TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 11817-2:2017
ISO/IEC 9798-2:2008

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - XÁC THỰC THỰC THỂ - PHẦN 2: CƠ CHẾ SỬ DỤNG THUẬT TOÁN MÃ HÓA ĐỐI XỨNG

Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms

HÀ NỘI - 2017

Mục lục

Lời nói đầu

TCVN 11817-2:2017 hoàn toàn tương đương với ISO/IEC 9798-2:2008 và đính chính kỹ thuật 3:2013.

TCVN 11817-2:2017 (ISO/IEC 9798-2:2008) do Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã biên soạn, Ban Cơ yếu Chính phủ đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Bộ tiêu chuẩn TCVN 11817:2017 *Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể* gồm các tiêu chuẩn sau:

- TCVN 11817-1:2017 (ISO/IEC 9798-1:2010), Phần 1: Tổng quan.

- TCVN 11817-2:2017 (ISO/IEC 9798-2:2008), Phần 2: Cơ chế sử dụng thuật toán mã hóa đối xứng.

- TCVN 11817-3:2017 (ISO/IEC 9798-3:1998), Phần 3: Cơ chế sử dụng kỹ thuật chữ ký số.

Bộ ISO/IEC 9798 *Information technology – Security techniques – Entity authentication* còn các tiêu chuẩn sau:

- ISO/IEC 9798-4:1999, Part 4: Mechanisms using a cryptographic check function.

- ISO/IEC 9798-5:2009, Part 5: Mechanisms using zero-knowledge techniques.

- ISO/IEC 9798-6:2010, Part 6: Mechanisms using manual data transfer.

TIÊU CHUẨN QUỐC GIA **TCVN 11817-2 : 2017**

Công nghệ thông tin - Các kỹ thuật an toàn - Xác thực thực thể - Phần 2: Cơ chế sử dụng thuật toán mã hóa đối xứng

Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms

1 Phạm vi áp dụng

Tiêu chuẩn này quy định cơ chế xác thực thực thể sử dụng thuật toán mã hóa đối xứng. Có 4 cơ chế cung cấp xác thực thực thể giữa hai thực thể không có bên thứ ba tin cậy tham gia; hai trong các cơ chế đó là cơ chế xác thực một chiều của một thực thể này với một thực thể khác; hai cơ chế còn lại là cơ chế xác thực lẫn nhau của hai thực thể. Các cơ chế còn lại yêu cầu bên thứ ba tin cậy cho việc thiết lập khóa bí mật chung và thực hiện xác thực thực thể một chiều hoặc lẫn nhau.

Các cơ chế quy định trong tiêu chuẩn này sử dụng tham số biến thiên theo thời gian như tem thời gian, số tuần tự hoặc số ngẫu nhiên để ngăn chặn thông tin xác thực hợp lệ được chấp nhận sau đó hoặc sử dụng lại.

Nếu không có bên thứ ba tin cậy tham gia và tem thời gian hoặc số tuần tự được sử dụng, một chuyến cần thiết cho xác thực một chiều, và hai chuyến cần thiết để đạt được xác thực lẫn nhau. Nếu không có sự tham gia của bên thứ ba tin cậy và một thách thức và số ngẫu nhiên sử dụng phương pháp đáp ứng được sử dụng, hai chuyến là cần thiết cho xác thực một chiều, trong khi đó xác thực lẫn nhau yêu cầu phải sử dụng 3 chuyến. Nếu có sự tham gia của bên thứ ba tin cậy, bất kỳ giao tiếp bổ sung giữa thực thể và bên thứ ba tin cậy đòi hỏi phải bổ sung thêm hai chuyến trong việc trao đổi truyền thông.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên 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, bổ sung (nếu có).

TCVN 11817-1:2017 (ISO/IEC 9798-1): Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể - Phần 1: Tổng quan.

3 Thuật ngữ và định nghĩa

TCVN 11817-2 áp dụng các thuật ngữ và định nghĩa trong TCVN 11817-1 và dưới đây:

3.1

Mã hóa có xác thực (authenticaticated encryption)

(Khả nghịch) Phép biến đổi dữ liệu bằng thuật toán mật mã để tạo bản mã mà không thể thay đổi được bởi một thực thể trái phép mà không phát hiện, tức là cung cấp bảo mật, toàn vẹn và xác thực nguồn gốc dữ liệu.

3.2

Bản mã (ciphertext)

Dữ liệu đã được biến đổi để giấu nội dung thông tin của dữ liệu

3.3

Bên được xác thực (claimant)

Thực thể có định danh có thể được xác thực, bao gồm chức năng và dữ liệu cá nhân cần thiết để tham gia trao đổi xác thực thay mặt cho chủ thể.

[ISO/IEC 9798-5:2004]

3.4

Mã xác thực thông điệp (message authentication code)

MAC (MAC)

Xâu bit đầu ra của thuật toán MAC

CHÚ THÍCH MAC đôi khi được gọi là giá trị kiểm tra mật mã.

[ISO/IEC 9797-1:1999]

3.5

Thuật toán mã xác thực thông điệp (message authentication code (MAC) algorithm)

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

- Cho một khóa và xâu 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.

CHÚ THÍCH 1 Thuật toán MAC đôi khi còn gọi là hàm kiểm tra mật mã (xem ví dụ ISO 7498-2).

CHÚ THÍCH 2 Tính khả thi của việc tính toán phụ thuộc vào môi trường và các yêu cầu an toàn cụ thể của người dùng.

[ISO/IEC 9797-1]

3.6

Tem thời gian (time stamp)

Tham số biến thiên theo thời gian đánh dấu một thời điểm tromg một hệ tham chiếu về thời gian thông thường

[ISO/IEC 18014-1:2008]

3.7

Bên thứ ba tin cậy (trusted third party)

Một tổ chức có thẩm quyền về an toàn, hoặc đại diện đủ tư cách của cơ quan đó, được tin cậy bởi các thực thể khác về khía cạnh hoạt động liên quan đến an toàn

[ISO/IEC 18014-1:2008]

4 Ký hiệu và từ viết tắt

A, B	Nhãn được sử dụng cho các thực thể tham gia vào một cơ chế.
d_K	Quá trình giải mã được xác thực sử dụng khóa bí mật K.
e_K	Quá trình mã hóa được xác thực thực thi sử dụng khóa bí mật K.
$e_K(X)$	Kết quả của quá trình mã hóa dữ liệu X dùng thuật toán mã hóa đối xứng sử dụng khóa K.
I_U	Định danh phân biệt của thực thể U.
K	Khóa bí mật sử dụng trong quá trình mã hóa và giải mã.
K_{UV}	Khóa bí mật được chia sẻ giữa thực thể U và V và chỉ sử dụng trong kỹ thuật mật mã đối xứng.
N_U	Số tuần tự được cấp bởi thực thể U.
P	Ký hiệu mô tả bên thứ ba tin cậy.
R_U	Số ngẫu nhiên được cấp bởi thực thể U.
TN_U	Tham số biến thiên theo thời gian có nguồn gốc từ thực thể U hoặc là tem thời gian T_U hoặc số tuần tự N_U.
$Token_{UV}$	Thẻ được gửi từ thực thể U đến thực thể V.
T_U	Tem thời gian được cấp bởi thực thể U.
TVP_U	Tham số biến thiên theo thời gian có nguồn gốc từ thực thể U, đó là tem thời gian T_U, số tuần tự N_U hoặc số ngẫu nhiên R_U.
$X \|\| Y$	Kết quả của phép ghép nối mục dữ liệu X và Y theo trình tự quy định. Trong trường hợp kết quả của phép ghép hai hoặc nhiều mục dữ liệu được mã hóa như một phần của các cơ chế được đặc tả trong phần này của bộ tiêu chuẩn này, kết quả này được sắp đặt theo một trật tự vì vậy nó có thể là kết quả duy nhất đối với các xâu dữ liệu cấu thành, tức là để không có khả năng không rõ ràng trong việc biên dịch. Tính chất này có thể đạt được bằng nhiều cách khác nhau tùy thuộc vào ứng dụng. Ví dụ, nó có thể được đảm bảo bằng cách (a) ấn định chiều dài của mỗi xâu con trong suốt miền của cơ chế hoặc (b) mã hóa tuần

	tự phép ghép xâu sử dụng một phương pháp đảm bảo việc giải mã duy nhất, ví dụ sử dụng các quy tắc giải mã phân biệt được định nghĩa trong ISO/IEC 8825-1[1]. CHÚ THÍCH Không chỉ việc ghép nối các xâu mà trật tự của chúng cũng cần thiết. Thông thường, các ký hiệu cho trật tự này là $[X_1, ..., X_n]$.

5. Các yêu cầu

Trong các cơ chế xác thực được quy định trong tiêu chuẩn này, thực thể được xác thực chứng thực định danh của mình bằng cách chứng minh thông tin của mình về khóa xác thực bí mật. Thực thể đạt được điều này bằng cách sử dụng khóa bí mật của mình để mã hóa dữ liệu cụ thể. Các dữ liệu được mã hóa có thể được giải bởi bất kỳ ai được chia sẻ khóa xác thực bí mật của thực thể đó. Dữ liệu được mã hóa phải bao gồm tham số biến thiên theo thời gian. Tham số đó có thể được xác thực theo các cách sau đây:

1. Nếu là số ngẫu nhiên, khi đó bên nhận cần chắc chắn rằng nó giống hệt với số thách thức ngẫu nhiên được gửi tới bên được xác thực. Đối với việc tạo và sử dụng số ngẫu nhiên, tham khảo tiêu chuẩn ISO/IEC 18031.

2. Nếu là tem thời gian, bên nhận phải kiểm tra tính hợp lệ của tem thời gian đó.

3. Nếu là số tuần tự, khi đó bên nhận phải có khả năng so sánh nó với số tuần tự được nhận trước đó hoặc lưu trữ (các) số tuần tự để chắc rằng nó không được phát lại.

Các cơ chế xác thực có các yêu cầu sau đây. Nếu một trong những yêu cầu sau không được đáp ứng thì quá trình xác thực có thể bị tổn hại hoặc không thể thực hiện được.

a) Bên được xác thực chứng thực chính bản thân mình để bên xác thực sẽ chia sẻ khóa xác thực bí mật chung với bên xác thực kia, trong trường hợp các cơ chế quy định tại Điều 6 được áp dụng hoặc mỗi thực thể cần chia sẻ khóa xác thực bí mật với bên thứ ba tin cậy chung, trong trường hợp các cơ chế trong Điều 7 được áp dụng. Các khóa cần được biết bởi các bên liên quan trước khi bắt đầu bất kỳ diễn ra một cơ chế xác thực. Các phương pháp để đạt được điều này nằm ngoài phạm vi của tiêu chuẩn này. Hướng dẫn về quản lý chia sẻ khóa bí mật được cung cấp trong tiêu chuẩn ISO/IEC 11770-1 và ISO/IEC 11770-2.

b) Nếu bên thứ ba tin cậy tham gia, thì các cơ chế cần được tin tưởng bởi cả bên được xác thực và bên xác thực.

c) Khóa xác thực bí mật được chia sẻ bởi bên được xác thực và bên xác thực hoặc bởi một thực thể và một bên thứ ba tin cậy, cần được biết chỉ hai bên đó và có thể, các thực thể khác mà cả hai đều tin tưởng không sử dụng sai khóa, ví dụ sự giả mạo là một trong các bên tham gia.

CHÚ THÍCH Thuật toán mật mã và thời gian sử dụng khóa cần được chọn sao cho không khả thi về mặt tính toán với khóa được suy ra trong suốt chu kỳ sống của khóa đó. Ngoài ra thời gian sử dụng khóa cần được chọn để ngăn chặn tấng công biết bản rõ hoặc bản rõ được lựa chọn.

d) Các thẻ được sử dụng trong các cơ chế phải không thể giả được ngay cả biết những thông tin của thẻ cũ. Nói cách khác, thẻ cũ không thể tái sử dụng trong bất kỳ cách nào (một phần hoặc toàn bộ) để tạo thẻ mới. Đối với mỗi khóa bí mật K, hàm mã hóa e_K và hàm giải mã d_K tương ứng cần có các thuộc

tính sau. Quá trình giải mã d_K, khi áp dụng với một xâu $e_K(X)$ phải cho bên nhận xâu đó phát hiện giả mạo hay thay đổi dữ liệu, tức là chỉ bên sử dụng khóa bí mật đó mới có thể tạo ra xâu mà sẽ được "chấp nhận" được đưa ra trong quá trình giải mã d_K.

CHÚ THÍCH Trong thực tế, vấn đề này có thể đạt được bằng nhiều cách. Các phương pháp tiếp cận được khuyến nghị là sử dụng khóa bí mật K với kỹ thuật mã hóa được xác thực mà cung cấp cả bảo vệ bí mật và toàn vẹn, như được tiêu chuẩn hóa trong tiêu chuẩn ISO/IEC 19772.

e) Các cơ chế trong tiêu chuẩn này yêu cầu sử dụng các tham số biến thiên theo thời gian như tem thời gian, số tuần tự hoặc số ngẫu nhiên. Các thuộc tính các tham số này, đặc biệt là không tính đến chúng để lặp lại trong thời gian sử dụng của một khóa xác thực bí mật, rất quan trọng cho các cơ chế này. Để biết thêm thông tin xem Phụ lục B TCVN 11817-1.

f) Khóa xác thực bí mật trong việc thực hiện một trong số các cơ chế được đặc tả trong phần này của Bộ tiêu chuẩn này phải khác biệt với các khóa đã sử dụng cho bất kỳ mục đích khác.

g) Xâu dữ liệu đã được mã hóa tại các điểm khác nhau trong một cơ chế xác thực không được sắp xếp theo thứ tự vì vậy chúng có thể thay đổi lẫn nhau.

CHÚ THÍCH Điều này có thể được thực hiện bằng cách bao gồm các yếu tố trong mỗi xâu dữ liệu đã được mã hóa sau đây:

- Định danh đối tượng được đặc tả trong Phụ lục A, phần tiêu chuẩn ISO định danh cụ thể, phần số và cơ chế xác thực;

- Một hằng số xác định duy nhất một xâu đã được mã hóa trong một cơ chế. Hằng số này có thể được bỏ qua trong cơ chế chỉ có một xâu đã được mã hóa.

Người nhận xâu dữ liệu đã được mã hóa có thể kiểm tra định danh đối tượng và hằng số xác định vị trí ký trong cơ chế được kỳ vọng.

h) Trong các cơ chế được đặc tả trong Điều 7, người giữ khóa K_{AP} hoặc K_{BP} phải sử dụng theo cùng một cách, nghĩa là việc thực thi hoặc là như TTP P hoặc là như thực thể A (hoặc B). Nghĩa là không có thực thể nào hoạt động như một TTP trong một trường hợp một giao thức và hoạt động như A hoặc B trong trường hợp giao thức khác, và sử dụng chung một khóa cho cả hai trường hợp.

6 Cơ chế không liên quan đến bên thứ ba tin cậy

Trong các cơ chế này các thực thể A và B sẽ chia sẻ một khóa xác thực bí mật chung là K_{AB} và hai khóa bí mật một chiều K_{AB} và K_{BA} trước khi bắt đầu diễn ra bất kỳ một cơ chế xác thực. Trong các trường hợp sau khóa một chiều K_{AB} và K_{BA} được sử dụng tương ứng cho việc xác thực A bởi B và ngược lại.

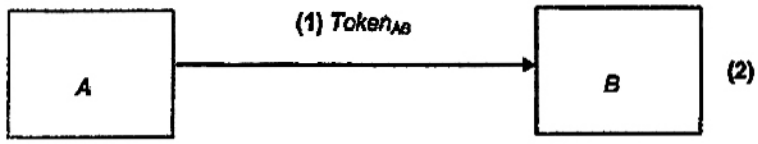
Tất cả các trường văn bản được quy định trong các cơ chế sau đây có sẵn để sử dụng trong các ứng dụng ngoài phạm vi của tiêu chuẩn này (chúng có thể rỗng). Mối quan hệ và nội dung phụ thuộc vào từng ứng dụng cụ thể. Xem Phụ lục B về thông tin sử dụng các trường văn bản.

6.1 Xác thực một chiều

Xác thực một chiều có nghĩa rằng chỉ một trong hai thực thể được xác thực bằng sử dụng cơ chế này.

6.1.1 Cơ chế 1 – Xác thực đơn chuyến

Trong cơ chế xác thực này bên được xác thực A khởi tạo quá trình và được xác thực bởi Bên xác thực B. Tính duy nhất/đúng lúc được kiểm soát bằng cách tạo ra và kiểm tra tem thời gian hoặc số tuần tự (Xem Phụ lục B TCVN 11817-1). Cơ chế này được minh họa trong Hình 1.



Hình 1: Cơ chế 1 – Xác thực đơn chuyến

Hình thức của thẻ ($Token_{AB}$), được gửi bởi Bên được xác thực *A* đến Bên xác thực *B* là:

$$Token_{AB} = Text_2 \,||\, e_{K_{AB}}(TN_A \,||\, I_B \,||\, Text_1)$$

Bên khiếu nại *A* sử dụng tham số biến thiên theo thời gian TN_A là tem thời gian T_A hoặc số tuần tự N_A. Sự lựa chọn phụ thuộc vào khả năng kỹ thuật của bên được xác thực và bên xác thực cũng như đối với môi trường.

Việc đưa định danh phân biệt I_B trong $Token_{AB}$ là tùy chọn.

CHÚ THÍCH Định danh phân biệt I_B bao gồm trong $Token_{AB}$ để ngăn chặn việc tái sử dụng $Token_{AB}$ trên thực thể A bởi một kẻ mạo danh như là thực thể *B*. Việc bao gồm này là tùy chọn do đó trong môi trường mà các kẻ tấn công không thể xảy ra, có thể được bỏ qua. Định danh phân biệt I_B có thể cũng được bỏ qua nếu khóa một chiều được sử dụng.

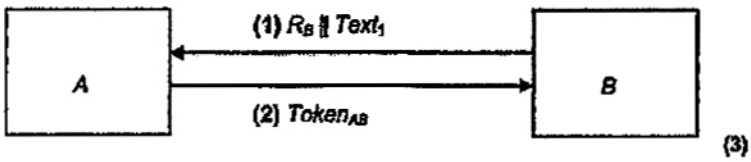
Sau đây là mô tả cơ chế 1 – Xác thực đơn chuyến.

(1) *A* tạo và gửi $Token_{AB}$ cho *B*

(2) Khi nhận được thông báo chứa $Token_{AB}$, *B* xác thực $Token_{AB}$ bằng giải mã phần mã (giải mã ngụ ý rằng đáp ứng các yêu cầu được đưa ra trong Điều 5 d) và sau đó kiểm tra tính đúng đắn của định danh phân biệt I_B, nếu có, cũng như tem thời gian hoặc số tuần tự.

6.1.2 Cơ chế 2 – Xác thực hai chuyến

Trong cơ chế này bên được xác thực *A* được xác thực bởi bên xác thực *B* để khởi tạo quá trình. Tính duy nhất/đúng lúc được kiểm soát bằng cách tạo ra và kiểm tra số ngẫu nhiên R_B (xem Phụ lục B TCVN 11817-1). Cơ chế xác thực được minh họa trong Hình 2.



Hình 2: Cơ chế 2 – Xác thực hai chuyến

Hình thức của thẻ ($Token_{AB}$), được gửi bởi Bên được xác thực *A* đến Bên xác thực *B* là:

$$Token_{AB} = Text_3 \,||\, e_{K_{AB}}(R_B \,||\, I_B \,||\, Text_2)$$

Việc đưa định danh phân biệt I_B trong $Token_{AB}$ là tùy chọn.

CHÚ THÍCH 1 Để ngăn chặn khả năng tấn công bản rõ được chọn, tức là tấn công phân tích mã trong đó người phân tích mã biết bản rõ hoàn chỉnh của một hay nhiều xâu bản mã, thực thể *A* có thể bao gồm số ngẫu nhiên R_A trong $Text_2$.

CHÚ THÍCH 2 Định danh phân biệt I_B được bao gồm trong $Token_{AB}$ để ngăn chặn bất kỳ bên nào sử dụng $Token_{AB}$ như $Token_{BA}$. Việc đưa định danh phân biệt I_B là tùy chọn do đó trong môi trường mà các cuộc tấn công không thể xảy ra thì có thể bỏ qua. Định danh phân biệt I_B có thể được bỏ qua nếu khóa một chiều được sử dụng.

Sau đây là mô tả cơ chế 2 – Xác thực hai chuyến.

(1) *B* tạo ra một số ngẫu nhiên R_B và gửi nó, tùy chọn, một trường văn bản $Text_1$ tới *A*.

(2) *A* tạo ra và gửi $Token_{AB}$ cho *B*.

(3) Khi nhận được thông báo có chứa $Token_{AB}$, *B* xác minh $Token_{AB}$ bằng cách giải mã phần mã (giải mã ngụ ý rằng đáp ứng các yêu cầu được đưa ra trong Điều 5 d) và kiểm tra tính đúng đắn của định danh phân biệt I_B, nếu có, và số ngẫu nhiên R_B, gửi đến *A* trong bước (1), đồng ý với số ngẫu nhiên chứa trong $Token_{AB}$.

6.2 Xác thực lẫn nhau

Xác thực lẫn nhau nghĩa là hai thực thể giao tiếp được chứng thực với nhau bằng cách sử dụng cơ chế này.

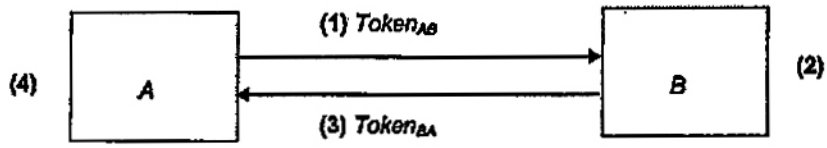
Hai cơ chế được mô tả trong Điều 6.1.1 và 6.1.2 là tương ứng tương thích trong Điều 6.2.1 và 6.2.2, để đạt được xác thực lẫn nhau. Trong cả hai trường hợp này đòi hỏi nhiều chuyến hơn và nhiều kết quả hơn trong hai bước tiếp.

CHÚ THÍCH Cơ chế xác thực thứ ba để xác thực lẫn nhau có thể được xây dựng từ hai trường hợp của cơ chế được quy định trong 6.1.2, một bắt đầu bởi thực thể *A* và một bắt đầu bởi thực thể *B*.

6.2.1 Cơ chế 3 – Xác thực hai chuyến

Trong cơ chế xác thực này tính duy nhất/đúng lúc được kiểm soát bằng cách tạo và kiểm tra tem thời gian hoặc số tuần tự (xem Phụ lục B TCVN 11817-1).

Cơ chế xác thực này được minh họa trong Hình 3.



Hình 3: Cơ chế 3 – Xác thực hai chuyến

Hình thức của thẻ ($Token_{AB}$), được gửi từ *A* đến *B*, là giống như quy định trong 6.1.1.

$$Token_{AB} = Text_2 \,||\, e_{K_{AB}} (TN_A \,||\, I_B \,||\, Text_1)$$

Hình thức của thẻ ($Token_{BA}$), được gửi từ *B* đến *A* là:

$$Token_{BA} = Text_4 \,||\, e_{K_{AB}} (TN_B \,||\, I_A \,||\, Text_3)$$

Việc đưa định danh phân biệt I_B trong $Token_{AB}$ và việc bao gồm định danh phân biệt I_A trong $Token_{BA}$ là (một cách độc lập) tùy chọn.

CHÚ THÍCH Định danh phân biệt I_B được bao gồm trong $Token_{AB}$ để ngăn chặn việc tái sử dụng $Token_{AB}$ trên thực thể *A* bởi kẻ tấn công giả mạo như là thực thể B. Với những lý do tương tự định danh phân biệt I_A có trong $Token_{BA}$. Việc bao gồm được

thực hiện tùy chọn do đó, trong các môi trường mà các cuộc tấn công như vậy không xảy ra, một hoặc cả hai có thể bỏ qua. Các định danh phân biệt I_A và I_B cũng có thể được bỏ qua nếu sử dụng khóa một chiều (xem bên dưới).

Sự lựa chọn việc sử dụng hoặc tem thời gian hoặc số tuần tự trong cơ chế này phụ thuộc vào khả năng của bên được xác thực và bên xác thực cũng như đối với môi trường.

Sau đây là mô tả cơ chế 3 - xác thực hai chuyến:

(1) *A* tạo ra và gửi $Token_{AB}$ cho *B*.

(2) Khi nhận được thông báo có chứa $Token_{AB}$, *B* xác minh $Token_{AB}$ bằng cách giải mã phần mã [giải mã ngụ ý rằng đáp ứng các yêu cầu được đưa ra trong Điều 5 d] và kiểm tra tính đúng đắn của định danh phân biệt I_B, nếu có, cũng như tem thời gian và số tuần tự.

(3) *B* tạo ra và gửi $Token_{BA}$ cho *A*.

(4) Thông báo trong bước (3) được xử lý một cách tương tự như trong bước (2) của 6.1.1.

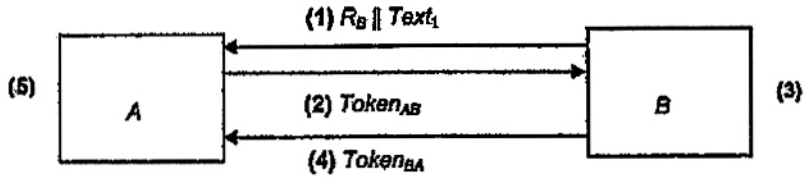
CHÚ THÍCH Hai thông báo của cơ chế này không bị ràng buộc với nhau trong bất kỳ cách nào, khác với hoàn toàn kịp thời gian; cơ chế này liên quan đến việc sử dụng độc lập cơ chế 6.1.1 hai lần. Hơn nữa ràng buộc với nhau của các thông báo có thể đạt được bằng cách sử dụng hợp lý các trường văn bản.

Nếu khóa một chiều được sử dụng khi đó khóa K_{AB} trong $Token_{BA}$ được thay thế bằng khóa một chiều K_{BA}, và các khóa thích hợp được sử dụng trong bước (4).

6.2.2 Cơ chế 4 - xác thực ba chuyến

Trong cơ chế xác thực này tính duy nhất/đúng lúc được kiểm soát bằng cách tạo và kiểm tra số ngẫu nhiên (xem Phụ lục B TCVN 11817-1).

Cơ chế xác thực này được minh họa trong Hình 4.



Hình 4 - Cơ chế 4 - xác thực ba chuyến

Các thẻ có dạng sau:

$$Token_{AB} = Text_3 \| e_{K_{AB}} (R_A \| R_B \| I_B \| Text_2)$$

$$Token_{BA} = Text_5 \| e_{K_{AB}} (R_B \| R_A \| Text_4)$$

Việc đưa định danh phân biệt I_B trong $Token_{AB}$ là tùy chọn.

CHÚ THÍCH Khi có mặt định danh phân biệt I_B được bao gồm trong $Token_{AB}$ để ngăn chặn tấn công phản xạ. Cuộc tấn công như vậy được đặc trưng bởi thực tế là một kẻ xâm nhập 'phản xạ' thách thức R_B đến *B* giả vờ là *A*. Sự bao gồm định danh phân biệt I_B là tùy chọn do đó, trong môi trường mà các cuộc tấn công như vậy không thể xảy ra, thì có thể bỏ qua. Định danh phân biệt I_B cũng có thể được bỏ qua nếu sử dụng khóa một chiều (xem bên dưới).

Sau đây là mô tả cơ chế 4 - xác thực ba chuyến:

(1) *B* tạo số ngẫu nhiên R_B và gửi nó, tùy chọn, trường văn bản $Text_1$ cho A.

(2) *A* tạo số ngẫu nhiên R_A, và tạo ra và gửi $Token_{AB}$ đến *B*.

(3) Khi nhận được thông báo có chứa $Token_{AB}$, *B* xác minh $Token_{AB}$ bằng cách giải mã phần mã (giải mã ngụ ý rằng đáp ứng các yêu cầu được đưa ra trong Điều 5d) và kiểm tra tính đúng đắn của định danh phân biệt I_B, nếu có, cũng số ngẫu nhiên R_B, được gửi đến *A* trong bước (1), đồng ý với số ngẫu nhiên được chứa trong $Token_{AB}$.

(4) *B* tạo ra và gửi $Token_{BA}$ đến *A*.

(3) Khi nhận được thông báo có chứa $Token_{BA}$, *A* xác minh $Token_{BA}$ bằng cách giải mã phần mã [giải mã ngụ ý rằng đáp ứng các yêu cầu được đưa ra trong Điều 5 d] và kiểm tra tính đúng đắn của định danh phân biệt I_B, nếu có, cũng số ngẫu nhiên R_B, được nhận từ *B* trong bước (1), đồng ý với số ngẫu nhiên được chứa trong $Token_{BA}$ và số ngẫu nhiên R_A, được gửi tới *B* trong bước (2), đồng ý với số ngẫu nhiên được chứa trong $Token_{BA}$.

Nếu khóa một chiều được sử dụng thì khóa K_{AB} trong $Token_{BA}$ được thay thế bằng khóa K_{BA} và khóa thích hợp được sử dụng trong bước (5).

7 Cơ chế liên quan đến bên thứ ba tin cậy

Cơ chế xác thực trong Điều này không sử dụng khóa bí mật được chia sẻ bởi hai thực thể trước quá trình xác thực. Tuy nhiên Cơ chế này sử dụng bên thứ ba tin cậy (ký hiệu là *P*) mà mỗi thực thể *A* và *B* chia sẻ khóa bí mật K_{AP} và K_{BP} tương ứng. Trong cả hai cơ chế một trong những thực thể yêu cầu khóa K_{AB} từ bên thứ ba tin cậy. Cơ chế này mô phỏng theo các cơ chế được mô tả trong 6.2.1 và 6.2.2 tương ứng.

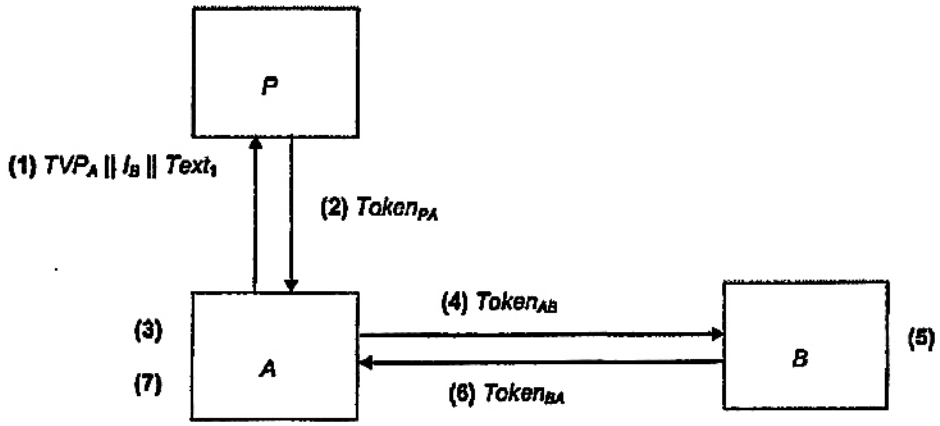
Như đã mô tả bên dưới các chuyến nhất định có thể bỏ qua ở mỗi cơ chế nếu yêu cầu chỉ xác thực một chiều.

Tất cả các trường văn bản được quy định trong các cơ chế sau đây có sẵn để sử dụng trong các ứng dụng nằm ngoài phạm vi của tiêu chuẩn này (chúng có thể rỗng). Mối quan hệ và nội dung phụ thuộc vào từng ứng dụng cụ thể. Xem Phụ lục B về thông tin sử dụng các trường văn bản.

7.1 Cơ chế 5 - xác thực bốn chuyến

Cơ chế này tương đương với cơ chế thiết lập khóa số 8 của tiêu chuẩn ISO/IEC 11770-2:2008.

Cơ chế xác thực này được minh họa trong Hình 5.



Hình 5 - Cơ chế số 4 - xác thực bốn chuyến

Hình thức của thẻ ($Token_{PA}$), được gửi từ *P* đến *A* là:

$$Token_{PA} = Text_4 \| e_{K_{AP}}(TVP_A \| K_{AB} \| I_B \| Text_3) \| e_{K_{BP}}(TN_P \| K_{AB} \| I_A \| Text_2)$$

Hình thức của thẻ ($Token_{AB}$), được gửi từ *A* đến *B* là:

$$Token_{AB} = Text_6 \| e_{K_{BP}}(TN_P \| K_{AB} \| I_A \| Text_2) \| e_{K_{AB}}(TN_A \| I_B \| Text_5)$$

Hình thức của thẻ ($Token_{BA}$), được gửi từ B đến A là:

$$Token_{BA} = Text_8 \| e_{K_{AB}}(TN_B \| I_A \| Text_7)$$

Sự lựa chọn việc sử dụng hoặc tem thời gian hoặc số tuần tự trong cơ chế này phụ thuộc vào khả năng của các thực thể cũng như đối với môi trường.

Việc sử dụng tham số biến thiên theo thời gian TVP_A trong các bước (1) đến (3) trong Hình 5 theo quy định dưới đây hơi khác so với sử dụng bình thường của nó. Nó cho phép *A* kết hợp thông báo đáp ứng (2) với thông báo yêu cầu (1). Các đặc tính quan trọng của tham số biến thiên theo thời gian ở đây là không lặp lại, để hạn chế việc tái sử dụng có thể của một $Token_{PA}$ được sử dụng trước đó.

CHÚ THÍCH Tham số biến thiên theo thời gian TVP_A có thể là số ngẫu nhiên. Tuy nhiên không giống như số ngẫu nhiên được sử dụng trong một số cơ chế trong tiêu chuẩn TCVN 11817, nó không cần thiết rằng TVP_A không thể đoán trước cho bên thứ ba và giá trị đếm không lặp sẽ thích hợp như nhau.

Sau đây là mô tả cơ chế số 5 - xác thực bốn chuyến:

(1) *A* tạo ra tham số biến thiên theo thời gian TVP_A, và gửi nó, định danh phân biệt I_B và, tùy chọn, trường văn bản $Text_1$ đến bên thứ ba tin cậy *P*.

(2) Bên thứ ba tin cậy *P* tạo và gửi $Token_{PA}$ cho *A*.

(3) Khi nhận được thông báo có chứa $Token_{PA}$, A xác minh $Token_{PA}$ bằng cách giải mã phần mã sử dụng K_{AP} (giải mã ngụ ý rằng đáp ứng các yêu cầu được đưa ra trong Điều 5 d) và kiểm tra tính đúng đắn của định danh phân biệt I_B và tham số biến thiên theo thời gian, được gửi từ *P* ở bước (1), đồng ý với tham số biến thiên theo thời gian chứa trong $Token_{PA}$. Ngoài ra, *A* nhận được khóa xác thực bí mật K_{AB}. *A* sau đó trích xuất.

$$e_{K_{BP}}(TN_P \| K_{AB} \| I_A \| Text_2)$$

từ $Token_{PA}$ và sử dụng nó để xây dựng $Token_{AB}$.

(4) *A* tạo ra và gửi cho *B* $Token_{AB}$.

(5) Khi nhận được thông báo có chứa $Token_{AB}$, *B* xác minh $Token_{AB}$ bằng cách giải mã phần mã [giải mã ngụ ý rằng đáp ứng các yêu cầu được đưa ra trong Điều 5 d)] và kiểm tra tính đúng đắn của định danh phân biệt I_A và I_B cũng như (các) tem thời gian hoặc (các) số tuần tự. Ngoài ra *B* nhận khóa xác thực bí mật K_{AB}.

(6) *B* tạo ra và gửi cho *A* $Token_{BA}$.

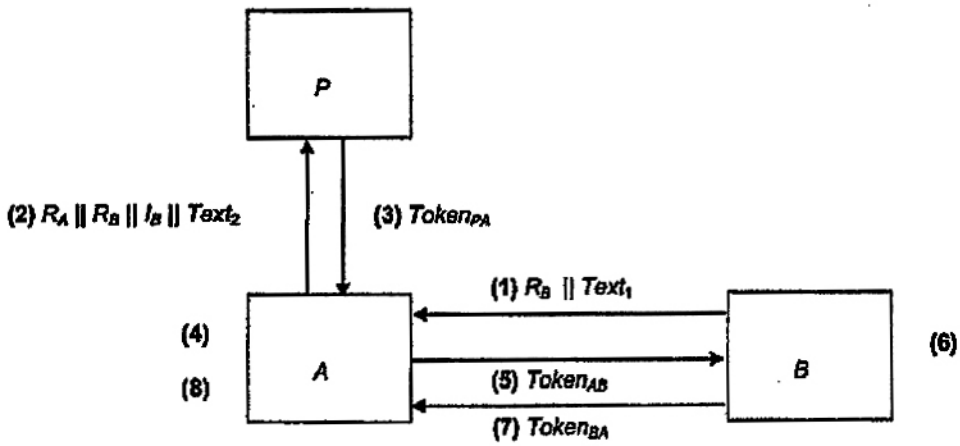
(7) Khi nhận được thông báo có chứa $Token_{BA}$, *A* xác minh $Token_{BA}$ bằng cách giải mã phần mã (giải mã ngụ ý rằng đáp ứng các yêu cầu được đưa ra trong Điều 5 d) và kiểm tra tính đúng đắn của định danh phân biệt I_A cũng như tem thời gian hoặc số tuần tự.

Các bước (6) và (7) có thể được bỏ qua nếu chỉ yêu cầu xác thực một chiều của *A* tới *B*.

7.2 Cơ chế 6 - xác thực năm chuyến

Trong cơ chế xác thực lẫn nhau này tính duy nhất/đúng lúc được kiểm soát bằng cách tạo và kiểm tra số ngẫu nhiên (xem Phụ lục B TCVN 11817-1). Cơ chế này tương đương với cơ chế thiết lập khóa số 9 của tiêu chuẩn ISO/IEC 11770-2.

Cơ chế xác thực này được minh họa trong Hình 6.



Hình 6 - Cơ chế 6 - xác thực năm chuyến

Hình thức của thẻ ($Token_{PA}$), được gửi từ *P* đến *A* là:

$$Token_{PA} = Text_5 \| e_{K_{AP}}(R_A \| K_{AB} \| I_B \| Text_4) \| e_{K_{BP}}(R_B \| K_{AB} \| I_A \| Text_3)$$

Hình thức của thẻ ($Token_{AB}$), được gửi từ *A* đến *B* là:

$$Token_{AB} = Text_7 \| e_{K_{BP}}(R_B \| K_{AB} \| I_A \| Text_3) \| e_{K_{AB}}(R'_A \| R_B \| Text_6)$$

Hình thức của thẻ ($Token_{BA}$), được gửi từ *B* đến *A* là:

$$Token_{BA} = Text_9 \| e_{K_{AB}}(R_B \| R'_A \| Text_8)$$

Sau đây là mô tả cơ chế số 6 - xác thực năm chuyến:

(1) *B* tạo số ngẫu nhiên R_B và gửi nó, tùy chọn, và trường văn bản $Text_1$ đến *A*.

(2) *A* tạo số ngẫu nhiên R_A và gửi nó, số ngẫu nhiên R_B, định danh phân biệt I_B và, tùy chọn, trường văn bản $Text_2$ đến bên thứ ba tin cậy *P*.

(3) Bên thứ ba tin cậy *P* tạo ra và gửi $Token_{PA}$ đến *A*.

(4) Khi nhận được thông báo có chứa $Token_{PA}$, *A* xác minh $Token_{PA}$ bằng cách giải mã phần mã sử dụng K_{AP} [giải mã ngụ ý rằng đáp ứng các yêu cầu được đưa ra trong Điều 5 d] và kiểm tra tính đúng đắn của định danh phân biệt I_B và số ngẫu nhiên R_A, được gửi tới *P* ở bước (2), đồng ý với số ngẫu nhiên chứa trong $Token_{PA}$. Ngoài ra, *A* nhận được khóa xác thực bí mật K_{AB}. *A* sau đó trích xuất.

$$e_{K_{BP}}(R_B \| K_{AB} \| I_A \| Text_3)$$

từ $Token_{PA}$ và sử dụng nó để xây dựng $Token_{AB}$.

(5) *A* tạo ra số ngẫu nhiên thứ hai R'_A và tạo ra và gửi $Token_{AB}$ đến *B*.

(6) Khi nhận được thông báo có chứa $Token_{AB}$, *B* xác minh $Token_{AB}$ bằng cách giải mã phần mã (giải mã ngụ ý rằng đáp ứng các yêu cầu được đưa ra trong Điều 5 d) và kiểm tra tính đúng đắn của định danh phân biệt I_A và số ngẫu nhiên R_B, được gửi tới *A* trong bước (1), đồng ý với hai bản sao được chứa trong $Token_{AB}$. Ngoài ra *B* lấy khóa xác thực bí mật K_{AB}.

(7) *B* tạo ra và gửi $Token_{BA}$ đến *A*.

(8) Khi nhận được thông báo có chứa $Token_{BA}$, *A* xác minh $Token_{BA}$ bằng cách giải mã phần mã (giải mã ngụ ý rằng đáp ứng các yêu cầu được đưa ra trong Điều 5 d) và kiểm tra số ngẫu nhiên R_B được nhận từ *B* trong bước (1), đồng ý với số ngẫu nhiên được chứa trong $Token_{BA}$ và số ngẫu nhiên R'_A, được gửi đến *B* trong bước (5), đồng ý với số ngẫu nhiên được chứa trong $Token_{BA}$.

Các bước (7) và (8) có thể được bỏ qua nếu chỉ yêu cầu xác thực một chiều của *A* tới *B*.

Phụ lục A
(Quy định)

OID và cú pháp ASN.1

A.1 Định nghĩa chính thức

```
EntityAuthenticationMechanisms-2 {

   iso(1) standard(0) e-auth-mechanisms(9798) part2(2)

      asn1-module(0) object-identifiers(0) }

   DEFINITIONS EXPLICIT TAGS ::= BEGIN
-- Xuất ra toàn bộ --
-- Nhập vào là None--
OID ::= OBJECT IDENTIFIER -- alias
-- Đồng bộ --
is9798-2 OID ::= { iso(1) standard(0) e-auth-mechanisms(9798) part2(2) }

mechanism OID ::= { is9798-2 mechanisms(1) }
-- Cơ chế xác thực đơn chuyến và xác thực lẫn nhau không có bên thứ 3
tin cậy --
ua-one-pass OID ::= { mechanism 1 }

ua-two-pass OID ::= { mechanism 2 }

ma-two-pass OID ::= { mechanism 3 }

ma-three-pass OID ::= { mechanism 4 }
-- Cơ chế xác thực lẫn nhau có bên thứ 3 tin cậy --
ttp-ma-four-pass OID ::= { mechanism 5 }

ttp-ma-five-pass OID ::= { mechanism 6 }

END -- EntityAuthenticationMechanisms-2 --
```

A.2 Sử dụng định danh đối tượng tiếp theo

Mỗi cơ chế xác thực thực thể sử dụng kỹ thuật mã hóa đối xứng. Do đó, định danh đối tượng của cơ chế xác thực thực thể có thể theo sau bởi một định danh đối tượng quy định cụ thể kỹ thuật mã hóa được sử dụng, ví dụ định danh cho một trong các cơ chế được quy định trong ISO/IEC 19772.

A.3 Ví dụ mã hóa phù hợp với quy tắc mã hóa cơ bản của ASN.1

Để phù hợp với tiêu chuẩn ISO/IEC 8825-1, định danh đối tượng bao gồm một hoặc nhiều bộ tám. Mỗi dãy mã hóa một số.

- Bit 8 (bit có trọng số cao nhất) được thiết lập bằng 0 trong bộ tám cuối cùng của một dãy và một trong bộ tám trước đó, nếu có nhiều hơn một bộ tám.

- Nối các bit 7 đến 1 của bộ tám của một dãy mã hóa một số. Mỗi số cần mã hóa bằng cách sử dụng các bộ tám ít nhất có thể, bộ tám '80' là không hợp lệ ở vị trí đầu tiên của một dãy.

- Số đầu tiên của số tiêu chuẩn; số thứ hai, nếu có, là một phần trong tiêu chuẩn gồm nhiều phần.

Một định danh đối tượng có thể tham chiếu tới bất kỳ cơ chế nào được định nghĩa trong tiêu chuẩn này.

- Để xác định một tiêu chuẩn ISO, bộ tám đầu tiên được thiết lập là '28', tức là 40 theo hệ thập phân (xem ISO/IEC 8825-1).

- Hai bộ tám tiếp theo được thiết lập bằng 'CC46'. 9798 bằng '2646' trong hệ thập lục phân, tức là 0010 0110 0100 0110, tức là hai khối của bảy bit 1001100 1000110. Sau khi chèn các giá trị thích hợp của 8 bit trong mỗi bộ tám, việc mã hóa dãy đó là 11001100 01000110, tức là 'CC46'.

- Các bộ tám tiếp theo được thiết lập bằng '02' để xác định phần 2.

- Các bộ tám tiếp theo định danh một cơ chế xác thực.

- '01' định danh cơ chế xác thực một chiều đơn chuyển không liên quan đến bên thứ ba tin cậy.

- '02' định danh cơ chế xác thực một chiều hai chuyển không liên quan đến bên thứ ba tin cậy.

- '03' định danh cơ chế xác thực lẫn nhau hai chuyển không liên quan đến bên thứ ba tin cậy.

- '04' định danh cơ chế xác thực lẫn nhau ba chuyển không liên quan đến bên thứ ba tin cậy.

- '05' định danh cơ chế xác thực lẫn nhau bốn chuyển liên quan đến bên thứ ba tin cậy.

- '06' định danh cơ chế xác thực lẫn nhau năm chuyển liên quan đến bên thứ ba tin cậy.

Ví DỤ các phần tử '28 CC 46 02 05' đọc {tiêu chuẩn iso 9798 2 5}, tức là cơ chế thứ năm trong tiêu chuẩn này, tức là cơ chế xác thực lẫn nhau bốn chuyển liên quan đến bên thứ ba tin cậy. Phần tử dữ liệu có thể được chuyển tải trong đối tượng dữ liệu BER-TLV sau đây (xem các quy tắc mã hóa cơ bản của ASN.1, ISO/IEC 8825-1, thẻ lớp toàn cầu '06') nơi các dấu gạch ngang và dấu ngoặc nhọn không quan trọng và được chèn vào chỉ cho rõ ràng.

Đối tượng dữ liệu = {'06'-'05'-'28 CC 46 02 05'}

Phụ lục B
(Tham khảo)

Sử dụng trường văn bản

Thẻ được quy định trong Điều 6 và Điều 7 của tiêu chuẩn này chứa các trường văn bản. Việc sử dụng thực tế và mối quan hệ giữa các trường văn bản khác nhau trong một chuyến cho trước phụ thuộc vào ứng dụng. Một ví dụ được đưa ra dưới đây; xem thêm Phụ lục A TCVN 11817-1.

- Bất kỳ thông tin cần bảo mật hoặc chứng thực nguồn gốc nên cần đặt ở phần được mã hóa của thẻ.

Phụ lục C
(Tham khảo)

Tính chất của các cơ chế xác thực thực thể

Bảng C.1 tóm tắt các thuộc tính chính của các cơ chế xác thực thực thể được quy định trong tiêu chuẩn này. Các tùy chọn được hiển thị trong dấu ngoặc, ví dụ cơ chế số 5 có một tùy chọn phiên bản ba chuyến của giao thức để đạt được xác thực một chiều.

Bảng C.1 - Tính chất của các cơ chế

Cơ chế	1	2	3	4	5	6
Số chuyến	1	2	2	3	4 (hoặc tùy chọn 3)	5 (hoặc tùy chọn 4)
Một chiều/Lẫn nhau giữa bên xác thực và bên được xác thực	Một chiều	Một chiều	Lẫn nhau	Lẫn nhau	Lẫn nhau (Một chiều)	Lẫn nhau (Một chiều)
(Các) biến đảm bảo tính chất mới (CHÚ THÍCH 1)	TN_A	R_B	TN_A và TN_B	R_A và R_B	TVP_A, TN_B và TN_P	R_A và R_B
Thực thể khởi tạo cơ chế (xác thực)	*A*	*B*	*A*	*B*	*A*	*B*
Bên được xác thực biết được thành công	Không	Không	Chỉ cho *A*	Chỉ cho *A*	Chỉ cho *A*	Chỉ cho A

Các chú thích sau được áp dụng cho bảng trên:

CHÚ THÍCH 1 Đối với cơ chế số 2, 4 và 6 sử dụng (các) số ngẫu nhiên để đảm bảo tính chất mới thì không cần thiết để duy trì hoặc đồng hồ đồng bộ hoặc số tuần tự giữa hai thực thể.

CHÚ THÍCH 2 Trong cơ chế xác thực được mô tả trong tiêu chuẩn này bên được xác thực gửi bằng chứng nhận dạng trong hình thức của thẻ được mã hóa. Trong một số trường hợp không có đáp ứng từ các thực thể khác chỉ ra rằng các bằng chứng được chấp nhận thành công. Hàng cuối cùng trong Bảng C.1 chỉ ra nơi mà các giao thức vốn đảm bảo thông tin xác thực thành công. Trong tất cả các trường hợp khác, nếu cần thiết hệ thống đã cung cấp thông tin về thành công.

Thư mục tài liệu tham khảo

[1] ISO/IEC 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

[2] ISO/IEC 9797-1:1999, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

[3] ISO/IEC 9798-5:2004, *Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques*

[4] ISO/IEC 10116:2006, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

[5] ISO/IEC 11770-1, *Information technology — Security techniques — Key management — Part 1: Framework*

[6] ISO/IEC 11770-2:2008, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*

[7] ISO/IEC 18014-1:2008, *Information technology — Security techniques — Time-stamping services — Part 1: Framework*

[8] ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

[9] ISO/IEC 19772:—[2)], *Information technology — Security techniques — Authenticated encryption*

[10] D. Basin, C. Cremers and S. Meier, 'Provably repairing the ISO/IEC 9798 standard for entity authentication'. In: P. Degano, J. D. Guttman (eds.), Principles of Security abd Trust – First International Conferencw, POST 2012, Tallinn, Esstinia, March 24 - April 1, 2012, Proceedings Springer LNCS 7215, pp.129-148, 2012