAC_{TTP}(z_1)$)

sử dụng khóa *ttp* và trả trá trị $SENV_A(NROT)$ về A.

c. Thực thể A xác minh rằng $SENV_A(NROT)$ đến từ TTP.



(1.a) $SENV_A(z'_1)$

(1.b) $SENV_A(NROT)$

(2) (m, NROT)

(3.a) $(SENV_B(NROT)$ *và* $SENV_B(z'_2)$

(3.b) $SENV_B((PON, NROT, NRDT))$ *hoặc* $SENV_B((PON, NROT))$

(4) NRDT

(5.a) $SENV_A(NRDT)$

(5.b) $SENV_A((PON, NRDT))$

Hình A.1 - Cơ chế M1

A.2.3 Giao dịch 2 - từ nguồn phát A tới bên nhận B

Thực thể A gửi tới B: *(m, NROT)*

A.2.4 Giao dịch 3 - giữa bên nhận B và TTP

a. Thực thể B xác minh giá trị của *Imp(m)* trong z_1, sau đó tạo ra $SENV_B(NROT)$ và $SENV_B(z'_2)$, trong đó z'_2 là z_2 như đã xác định trong 8.3.3 với phần dữ liệu *TG* là rỗng, sử dụng khóa *b* và gửi nó tới TTP để yêu cầu xác minh rằng *NROT* đã nhận từ A và tạo ra *NRDT*.

b. TTP kiểm tra $SENV_B(NROT)$ và *NROT*. Nếu cả hai cùng hợp lệ thì TTP xác minh là $SENV_B(z'_2)$ đến từ thực thể B. Nếu đúng như vậy, TTP hoàn thành z_2 bằng cách chèn thêm phần dữ liệu *TG* và thực hiện tính:

NRDT = *(text,* z_2, $MAC_{TTP}(z_2)$*)*

sử dụng khóa *ttp* và gửi giá trị:

$SENV_B((PON, NROT, NRDT))$

tới B, trong đó *PON* là đúng.

Nếu như vỏ bọc bảo vệ $SENV_B(NROT)$ là hợp lệ, song *NROT* không hợp lệ thì TTP sẽ gửi:

$SENV_B((PON, NROT))$,

tới B, trong đó *PON* là sai.

c. Thực thể B xác minh $SENV_B((PON, NROT, NRDT))$ là đến từ TTP. Nếu giá trị là hợp lệ và *PON* là đúng, thì chống chối bỏ nguồn phát (nghĩa là thông điệp đã đến từ A) được thiết lập.

d. *NROT* được lưu giữ để chống chối bỏ nguồn phát sau này.

A.2.5 Giao dịch 4 - từ bên nhận B tới nguồn phát A

Thực thể B gửi *NRDT* tới A.

A.2.6 Giao dịch 5 - giữa nguồn phát A và bên nhận TTP

a. Thực thể A xác minh giá trị của *Imp(m)* chứa trong z_2, sau đó tạo $SENV_A(NRDT)$ sử dụng khóa *a* và gửi nó tới TTP để yêu cầu xác minh rằng *NRDT* nhận được từ B.

b. TTP xác minh $SENV_A(NRDT)$ là đến từ A và cũng xác minh rằng *NRDT* là xác thực. Nếu cả hai giá trị là hợp lệ, TTP gửi $SENV_A((PON, NRDT))$, trong đó *PON* là đúng, tới A. Nếu *NRDT* không hợp lệ, thì TTP gửi $SENV_A((PON, NROT))$, trong đó *PON* là sai, tới A.

c. Thực thể A xác minh $SENV_A((PON, NRDT))$ là đến từ TTP. Nếu nó là hợp lệ và việc xác minh là đúng, thì chống chối bỏ chuyển phát được thiết lập.

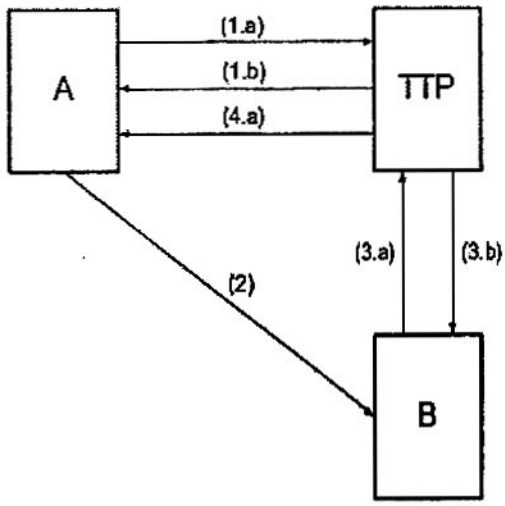
d. Thực thể A lưu *NRDT* để chống chối bỏ chuyển phát sau này.

A.3 Cơ chế M2: NRO bắt buộc, NRD bắt buộc

A.3.1 Bốn giao dịch của cơ chế M2

Chống chối bỏ nguồn phát và chống chối bỏ chuyển phát được thiết lập trong bốn giao dịch giữa hai thực thể và TTP. Trong cơ chế này, TTP gửi thông điệp đã nhận trực tiếp tới A trong một *SENV* ở cùng thời điểm mà nó gửi tới B.

Các giao dịch của cơ chế M2 được thiết kế như sau (xem Hình A.2):



(1.a) $SENV_A(z'_1)$

(1.b) $SENV_A(NROT)$

(2) *(m, NROT)*

(3.a) *($SENV_B(NROT)$ và $SENV_B(z'_2)$*

(3.b) *$SENV_B((PON, NROT, NRDT))$ hoặc $SENV_B((PON, NROT))$*

(4.a) *$SENV_A(NRDT)$*

Hình A.2 - Cơ chế M2

A.3.2 Giao dịch 1 - giữa nguồn phát A và TTP

a. Thực thể A tạo một vỏ bọc bảo vệ $SENV_A(z'_1)$ sử dụng khóa *a*, với z'_1 là z_1 như đã xác định trong 8.3.2 với phần dữ liệu *TG* là rỗng. Sau đó thực thể A yêu cầu một *NROT* bằng cách gửi vỏ bọc bảo vệ tới TTP.

b. TTP xác minh vỏ bọc bảo vệ đó là đến từ A. Nếu đúng như vậy, TTP hoàn thành z_1 bằng cách chèn thêm phần dữ liệu *TG* và sau đó tính:

$NROT = (text, z_1, MAC_{TTP}(z_1))$

sử dụng khóa *ttp* và gửi lại $SENV_A(NROT)$ tới A sử dụng khóa *a*.

c. Thực thể A xác minh rằng $SENV_A(NROT)$ đến từ TTP.

A.3.3 Giao dịch 2 - từ nguồn A tới bên nhận B

Thực thể A gửi tới B: *(m, NROT).*

A.3.4 Giao dịch 3 - giữa bên nhận B và TTP

a. Thực thể B xác minh giá trị *Imp(m)* chứa trong z_1, sau đó tạo $SENV_B(NROT)$ và $SENV_B(z'_2)$, trong đó z'_2 là z_2 như đã xác định trong 8.3.3 với phần dữ liệu *TG* là rỗng, sử dụng khóa *b* và gửi nó tới TTP để yêu cầu xác minh rằng *NROT* đã nhận được từ A và tạo ra *NRDT*.

b. TTP xác minh $SENV_B(NROT)$ là đến từ B và *NROT* là xác thực. Nếu cả hai là hợp lệ, TPP xác minh rằng vỏ bọc bảo vệ $SENV_B(z'_2)$ đến từ thực thể B. Nếu là đúng như vậy, thì TTP hoàn thành z_2 bằng cách chèn thêm phần dữ liệu *TG* và tính:

$NRDT = (text, z_2, MAC_{TTP}(z_2))$

sử dụng khóa *ttp* và gửi:

$SENV_B((PON, NROT, NRDT))$,

tới B, trong đó *PON* là đúng. Nếu vỏ bọc bảo vệ $SENV_B(NROT)$ là hợp lệ, song *NROT* không hợp lệ, thì TTP sẽ gửi:

$SENV_B((PON, NROT))$

tới B, trong đó *PON* là sai.

c. Thực thể B xác minh $SENV_B((PON, NROT, NRDT))$ là đến từ TTP. Nếu nó hợp lệ và *PON* là đúng thì chống chối bỏ nguồn phát được thiết lập.

d. Thực thể B lưu *NROT* để chống chối bỏ nguồn sau này.

A.3.5 Giao dịch 4 - giữa TTP và nguồn phát A

a. Ngay sau khi gửi *NRDT* tới B trong giao dịch 3, TTP cũng gửi $SENV_A(NRDT)$ tới A.

b. Thực thể A kiểm tra $SENV_A(NRDT)$ và *NRDT*. Nếu cả hai đều hợp lệ, thì chống chối bỏ chuyển phát (nghĩa là thông điệp đã được nhận bởi B) được thiết lập.

c. Thực thể A lưu *NRDT* để chống chối bỏ chuyển phát sau này.

A.4 Cơ chế M3: NRO và NRD bắt buộc với TTP trung gian

A.4.1 Bốn giao dịch của cơ chế M3

Chống chối bỏ nguồn phát và chống chối bỏ chuyển phát được thiết lập trong bốn giao dịch giữa hai thực thể và TTP. Trong cơ chế M3, TTP hoạt động như một trạm trung gian giữa nguồn phát và bên nhận - hai thực thể không bao giờ tương tác trực tiếp. Để thực hiện điều này, thực thể A gửi thông điệp tới B như là một phần của giao dịch 1 và, TTP chuyển nó tới thực thể B như là một phần của giao dịch 2 (xem Hình A.3).

Do TTP trong cơ chế này đóng vai trò tổ chức chuyển phát, nó có thể tùy ý tạo ra và gửi các thẻ chống chối bỏ việc đệ trình và chống chối bỏ việc vận chuyển tới thực thể nguồn phát.

A.4.2 Giao dịch 1 - giữa nguồn phát A và TTP

Các giao dịch của cơ chế M3 (xem Hình A.3) được thiết kế như sau:

a. Thực thể A tạo ra một vỏ bọc bảo vệ $SENV_A(z'_1)$ sử dụng khóa *a* với z'_1 là z_1 như đã xác định trong 8.3.2 với phần dữ liệu *TG* là rỗng. Sau đó thực thể A yêu cầu một *NROT* bằng cách gửi vỏ bọc bảo vệ cùng với thông điệp *m* tới TTP.

b. TTP xác minh rằng vỏ bọc bảo vệ là đến từ thực thể A. Nếu đúng như vậy, TTP hoàn thành z_1 bằng cách chèn thêm phần dữ liệu *TG* và tính

$NROT = (text, z_1, MAC_{TTP}(z_1))$

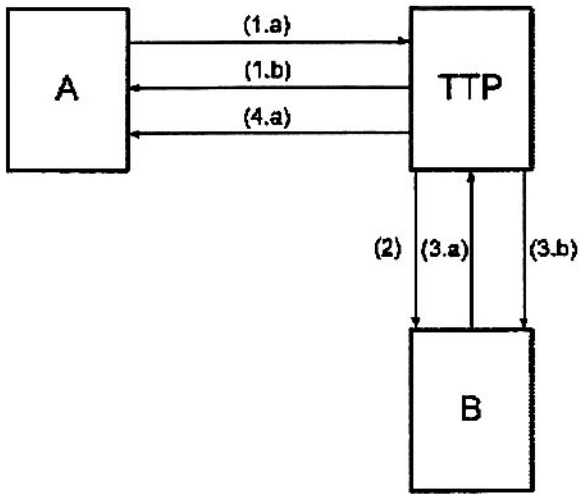
sử dụng khóa *ttp* và gửi lại:

$SENV_A(NROT)$

tới A sử dụng khóa *a*.

c. Thực thể A xác minh rằng $SENV_A(NROT)$ là đến từ TTP.

CHÚ THÍCH: Thực thể A phải liên lạc với TTP trong trường hợp xác minh ở bước c bị sai; thủ tục xử lý tình huống này nằm ngoài phạm vi của tiêu chuẩn này.



(1.a) $(m, SENV_A(z'_1))$

(1.b) $SENV_A(NROT)$

(2) $(m, NROT)$

(3.a) $(SENV_B(NROT)$ và $SENV_B(z'_2)$

(3.b) $SENV_B((PON, NROT, NRDT))$ hoặc $SENV_B((PON, NROT))$

(4.a) $SENV_A(NRDT)$

Hình A.3 - Cơ chế M3

A.4.3 Giao dịch 2 - từ TTP tới bên nhận B

TTP gửi *m* và *NROT* tới B.

A.4.4 Giao dịch 3 - giữa bên nhận B và TTP

a. Vì *NROT* không được nhận trong vỏ bọc bảo vệ, nên B phải xác minh nó với TTP, vì vậy B xác minh *Imp(m)* và gửi $SENV_B(NROT)$ và $SENV_B(z'_2)$, trong đó z'_2 là z_2 như đã xác định trong 8.3.3 với phần dữ liệu *TG* rỗng, tới TTP để yêu cầu xác minh rằng *NROT* đã được nhận từ A và tạo ra *NRDT*.

b. TTP xác minh $SENV_B(NROT)$ là đến từ B và cũng xác minh tính xác thực của *NROT*. Nếu cả hai đều hợp lệ, thì TTP xác minh xem vỏ bọc bảo vệ $SENV_B(z'_2)$ có phải đến từ B không. Nếu là đúng như vậy, TTP hoàn thành z_2 bằng cách chèn thêm dữ liệu *TG* và tính:

$NRDT = (text, z_2, MAC_{TTP}(z_2))$

sử dụng khóa *ttp* và phúc đáp lại B với giá trị PON đúng bằng cách gửi:

$SENV_B((PON, NROT, NRDT))$

Nếu vỏ bọc bảo vệ $SENV_B(NROT)$ là hợp lệ, song *NROT* không hợp lệ, thì TTP gửi:

$SENV_B((PON, NROT))$

tới B, trong đó *PON* là sai.

c. B xác minh rằng *SENV* là đến từ TTP. Nếu nó hợp lệ và *PON* là đúng, thì chống chối bỏ nguồn phát được thiết lập.

d. *NROT* được lưu để chống chối bỏ nguồn phát sau này.

A.4.5 Giao dịch 4 - giữa TTP và nguồn phát A

a. Ngay sau khi gửi *NRDT* tới B trong giao dịch 3, TTP cũng gửi $SENV_A(NRDT)$ tới A.

b. A xác minh rằng nó đã được nhận từ TTP, và chống chối bỏ chuyển phát được thiết lập.

c. *NRDT* được lưu để chống chối bỏ chuyển phát sau này.

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 9797 (all parts) – Information technology – Security techniques - Message Authentication Codes MACs *(Công nghệ thông tin – Kỹ thuật an toàn – Mã xác thực thông điệp).*

[3] 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).*

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

[5] TCVN 7817-1:2007 (ISO/IEC 11770-1:1996) *Công nghệ thông tin – Kỹ thuật mật mã – Quản lý khóa – Phần 1: Khung tổng quát.*

[6] TCVN 7817-2:2010 (ISO/IEC 11770-2:2008) *Công nghệ thông tin – Kỹ thuật an ninh – Quản lý khóa – Phần 2: Cơ chế sử dụng kỹ thuật đối xứng.*

[7] TCVN 7817-3:2007 (ISO/IEC 11770-3:1999) *Công nghệ thông tin – Kỹ thuật mật mã – Quản lý khóa – Phần 3: Các cơ chế sử dụng kỹ thuật phi đối xứng.*

[8] TCVN 7818 (*ISO/IEC 18014*), Công nghệ thông tin – Các kỹ thuật mật mã – Dịch vụ tem thời gian.