TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN ISO 9735-6 : 2004

ISO 9735-6 : 2002

Xuất bản lần 1

TRAO ĐỔI DỮ LIỆU ĐIỆN TỬ TRONG QUẢN LÝ HÀNH CHÍNH, THƯƠNG MẠI VÀ VẬN TẢI (EDIFACT) - CÁC QUY TẮC CÚ PHÁP MỨC ỨNG DỤNG (SỐ HIỆU PHIÊN BẢN CÚ PHÁP: 4, SỐ HIỆU PHÁT HÀNH CÚ PHÁP: 1) - PHẦN 6: THÔNG ĐIỆP XÁC THỰC VÀ BÁO NHẬN AN NINH (KIỂU THÔNG ĐIỆP - AUTACK)

Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules (Syntax version number: 4, Syntax release number: 1)

Part 6: Secure authentication and acknowledgement message (message type - AUTACK)

HÀ NỘI - 2008

Mục lục

Lời giới thiệu **5**

1 Phạm vi áp dụng **7**

2 Sự phù hợp **7**

3 Tiêu chuẩn viện dẫn **8**

4 Thuật ngữ và định nghĩa **8**

5 Quy tắc sử dụng thông điệp xác thực và báo nhận an ninh **8**

5.1 Định nghĩa hàm 8
5.2 Phạm vi áp dụng 8
5.3 Nguyên tắc 9
5.3.1 Khái quát 9
5.3.2 Sử dụng AUTACK cho chức năng xác thực 10
5.3.3 Sử dụng AUTACK cho chức năng báo nhận 10
5.4 Định nghĩa thông điệp 11
5.4.1 Giải thích đoạn dữ liệu 11
5.4.2 Cấu trúc thông điệp 15

Phụ lục A (tham khảo) **Ví dụ minh họa về thông điệp AUTACK** **16**

A.1 Giới thiệu 16
A.2 Ví dụ 1: Dịch vụ không-từ chối gốc được cung cấp bởi một thông điệp AUTACK 16
A.2.1 Tình huống 16
A.2.2 Chi tiết an ninh 17
A.3 Ví dụ 2: Đảm bảo an ninh cho một số thông điệp với AUTACK 20
A.3.1 Tình huống 20
A.3.2 Chi tiết an ninh 21
A.4 Ví dụ 3: Báo nhận an ninh của một thông điệp nhận được bởi AUTACK 25
A.4.1 Tình huống 25

Phụ lục B (tham khảo) **Dịch vụ và thuật toán an ninh** **30**

B.1 Mục đích và phạm vi áp dụng 30
B.2 Tổ hợp sử dụng các thuật toán đối xứng và AUTACK cho thực thể được tham chiếu 31
B.3 Tổ hợp sử dụng các khóa không đối xứng và AUTACK cho thực thể được tham chiếu 33
B.4 Tổ hợp sử dụng AUTACK cho báo nhận 36

Tài liệu tham khảo ..... Error! Bookmark not defined.

Lời nói đầu

TCVN ISO 9735-6 : 2004 hoàn toàn tương đương với **ISO 9735-6 : 2002**;

TCVN ISO 9735-6 : 2004 do Ban kỹ thuật tiêu chuẩn TCVN/TC 154 *Quá trình, các yếu tố dữ liệu và tài liệu trong thương mại, công nghiệp và hành chính* biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ ban hành.

Tiêu chuẩn này được chuyển đổi năm 2008 từ Tiêu chuẩn Việt Nam cùng số hiệu thành Tiêu chuẩn Quốc gia theo quy định tại khoản 1 Điều 69 của Luật Tiêu chuẩn và Quy chuẩn kỹ thuật và điểm a khoản 1 Điều 6 Nghị định số 127/2007/NĐ-CP ngày 1/8/2007 của Chính phủ quy định chi tiết thi hành một số điều của Luật Tiêu chuẩn và Quy chuẩn kỹ thuật.

Lời giới thiệu

Bộ tiêu chuẩn TCVN ISO 9735 gồm những phần sau, với tiêu đề chung "Trao đổi dữ liệu điện tử trong quản lý hành chính, thương mại và vận tải (EDIFACT) - Các quy tắc mức ứng dụng (Số hiệu phiên bản cú pháp: 4, Số hiệu phát hành cú pháp: 1)":

- Phần 1: Quy tắc cú pháp chung
- Phần 2: Quy tắc cú pháp đặc trưng cho EDI lô
- Phần 3: Quy tắc cú pháp đặc trưng cho EDI tương tác
- Phần 4: Thông điệp báo cáo dịch vụ và cú pháp cho EDI lô (Kiểu thông điệp - CONTRL)
- Phần 5: Quy tắc bảo mật cho EDI lô (tính xác thực, tính toàn vẹn và thừa nhận nguồn gốc)
- Phần 6: Thông điệp báo nhận và xác thực bảo mật (Kiểu thông điệp - AUTACK)
- Phần 7: Quy tắc bảo mật cho EDI lô (tính bảo mật)
- Phần 8: Dữ liệu kết hợp trong EDI
- Phần 9: Thông điệp quản lý chứng nhận và khoá bảo mật (Kiểu thông điệp KEYMAN)
- Phần 10: Danh mục cú pháp dịch vụ.

Các phụ lục A, B, C trong tiêu chuẩn này chỉ để tham khảo.

Trao đổi dữ liệu điện tử trong quản lý hành chính, thương mại và vận tải (EDIFACT) - Các quy tắc cú pháp mức ứng dụng (Số hiệu phiên bản cú pháp: 4, Số hiệu phát hành cú pháp: 1) -

Phần 6: Thông điệp xác thực và báo nhận an ninh (Kiểu thông điệp - AUTACK)

Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules(Syntax version number:4, Syntax release number: 1)-

Part 6: Secure authentication and acknowledgement message (message type - AUTACK)

1 Phạm vi áp dụng

Tiêu chuẩn này áp dụng cho an ninh EDIFACT, xác định thông điệp xác thực và báo nhận an ninh (AUTACK).

2 Sự phù hợp

Do tiêu chuẩn này sử dụng số hiệu phiên bản "4'' trong phần tử dữ liệu bắt buộc 0002 (*số hiệu phiên bản cú pháp*), và sử dụng số hiệu phát hành "01" trong phần tử dữ liệu điều kiện 0076 (*số hiệu phát hành cú pháp*), mỗi số hiệu đều xuất hiện trong đoạn UNB *(tiêu đề trao đổi)*, nên các trao đổi vẫn sử dụng cú pháp đã định nghĩa trong các phiên bản trước, phải sử dụng các số hiệu phiên bản cú pháp sau đây, để phân biệt chúng với nhau và với tiêu chuẩn này:

- ISO 9735: 1988: *Số hiệu phiên bản cú pháp: 1*
- ISO 9735: 1988 (Bổ sung và in lại năm 1990): *Số hiệu phiên bản cú pháp: 2*
- ISO 9735: 1988 và Bổ sung 1 :1992: *Số hiệu phiên bản cú pháp: 3*
- ISO 9735: 1998: *Số hiệu phiên bản cú pháp: 4*

Sự phù hợp với một tiêu chuẩn có nghĩa là tất cả mọi yêu cầu, bao gồm cả các lựa chọn phải được hỗ trợ. Nếu tất cả các lựa chọn không được hỗ trợ thì phải công bố rõ các lựa chọn nào là phù hợp. Dữ liệu được trao đổi là phù hợp nếu cấu trúc và biểu diễn dữ liệu đó phù hợp với các quy tắc cú pháp được quy định trong tiêu chuẩn này.

Các thiết bị hỗ trợ tiêu chuẩn này là phù hợp khi chúng có thể tạo và/hoặc thông dịch dữ liệu được cấu trúc và trình bày phù hợp với tiêu chuẩn này.

Sự phù hợp với tiêu chuẩn này bao gồm sự phù hợp với TCVN ISO 9735-1, TCVN ISO 9735-2 và TCVN ISO 9735-10 .

Khi được định danh trong tiêu chuẩn này, các điều khoản được định nghĩa trong các tiêu chuẩn liên quan tạo thành bộ tiêu chuẩn phù hợp.

3 Tiêu chuẩn viện dẫn

- TCVN ISO 9735-1: 2003, Trao đổi dữ liệu điện tử trong quản lý hành chính, thương mại và vận tải (EDIFACT) - quy tắc cú pháp mức áp dụng (Số hiệu phiên bản cú pháp: 4, Số hiệu phát hành cú pháp: 1) - Phần 1: Quy tắc cú pháp chung.
- TCVN ISO 9735-2: 2003, Trao đổi dữ liệu điện tử trong quản lý hành chính, thương mại và vận tải (EDIFACT) - quy tắc cú pháp mức áp dụng (Số hiệu phiên bản cú pháp: 4, số hiệu phát hành cú pháp: 1) - Phần 2: Quy tắc cú pháp đặc trưng cho EDI Lô.
- TCVN ISO 9735-5, Trao đổi dữ liệu điện tử trong quản lý hành chính, thương mại và vận tải (EDIFACT) - quy tắc cú pháp mức áp dụng (Số hiệu phiên bản cú pháp: 4, Số hiệu phát hành cú pháp: 1) - Phần 5: Quy tắc an ninh cho EDI Lô (tính xác thực, tính toàn vẹn và không-từ chối gốc).
- TCVN ISO 9735-10, Trao đổi dữ liệu điện tử trong quản lý hành chính, thương mại và vận tải (EDIFACT)- quy tắc cú pháp mức áp dụng (Số hiệu phiên bản cú pháp: 4, Số hiệu phát hành cú pháp: 1). Phần 10: Danh mục cú pháp dịch vụ.

4 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong TCVN ISO 9735-1.

5 Quy tắc sử dụng thông điệp xác thực và báo nhận an ninh

5.1 Định nghĩa hàm

AUTACK là một thông điệp xác thực gửi đi, hoặc cung cấp việc báo nhận an ninh của trao đổi, nhóm, thông điệp hoặc các gói nhận được.

Một thông điệp xác thực và báo nhận an ninh có thể được sử dụng để:

a) cung cấp dịch vụ xác thực an ninh, tính toàn vẹn hoặc không-từ chối gốc cho thông điệp, gói, nhóm hoặc trao đổi;

b) cung cấp dịch vụ báo nhận an ninh hoặc không-từ chối nhận của bên nhận để bảo vệ thông điệp, gói, nhóm hoặc trao đổi.

5.2 Phạm vi áp dụng

Thông điệp xác thực và báo nhận an ninh (AUTACK) được sử dụng cho cả trao đổi mậu dịch nội địa và quốc tế. Thông điệp này dựa trên cơ sở thực tiễn chung liên quan đến quản lý hành chính, thương mại và vận tải, không phụ thuộc vào loại hình kinh doanh hoặc ngành công nghiệp.

5.3 Nguyên tắc

5.3.1 Khái quát

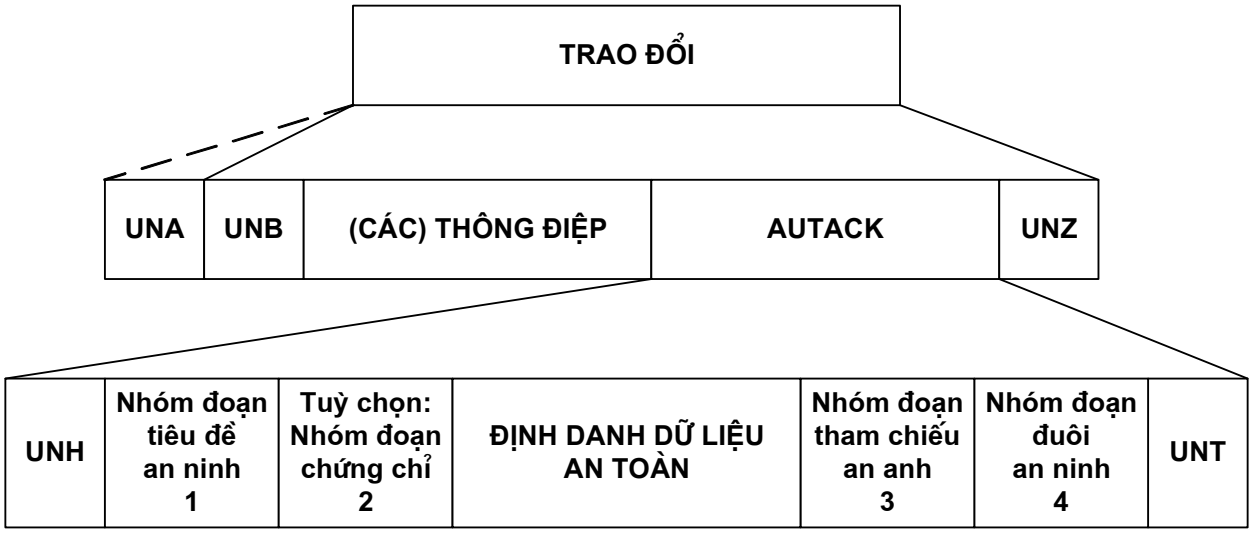
Các thủ tục an ninh được áp dụng phải được đồng thuận bởi các bên giao dịch và được quy định trong một thoả thuận trao đổi.

Thông điệp xác thực và báo nhận an ninh (AUTACK) áp dụng các dịch vụ an ninh cho cấu trúc EDIFACT khác (thông điệp, gói, nhóm, hoặc trao đổi) và cung cấp báo nhận an ninh để bảo vệ cho cấu trúc EDIFACT. Có thể áp dụng thông điệp AUTACK cho tổ hợp cấu trúc EDIFACT cần được bảo vệ giữa hai đối tác.

Cơ chế mật mã hóa cung cấp các dịch vụ an ninh áp dụng cho nội dung cấu trúc EDIFACT gốc. Kết quả của cơ chế này tạo nên thân thông điệp AUTACK, bổ sung bởi dữ liệu liên quan như tham chiếu của phương pháp mật mã hóa được sử dụng, số hiệu tham chiếu cho cấu trúc EDIFACT, ngày tháng và thời gian của cấu trúc gốc.

Thông điệp AUTACK phải sử dụng nhóm tiêu đề và đuôi an ninh tiêu chuẩn.

Thông điệp AUTACK có thể áp dụng cho một hoặc nhiều thông điệp, gói hoặc nhóm từ một hoặc nhiều trao đổi tới một hoặc nhiều trao đổi. Ví dụ, hình 1 mô tả một trao đổi sử dụng thông điệp AUTACK cùng với một hoặc nhiều thông điệp.



Hình 1 - Trao đổi với an ninh có sử dụng thông điệp AUTACK tại mức thông điệp (biểu đồ)

5.3.2 Sử dụng AUTACK cho chức năng xác thực

5.3.2.1 Khái quát

Thông điệp AUTACK được sử dụng như một thông điệp xác thực phải được gửi bởi bên khởi tạo một hoặc nhiều cấu trúc EDIFACT khác, hoặc bởi một bên có quyền đại diện cho bên khởi tạo đó. Mục đích của thông điệp AUTACK là tạo thuận lợi cho các dịch vụ an ninh được xác định trong TCVN ISO 9735-5, như tính xác thực, tính toàn vẹn và không-từ chối gốc của cấu trúc EDIFACT kết hợp với thông điệp này.

Thông điệp xác thực AUTACK có thể thực hiện theo hai cách. Cách thứ nhất là truyền các giá trị băm của cấu trúc EDIFACT tham chiếu được bảo vệ bởi chính thông điệp AUTACK; cách thứ hai là chỉ sử dụng AUTACK để truyền các chữ ký số của cấu trúc EDIFACT được tham chiếu.

5.3.2.2 Xác thực có sử dụng các giá trị băm của cấu trúc EDIFACT được tham chiếu

Cấu trúc EDIFACT được bảo vệ phải được tham chiếu trong một lần xuất hiện của đoạn USX (tham chiếu an ninh). Mỗi USX đó phải tương ứng ít nhất một đoạn USY (an ninh trên tham chiếu), đoạn này bao gồm kết quả an ninh, ví dụ giá trị băm của chức năng an ninh được thực hiện trên cấu trúc EDIFACT được tham chiếu.

Chi tiết về chức năng an ninh được thực hiện phải được chứa trong nhóm tiêu đề an ninh AUTACK. Đối với cấu trúc EDIFACT được tham chiếu phải được liên kết bằng cách sử dụng các phần tử dữ liệu số hiệu tham chiếu trong cả hai đoạn USY và USH.

Bước cuối cùng, tất cả thông tin được truyền trong AUTACK phải được bảo vệ bằng cách sử dụng ít nhất một cặp nhóm tiêu đề và đuôi an ninh.

CHÚ THÍCH AUTACK sử dụng đoạn USX tham chiếu tới một hoặc nhiều thông điệp, gói hoặc nhóm trong một hoặc nhiều trao đổi, hoặc tham chiếu tới một trao đổi hoàn chỉnh. Đối với mỗi đoạn USX tương ứng một đoạn USY bao gồm kết quả của phương pháp băm, tính xác thực hoặc không-từ chối nhận áp dụng cho cấu trúc EDIFACT được tham chiếu.

5.3.2.3 Xác thực có sử dụng các chữ ký số của cấu trúc EDIFACT được tham chiếu

Cấu trúc EDIFACT được bảo vệ phải được tham chiếu trong một lần xuất hiện của đoạn USX (tham chiếu an ninh), Đối với mỗi USX tương ứng với ít nhất một đoạn USY (an ninh trên tham chiếu) phải được đưa ra, đoạn này bao gồm chữ ký số của cấu trúc EDIFACT được tham chiếu. Chi tiết về chức năng an ninh đã được phải có trong nhóm tiêu đề an ninh AUTACK. Bởi vì một cấu trúc EDIFACT được tham chiếu đơn được bảo vệ nhiều hơn một lần, nên USY và nhóm tiêu đề liên quan phải được liên kết bằng cách sử dụng các phần tử dữ liệu số hiệu tham chiếu an ninh trong cả hai đoạn.

Nếu chữ ký số của cấu trúc EDIFACT tham chiếu được chứa trong AUTACK (đúng hơn là một giá trị băm), thì bản thân AUTACK không yêu cầu được bảo vệ.

5.3.3 Sử dụng AUTACK cho chức năng báo nhận

Một thông điệp AUTACK sử dụng như một thông điệp báo nhận phải được gửi bởi bên nhận của một hay nhiều cấu trúc EDIFACT được nhận một cách an toàn trước đó, hoặc bởi một bên có quyền đại diện cho bên nhận. Mục đích là để tạo thuận lợi cho việc xác nhận việc nhận, xác nhận tính hợp lệ của sự

toàn vẹn về nội dung, xác nhận tính hợp lệ của sự hoàn chỉnh và/hoặc không-từ chối nhận của bên nhận cấu trúc EDIFACT liên kết.

Chức năng báo nhận chỉ áp dụng cho cấu trúc EDIFACT được bảo vệ. Cấu trúc EDIFACT được bảo vệ phải được tham chiếu trong một lần xuất hiện của đoạn USX (tham chiếu an ninh). Mỗi USX đó phải tương ứng ít nhất một đoạn USY (an ninh trên tham chiếu), đoạn này bao gồm hoặc giá trị băm hoặc chữ ký số của cấu trúc EDIFACT được tham chiếu. USY phải được liên kết với nhóm tiêu đề an ninh của cấu trúc EDIFACT được tham chiếu, hoặc của thông điệp AUTACK bảo vệ, bằng cách sử dụng phần tử dữ liệu số hiệu tham chiếu an ninh. Tiêu đề an ninh tương ứng liên quan đến cấu trúc EDIFACT được tham chiếu bao gồm chi tiết về chức năng an ninh được thực hiện trên cấu trúc EDIFACT tham chiếu.

Bước cuối cùng trong giai đoạn tạo thông điệp báo nhận, tất cả thông tin được truyền trong AUTACK phải được bảo vệ bằng cách sử dụng ít nhất một cặp nhóm tiêu đề và đuôi an ninh.

AUTACK cũng được sử dụng cho việc không-báo nhận trong trường hợp có vấn đề về việc xác minh các kết quả an ninh.

CHÚ THÍCH Báo nhận an ninh chỉ có nghĩa đối với cấu trúc EDIFACT được bảo vệ. Bảo vệ cấu trúc EDIFACT được thực hiện nhờ sử dụng các đoạn an ninh tích hợp (xem TCVN ISO 9735-5) hoặc xác thực AUTACK.

Để tránh vòng lặp vô hạn, một AUTACK được sử dụng cho chức năng báo nhận an ninh không yêu cầu bên nhận gửi trở lại một thông điệp báo nhận AUTACK.

5.4 Định nghĩa thông điệp

5.4.1 Giải thích đoạn dữ liệu

0010 **UNH, tiêu đề thông điệp**

Đoạn dịch vụ bắt đầu và xác định duy nhất một thông điệp.

Mã kiểu thông điệp cho thông điệp xác thực và báo nhận an ninh là AUTACK.

Định danh chức năng phụ của loại thông điệp phần tử dữ liệu được sử dụng để chỉ rõ cách sử dụng chức năng AUTACK là hoặc xác thực, báo nhận hoặc từ chối báo nhận.

Thông điệp xác thực và báo nhận an ninh phù hợp với tiêu chuẩn này phải gồm dữ liệu sau trong đoạn UNH, phần tử dữ liệu hỗn hợp S009:

Phần tử dữ liệu	0065	AUTACK
	0052	4
	0054	1
	0051	UN

0020 **Nhóm đoạn 1: USH - USA - SG2 (nhóm tiêu đề an ninh)**

Nhóm đoạn xác định dịch vụ an ninh và các cơ chế an ninh được áp dụng và gồm dữ liệu cần thiết để tiến hành các tính toán hợp lý (xem TCVN ISO 9735-5).

Nhóm đoạn này phải quy định dịch vụ và (các) thuật toán an ninh được áp dụng cho thông điệp AUTACK hoặc cho cấu trúc EDIFACT được tham chiếu.

Mỗi nhóm tiêu đề an ninh phải được liên kết với một nhóm đuôi an ninh và vài nhóm có thể được liên kết bổ sung với các đoạn USY.

0030 **USH, Tiêu đề an ninh**

Đoạn quy định một dịch vụ an ninh được áp dụng cho thông điệp/gói chứa đoạn đó hoặc áp dụng cho cấu trúc EDIFACT được tham chiếu (xem TCVN ISO 9735-5).

Phần tử dữ liệu dịch vụ an ninh phải quy định chức năng an ninh áp dụng cho thông điệp AUTACK hoặc cấu trúc EDIFACT được tham chiếu:

- các dịch vụ an ninh: xác thực gốc hoặc không-từ chối gốc thông điệp chỉ được sử dụng cho chính thông điệp AUTACK này;
- các dịch vụ an ninh: tính toàn vẹn, xác thực gốc và không-từ chối gốc cấu trúc EDIFACT được tham chiếu chỉ được bên gửi sử dụng để bảo vệ cấu trúc EDIFACT được tham chiếu của AUTACK;
- các dịch vụ an ninh: xác thực nhận và không-từ chối nhận chỉ được sử dụng bởi bên nhận cấu trúc EDIFACT đã được bảo vệ để bảo vệ việc báo nhận.

Phạm vi áp dụng dịch vụ an ninh phải được quy định như trong TCVN ISO 9735-5. Trong một thông điệp AUTACK, có bốn phạm vi áp dụng an ninh:

- hai phạm vi đầu tiên được định nghĩa trong mục 5 của TCVN ISO 9735-5;
- phạm vi thứ ba gồm toàn bộ cấu trúc EDIFACT, trong đó, phạm vi áp dụng an ninh là từ ký tự đầu tiên của thông điệp, gói, nhóm hoặc trao đổi được tham chiếu (ký tự "U") tới ký tự cuối cùng của thông điệp, gói, nhóm hoặc trao đổi đó;
- phạm vi thứ tư do người sử dụng xác định, phạm vi áp dụng an ninh này được quy định trong thoả thuận giữa bên gửi và bên nhận.

0040 **USA, thuật toán an ninh**

Đoạn xác định một thuật toán an ninh, kỹ thuật sử dụng và gồm cả các tham số kỹ thuật được yêu cầu (xem TCVN ISO 9735-5).

0050 **Nhóm đoạn 2: USC - USA - USR (nhóm chứng chỉ)**

Nhóm đoạn chứa dữ liệu cần thiết để xác minh tính hợp lệ của các phương pháp an ninh được áp dụng cho thông điệp/gói, khi sử dụng các thuật toán đối xứng (xem TCVN ISO 9735-5).

0060 **USC, chứng chỉ**

Đoạn chứa các thông tin về bên sở hữu chứng chỉ và xác định tổ chức chứng nhận đã phát hành chứng chỉ đó (xem TCVN ISO 9735-5).

0070 **USA, thuật toán an ninh**

Đoạn xác định một thuật toán an ninh, kỹ thuật sử dụng và bao gồm các tham số kỹ thuật được yêu cầu (xem TCVN ISO 9735-5).

0080 **USR, kết quả an ninh**

Đoạn chứa kết quả của chức năng an ninh được tổ chức chứng nhận áp dụng cho chứng chỉ (xem TCVN ISO 9735-5).

0090 **USB, định danh dữ liệu an toàn**

Đoạn gồm định danh của bên gửi và bên nhận trao đổi, thẻ thời gian an ninh liên quan của AUTACK và AUTACK phải quy định là có yêu cầu báo nhận an ninh từ bên nhận thông điệp AUTACK hay không. Nếu có yêu cầu, bên gửi thông điệp sẽ đợi một thông điệp báo nhận AUTACK gửi trở lại từ bên nhận thông điệp.

Bên gửi trao đổi và bên nhận trao đổi trong USB phải đề cập đến bên gửi và bên nhận trao đổi đoạn có chứa thông điệp AUTACK này, để bảo mật thông tin.

0100 **Nhóm đoạn 3: USX - USY**

Nhóm đoạn này phải được sử dụng để xác định bên tham gia trong quá trình an ninh và để đưa ra thông tin an ninh trên cấu trúc EDIFACT được tham chiếu.

0110 **USX, tham chiếu an ninh**

Đoạn này chứa tham chiếu tới các bên tham gia liên quan trong quá trình an ninh.

Phần tử dữ liệu hỗn hợp an ninh ngày tháng và thời gian có thể chứa ngày tháng và thời gian khởi tạo gốc của cấu trúc EDIFACT được tham chiếu.

Nếu phân tử dữ liệu 0020 cómặt và các phần tử dữ liệu 0048, 0062 và 0800 không có mặt thì toàn bộ trao đổi được tham chiếu.

Nếu phần tử dữ liệu 0020 và 0048 có mặt còn các phần tử 0062 và 0800 không có mặt thì nhóm được tham chiếu.

0120 **USY, an ninh trên tham chiếu**

Đoạn chứa liên kết tới một nhóm tiêu đề an ninh và kết quả của các dịch vụ an ninh áp dụng cho cấu trúc EDIFACT được tham chiếu như quy định trong nhóm tiêu đề an ninh được liên kết đó.

Khi các cấu trúc EDIFACT tham chiếu được bảo vệ bởi cùng một dịch vụ an ninh, với cùng thông số an ninh liên quan thì có thể liên kết nhiều đoạn USY tới cùng nhóm tiêu đề an ninh. Trong trường hợp này, giá trị liên kết giữa nhóm tiêu đề an ninh và các đoạn USY liên quan là giống nhau.

Khi AUTACK được sử dụng cho chức năng báo nhận, nhóm tiêu đề an ninh tương ứng hoặc phải là cấu trúc EDIFACT được tham chiếu hoặc là một thông điệp AUTACK được sử dụng để cung cấp cấu trúc EDIFACT được tham chiếu có chức năng xác thực.

Trong một đoạn USY, giá trị của phần tử dữ liệu 0534 phải giống với giá trị của phần tử dữ liệu 0534 trong đoạn USH tương ứng của hoặc:

- thông điệp AUTACK hiện tại, nếu sử dụng chức năng xác thực (dịch vụ an ninh: xác thực gốc cấu trúc EDIFACT được tham chiếu, toàn vẹn cấu trúc EDIFACT

được tham chiếu hoặc không-từ chối gốc cấu trúc EDIFACT được tham chiếu);

- chính cấu trúc EDIFACT được tham chiếu hoặc thông điệp AUTACK cung cấp chức năng xác thực cho cấu trúc EDIFACT được tham chiếu, nếu sử dụng chức năng báo nhận (dịch vụ an ninh: không-từ chối nhận hoặc xác thực nhận).

0130 **Nhóm đoạn 4: UST - USR (nhóm đuôi an ninh)**

Một nhóm các đoạn chứa một liên kết với nhóm đoạn tiêu đề an ninh và kết quả của các chức năng an ninh áp dụng cho thông điệp/gói (xem TCVN ISO 9735-5).

Đoạn USR có thể được lược bỏ nếu nhóm đuôi an ninh liên kết tới một nhóm tiêu đề an ninh liên quan với một cấu trúc EDIFACT được tham chiếu. Trong trường hợp này, các kết quả tương ứng của chức năng an ninh phải được tìm thấy trong đoạn USY được liên kết với nhóm tiêu đề an ninh liên quan.

0140 **UST, đuôi an ninh**

Đoạn thiết lập một liên kết giữa nhóm đoạn tiêu đề và đuôi an ninh và chỉ rõ số lượng đoạn an ninh được chứa trong các nhóm này (xem TCVN ISO 9735-5).

0150 **USR, Kết quả an ninh**

Đoạn chứa kết quả của chức năng an ninh áp dụng cho thông điệp/gói được quy định trong nhóm tiêu đề an ninh liên kết (xem TCVN ISO 9735-5). Kết quả an ninh trong đoạn này phải áp dụng cho chính thông điệp AUTACK đó.

0160 **UNT, đuôi thông điệp**

Đoạn dịch vụ kết thúc một thông điệp, đưa ra tổng số đoạn và số tham chiếu kiểm soát của thông điệp.

5.4.2 Cấu trúc thông điệp

Bảng 1 - Bảng đoạn

VỊ TRÍ	THẺ	Tên	S	R	Chú thích
0010	UNH	Tiêu đề thông điệp	M	1	
0020	- - -	Nhóm đoạn 1 - - - - - - - -	M	99	
0030	USH	Tiêu đề an ninh	M	1	
0040	USA	Thuật toán an ninh	C	3	
0050	- - -	Nhóm đoạn 2 - - - - - - - -	C	2	
0060	USC	Chứng chỉ	M	1	
0070	USA	Thuật toán an ninh	C	3	
0080	USR	Kết quả an ninh	C	1	
0090	USB	Định danh dữ liệu an toàn	M	1	
0100	- - -	Nhóm đoạn 3 - - - - - - -	M	9999	
0110	USX	Tham chiếu an ninh	M	1	
0120	USY	An ninh trên tham chiếu	M	9	
0130	- - -	Nhóm đoạn 4 - - - - - - -	M	99	
0140	UST	Đuôi an ninh	M	1	
0150	USR	Kết qủa an ninh	C	1	
0160	UNT	Đuôi thông điệp	M	1	

CHÚ THÍCH Thân thông điệp AUTACK bao gồm đoạn USB và nhóm đoạn 3.

Phụ lục A

(Tham khảo)

Ví dụ minh họa về thông điệp AUTACK

A.1 Giới thiệu

Ba ví dụ trong phụ lục này minh họa cho các ứng dụng khác nhau của thông điệp AUTACK.

Ví dụ đầu tiên chỉ ra cách sử dụng thông điệp AUTACK để bảo vệ một thông điệp được gửi trước đó, để cung cấp dịch vụ an ninh về không-từ chối gốc. Yêu cầu một thông điệp báo nhận AUTACK.

Ví dụ thứ hai chỉ ra cách một thông điệp AUTACK có thể bảo vệ hai thông điệp với các dịch vụ an ninh khác nhau: không-từ chối gốc cho một thông điệp và xác thực gốc cho thông điệp còn lại.

Ví dụ thứ ba minh họa cách sử dụng thông điệp AUTACK để báo nhận an ninh. Ví dụ này chỉ ra thông điệp báo nhận AUTACK được yêu cầu bởi thông điệp AUTACK trong ví dụ 1.

A.2 Ví dụ 1: Dịch vụ không-từ chối gốc được cung cấp bởi một thông điệp AUTACK

A.2.1 Tình huống

Ngân hàng A muốn sử dụng dịch vụ an ninh không-từ chối gốc cho đơn đặt hàng thanh toán của ông Smith ở Công ty A, khi đơn đặt hàng thanh toán này vượt quá một lượng tiền nhất định.

Ngân hàng A yêu cầu thiết lập dịch vụ an ninh không-từ chối gốc trong thoả thuận trao đổi để hoàn tất các đơn đặt hàng thanh toán của ông Smith ở Công ty A bằng cách sử dụng một chữ ký số.

Cả hai bên đồng ý rằng chữ ký số này được điện tử hóa bởi 512 bít RSA (thuật toán không đối xứng) dựa trên một giá trị băm được tính toán bằng cách sử dụng thuật toán MD5.

Chứng chỉ xác định khóa công bố của ông Smith được phát hành bởi một tổ chức được cả hai bên uỷ quyền, bên phát hành chứng chỉ.

Trong điều kiện này, bởi vì chữ ký số của thông điệp PAYORD được chứa trong thông điệp AUTACK, nên bản thân thông điệp AUTACK không cần ký nhận.

Thông điệp PAYORD được bảo vệ bởi AUTACK là thông điệp thứ ba trong trao đổi đầu tiên được ông Smith gửi tới Ngân hàng A. Thông điệp này được tạo ra lúc 10:00:00 giờ, ngày 15/01/1996.

Bản thân AUTACK là thông điệp thứ 5 trong trao đổi và được tạo ra lúc 10:05:32 ngày 15/01/1996.

Các đoạn an ninh sau đây xuất hiện:

- USH để chỉ ra dịch vụ an ninh áp dụng cho thông điệp PAYORD;
- USC - USA - USA - USA - USR, chứng chỉ của ông Smith;
- USB;
- USX - USY với tham chiếu và kết quả an ninh (cho thông điệp PAYORD);
- UST, không có USR, tham chiếu USH.

A.2.2 Chi tiết an ninh

TIÊU ĐỀ AN NINH	
DỊCH VỤ AN NINH, ĐÃ MÃ HÓA	Không-từ chối gốc
SỐ HIỆU THAM CHIẾU AN NINH	Số tham chiếu của tiêu đề là 1
HÌNH THỨC ĐÁP ỨNG	Báo nhận được yêu cầu: 1.
CHỨC NĂNG LỌC	Tất cả giá trị nhị phân (các chữ ký) được lọc với bộ lọc 16.
MÃ HOÁ BỘ KÝ TỰ GỐC	Thông điệp được mã hoá theo mã ASCII 8 bít khi chữ ký được phát hành.
CHỨNG CHỈ	Chứng chỉ của Ông Smith
THAM CHIẾU CHỨNG CHỈ	Chứng chỉ này được tham chiếu bởi BÊN CHỨNG NHẬN: 00000001
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên an ninh	Chủ sở hữu chứng chỉ (Ông Smith ở Công ty A)
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên an ninh Tên khóa	Bên phát hành chứng chỉ (chứng chỉ của Ông Smith được tạo bởi một Bên có thẩm quyền gọi là: BÊN CHỨNG NHẬN.) Khóa công bố của BÊN CHỨNG NHẬN được sử dụng để phát hành ra chứng chỉ của Ông Smith là PK1.
PHIÊN BẢN CÚ PHÁP CHỨNG CHỈ	Phiên bản chứng chỉ của danh mục đoạn dịch vụ UN/EDIFACT.
HÀM LỌC	Tất cả giá trị nhị phân các (khóa và chữ ký số) được lọc với bộ lọc 16
MÃ HÓA BỘ KÝ TỰ GỐC	Thông tin về chứng chỉ đã mã hóa dưới dạng mã ASCII 8 bít khi chứng chỉ được phát hành.
KÝ TỰ DỊCH VỤ CHỮ KÝ Hạn định ký tự dịch vụ chữ ký Ký tự dịch vụ chữ ký	Ký tự dịch vụ được sử dụng khi chữ ký được điện tử hóa. Ký tự dịch vụ là kết thúc đoạn. Giá trị " ' " (dấu nháy)
KÝ TỰ DỊCH VỤ CHỮ KÝ Hạn định ký tự dịch vụ chữ ký Ký tự dịch vụ chữ ký	Ký tự dịch vụ được sử dụng khi chữ ký được điện tử hóa. Ký tự dịch vụ là dấu phân tách phần tử dữ liệu. Giá trị " + " (dấu cộng)
KÝ TỰ DỊCH VỤ CHỮ KÝ Hạn định ký tự dịch vụ chữ ký Ký tự dịch vụ chữ ký	Ký tự dịch vụ được sử dụng khi chữ ký được điện tử hóa. Ký tự dịch vụ là dấu phân tách phần tử dữ liệu thành phần. Giá trị " : " (dấu hai chấm)
KÝ TỰ DỊCH VỤ CHỮ KÝ Hạn định ký tự dịch vụ chữ ký Ký tự dịch vụ chữ ký	Ký tự dịch vụ được sử dụng khi chữ ký được điện tử hóa. Ký tự dịch vụ là dấu phân tách lặp lại. Giá trị " * " (dấu sao)
KÝ TỰ DỊCH VỤ CHỮ KÝ Hạn định ký tự dịch vụ chữ ký Ký tự dịch vụ chữ ký	Ký tự dịch vụ được sử dụng khi chữ ký được điện tử hóa. Ký tự dịch vụ là ký tự phát hành. Giá trị " ? " (dấu hỏi)
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày tháng và thời gian	Thời gian phát hành chứng chỉ Chứng chỉ của Ông Smith được phát hành vào ngày 151293 lúc 14:12:00.

NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày tháng và thời gian	Bắt đầu kỳ hạn có hiệu lực của chứng chỉ Kỳ hạn chứng chỉ của Ông Smith bắt đầu có hiệu lực : 1996 01 01 000000.
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày tháng và thời gian	Kết thúc kỳ hạn có hiệu lực của chứng chỉ Kỳ hạn chứng chỉ của ông Smith hết hiệu lực: 1996 12 31 235959.
THUẬT TOÁN AN NINH	Thuật toán không đối xứng được Ông Smith dùng để ký.
THUẬT TOÁN AN NINH Sử dụng thuật toán Phương thức hoạt động mật mã hoá Thuật toán	Chủ sở hữu sử dụng một thuật toán để ký Không có phương thức hoạt động nào liên quan ở đây RSA là thuật toán không đối xứng.
THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	Xác định thông số thuật toán như hàm mũ công bố để xác minh chữ ký. Khóa công bố của Ông Smith
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	Xác định thông số thuật toán như một Môđun để xác minh chữ ký. Các Môđun của Ông Smith
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	Xác định thông số thuật toán như độ dài của các Môđun của Ông Smith (theo bít). Độ dài của các Môđun của Ông Smith là 512 bit.
THUẬT TOÁN AN NINH	Hàm băm được sử dụng bởi cơ quan thẩm quyền để tạo chứng chỉ của Ông Smith
THUẬT TOÁN AN NINH Sử dụng thuật toán Phương thức hoạt động mật mã hoá Thuật toán	Bên phát hành Sử dụng thuật toán băm. Hàm băm CD 10118-2 hàm băm sử dụng một thuật toán mã khối n-bit để sinh ra một mã băm có độ dài gấp đôi (128 bít); giá trị ban đầu: A = 01234567 B = 89 ABCDEF C = FEDCBA98 D = 76543210 Thuật toán tài liệu liệt kê-thông điệp MD5 được sử dụng
THUẬT TOÁN AN NINH	Thuật toán không đối xứng được cơ quan thẩm quyền dùng để ký.
THUẬT TOÁN AN NINH Sử dụng thuật toán Phương thức hoạt động mật mã hoá Thuật toán	Bên phát hành Sử dụng một thuật toán để ký. Không có phương thức hoạt động nào liên quan ở đây RSA là thuật toán không đối xứng.
THAM SỐ THUẬT TOÁN Hạn định thông số thuật toán Giá trị tham số thuật toán	Xác định tham số thuật toán như hàm mũ công bố để xác minh chữ ký. Khóa công bố của bên chứng nhận.

THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định tham số thuật toán như một Môđun để xác minh chữ ký. Các Môđun của bên chứng nhận.
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định tham số thuật toán như chiều dài của các môđun của bên chứng nhận (theo bít). Độ dài của các Môđun của bên chứng nhận dài 512 bít.
KẾT QUẢ AN NINH	Chữ ký số của chứng chỉ
KẾT QUẢ HỢP LỆ Hạn định giá trị hợp lệ Giá trị hợp lệ	 Giá trị hợp lệ duy nhất là 1 Chữ ký số hexa 512 bít.
ĐỊNH DANH DỮ LIỆU AN TOÀN	
HÌNH THỨC ĐÁP ỨNG, ĐÃ MÃ HÓA	Báo nhận an toàn từ Ngân hàng A được yêu cầu.
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày tháng và thời gian Ngày xảy ra sự kiện Thời gian xảy ra sự kiện	 Việc đảm bảo an ninh liên quan đến thẻ-thời gian của AUTACK. Thẻ thời gian an ninh là: ngày: 1996 01 15. Thời gian: 10:05:32
NGƯỜI GỬI TRAO ĐỔI Định danh bên gửi trao đổi	Định danh của bên gửi trao đổi Định danh của Ông Smith, Công ty A
NGƯỜI NHẬN TRAO ĐỔI Định danh bên gửi trao đổi	Định danh của bên nhận trao đổi Định danh của Ngân hàng A
THAM CHIẾU AN NINH	Tham khảo tới thực thể an ninh (PAYORD liên quan tới dịch vụ không-từ chối gốc) và ngày, giờ liên quan.
THAM CHIẾU KIỂM SOÁT TRAO ĐỔI	Xác định số tham chiếu được ấn định bởi bên gửi cho trao đổi của thông điệp PAYORD: 1.
BÊN GỬI TRAO ĐỔI Định danh bên gửi trao đổi	 Xác định bên gửi của trao đổi thông điệp PAYORD: Ông Smith từ Công ty A.
BÊN NHẬN TRAO ĐỔI Định danh bên nhận trao đổi	 Xác định bên nhận của trao đổi thông điệp PAYORD: Ngân hàng A.
SỐ THAM CHIẾU THÔNG ĐIỆP	Xác định số tham chiếu được ấn định bởi bên gửi cho thông điệp PAYORD: 3.
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày tháng và thời gian Ngày xảy ra sự kiện Thời gian xảy ra sự kiện	 Việc đảm bảo an ninh liên quan đến thẻ thời gian tham khảo PAYORD. Thẻ thời gian an ninh là ngày: 1996 01 15. Thời gian: 10:00:00

AN NINH TRÊN THAM CHIẾU	Xác định tiêu đề có thể áp dụng (kết hợp với các chức năng an ninh áp dụng cho thông điệp PAYORD), và kết quả của việc áp dụng các chức năng này đối với thông điệp PAYORD.
SỐ THAM CHIẾU AN NINH	Số hiệu liên kết kết quả hợp lệ tương ứng với đoạn USH. Trong trường hợp này giá trị là 1.
KẾT QUẢ HỢP LỆ Hạn định giá trị hợp lệ Giá trị hợp lệ	 Giá trị hợp lệ duy nhất là 1 Chữ ký số hexa 512 bít (của thông điệp PAYORD).
ĐUÔI AN NINH	
SỐ THAM CHIẾU AN NINH	Số tham chiếu của đuôi an ninh là 1.
SỐ LƯỢNG ĐOẠN AN NINH	Số lượng đoạn an ninh là 7.

A.3 Ví dụ 2: Đảm bảo an ninh cho một số thông điệp với AUTACK

A.3.1 Tình huống

Ngân hàng A muốn sử dụng dịch vụ an ninh không-từ chối gốc cho đơn đặt hàng thanh toán của ông Smith ở Công ty A, khi những đơn đặt hàng thanh toán này vượt quá một lượng cố định. Để cho đơn đặt hàng thanh toán không vượt quá số lượng thì dịch vụ xác thực gốc được yêu cầu.

Ngân hàng A yêu cầu thiết lập dịch vụ an ninh không-từ chối gốc trong thoả thuận trao đổi để hoàn tất các đơn đặt hàng thanh toán của ông Smith ở Công ty A bằng cách sử dụng một chữ ký số. Cả hai bên đồng ý chữ ký số này được điện tử hóa bởi 512 bít RSA (thuật toán không đối xứng) dựa trên một giá trị băm được tính toán bằng cách sử dụng thuật toán MD5.

Ngoài ra, xác thực gốc thông điệp đạt được bằng việc tạo một "Mã Xác thực Thông điệp" (MAC) với DES đối xứng theo ISO 8731-1 tại bên gửi.

Chứng chỉ xác định khóa công bố nhận của ông Smith được phát hành bởi một tổ chức được cả hai bên uỷ quyền, bên phát hành chứng chỉ.

Thông điệp PAYORD đầu tiên gửi đi được bảo vệ bởi AUTACK với một chữ ký số. Nó là thông điệp thứ 5 của trao đổi đầu tiên được ông Smith gửi tới Ngân hàng A. Nó được gửi vào ngày 15/01/1996 lúc 08:00:00.

Thông điệp PAYORD thứ hai gửi đi được bảo vệ bởi AUTACK với một MAC. Nó là thông điệp thứ 7 của trao đổi đầu tiên. Nó được gửi vào ngày 15/01/1996 lúc 09:00:00.

AUTACK bản thân nó là thông điệp thứ 10 của trao đổi thứ nhất. Nó được gửi vào ngày 15/01/1996 lúc 10:05:32.

Khi thông điệp PAYORD đầu tiên được bảo vệ với một chữ ký số , AUTACK không cần được ký nhận.

Kết quả, các đoạn an ninh xuất hiện như sau:

- USH chỉ ra dịch vụ không-từ chối gốc được áp dụng cho thông điệp PAYORD đầu tiên;
- USC - USA - USA - USA - USR, chứng chỉ của ông Smith;
- USH chỉ ra dịch vụ xác thực thông điệp được áp dụng cho thông điệp PAYORD thứ hai;

- USB;
- USX - USY với tham chiếu và kết quả an ninh (chữ ký số) cho thông điệp thứ nhất;
- USX - USY với tham chiếu và kết quả an ninh (MAC) cho thông điệp PAYORD thứ hai;
- UST, không có USR, tham chiếu đến USH đầu tiên;
- UST, không có USR, tham chiếu đến USH thứ hai.

A.3.2 Chi tiết an ninh

TIÊU ĐỀ AN NINH	Tiêu đề gồm thông tin về chức năng an ninh được tiến hành trên thực thể được tham chiếu (thông điệp PAYORD đầu tiên)
DỊCH VỤ AN NINH, ĐÃ MÃ HÓA	Không-từ chối gốc đối với PAYORD thứ nhất
SỐ THAM CHIẾU AN NINH	Số tham chiếu của tiêu đề là 1
CHỨC NĂNG LỌC	Tất cả giá trị nhị phân được lọc với bộ lọc 16
MÃ HOÁ BỘ KÝ TỰ GỐC	Thông điệp được mã hoá theo mã ASCII 8 bít khi chữ ký của nó được phát hành
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên an ninh	Bên gửi thông điệp (ông Smith từ Công ty A)
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên an ninh	Bên nhận thông điệp (Ngân hàng A)
CHỨNG CHỈ	Chứng chỉ của ông Smith
THAM CHIẾU CHỨNG CHỈ	Chứng chỉ này được tham chiếu bởi bên có thẩm quyền : 00000001
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên an ninh	Chủ sở hữu chứng chỉ (ông Smith của Công ty A)
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên an ninh Tên khóa	Bên phát hành chứng chỉ (chứng chỉ của ông Smith được phát hành bởi một người có thẩm quyền gọi là bên chứng nhận) Khóa công bố của bên chứng nhận sử dụng để phát hành chứng chỉ của ông Smith là PK1
PHIÊN BẢN CÚ PHÁP CHỨNG CHỈ	Phiên bản chứng chỉ của danh mục đoạn dịch vụ UN/EDIFACT
CHỨC NĂNG LỌC	Tất cả giá trị nhị phân (khóa và chữ ký số) được lọc với bộ lọc 16
KÝ TỰ DỊCH VỤ CHỮ KÝ Hạn định ký tự dịch vụ chữ ký Ký tự dịch vụ chữ ký	Ký tự dịch vụ được sử dụng khi chữ ký được điện tử hóa Ký tự dịch vụ là kết thúc đoạn Giá trị " ' " (dấu nháy)
KÝ TỰ DỊCH VỤ CHỮ KÝ Hạn định ký tự dịch vụ chữ ký Ký tự dịch vụ chữ ký	Ký tự dịch vụ được sử dụng khi chữ ký được điện tử hóa Ký tự dịch vụ là dấu phân tách phần tử dữ liệu Giá trị " + " (dấu cộng)
KÝ TỰ DỊCH VỤ CHỮ KÝ Hạn định ký tự dịch vụ chữ ký Ký tự dịch vụ chữ ký	Ký tự dịch vụ được sử dụng khi chữ ký được điện tử hóa Ký tự dịch vụ là dấu phân tách phần tử dữ liệu thành phần Giá trị " : " (dấu hai chấm)
KÝ TỰ DỊCH VỤ CHỮ KÝ	Ký tự dịch vụ được sử dụng khi chữ ký được điện tử hóa

Hạn định ký tự dịch vụ chữ ký Ký tự dịch vụ chữ ký	Ký tự dịch vụ là dấu phân tách lặp lại Giá trị " * " (dấu sao)
KÝ TỰ DỊCH VỤ CHỮ KÝ Hạn định ký tự dịch vụ chữ ký Ký tự dịch vụ chữ ký	Ký tự dịch vụ được sử dụng khi chữ ký được điện tử hóa Ký tự dịch vụ là ký tự phát hành Giá trị " ? " (dấu hỏi)
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày tháng và thời gian	Thời gian phát hành chứng chỉ Chứng chỉ của ông Smith được phát hành vào ngày 931215 lúc 14:12:00
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày tháng và thời gian	Bắt đầu kỳ hạn có hiệu lực của chứng chỉ Kỳ hạn chứng chỉ của ông Smith bắt đầu có hiệu lực: 1996 01 01 000000
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày tháng và thời gian	Kết thúc kỳ hạn có hiệu lực của chứng chỉ Kỳ hạn chứng chỉ của ông Smith hết hiệu lực: 1996 12 31 235959
THUẬT TOÁN AN NINH	Thuật toán không đối xứng được ông Smith dùng để ký
THUẬT TOÁN AN NINH Sử dụng thuật toán Phương thức hoạt động mật mã hoá Thuật toán	 Chủ sở hữu sử dụng một thuật toán để ký Không có phương thức hoạt động nào liên quan ở đây RSA là thuật toán không đối xứng
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định tham số thuật toán như hàm mũ công bố để xác minh chữ ký. Khóa công bố của ông Smith
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định tham số thuật toán như một Môđun để xác minh chữ ký. Các Môđun của ông Smith
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định tham số thuật toán như một độ dài các môđun của ông Smith (theo bít). Độ dài của các Môđun của ông Smith là 512 bít.
THUẬT TOÁN AN NINH	Hàm băm được sử dụng bởi cơ quan thẩm quyền để tạo chứng chỉ của ông Smith
THUẬT TOÁN AN NINH Sử dụng thuật toán Phương thức hoạt động mật mã hoá Thuật toán	 Bên phát hành sử dụng một thuật toán băm. Hàm băm CD, 10118-2 hàm băm sử dụng thuật toán mã khối n-bit để sinh ra một mã băm có độ dài gấp đôi (128 bít); giá trị ban đầu: A = 01234567 B = 89ABCDEF C = FEDCBA98 D = 76543210 Thuật toán tài liệu liệt kê-thông điệp MD5 được sử dụng
THUẬT TOÁN AN NINH	Thuật toán không đối xứng được bên chứng nhận sử dụng để ký

THUẬT TOÁN AN NINH Sử dụng thuật toán Phương thức hoạt động mật mã hoá Thuật toán	 Bên phát hành sử dụng một thuật toán để ký Không có phương thức hoạt động nào liên quan ở đây RSA là thuật toán không đối xứng
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định tham số thuật toán như hàm mũ công bố để xác minh chữ ký Khóa công bố của bên chứng nhận
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định tham số thuật toán như một Môđun cho việc xác minh chữ chữ ký Các Môđun của bên chứng nhận
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định tham số thuật toán như chiều dài của các môđun của bên chứng nhận (theo bít) Các Môđun của bên chứng nhận dài 512 bít
KẾT QUẢ AN NINH	Chữ ký số của chứng chỉ
KẾT QUẢ HỢP LỆ Hạn định giá trị hợp lệ Giá trị hợp lệ	 Giá trị hợp lệ duy nhất là 1 Chữ ký số hexa 512 bít
TIÊU ĐỀ AN NINH	Tiêu đề gồm thông tin về chức năng an ninh được tiến hành trên thực thể được tham chiếu (thông điệp PAYORD thứ hai)
DỊCH VỤ AN NINH, ĐÃ MÃ HÓA	Xác thực nguồn gốc thông điệp cho PAYORD thứ hai
SỐ THAM CHIẾU AN NINH	Số tham chiếu của tiêu đề là 2
CHỨC NĂNG LỌC	Tất cả giá trị nhị phân được lọc với bộ lọc 16
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên an ninh	 Bên gửi thông điệp (ông Smith từ Công ty A)
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên an ninh	 Bên nhận thông điệp (Ngân hàng A)
THUẬT TOÁN AN NINH	
THUẬT TOÁN AN NINH Sử dụng thuật toán Phương thức hoạt động mật mã hoá Thuật toán	 Một thuật toán đối xứng được sử dụng để đạt được tính xác thực nguồn gốc thông điệp Một MAC được tính toán theo ISO 8731-1 Thuật toán DES được sử dụng
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định các giá trị tham số thuật toán này bằng tên của khóa đối xứng được trao đổi trước 1234567890ABCDEF
ĐỊNH DANH DỮ LIỆU AN TOÀN	

HÌNH THỨC ĐÁP ỨNG, ĐÃ MÃ HÓA	Không yêu cầu báo nhận từ Ngân hàng A
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày tháng và thời gian Ngày xảy ra sự kiện Thời gian xảy ra sự kiện	 Việc đảm bảo an ninh liên quan đến thẻ thời gian của AUTACK Thẻ thời gian an ninh là: ngày: 1996 01 15 Thời gian: 10:05:32
BÊN GỬI TRAO ĐỔI Xác nhận bên gửi trao đổi	Xác nhận của bên gửi trao đổi Xác nhận của ông Smith, Công ty A
BÊN NHẬN TRAO ĐỔI Xác nhận bên gửi trao đổi	Xác nhận của bên nhận trao đổi Xác nhận của Ngân hàng A
THAM CHIẾU AN NINH	Tham khảo tới thực thể an ninh (PAYORD thứ hai)
THAM CHIẾU KIỂM SOÁT TRAO ĐỔI	Xác định số tham chiếu được ấn định bởi bên gửi cho trao đổi của thông điệp PAYORD: 1
BÊN GỬI TRAO ĐỔI Xác nhận bên gửi trao đổi	 Xác định bên gửi của trao đổi thông điệp PAYORD: ông Smith ở Công ty A
BÊN NHẬN TRAO ĐỔI Xác nhận bên nhận trao đổi	 Xác định bên nhận trao đổi thông điệp PAYORD: Ngân hàng A
SỐ HIỆU THAM CHIẾU THÔNG ĐIỆP	Xác định số tham chiếu được ấn định bởi bên gửi cho thông điệp PAYORD: 7
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày xảy ra sự kiện Thời gian xảy ra sự kiện	 Thẻ thời gian an ninh là ngày: 1996 01 15 Giờ: 09:00:00
AN NINH TRÊN THAM CHIẾU	Xác định tiêu đề có thể áp dụng (kết hợp với các chức năng an ninh áp dụng cho thông điệp PAYORD thứ hai), và kết quả của việc áp dụng các chức năng này đối với thông điệp PAYORD
SỐ THAM CHIẾU AN NINH	Số hiệu liên kết kết quả hợp lệ tương ứng với đoạn USH. Trong trường hợp này có giá trị là 2
KẾT QUẢ HỢP LỆ Hạn định giá trị hợp lệ Giá trị hợp lệ	 MAC (Mã Xác thực Thông điệp) 12345678 - Đây là một giá trị 4 byte
THAM CHIẾU AN NINH	Tham khảo tới thực thể an ninh (PAYORD đầu tiên) và ngày, giờ tương ứng
THAM CHIẾU KIỂM SOÁT TRAO ĐỔI	Xác định số tham chiếu được ấn định bởi bên gửi cho trao đổi của thông điệp PAYORD:1
BÊN GỬI TRAO ĐỔI Xác nhận bên gửi trao đổi	 Xác định bên gửi của trao đổi thông điệp PAYORD: ông Smith từ Công ty A
BÊN NHẬN TRAO ĐỔI Xác nhận bên nhận trao đổi	 Xác định bên nhận của trao đổi thông điệp PAYORD: Ngân hàng A

SỐ THAM CHIẾU THÔNG ĐIỆP	Xác định số tham chiếu được ấn định bởi bên gửi cho thông điệp PAYORD đầu tiên: 5
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày xảy ra sự kiện Thời gian xảy ra sự kiện	 Thẻ thời gian an ninh là: ngày: 1996 01 15 Giờ: 08:00:00
AN NINH TRÊN THAM CHIẾU	Xác định tiêu đề có thể áp dụng (kết hợp với các chức năng an ninh áp dụng cho thông điệp PAYORD đầu tiên), và kết quả của việc áp dụng các chức năng này đối với thông điệp PAYORD đầu tiên
SỐ THAM CHIẾU AN NINH	Số liên kết kết quả hợp lệ tương ứng với đoạn USH. Trong trường hợp này có giá trị là 1
KẾT QUẢ HỢP LỆ Hạn định giá trị hợp lệ Giá trị hợp lệ	 Giá trị hợp lệ duy nhất là 1 Chữ ký số hexa lọc 512 bít (của thông điệp PAYORD thứ nhất)
ĐUÔI AN NINH	
SỐ THAM CHIẾU AN NINH	Số tham chiếu của đuôi an ninh là 2
SỐ LƯỢNG ĐOẠN AN NINH	Số lượng đoạn an ninh là 2
ĐUÔI AN NINH	
SỐ THAM CHIẾU AN NINH	Số tham chiếu của đuôi an ninh là 1
SỐ LƯỢNG ĐOẠN AN NINH	Số lượng đoạn an ninh là 7

A.4 Ví dụ 3: Báo nhận an ninh của một thông điệp nhận được bởi AUTACK

A.4.1 Tình huống

Trong ví dụ 1, AUTACK đã được sử dụng bởi bên gửi (ông Smith ở Công ty A) của thông điệp PAYORD trước đó. Thông điệp AUTACK được yêu cầu báo nhận từ Ngân hàng A.

Ví dụ này, chỉ ra cách sử dụng thông điệp AUTACK như một báo nhận an ninh.

Nó được thiết lập để thông điệp AUTACK hoạt động như một báo nhận an ninh và được bảo vệ với dịch vụ không-từ chối gốc nhờ sử dụng chữ ký số.

Thông điệp AUTACK được tạo ra ngày 1996.01.16 lúc 11:00:00, là thông điệp thứ 20 của trao đổi.

Các đoạn an ninh xuất hiện như sau:

- USH, để xác định dịch vụ an ninh áp dụng cho thông điệp AUTACK;
- USH, để xác định dịch vụ an ninh áp dụng cho thực thể được báo nhận;
- USC-USA(3)-USR, chứng chỉ của Ngân hàng A;
- USB, gồm các chi tiết của AUTACK;
- USX-USY, gồm tham chiếu cho thực thể được báo nhận và chữ ký số;
- UST, Đuôi An ninh không có USR;

- UST-USR để bảo vệ chính AUTACK.

A.4.2 Chi tiến an ninh

TIÊU ĐỀ AN NINH	
DỊCH VỤ AN NINH, ĐÃ MÃ HÓA	Không-từ chối gốc
SỐ THAM CHIẾU AN NINH	Tham chiếu tiêu đề là 1
CHỨC NĂNG LỌC	Tất cả giá trị nhị phân được lọc với bộ lọc 16
MÃ HOÁ BỘ KÝ TỰ GỐC	Thông điệp được mã hoá dưới mà ASCII 8 bít khi MAC được phát hành
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên an ninh	Bên gửi thông điệp (bên tạo ra chữ ký số): Ngân hàng A
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên an ninh	Bên nhận thông điệp (bên xác minh chữ ký số): Ông Smith ở Công ty A
SỐ HIỆU THỨ TỰ AN NINH	Số hiệu thứ tự an ninh của thông điệp này là 20
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày xảy ra sự kiện Giờ xảy ra sự kiện	Thẻ thời gian là: ngày: 1996.01.16 Giờ: 11:00:00
CHỨNG CHỈ	Chứng chỉ của Ngân hàng A
THAM CHIẾU CHỨNG CHỈ	Chứng chỉ này được tham chiếu bởi người có thẩm quyền : 00000010.
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên an ninh	Chủ sở hữu chứng chỉ (Ngân hàng A)
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên an ninh Tên khóa	Bên phát hành chứng chỉ (chứng chỉ của Ngân hàng A được phát hành bởi một tổ chức có thẩm quyền gọi là: bên chứng nhận.) Khóa công bố của BÊN CHỨNG NHẬN được sử dụng để phát hành chứng chỉ của Ngân hàng A là PK1.
PHIÊN BẢN CÚ PHÁP CHỨNG CHỈ	Phiên bản chứng chỉ của danh mục đoạn dịch vụ UN/EDIFACT.
CHỨC NĂNG LỌC	Tất cả giá trị nhị phân (các khóa và chữ ký số) được lọc với bộ lọc 16
MÃ HOÁ BỘ KÝ TỰ GỐC	Thông tin về chứng chỉ được mã hóa dưới dạng mã ASCII 8 bít khi chứng chỉ được phát hành.
KÝ TỰ DỊCH VỤ CHỮ KÝ Hạn định ký tự dịch vụ chữ ký Ký tự dịch vụ chữ ký	Ký tự dịch vụ được sử dụng khi chữ ký được điện tử hóa. Ký tự dịch vụ là kết thúc đoạn. Giá trị " ' " (dấu nháy)
KÝ TỰ DỊCH VỤ CHỮ KÝ Hạn định ký tự dịch vụ chữ ký Ký tự dịch vụ chữ ký	Ký tự dịch vụ được sử dụng khi chữ ký được điện tử hóa. Ký tự dịch vụ là dấu phân tách phần tử dữ liệu. Giá trị " + " (dấu cộng)

KÝ TỰ DỊCH VỤ CHỮ KÝ Hạn định ký tự dịch vụ chữ ký Ký tự dịch vụ chữ ký	Ký tự dịch vụ được sử dụng khi chữ ký được điện tử hóa. Ký tự dịch vụ là dấu phân tách phần tử dữ liệu thành phần. Giá trị " : " (dấu hai chấm)
KÝ TỰ DỊCH VỤ CHỮ KÝ Hạn định ký tự dịch vụ chữ ký Ký tự dịch vụ chữ ký	Ký tự dịch vụ được sử dụng khi chữ ký được điện tử hóa. Ký tự dịch vụ là dấu phân tách lặp lại. Giá trị " * " (dấu sao)
KÝ TỰ DỊCH VỤ CHỮ KÝ Hạn định ký tự dịch vụ chữ ký Ký tự dịch vụ chữ ký	Ký tự dịch vụ được sử dụng khi chữ ký được điện tử hóa. Ký tự dịch vụ là ký tự phát hành. Giá trị " ? " (dấu hỏi)
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày tháng và thời gian	Thời gian phát hành chứng chỉ Chứng chỉ của Ngân hàng A được phát hành vào ngày 1995 12 31 lúc 14:00:00.
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày tháng và thời gian	Bắt đầu kỳ hạn có hiệu lực của chứng chỉ Kỳ hạn chứng chỉ của Ngân hàng A bắt đầu có hiệu lực: 1996 01 01 000000.
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày tháng và thời gian	Kết thúc kỳ hạn có hiệu lực của chứng chỉ Kỳ hạn chứng chỉ của Ngân hàng A hết hiệu lực: 1996 12 31 235959.
THUẬT TOÁN AN NINH	Thuật toán không đối xứng được Ngân hàng A sử dụng để ký.
THUẬT TOÁN AN NINH Sử dụng thuật toán Phương thức hoạt động mật mã hoá Thuật toán	 Chủ sở hữu sử dụng một thuật toán để ký. Không có phương thức hoạt động nào liên quan ở đây RSA là thuật toán không đối xứng.
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định tham số thuật toán này như hàm mũ công bố để xác minh chữ ký. Khóa công bố của Ngân hàng A.
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định tham số thuật toán như một Môđun để xác minh chữ ký. Các Môđun của Ngân hàng A.
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định tham số thuật toán như chiều dài các môđun của Ngân hàng A (theo bít). Độ dài các Môđun của ngân hàng A: 512 bít.
THUẬT TOÁN AN NINH	Hàm băm được sử dụng bởi BÊN CHỨNG NHẬN để phát hành chứng chỉ của Ngân hàng A.
THUẬT TOÁN AN NINH Sử dụng thuật toán Phương thức hoạt động mật mã hoá	 Bên phát hành sử dụng một thuật toán băm. Hàm băm CD 10118-2 hàm băm sử dụng thuật toán mã khối n-bit được áp dụng để sinh ra một mã băm có độ dài gấp đôi (128 bít); giá trị ban đầu:

Thuật toán	A = 01234567 B = 89ABCDEF C = FEDCBA98 D = 76543210 Thuật toán tài liệu liệt kê-thông điệp MD5 được sử dụng
THUẬT TOÁN AN NINH	Thuật toán không đối xứng được bên chứng nhận sử dụng để ký.
THUẬT TOÁN AN NINH Sử dụng thuật toán Phương thức hoạt động mật mã hoá Thuật toán	 Bên phát hành sử dụng một thuật toán để ký. Không có phương thức hoạt động nào liên quan ở đây RSA là thuật toán không đối xứng.
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định tham số thuật toán như hàm mũ công bố để xác minh chữ ký. Khóa công bố của bên chứng nhận.
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định tham số thuật toán như một Môđun để xác minh chữ ký. Các Môđun của bên chứng nhận
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định tham số thuật toán như chiều dài của các môđun của bên chứng nhận (theo bít). Các Môđun của bên chứng nhận dài 512 bít.
KẾT QUẢ AN NINH	Chữ ký số của Chứng chỉ
KẾT QUẢ HỢP LỆ Hạn định giá trị hợp lệ Giá trị hợp lệ	 Giá trị hợp lệ duy nhất là 1 Chữ ký số hexa 512 bit.
TIÊU ĐỀ AN NINH	Tiêu đề gồm thông tin về chức năng an ninh được tiến hành trên thực thể tham chiếu (PAYORD) được báo nhận.
DỊCH VỤ AN NINH, ĐÃ MÃ HÓA	Không-từ chối gốc.
SỐ THAM CHIẾU AN NINH	Tham chiếu của tiêu đề là 2.
CHỨC NĂNG LỌC	Tất cả giá trị nhị phân (các chữ ký) được lọc với bộ lọc 16.
MÃ HOÁ BỘ KÝ TỰ GỐC	Thông điệp đã mã hóa dưới dạng mã ASCII 8 bít khi chữ ký được phát hành.
ĐỊNH DANH DỮ LIỆU AN TOÀN	
NGÀY THÁNG VÀ THỜI GIAN AN NINH	Thẻ thời gian cho thông điệp AUTACK này là: ngày: 1996.01.16 Thời gian: 11:00:00.
BÊN GỬI TRAO ĐỔI Xác nhận bên gửi trao đổi	Xác nhận của bên gửi trao đổi Xác nhận của Ngân hàng A
BÊN NHẬN TRAO ĐỔI Xác nhận bên nhận trao đổi	Xác nhận của bên nhận trao đổi Xác nhận của ông Smith, Công ty A

THAM CHIẾU AN NINH	Tham khảo tới thực thể an ninh (thông điệp được báo nhận) và ngày, giờ liên quan.
THAM CHIẾU KIỂM SOÁT TRAO ĐỔI	Xác định số tham chiếu trao đổi của thông điệp PAYORD được báo nhận: 1.
BÊN GỬI TRAO ĐỔI Xác nhận bên gửi trao đổi	Xác định bên gửi của trao đổi thuộc thông điệp được báo nhận: ông Smith Công ty A.
BÊN NHẬN TRAO ĐỔI Xác nhận bên nhận trao đổi	Xác định bên nhận trao đổi của thông điệp được báo nhận: Ngân hàng A.
SỐ THAM CHIẾU THAM SỐ	Xác định số tham chiếu được ấn định bởi bên gửi cho thông điệp được báo nhận: 3 *(xem ví dụ 1).*
NGÀY THÁNG VÀ THỜI GIAN AN NINH	Thẻ thời gian an nình của PAYORD là: ngày:1996.01.15, giờ: 10:00:00
AN NINH TRÊN THAM CHIẾU	
SỐ THAM CHIẾU AN NINH	Xác định hai tiêu đề có thể áp dụng.
KẾT QUẢ HỢP LỆ Hạn định giá trị tính hợp lệ Giá trị hợp lệ	Giá trị hợp lệ duy nhất 1. 512 bít chữ ký số của P đã báo nhận được lọc bằng bộ lọc 16 mã
ĐUÔI AN NINH	
SỐ THAM CHIẾU AN NINH	Số tham chiếu của đuôi an ninh là 2
SỐ LƯỢNG CÁC ĐOẠN AN NINH	Số lượng các đoạn an ninh là 3
ĐUÔI AN NINH	
SỐ THAM CHIẾU AN NINH	Số tham chiếu của đuôi an ninh là 1
SỐ LƯỢNG ĐOẠN AN NINH	Số lượng các đoạn an ninh là 7
KẾT QUẢ AN NINH	
KẾT QUẢ HỢP LỆ Hạn định giá trị tính hợp lệ Giá trị hợp lệ	Giá trị hợp lệ duy nhất là 1. 512 bít chữ ký số của AUTACK được lọc bằng mã16

Phụ lục B

(tham khảo)

Dịch vụ và thuật toán an ninh

B.1 Mục đích và phạm vi áp dụng

Phụ lục này đưa ra các ví dụ về các tổ hợp có thể có của các phần tử dữ liệu và các giá trị mã khác nhau từ các nhóm đoạn an ninh. Các ví dụ này được chọn để minh họa cho các kỹ thuật an ninh đã được sử dụng rộng rãi, dựa trên cơ sở các tiêu chuẩn quốc tế.

Bộ đầy đủ các tổ hợp có thể là rất lớn, nên trong phụ lục này chỉ đưa ra một vài ví dụ. Các ví dụ được lựa chọn ở đây không được xem như một sự xác nhận các thuật toán hoặc phương thức hoạt động. Người sử dụng được quyền lựa chọn các kỹ thuật thích hợp cho mối đe dọa an ninh mà họ muốn được bảo vệ.

Mục đích của phụ lục này là cung cấp cho người sử dụng, thêm một lần nữa họ đã chọn lựa các kỹ thuật an ninh, với một điểm khởi đầu toàn diện để thực hiện một giải pháp phù hợp cho áp dụng cụ thể của họ.

Để đọc và hiểu một cách dễ dàng, chủ đề đã được chia thành 3 đoạn, mỗi đoạn tập trung vào các nguyên tắc cơ bản khác nhau cho việc áp dụng an ninh.

Ba phần đó là:

1. Liên kết sử dụng các thuật toán đối xứng và AUTACK cho thực thể được tham chiếu;
2. Liên kết sử dụng các thuật toán không đối xứng và AUTACK cho thực thể được tham chiếu;
3. Liên kết sử dụng AUTACK để báo nhận.

Danh sách mã được sử dụng trong các ma trận (một phần của danh sách mã hoàn chỉnh).

0501	***Dịch vụ an ninh, đã mã hóa***
1	Không-từ chối gốc
2	Xác thực nguồn gốc thông điệp
9	Tính toàn vẹn cấu trúc EDIFACT được tham chiếu

0505	***Chức năng lọc, đã mã hóa***
6	Bộ lọc ECD UN/EDIFACT

0523	***Sử dụng thuật toán, đã mã hóa***
1	Hàm băm của chủ sở hữu
2	Thuật toán đối xứng của chủ sở hữu
3	Ký nhận của bên phát hành
4	Hàm băm của bên phát hành (CA)
6	Ký nhận của chủ sở hữu (CA)

0527	***Thuật toán, đã mã hóa***
1	DES (Tiêu chuẩn Mã hóa Dữ liệu)
10	RSA (Rivest, Shamir, Adleman)
37	MAC (Mã Xác thực Thông điệp)
40	MDC2 (Mã phát hiện thay đổi)
42	HDS2 (Hàm băm)

0531	*Hạn định thông số thuật toán*
12	Các Môđun
13	Số mũ
14	Độ dài môđun

0563	*Hạn định giá trị hợp lệ*
1	Giá trị hợp lệ duy nhất

0577	*Hạn định bên an ninh*
1	Bên gửi thông điệp
2	Bên nhận thông điệp
3	Chủ sở hữu chứng chỉ
4	Bên xác thực

Các từ viết tắt:

a, b, c, d	=	Biểu diễn của Số Tham chiếu An ninh
CA	=	Tổ chức chứng nhận
Enc-Key	=	Khóa đã mã hóa
Hash	=	Giá trị băm
Key-N	=	Tên khóa
MAC	=	Mã xác thực thông điệp
Mod	=	Môđun
Mod-L	=	Độ dài môđun
PK/CA	=	Khóa công bố của tổ chức chứng nhận
Pub-K	=	Khóa công bố
Sig	=	Chữ ký.

B.2 Liên kết sử dụng các thuật toán đối xứng và AUTACK cho thực thể được tham chiếu

Ma trận trong bảng B.1 thiết lập các mối tương quan trong các trường hợp cụ thể sau:

- An ninh thực thể được tham chiếu cung cấp bởi thông điệp AUTACK (TCVN ISO 9735-6);
- Chỉ sử dụng thuật toán đối xứng;
- Các dịch vụ an ninh được cung cấp là xác thực gốc cấu trúc EDIFACT được tham chiếu cho thông điệp được tham chiếu và xác thực gốc thông điệp cho thông điệp AUTACK. Xác thực gốc cấu trúc EDIFACT tham chiếu được cung cấp bởi tổ hợp của tính toàn vẹn cấu trúc EDIFACT được tham chiếu và xác thực gốc thông điệp của AUTACK;
- Tính toàn vẹn cấu trúc EDIFACT được tham chiếu được cung cấp bởi hàm băm dựa trên cơ sở thuật toán DES sử dụng trong chế độ MDC, theo ISO/IEC 10118-2. Không có khóa bí mật dùng

chung giữa bên gửi và bên nhận. Giá trị băm được truyền trong AUTACK và được bảo vệ an ninh trên thông điệp AUTACK;

- Xác thực gốc thông điệp cho AUTACK được cung cấp nhờ tính toán một MAC (Mã Xác thực Thông điệp) trên thông điệp AUTACK. Trong ví dụ này, thuật toán được sử dụng là DES ở chế độ CBC với một khóa bí mật được biết bởi bên nhận thông điệp và chỉ được tham chiếu bằng tên khóa. Ví dụ này tuân theo ISO 8731-1;

- Mặc dù bên nhận và bên gửi dùng chung các khóa, các cơ chế mật mã hóa không được thoả thuận trước. Do đó, tất cả các thuật toán và phương thức hoạt động sử dụng được đặt tên rõ ràng;

- Chỉ trình bày các trường an ninh liên quan tới các kỹ thuật an ninh, các thuật toán và các phương thức hoạt động được sử dụng trên thực tế.

Bảng B.1 - Ma trận tương quan khi chỉ sử dụng các thuật toán đối xứng

THẺ	Tên	S	R	Toàn vẹn cấu trúc EDIFACT được tham chiếu ISO/IEC 10118-2	Thông điệp xác thực gốc AUTACK ISO 8731-1	Chú thích
SG 1		M	99	Mỗi cho một dịch vụ an ninh		
USH	TIÊU ĐỀ AN NINH	M	1			
0501	DỊCH VỤ AN NINH, ĐÃ MÃ HÓA	M	1	9	2	
0534	SỐ THAM CHIẾU AN NINH	M	1	a	b	1
0505	CHỨC NĂNG LỌC, ĐÃ MÃ HÓA	C	1	6	6	
S500	CHI TIẾT ĐỊNH DANH AN NINH	C	2			
0577	Hạn định bên an ninh	M		1	1	2
0538	Tên khóa	C			Key-N	3
S500	CHI TIẾT ĐỊNH DANH AN NINH	C	2			
0577	Hạn định bên an ninh	M		2	2	4
USA	THUẬT TOÁN AN NINH	C	3			
S502	THUẬT TOÁN AN NINH	M	1			
0523	Thuật toán sử dụng , đã mã hóa	M		1	2	
0525	Phương thức mã hóa hoạt động đã mã hóa	C		-	-	
0527	Thuật toán, đã mã hóa	C		40	37	
USB	ĐỊNH DANH DỮ LIỆU AN TOÀN	M	1	Tham chiếu tới cấu trúc dữ liệu an toàn		
SG3		M	9999			
USX	THAM CHIẾU AN NINH	M	1			
USY	AN NINH TRÊN THAM CHIẾU	M	9			
0534	SỐ THAM CHIẾU AN NINH	M	1	a	-	5

THẺ	Tên	S	R	Toàn vẹn cấu trúc EDIFACT được tham chiếu ISO/IEC 10118-2	Thông điệp xác thực gốc AUTACK ISO 8731-1	Chú thích
S508	KẾT QUẢ HỢP LỆ	C	2			
0563	Hạn định giá trị hợp lệ	M		1		
0560	Giá trị hợp lệ	C		Hash		6
SG 4		M	99			
UST	ĐUÔI AN NINH	M	1			
0534	SỐ THAM CHIẾU AN NINH	M	1	a	B	7
0588	SỐ LƯỢNG ĐOẠN AN NINH	M	1			
USR	KẾT QUẢ AN NINH	C	1			
S508	KẾT QUẢ HỢP LỆ	M	2			
0563	Hạn định giá trị hợp lệ	M			1	
0560	Giá trị hợp lệ	C			MAC	8

CHÚ THÍCH

1. Một tiêu đề an ninh đề cập tới đuôi an ninh AUTACK và tiêu đề an ninh khác đề cập đến đoạn an ninh trên tham chiếu;
2. Bên gửi thông điệp;
3. Tên khóa bí mật được dùng chung cho bên gửi và bên nhận AUTACK;
4. Bên nhận thông điệp;
5. Tham chiếu một trong các tiêu đề an ninh
6. Giá trị băm được tính toán trên cấu trúc EDIFACT được tham chiếu. Nó được bảo vệ bởi MAC được tính toán trên thông điệp AUTACK
7. Tham chiếu một trong các tiêu đề an ninh
8. MAC được tính toán trên thông điệp AUTACK

B.3 Liên kết sử dụng các khóa không đối xứng và AUTACK cho thực thể được tham chiếu

Ma trận trong bảng B.2 thiết lập các mối tương quan cho các trường hợp sau:

- An ninh thực thể được tham chiếu cung cấp bởi thông điệp AUTACK (TCVN ISO 9735-6);

- Các dịch vụ an ninh được cung cấp là không-từ chối gốc cấu trúc EDIFACT được tham chiếu và không-từ chối gốc thông điệp cho thông điệp AUTACK. Không-từ chối gốc cấu trúc EDIFACT được tham chiếu được cung cấp bởi sự liên kết tính toàn vẹn cấu trúc EDIFACT được tham chiếu và không-từ chối gốc của AUTACK;

- Thuật toán không đối xứng là RSA;

- Hàm băm là thuật toán DES ở chế độ MDC. Giống hàm băm cũng được sử dụng để tính toán giá trị băm trên cấu trúc EDIFACT được tham chiếu và thông điệp AUTACK;

- Các chứng chỉ được thừa nhận là không được trao đổi trước;

- Đoạn USC định danh chính xác hàm băm và hàm chữ ký được tổ chức chứng nhận sử dụng để ký chứng chỉ. Bên nhận dã biết khóa công bố cần cho việc kiểm tra chữ ký chứng nhận của tổ chức chứng nhận. Khoá công bố này được chỉ định bằng tên trong đoạn USH;
- Chỉ chứa một chứng chỉ, cần cái thứ hai nếu chỉ sử dụng một khóa công bố của bên nhận.

Bảng B.2 - Ma trận quan hệ khi sử dụng các thuật toán không đối xứng

THẺ	Tên	S	R	Toàn vẹn cấu trúc EDIFACT được tham chiếu ISO/IEC 10118-2	Thông điệp không-từ chối gốc AUTACK (RSA)	Chú thích
SG 1		M	99	Mỗi cho một dịch vụ an ninh		
USH	TIÊU ĐỀ AN NINH	M	1			
0501	DỊCH VỤ AN NINH, ĐÃ MÃ HÓA	M	1	9	1	1
0534	SỐ THAM CHIẾU AN NINH	M	1	c	d	
0505	CHỨC NĂNG LỌC, ĐÃ MÃ HÓA	C	1	6	6	
S500	CHI TIẾT ĐỊNH DANH AN NINH	C	2			
0577	Hạn định bên an ninh	M		1	1	2
S500	CHI TIẾT ĐỊNH DANH AN NINH	C	2			
0577	Hạn định bên an ninh	M		2	2	3
USA	THUẬT TOÁN AN NINH	C	3			
S502	THUẬT TOÁN AN NINH	M	1			
0523	Thuật toán sử dụng , được mã hóa	M		1	1	4
0525	Phương thức mật mã hóa hoạt động, đã mã hóa	C		-	-	
0527	Thuật toán, đã mã hóa	C		40	40	
SG 2		C	2		Chỉ 1: chứng chỉ bên gửi	
USC	CHỨNG CHỈ	M	1			
0536	THAM CHIẾU CHỨNG CHỈ	C	1		Tham chiếu của chứng chỉ này	
S500	CHI TIẾT ĐỊNH DANH AN NINH	C	2		(Chủ thể chứng chỉ)	
0577	Hạn định bên an ninh	M			3	5
S500	CHI TIẾT ĐỊNH DANH AN NINH	C	2		(Bên xác thực)	
0577	Hạn định bên an ninh	M			4	6
0538	Tên khóa	C			(Tên PK/CA)	
USA	THUẬT TOÁN AN NINH	C	3		(Chức năng chữ ký của bên gửi)	

S502	THUẬT TOÁN AN NINH	M	1			
0523	Thuật toán sử dụng , đã mã hóa	M			6	7
0527	Thuật toán, đã mã hóa	C			10	
S503	THAM SỐ THUẬT TOÁN	C	9		(Độ dài các môđun)	
0531	Hạn định tham số thuật toán	M			14	
0554	Giá trị tham số thuật toán	M			Mod-L	
S503	THAM SỐ THUẬT TOÁN	C	9		(Các môđun)	
0531	Hạn định tham số thuật toán	M			12	
0554	Giá trị tham số thuật toán	M			Mod	
S503	THAM SỐ THUẬT TOÁN	C	9		(Số mũ công bố)	
0531	Hạn định tham số thuật toán	M			13	
0554	Giá trị tham số thuật toán	M			Pub-K	
USA	THUẬT TOÁN AN NINH	C	3		(Hàm băm của CA cho chữ ký chứng chỉ)	
S502	THUẬT TOÁN AN NINH	M	1			
0523	Thuật toán sử dụng, đã mã hóa	M			4	8
0525	Phương thức mật mã hóa hoạt động, đã mã hóa	C			-	
0527	Thuật toán, đã mã hóa	C			42	
USA	THUẬT TOÁN AN NINH	C	3		(Chức năng chữ ký của CA cho chữ ký chứng chỉ)	
S502	THUẬT TOÁN AN NINH	M	1			
0523	Thuật toán sử dụng, đã mã hóa	M			3	9
0527	Thuật toán, mã hóa	C			10	
USR	KẾT QUẢ AN NINH	C	1			
S508	KẾT QUẢ HỢP LỆ	M	2			11
0563	Hạn định giá trị hợp lệ	M			1	
0560	Giá trị hợp lệ	C			Sig	
USB	ĐỊNH DANH DỮ LIỆU ĐƯỢC BẢO VỆ	M	1	Tham chiếu tới các dữ liệu an toàn		
SG 3		M	9999			
USX	THAM CHIẾU AN NINH	M	1			
USY	AN NINH TRÊN THAM CHIẾU	M	9			
0534	SỐ THAM CHIẾU AN NINH	M	1	c	-	
S508	KẾT QUẢ HỢP LỆ	C	2			11

0563	Hạn định giá trị hợp lệ	M		1	-	
0560	Giá trị hợp lệ	C		Hash	-	
SG 4		M	99			
UST	ĐUÔI AN NINH	M	1			
0534	SỐ THAM CHIẾU AN NINH	M	1	c	d	
0588	SỐ LƯỢNG CÁC ĐOẠN AN NINH	M	1			
USR	KẾT QUẢ AN NINH	C	1			
S508	KẾT QUẢ HỢP LỆ	M	2			11
0563	Hạn định giá trị hợp lệ	M			1	
0560	Giá trị hợp lệ	C		-	Sig	

CHÚ THÍCH

1. Xác thực gốc và tính toàn vẹn thông điệp cho AUTACK đã nhận được chứa trong dịch vụ không-từ chối gốc. Không-từ chối gốc cấu trúc EDIFACT tham chiếu được cung cấp bởi việc liên kết tính toàn vẹn của cấu trúc EDIFACT tham chiếu và không-từ chối gốc của AUTACK;
2. Bên gửi thông điệp;
3. Bên nhận thông điệp;
4. Hàm băm được áp dụng bởi bên gửi trên cấu trúc được bảo vệ;
5. Chủ sở hữu chứng chỉ các chi tiết định danh giống như trong USH S500 đối với thông điệp bên gửi ;
6. Bên xác thực: Tổ chức chứng nhận (CA);
7. Hàm ký của bên gửi;
8. Hàm băm của CA;
9. Hàm ký của CA;
10. Một số thuật toán ký (ví dụ DSA) yêu cầu hai tham số kết quả.

B.4 Liên kết sử dụng AUTACK cho báo nhận

Các khả năng tổ hợp cho báo nhận AUTACK theo các trường hợp mô tả ở trên.

Cụ thể:

- Đối với USH 0501 mã 6 (xác thực nhận), áp dụng các liên kết của ma trận 1;
- Đối với USH 0501 mã 5 (không-từ chối nhận), áp dụng các liên kết của ma trận 2.