TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN ISO 9735-5 : 2004
ISO 9735-5 : 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 5: QUY TẮC AN NINH CHO EDI LÔ (TÍNH XÁC THỰC, TÍNH TOÀN VẸN VÀ KHÔNG TỪ CHỐI GỐC)

Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules (Syntax version number: 4, Syntax release number: 1) Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)

HÀ NỘI – 2008

Mục lục

Lời nói đầu

TCVN ISO 9735-5 : 2004 hoàn toàn tương đương với ISO 9735-5: 2002.

TCVN ISO 9735-5 : 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 an ninh cho EDI lô (tính xác thực, tính toàn vẹn và thừa nhận nguồn gốc)
- Phần 6: Thông điệp báo nhận và xác thực an ninh (kiểu thông điệp - AUTACK)
- Phần 7: Quy tắc an inh cho EDI lô (tính tin cậy)
- Phần 8: Dữ liệu liên kết trong EDI
- Phần 9: Thông điệp quản lý chứng nhận và khoá an ninh (liểu thông điệp KEYMAN)
- Phần 10: Danh mục dịch vụ cú pháp.

Tiêu chuẩn này bao gồm các quy tắc mức ứng dụng cho cấu trúc dữ liệu trong trao đổi thông điệp điện tử trong một môi trường mở, được dựa trên các yêu cầu của cả hai xử lý lô hoặc tương tác.

Các giao thức và đặc tả về truyền thông nằm ngoài phạm vi của tiêu chuẩn này.

Phần này cung cấp một khả năng tuỳ ý về bảo mật các cấu trúc EDIFACT lô, nghĩa là các thông điệp, các gói, các nhóm hoặc trao đổi.

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 5: Quy tắc an ninh cho EDI lô (tính xác thực, tính toàn vẹn và không từ chối gốc)

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

Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các quy tắc cú pháp an ninh EDIFACT và cung cấp một phương pháp tạo quy tắc an ninh mức thông điệp/gói, nhóm và trao đổi đối với tính xác thực, tính toàn vẹn và không từ chối gốc, phù hợp với các cơ chế an ninh đã được xác lập.

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), mà 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 của tiêu chuẩn đó, bao gồm tất cả các lựa chọn đều phải được tuân thủ. Nếu không tuân thủ tất cả các lựa chọn thì phải công bố rõ các lựa chọn được công bố 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 biểu diễn phù hợp với tiêu chuẩn này.

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

Khi được nêu trong tiêu chuẩn này, các điều khoản được định nghĩa trong các tiêu chuẩn liên quan phải là những chuẩn mực về sự 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) - Các quy tắc cú pháp mức ứng 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, thơng 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 2: Quy tắc cú pháp đặc trng cho EDI lô.
- TCVN ISO 9735- 6 : 2004, Trao đổi dữ liệu điện tử trong quản lý hành chính, thơng 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 báo nhận và xác thực an ninh (kiểu thông điệp - AUTACK).
- TCVN ISO 9735- 7 : 2004, Trao đổi dữ liệu điện tử trong quản lý hành chính, thơng 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 7: Quy tắc bảo mật cho EDI lô (độ tin cậy).
- TCVN ISO 9735- 8 : 2004, Trao đổi dữ liệu điện tử trong quản lý hành chính, thơng 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 8: Dữ liệu liên kết trong EDI.
- TCVN ISO 9735-10 : 2004, Trao đổi dữ liệu điện tử trong quản lý hành chính, thơng 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 10: Thư mục dịch vụ cú pháp.
- ISO/IEC 10181- 2 : 1996, Information technology - Open systems interconnection - Security frameworks for open systems: Authentication framework *(Công nghệ thông tin - Liên kết các hệ thống mở - Cơ cấu an ninh của các hệ thống mở: Cơ cấu xác thực).*
- ISO/IEC 10181- 4 : 1997, Information technology - Open systems interconnection - Security frameworks for open systems: Non-repudiation framework *(Công nghệ thông tin - Liên kết các hệ thống mở - Cơ cấu an ninh của các hệ thống mở: Cơ cấu chấp nhận).*

- ISO/IEC 10181- 6 : 1996, Information technology - Open systems interconnection - Security frameworks for open systems: Integrity framework *(Công nghệ thông tin - Liên kết các hệ thống mở - Cơ cấu an ninh của các hệ thống mở: Cơ cấu toàn vẹn).*

4 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong TCVN ISO 9735-1 : 2003

5 Quy tắc sử dụng các nhóm đoạn tiêu đề đuôi an ninh cho EDI lô.

5.1 An ninh mức thông điệp/gói - an ninh thông điệp/gói tích hợp

5.1.1 Khái quát

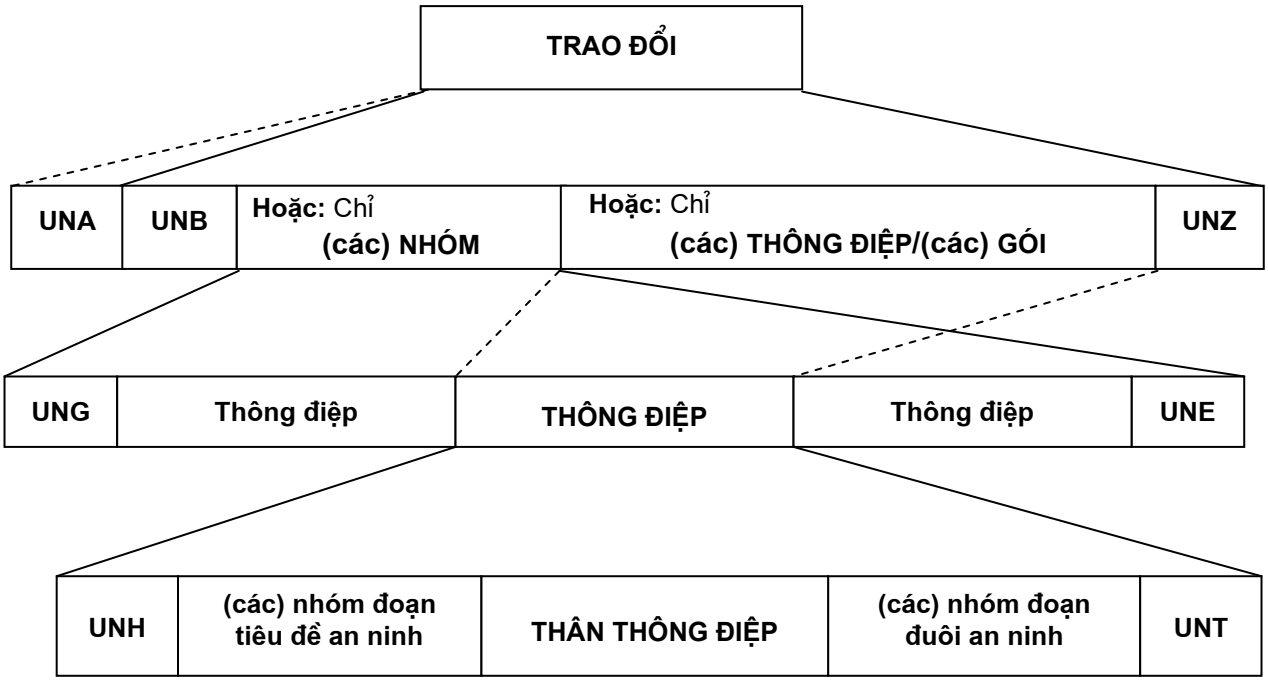
Mối đe dọa an ninh liên quan đến việc truyền thông điệp/gói và dịch vụ an ninh liên quan được trình bày trong các Phụ lục A và B.

Mục này mô tả cấu trúc an ninh mức thông điệp/gói EDIFACT.

Các dịch vụ an ninh được đề cập trong tiêu chuẩn này phải được đảm bảo bằng cách đặt các nhóm đoạn tiêu đề và đuôi an ninh sau đoạn UNH và trước đoạn UNT, cho mọi thông điệp, hoặc đặt sau đoạn UNO và trước đoạn UNP cho mọi gói.

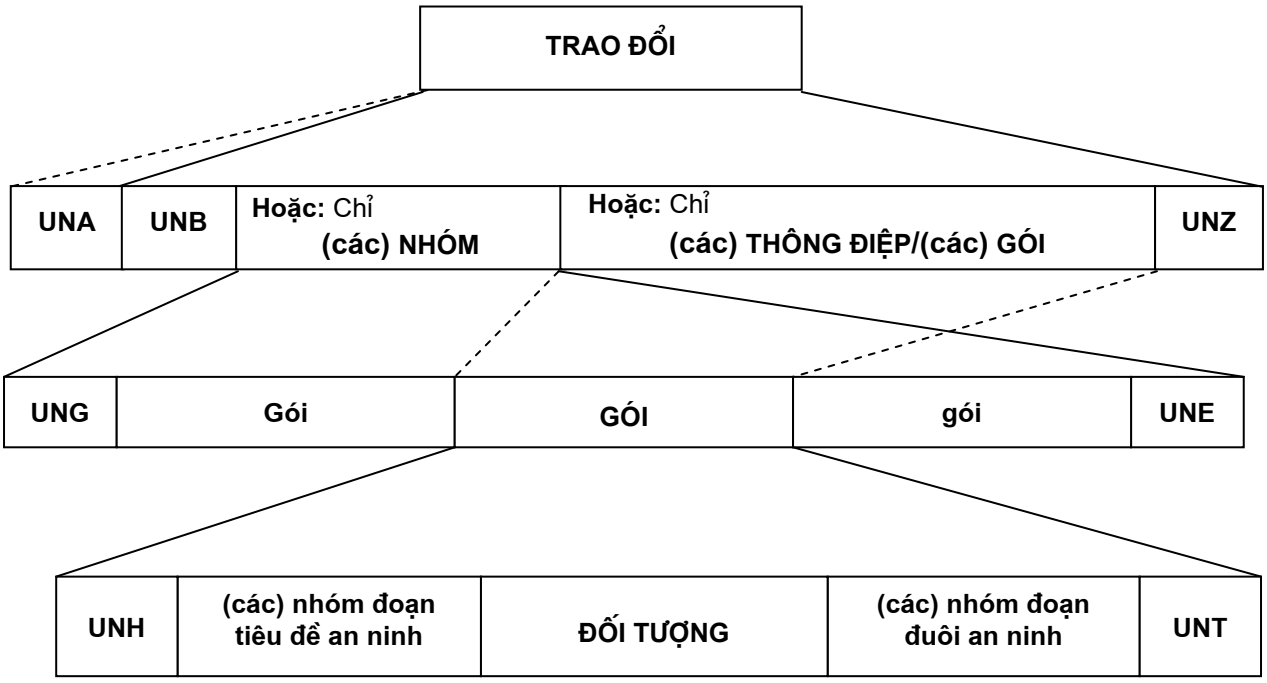
5.1.2 Các nhóm đoạn tiêu đề và các đuôi an ninh

Hình 1 mô tả một trao đổi với an ninh tại mức thông điệp.



Hình 1 - Trao đổi với an ninh tại mức thông điệp (giản đồ)

Hình 2 mô tả một trao đổi với an ninh tại mức gói.



Hình 2 - Trao đổi với an ninh tại mức gói (giản đồ)

5.1.3 Cấu trúc các nhóm đoạn tiêu đề và đuôi an ninh

Bảng 1 - Bảng các nhóm đoạn tiêu đề và đuôi an ninh (an ninh mức thông điệp)

Thẻ	Tên	S	R
UNH	Tiêu đề thông điệp	M	1
-----	Nhóm đoạn 1 ----------	C	99
USH	Tiêu đề an ninh	M	1
USA	Thuật toán an ninh	C	3
-----	Nhóm đoạn 2 ----------	C	2
USC	Chứng chỉ	M	1
USA	Thuật toán an ninh	C	3
USR	Kết quả an ninh	C	1
	Thân thông điệp		
-----	Nhóm đoạn n ----------	C	99
UST	Đuôi an ninh	M	1
USR	Kết quả an ninh	C	1
UNT	Đuôi thông điệp	M	1

Bảng 2 - Bảng các nhóm đoạn tiêu đề và đuôi an ninh (an ninh mức gói)

Thẻ	Tên	S	R
UNO	Tiêu đề đối tượng	M	1
-----	Nhóm đoạn 1 ----------	C	99
USH	Tiêu đề an ninh	M	1
USA	Thuật toán an ninh	C	3
-----	Nhóm đoạn 2 ----------	C	2
USC	Chứng chỉ	M	1
USA	Thuật toán an ninh	C	3
USR	Kết quả an ninh	C	1
	Đối tượng		
-----	Nhóm đoạn n ----------	C	99
UST	Đuôi an ninh	M	1
USR	Kết quả an ninh	C	1
UNT	Đuôi đối tượng	M	1

CHÚ THÍCH Đặc tả danh mục hoàn chỉnh của các đoạn và các phần tử dữ liệu, bao gồm các đoạn tiêu đề thông điệp UNH, đuôi thông điệp UNT, tiêu đề đối tượng UNO và đuôi đối tượng UNP được quy định trong TCVN ISO 9735-10. Danh mục phần tử dữ liệu của các đoạn này không được mô tả thêm nữa trong tiêu chuẩn này.

5.1.4 Giải thích đoạn dữ liệu

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 bao gồm dữ liệu cần thiết để tiến hành các tính toán về tính hợp lệ.

Có thể có một số nhóm đoạn tiêu đề an ninh khác nhau trong cùng một thông điệp/gói nếu có nhiều dịch vụ an ninh khác nhau được áp dụng cho thông điệp/gói đó (chẳng hạn như: tính toàn vẹn và không từ chối gốc) hoặc nếu nhiều bên cùng áp dụng một dịch vụ an ninh như vậy.

USH, Tiêu đề an ninh

Đoạn thuộc thông điệp/gói nào thì chỉ rõ dịch vụ an ninh áp dụng cho thông điệp/gói đó.

Các bên liên quan đến dịch vụ an ninh (bên tạo lập các phần tử an ninh và bên tiếp nhận các phần tử an ninh) có thể được định danh trong đoạn này, trừ khi các bên liên quan này được xác định rõ ràng thông qua các chứng chỉ (đoạn USC) khi sử dụng các thuật toán không đối xứng.

Các chi tiết định danh an ninh phần tử dữ liệu hỗn hợp (S500) phải được sử dụng trong đoạn USH,

- nếu sử dụng các thuật toán đối xứng, hoặc

- nếu sử dụng các thuật toán không đối xứng khi hai chứng chỉ cùng tồn tại nhằm phân biệt chứng chỉ của bên tạo lập và chứng chỉ của bên tiếp nhận.

Trong trường hợp sau, định danh bên tham gia trong phần tử S500 (một trong các phần tử dữ liệu S500/0511, S500/0513, S500/0515, S500/0586) phải giống định danh của bên được hạn định là "bên sở hữu chứng chỉ" của một trong các phần tử dữ liệu S500 tồn tại trong đoạn USC trong nhóm đoạn 2 và phần tử dữ liệu S500/0577 phải xác định chức năng (bên tiếp nhận hoặc bên tạo lập) của các bên tham gia đó.

Có thể sử dụng tên khoá phần tử dữ liệu trong phần tử dữ liệu hỗn hợp về chi tiết dịch vụ an ninh (S500/0538) để thiết lập mối quan hệ khoá giữa bên gửi và bên tiếp nhận.

Cũng có thể thiết lập mối quan hệ khoá bằng cách sử dụng định danh phần tử dữ liệu của khoá phần tử dữ liệu hỗn hợp về thông số thuật toán (S503/0554) trong đoạn USA của nhóm đoạn 1.

Có thể sử dụng S500/0538 trong đoạn USH nếu không có nhu cầu truyền đoạn USA trong nhóm đoạn 1 (bởi vì các cơ chế mật mã hoá đã được thoả thuận trước giữa các bên).

Tuy nhiên, trong cùng một nhóm tiêu đề an ninh, khuyến cáo sử dụng S500/0538 trong đoạn USH hoặc S503/0554 với hạn định thích hợp trong đoạn USA, nhưng không được sử dụng cả hai trong cùng một nhóm tiêu đề an ninh.

Đoạn USH có thể chỉ rõ hàm lọc được sử dụng cho các file nhị phân của đoạn USA trong nhóm đoạn 1 và của đoạn USR của nhóm đuôi an ninh tương ứng.

Đoạn USH có thể bao gồm một số hiệu thứ tự an ninh để quy định tính toàn vẹn thứ tự và ngày tạo các phần tử an ninh.

USA, thuật toán an ninh

Đoạn xác định một thuật toán an ninh, kỹ thuật sử dụng tạo ra thuật toán và các tham số kỹ thuật hoặc yêu cầu. Thuật toán này phải được áp dụng trực tiếp trên thông điệp/gói. Thuật toán này có thể là thuật toán đối xứng, hàm băm hoặc thuật toán nén. Ví dụ một chữ ký số chỉ ra hàm băm phụ thuộc–thông điệp được sử dụng.

Thuật toán không đối xứng không được đề cập trực tiếp trong đoạn USA của nhóm đoạn 1, nhưng có thể chỉ xuất hiện trong nhóm đoạn 2 và được khởi tạo bởi một đoạn USC.

Đoạn USA được phép xuất hiện ba lần. Một lần xuất hiện được sử dụng cho thuật toán đối xứng hoặc hàm băm được yêu cầu để cung cấp dịch vụ an ninh quy định trong đoạn USH. Hai lần xuất hiện khác được trình bày trong TCVN ISO 9735-7.

Nếu thích hợp, có thể sử dụng chỉ dẫn cơ chế đệm.

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

Nhóm đoạn chứa dữ liệu cần thiết để xác định tính hợp lệ của các phương pháp an ninh được áp dụng cho thông điệp/gói khi sử dụng các thuật toán không đối xứng. Nhóm đoạn chứng chỉ phải được sử

dụng khi sử dụng các thuật toán không đối xứng để xác định cặp khoá không đối xứng đã được sử dụng, thậm chí khi các chứng chỉ không được sử dụng.

Nhóm đoạn chứng chỉ đầy đủ (bao gồm cả đoạn USR) hoặc chỉ các phần tử dữ liệu cần thiết để xác định một cách rõ ràng cặp khoá không đối xứng đã được sử dụng phải có trong đoạn USC. Có thể không cần thiết đưa ra một chứng chỉ đầy đủ nếu chứng chỉ này vừa được trao đổi bởi hai bên tham gia hoặc có thể được gọi ra từ một cơ sở dữ liệu.

Khi áp dụng một chứng chỉ không phải là EDIFACT (ví dụ X.509), cú pháp và phiên bản chứng chỉ phải được xác định trong phần tử dữ liệu 0545 của đoạn USC. Các chứng chỉ này có thể được gửi trong một gói EDIFACT.

Nhóm đoạn này được phép xuất hiện hai lần, một lần là chứng chỉ của bên gửi thông điệp/gói (mà bên tiếp nhận thông điệp/gói sẽ sử dụng để xác minh chữ ký của bên gửi), lần xuất hiện khác là chứng chỉ bên tiếp nhận thông điệp/gói (chỉ dành cho tham chiếu chứng chỉ) trong trường hợp khi mà bên gửi sử dụng khoá công bố của bên tiếp nhận để đảm bảo tính bảo mật của khóa đối xứng.

Nếu nhóm đoạn này xuất hiện hai lần trong cùng một nhóm đoạn tiêu đề an ninh, thì phần tử dữ liệu hỗn hợp về chi tiết định danh an ninh (S500) cùng với phần tử dữ liệu tham chiếu chứng chỉ (0536) cho phép phân biệt chúng.

Nhóm đoạn này phải lược bỏ nếu không sử dụng thuật toán không đối xứng.

USC, chứng chỉ

Đoạn chứa các thông tin về năng lực của bên sở hữu chứng chỉ và xác định tổ chức chứng nhận cấp chứng chỉ. Hàm lọc phần tử dữ liệu, đã mã hoá là (0505), phải xác định hàm lọc được sử dụng cho các trường nhị phân của các đoạn USA và đoạn USR trong nhóm đoạn 2.

Phần tử dữ liệu S500 có thể xuất hiện hai lần trong Chứng chỉ USC: một lần cho bên sở hữu chứng chỉ (xác định bên đã ký cùng với khoá riêng kết hợp với khoá công bố trong chứng chỉ này), một lần cho bên phát hành chứng chỉ (tổ chức chứng nhận hoặc CA).

USA, thuật toán an ninh

Đoạn xác định một thuật toán an ninh, cách sử dụng kỹ thuật tạo ra thuật toán và chứa các tham số kỹ thuật được yêu cầu. Ba lần xuất hiện khác nhau của đoạn USA trong nhóm đoạn 2 là:

1. Bên phát hành chứng chỉ sử dụng thuật toán này để tính toán giá trị băm của chứng chỉ (hàm băm);
2. Bên phát hành chứng chỉ sử dụng thuật toán này để tạo ra chứng chỉ (nghĩa là ghi kết quả của hàm băm được tính toán vào nội dung chứng chỉ) (thuật toán không đối xứng);

3a - Bên gửi sử dụng thuật toán này để ghi vào thông điệp/gói (nghĩa là ghi kết quả của hàm băm được mô tả trong đoạn USH, được tính toán vào nội dung thông điệp/gói) (thuật toán không đối xứng); hoặc

3b - Bên gửi sử dụng thuật toán không đối xứng của bên tiếp nhận để mật mã hoá khoá được yêu cầu bởi một thuật toán đối xứng thích hợp với nội dung thông điệp/gói và được đưa ra bởi nhóm đoạn 1 được khởi tạo bởi đoạn USH (thuật toán không đối xứng).

Nếu thích hợp, có thể sử dụng chỉ dẫn cơ chế đệm.

USR, kết quả an ninh

Đoạn chứa kết quả của chức năng an ninh được áp dụng cho chứng chỉ bởi tổ chức chứng nhận. Kết quả này chính là chữ ký của chứng chỉ được tính toán bởi tổ chức chứng nhận bằng cách ký nhận kết quả băm được tính toán theo dữ liệu về khả năng.

Đối với chứng chỉ, việc tính toán chữ ký bắt đầu với ký tự đầu tiên của đoạn USC (ký tự "U") và kết thúc với ký tự cuối cùng của đoạn USA cuối cùng (bao gồm cả dấu phân tách theo sau đoạn USA).

Nhóm đoạn n: UST - USR (nhóm đuôi an ninh)

Nhóm đoạn chứa một liên kết với nhóm đoạn tiêu đề an ninh và kết quả của các chức năng an ninh được áp dụng cho thông điệp/gói.

UST, đuôi an ninh

Đoạn thiết lập một liên kết giữa nhóm đoạn tiêu đề an ninh và nhóm đoạn đuôi an ninh, và cho biết số lượng các đoạn an ninh chứa trong các nhóm này.

USR, kết quả an ninh

Đoạn chứa kết quả của các chức năng an ninh được áp dụng cho thông điệp/gói như quy định trong nhóm tiêu đề an ninh liên kết. Tùy thuộc vào các cơ chế an ninh quy định trong nhóm tiêu đề an ninh, kết quả này phải:

- được tính toán trực tiếp theo thông điệp/gói bằng thuật toán quy định trong đoạn USA trong nhóm đoạn 1 của nhóm tiêu đề an ninh, hoặc là
- được tính toán bằng cách ký nhận cùng với một thuật toán không đối xứng được quy định trong đoạn USA trong nhóm đoạn 2 của nhóm đoạn tiêu đề an ninh, một kết quả băm được tính toán theo thông điệp/gói bằng thuật toán được quy định trong đoạn USA trong nhóm đoạn 1 của nhóm đoạn tiêu đề an ninh.

5.1.5 Phạm vi áp dụng an ninh

Có hai khả năng cho phạm vi áp dụng an ninh:

1. Việc tính toán mỗi giá trị xác thực và toàn vẹn và tính toán các chữ ký số bắt đầu bằng và bao gồm cả nhóm đoạn tiêu đề an ninh hiện thời và thân thông điệp hoặc đối tượng. Trong trường hợp này, các nhóm đoạn tiêu đề an ninh và đuôi an ninh khác đều phải nằm ngoài phạm vi này.

Nhóm đoạn tiêu đề an ninh phải được tính từ ký tự đầu tiên, ký tự "U", đến dấu phân tách kết thúc nhóm đoạn tiêu đề an ninh này, gồm cả hai, thân thông điệp hoặc đối tượng từ ký tự đầu tiên sau dấu phân tách kết thúc nhóm đoạn tiêu đề an ninh cuối cùng đến dấu phân tách trước ký tự đầu tiên của nhóm đoạn đuôi an ninh đầu tiên.

Do đó trật tự các dịch vụ an ninh được tích hợp theo cách này đã được thực hiện, không cần quy định. Các dịch vụ an ninh này hoàn toàn độc lập với nhau.

Hình 3 minh họa trường hợp này (phạm vi áp dụng dịch vụ an ninh được xác định trong tiêu đề an ninh 2 được biểu diễn bằng các khối bóng).

UNH/ *UNO*	Nhóm đoạn tiêu đề an ninh 3	Nhóm đoạn tiêu đề an ninh 2	Nhóm đoạn tiêu đề an ninh 1	THÂN THÔNG ĐIỆP/ *ĐỐI TƯỢNG*	Nhóm đoạn đuôi an ninh 1	Nhóm đoạn đuôi an ninh 2	Nhóm đoạn đuôi an ninh 3	UNT/ *UNP*

Hình 3 - Phạm vi áp dụng: chỉ nhóm đoạn tiêu đề an ninh và thân thông điệp/đối tượng (giản đồ)

2. Tính toán bắt đầu và bao gồm nhóm đoạn tiêu đề an ninh hiện hành tới nhóm đoạn đuôi an ninh được liên kết. Trong trường hợp này nhóm đoạn tiêu đề an ninh hiện thời thân, thông điệp hoặc đối tượng, và tất cả các nhóm đoạn tiêu đề và đuôi an ninh được nhúng khác nằm trong phạm vi này.

   Phạm vi này phải bao gồm tất cả ký tự từ ký tự đầu tiên, ký tự "U", của nhóm đoạn tiêu đề an ninh hiện thời tới dấu phân tách trước ký tự đầu tiên của nhóm đoạn đuôi an ninh được liên kết.

Hình 4 minh họa trường hợp này (phạm vi áp dụng dịch vụ an ninh được xác định trong tiêu đề an ninh 2 được biểu diễn bằng các khối bóng).

UNH/ *UNO*	Nhóm đoạn tiêu đề an ninh 3	Nhóm đoạn tiêu đề an ninh 2	Nhóm đoạn tiêu đề an ninh 1	THÂN THÔNG ĐIỆP/ ĐỐI TƯỢNG	Nhóm đoạn đuôi an ninh 1	Nhóm đoạn đuôi an ninh 2	Nhóm đoạn đuôi an ninh 3	UNT/ *UNP*

Hình 4 - Phạm vi áp dụng: từ nhóm đoạn tiêu đề an ninh tới nhóm đoạn đuôi an ninh (giản đồ)

Đối với mỗi dịch vụ an ninh, có thể chọn một trong hai cách.

Trong cả hai trường hợp, mối quan hệ giữa nhóm đoạn tiêu đề an ninh và nhóm đoạn đuôi an ninh tương ứng phải được cung cấp bởi số hiệu tham chiếu an ninh của các phần tử dữ liệu trong đoạn UST và USH.

5.2 Nguyên tắc sử dụng

5.2.1 Lựa chọn dịch vụ

Nhóm đoạn tiêu đề an ninh có thể gồm thông tin chung sau:

- dịch vụ an ninh được áp dụng;
- định danh của các bên liên quan;
- cơ chế an ninh được sử dụng;
- giá trị "duy nhất" (số hiệu thứ tự và/hoặc thẻ thời gian);
- không-từ chối yêu cầu nhận.

Nếu có hơn một dịch vụ an ninh được yêu cầu cho cùng một cấu trúc EDIFACT thì nhóm đoạn tiêu đề an ninh có thể xuất hiện nhiều lần. Trong trường hợp này có nhiều cặp của các bên liên quan. Tuy nhiên, nếu nhiều dịch vụ được yêu cầu giữa hai bên thì chúng có thể được gộp trong một cặp nhóm đoạn tiêu đề và được bảo vệ khi mà chắc chắn các dịch vụ bao hàm nhau hoàn toàn.

5.2.2 Tính xác thực

Nếu có yêu cầu về xác thực gốc của một cấu trúc EDIFACT thì phải phù hợp với các nguyên tắc trong ISO/IEC 10181-2 bằng cách sử dụng một cặp nhóm đoạn tiêu đề an ninh và đuôi an ninh thích hợp.

Dịch vụ an ninh xác thực gốc phải quy định trong đoạn USH và thuật toán được định danh trong đoạn USA trong nhóm đoạn 1 phải là một thuật toán đối xứng.

Bên khởi tạo dịch vụ an ninh phải tính toán một giá trị xác thực được truyền trong đoạn USR của nhóm đoạn đuôi an ninh. Bên tiếp nhận dịch vụ an ninh phải kiểm tra giá trị xác thực.

Dịch vụ này có thể bao gồm dịch vụ toàn vẹn và có thể đạt được như dịch vụ phụ của dịch vụ không từ chối gốc.

Nếu thực hiện một cách thích hợp dịch vụ "xác thực gốc" dựa trên phần cứng chống giả mạo hoặc được chứng thực bởi bên thứ ba được xem như một trường hợp của dịch vụ "không từ chối gốc". Trên thực tế, dịch vụ này được xác định trong thoả thuận trao đổi.

5.2.3 Tính toàn vẹn

Nếu có yêu cầu về tính toàn vẹn nội dụng một cấu trúc EDIFACT thì phải phù hợp với các nguyên tắc trong ISO/IEC 10181-6 bằng cách sử dụng một cặp nhóm đoạn tiêu đề an ninh và đuôi an ninh thích hợp.

Dịch vụ an ninh về tính toàn vẹn phải quy định trong đoạn USH, và thuật toán được xác định trong đoạn USA của nhóm đoạn 1. Thuật toán này phải là hàm băm hoặc một thuật toán đối xứng.

Bên khởi tạo dịch vụ an ninh phải tính toán một giá trị toàn vẹn được truyền trong đoạn USR của nhóm đoạn đuôi an ninh. Bên tiếp nhận dịch vụ an ninh phải kiểm tra giá trị toàn vẹn.

Dịch vụ này có thể đạt được như dịch vụ phụ của dịch vụ xác thực gốc hoặc dịch vụ không từ chối gốc.

Nếu có yêu cầu về toàn vẹn thứ tự thì số hiệu thứ tự an ninh hoặc một thẻ thời gian an ninh hoặc cả hai phải được chứa trong nhóm đoạn tiêu đề an ninh và phải sử dụng hoặc dịch vụ về tính toàn vẹn nội dung hoặc dịch vụ xác thực gốc hoặc dịch vụ không từ chối gốc.

5.2.4 Không từ chối gốc

Nếu có yêu cầu không từ chối gốc một cấu trúc EDIFACT thì phải phù hợp với các nguyên tắc trong ISO/IEC 10181-4 bằng cách sử dụng một cặp nhóm đoạn tiêu đề an ninh và đuôi an ninh thích hợp.

Dịch vụ an ninh không từ chối gốc phải quy định trong đoạn USH và thuật toán băm phải quy định trong đoạn USA trong nhóm đoạn 1, và thuật toán không đối xứng được sử dụng cho chữ ký trong các đoạn USA của nhóm đoạn 2 nếu sử dụng các chứng chỉ.

Nếu chứng chỉ không được truyền trong thông điệp/gói thì thuật toán không đối xứng phải được xác định hoàn toàn bởi bên tiếp nhận. Trong trường hợp này, thuật toán không đối xứng phải được xác định trong thoả thuận trao đổi.

Bên khởi tạo dịch vụ an ninh phải tính toán một chữ ký số được truyền trong đoạn USR của nhóm đoạn đuôi an ninh. Bên tiếp nhận dịch vụ an ninh phải xác định giá trị chữ ký số này.

Dịch vụ này cũng cung cấp cả dịch vụ về tính toàn vẹn nội dung và xác thực gốc.

5.3 Các bộ lọc và biểu diễn nội bộ theo cú pháp EDIFACT

Có hai vấn đề khi sử dụng các thuật toán toán học để tính toán các giá trị toàn vẹn và các chữ ký số.

Vấn đề thứ nhất là kết quả tính toán phụ thuộc vào sự biểu diễn nội bộ của bộ ký tự. Do đó việc tính toán chữ ký số được thực hiện bởi bên gửi và bên tiếp nhận phải sử dụng cùng bộ ký tự mã hoá để xác định. Do đó bên gửi có thể chỉ ra việc biểu diễn được sử dụng để đưa ra kết quả an ninh gốc hợp lệ.

Vấn đề thứ hai là kết quả tính toán có vẻ như là một mẫu bít ngẫu nhiên. Đây có thể là nguyên nhân gây ra các vấn đề trong quá trình truyền và với phần mềm biên dịch. Để tránh các vấn đề này thì mẫu bít có thể được ánh xạ ngược tới một biểu diễn đặc biệt của bộ ký tự bằng phương pháp hàm lọc. Để đơn giản, mỗi dịch vụ an ninh chỉ sử dụng một hàm lọc. Bất kỳ hiện tượng kết thúc khác thường nào ở đầu ra ánh xạ này được giải quyết bằng một trình tự thoát.

6 Quy tắc sử dụng nhóm đoạn tiêu đề và đuôi an ninh của nhóm và trao đổi cho EDI lô

6.1 An ninh mức nhóm và mức trao đổi - an ninh thông điệp tích hợp

Các mối đe dọa an ninh liên quan đến việc truyền thông điệp/gói và các dịch vụ an ninh dùng để chống lại các mối đe dọa đó được mô tả trong các phụ lục A và B cũng hợp lệ đối với mức nhóm và trao đổi.

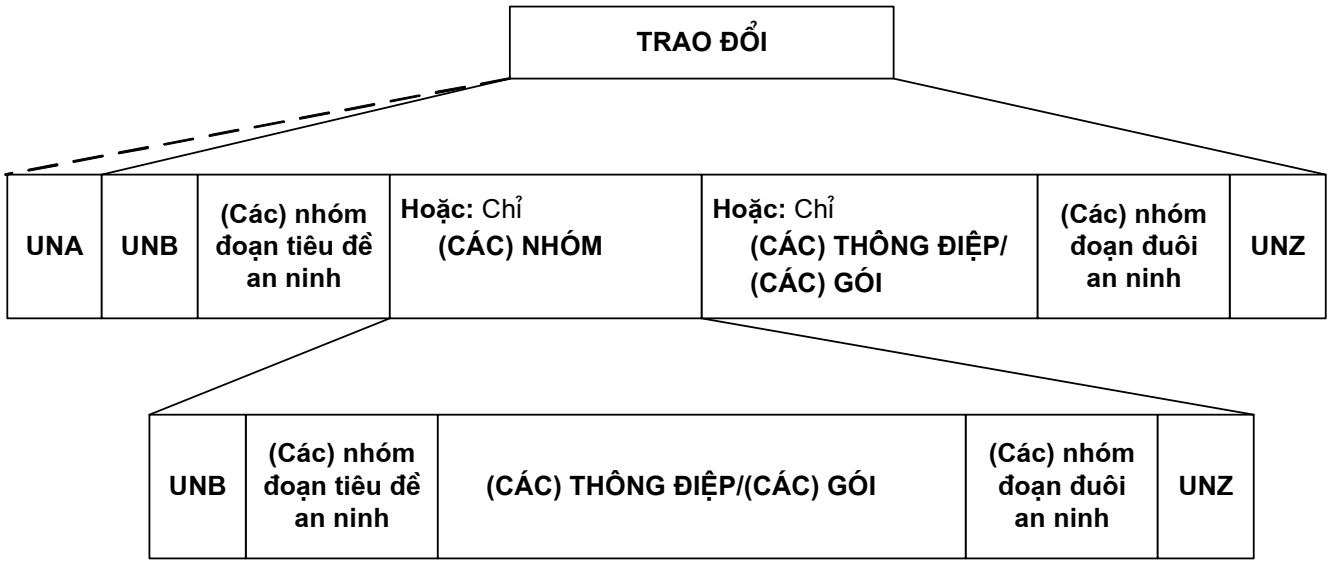
Các kỹ thuật đã mô tả ở mục trước về áp dụng an ninh cho các thông điệp/gói cũng có thể áp dụng cho nhóm và trao đổi.

Đối với an ninh mức nhóm và trao đổi, phải sử dụng cùng các nhóm đoạn tiêu đề và nhóm đoạn đuôi như đã mô tả ở mức thông điệp/gói, và sự tham chiếu ngang của tiêu đề - đuôi phải áp dụng tại cùng mức, cả khi dịch vụ an ninh được áp dụng riêng tại nhiều hơn một mức.

Khi dịch vụ an ninh được áp dụng tại mức thông điệp/gói cấu trúc được bảo vệ là thân thông điệp hoặc đối tượng. Tại mức nhóm, cấu trúc được bảo vệ là bộ các các thông điệp/gói trong nhóm bao gồm tất cả các tiêu đề và đuôi thông điệp/gói. Tại mức trao đổi, cấu trúc được bảo vệ là bộ các thông điệp/gói hoặc các nhóm trong trao đổi bao gồm tất cả các tiêu đề và đuôi thông điệp hoặc nhóm.

6.2 Nhóm đoạn tiêu đề và đuôi an ninh

Hình 5 – Mô tả một trao đổi với an ninh tại cả mức nhóm và mức trao đổi.



Hình 5 - Trao đổi với an ninh tại cả mức nhóm và mức trao đổi (giản đồ)

6.3 Cấu trúc các nhóm đoạn tiêu đề và đuôi an ninh

Bảng 3 - Bảng đoạn các nhóm đoạn tiêu đề và đuôi an ninh (chỉ an ninh mức trao đổi)

THẺ	Tên	S	R
UNB	Tiêu đề trao đổi	M	1
-----	Nhóm đoạn 1 ----------	C	99
USH	Tiêu đề an ninh	M	1
USA	Thuật toán an ninh	C	3
-----	Nhóm đoạn 2 ----------	C	2
USC	Chứng chỉ	M	1
USA	Thuật toán an ninh	C	3
USR	Kết quả an ninh	C	1
	(Các) Nhóm hoặc (các) Thông điệp/(các) Gói		
-----	Nhóm đoạn n ----------	C	99
UST	Đuôi an ninh	M	1
USN	Kết quả an ninh	C	1
URZ	Đuôi trao đổi	M	1

Bảng 4 – Bảng đoạn các nhóm đoạn tiêu đề và đuôi an ninh (chỉ an ninh mức nhóm)

THẺ	Tên	S	R
UNB	Tiêu đề nhóm	M	1
-----	Nhóm đoạn 1 ----------	C	99
USH	Tiêu đề an ninh	M	1
USA	Thuật toán an ninh	C	3
-----	Nhóm đoạn 2 ----------	C	2
USC	Chứng chỉ	M	1
USA	Thuật toán an ninh	C	3
USR	Kết quả an ninh	C	1
	(Các) Thông điệp/(các) Gói		
-----	Nhóm đoạn n ----------	C	99
UST	Đuôi an ninh	M	1
USN	Kết quả an ninh	C	1
URZ	Đuôi nhóm	M	1

CHÚ THÍCH Đặc tả danh mục hoàn chỉnh của các đoạn và phần tử dữ liệu bao gồm các đoạn tiêu đề trao đổi UNB, các đoạn đuôi trao đổi UNZ, tiêu đề nhóm UNG và đuôi nhóm UNE quy định trong tiêu chuẩn TCVN ISO 9735-10 không được mô tả trong tiêu chuẩn này.

6.4 Phạm vi áp dụng an ninh

Có hai khả năng phạm vi áp dụng an ninh

1. Tính toán mỗi giá trị xác thực và toàn vẹn và tính toán các chữ ký số bắt đầu và bao gồm với chính nhóm đoạn tiêu đề an ninh hiện hành và cả (các) thông điệp/(các) gói hoặc (các) nhóm. Trong trường hợp này, nhóm đoạn tiêu đề hoặc đuôi an ninh khác không thuộc phạm vi này.

   Nhóm đoạn tiêu đề an ninh được tính từ ký tự đầu tiên, ký tự "U", đến dấu phân tách kết thúc nhóm đoạn tiêu đề an ninh này, gồm cả hai, và (các) thông điệp/(các)gói hoặc (các) nhóm thì từ ký tự đầu tiên sau dấu phân tách kết thúc nhóm đoạn tiêu đề an ninh cuối cùng đến dấu phân tách trước ký tự đầu tiên của nhóm đoạn đuôi an ninh đầu tiên, bao gồm cả hai.

   Do đó thứ tự các dịch vụ an ninh được tích hợp theo cách này, không cần quy định. Các dịch vụ an ninh này hoàn toàn độc lập với nhau.

Hình 6 và 7 minh họa cho trường hợp này (phạm vi áp dụng dịch vụ an ninh xác định trong tiêu đề an ninh 2 được biểu diễn bằng các khối bóng).

UNB	Nhóm đoạn tiêu đề an ninh 3	Nhóm đoạn tiêu đề an ninh 2	Nhóm đoạn tiêu đề an ninh 1	(CÁC) NHÓM HOẶC (CÁC) THÔNG ĐIỆP/ (CÁC) GÓI	Nhóm đoạn đuôi an ninh 1	Nhóm đoạn đuôi an ninh 2	Nhóm đoạn đuôi an ninh 3	UNZ

Hình 6 – Phạm vi áp dụng: nhóm đoạn tiêu đề an ninh và (các) nhóm hoặc chỉ (các) thông điệp/(các) gói (giản đồ)

UNG	Nhóm đoạn tiêu đề an ninh 3	Nhóm đoạn tiêu đề an ninh 2	Nhóm đoạn tiêu đề an ninh 1	(CÁC) THÔNG ĐIỆP/ (CÁC) GÓI	Nhóm đoạn đuôi an ninh 1	Nhóm đoạn đuôi an ninh 2	Nhóm đoạn đuôi an ninh 3	UNE

Hình 7 – Phạm vi áp dụng: chỉ nhóm đoạn tiêu đề an ninh và (các) thông điệp/(các) gói (giản đồ)

2. Việc tính toán bắt đầu và bao gồm cả nhóm đoạn tiêu đề an ninh hiện tới nhóm đoạn đuôi an ninh được liên kết. Trong trường hợp này, nhóm đoạn tiêu đề an ninh hiện hành, (các) thông điệp/(các) gói hoặc (các) nhóm và tất cả các nhóm đoạn tiêu đề và nhóm đoạn đuôi an ninh được nhúng khác thuộc phạm vi này.

Phạm vi này bao gồm tất cả các ký tự từ ký tự đầu tiên, ký tự "U", của nhóm đoạn tiêu đề an ninh hiện hành, đến dấu phân tách trước ký tự đầu tiên của nhóm đoạn đuôi an ninh liên kết, bao gồm cả hai.

Hình 8 và 9 minh họa cho trường hợp này (phạm vi áp dụng dịch vụ an ninh xác định trong tiêu đề an ninh 2 được biểu diễn bằng các khối bóng).

UNB	Nhóm đoạn tiêu đề an ninh 3	Nhóm đoạn tiêu đề an ninh 2	Nhóm đoạn tiêu đề an ninh 1	(CÁC) NHÓM HOẶC (CÁC) THÔNG ĐIỆP/ (CÁC) GÓI	Nhóm đoạn đuôi an ninh 1	Nhóm đoạn đuôi an ninh 2	Nhóm đoạn đuôi an ninh 3	UNZ

Hình 8 – Phạm vi áp dụng: từ nhóm đoạn tiêu đề an ninh tới nhóm đoạn đuôi an ninh (giản đồ)

UNG	Nhóm đoạn tiêu đề an ninh 3	Nhóm đoạn tiêu đề an ninh 2	Nhóm đoạn tiêu đề an ninh 1	(CÁC) THÔNG ĐIỆP/ (CÁC) GÓI	Nhóm đoạn đuôi an ninh 1	Nhóm đoạn đuôi an ninh 2	Nhóm đoạn đuôi an ninh 3	UNE

Hình 9 – Phạm vi áp dụng: từ nhóm đoạn tiêu đề an ninh tới nhóm đoạn đuôi an ninh (giản đồ)

Đối với mỗi dịch vụ an ninh được bổ sung, có thể chọn một trong hai phương pháp trên.

Trong cả hai trường hợp, mối liên hệ giữa nhóm đoạn tiêu đề và đuôi an ninh được kết nối phải được cung cấp bởi số hiệu tham chiếu an ninh của các phần tử dữ liệu trong các đoạn UST và USH.

Phụ lục A

(tham khảo)

Các mối đe dọa và giải pháp cho an ninh EDIFACT

A.1 Giới thiệu

Phụ lục này mô tả các mối đe dọa an ninh chung do truyền thông điệp/gói giữa (các) bên khởi tạo thông điệp/gói và (các) bên tiếp nhận. Phương pháp tiếp cận chung để khắc phục các mối đe dọa này cũng được nói đến. Các mối đe dọa và giải pháp này liên quan đến tất cả các mức: thông điệp/gói, nhóm hoặc trao đổi.

A.2 Các mối đe dọa an ninh

Việc lưu trữ và truyền các thông điệp/gói EDIFACT qua môi trường và phương tiện điện tử dẫn đến một số mối đe dọa, đáng chú ý là:

- Để lộ nội dung thông điệp/gói một cách trái phép;
- chèn có chủ định các thông điệp/gói giả;
- sao chép, mất mát hoặc lặp lại các thông điệp/gói;
- thay đổi nội dung thông điệp/gói;
- xóa các thông điệp/gói;
- từ chối chịu trách nhiệm về thông điệp/gói của bên gửi hoặc bên tiếp nhận.

Các mối đe dọa trên có thể do cố ý như việc thao tác trái phép trên nội dung thông điệp/gói, hoặc do vô ý như một lỗi truyền thông làm thay đổi nội dung thông điệp/gói.

A.3 Các giải pháp an ninh - Các dịch vụ cơ bản và các nguyên tắc sử dụng

A.3.1 Khái quát

Để chống lại các mối đe dọa nói trên, một số cơ chế an ninh đã được xác định có sử dụng một hoặc nhiều phương pháp luận nhằm đáp ứng những mục đích tương ứng.

Điều quan trọng là có thể xác định rõ ràng các bên liên quan khi các thông điệp/gói được bảo vệ -bên khởi tạo an ninh, để cho đơn giản gọi là bên gửi, là bên khởi tạo dịch vụ an ninh thông điệp/gói trước khi truyền và bên tiếp nhận an ninh, để cho đơn giản gọi là bên tiếp nhận, là bên thực hiện kiểm tra thông điệp/gói nhận được. Các bên tham gia có thể được xác định trong các đoạn an ninh. Để xác định các bên có thể sử dụng các phương pháp được gọi là chứng chỉ (trong thực tế, hoặc là một chứng chỉ thật hoặc là một tham chiếu chứng chỉ), được giải thích bên dưới, nếu sử dụng các thuật toán không đối xứng.

Điển hình yêu cầu sử dụng một tổ chức chứng nhận trong một hệ thống mở. Đây là bên thứ ba được uỷ quyền bởi các bên liên quan với một mức độ giới hạn, cụ thể là để xác định và lưu trữ tất cả bên sử dụng cùng khóa công bố. Thông tin này được chuyển đến các bên sử dụng khác bằng cách sử dụng một chứng chỉ, đó là một chữ ký số do CA phát hành trên một thông điệp chứa thông tin định danh bên sử dụng cùng khóa công bố của bên sử dụng. Trong trường hợp này, sự ủy thác hoàn toàn mang tính chức năng và không liên quan đến bảo mật hoặc khoá riêng.

Ngoài ra, nếu sử dụng các kỹ thuật đối xứng để xác định các bên liên quan được chỉ ra trong các trường tên bên gửi/bên tiếp nhận an ninh.

Một thông điệp/gói có thể được bảo vệ bởi nhiều bên tham gia (ví dụ một thông điệp/gói có nhiều chữ ký số) và vì vậy các thông tin an ninh liên quan có thể được lặp lại để cho phép định danh nhiều nhiều bên tham gia ký nhận hoặc chứng nhận và bao gồm nhiều chữ ký điện tử và giá trị kiểm soát tương ứng.

Các yêu cầu và kỹ thuật được quy định để bảo vệ thông điệp/gói, nhóm hoặc trao đổi EDIFACT được trình bày bên dưới.

A.3.2 Toàn vẹn thứ tự

Tính toàn vẹn thứ tự bảo vệ ngăn ngừa sao chép, thêm, xóa, mất hoặc lặp lại một cấu trúc EDIFACT (thông điệp/gói, nhóm hoặc trao đổi).

Để phát hiện các thông điệp/gói, nhóm hoặc trao đổi bị mất:

- bên gửi và có thể cả bên tiếp nhận kiểm tra một số hiệu thứ tự (liên quan đến dòng thông điệp/gói giữa hai bên liên quan);
- bên gửi có thể yêu cầu và kiểm tra tin báo nhận;

Để phát hiện các thông điệp/gói, các nhóm hoặc trao đổi bị thêm hoặc nhân đôi;

- bên gửi và có thể cả bên tiếp nhận kiểm tra một số hiệu thứ tự;
- bên gửi và có thể cả bên tiếp nhận kiểm tra một thẻ thời gian;

Khi các số hiệu thứ tự được sử dụng chúng phải được thỏa thuận giữa các bên tham gia về cách thức quản lý.

Thẻ thời gian thường được tạo ra bởi hệ thống của bên gửi. Điều này hàm ý rằng, như trong dạng giấy, độ chính xác ban đầu của giá trị thẻ thời gian chỉ nằm dưới sự kiểm soát của bên gửi.

Để có sự bảo vệ đầy đủ, tính toàn vẹn của thẻ thời gian hoặc số hiệu thứ tự phải bảo đảm bằng một trong các chức năng khác được đề cập sau đây.

A.3.3 Toàn vẹn nội dung

Dịch vụ an ninh về tính toàn vẹn nội dung bảo vệ chống lại sự thay đổi dữ liệu.

Việc bảo vệ có thể được thực hiện bởi bên gửi bao gồm một giá trị kiểm soát tính toàn vẹn. Giá trị này được tính toán bằng cách sử dụng một thuật toán mật mã hoá thích hợp, chẳng hạn MDC (mã phát hiện sự thay đổi). Vì chính giá trị kiểm soát này không được bảo vệ nên cần bổ sung các phép đánh giá lên giá trị kiểm soát như gửi giá trị kiểm soát bằng một kênh dành riêng hoặc việc tính toán một chữ ký số, thậm chí cần thiết cung cấp cả an ninh không - từ chối gốc trên giá trị kiểm soát này. Ngoài ra, Để sự xác thực gốc đạt được bằng việc sử dụng một mã xác thực thông điệp phải bao gồm cả dịch vụ về tính toàn vẹn nội dung. Bên tiếp nhận tính toán giá trị kiểm soát toàn vẹn của dữ liệu thực sự nhận được thông qua việc sử dụng các thuật toán và tham số tương ứng và so sánh kết quả với giá trị nhận được.

Cuối cùng, dịch vụ về tính toàn vẹn nội dung trong EDI thường đạt được như là dịch vụ phụ của dịch vụ an ninh xác thực gốc hoặc không - từ chối gốc.

A.3.4 Xác thực gốc

Xác thực gốc bảo vệ bên tiếp nhận chống lại bên gửi thực tế một thông điệp/gói, một nhóm hoặc trao đổi tự cho là một bên tham gia (được phép) khác.

Sự bảo vệ có thể thực hiện nhờ một giá trị xác thực (ví dụ như MAC: Mã xác thực thông điệp). Giá trị này phụ thuộc vào cả nội dung dữ liệu và một khóa bí mật của bên gửi.

Dịch vụ này có thể bao gồm tính toàn vẹn nội dung và có thể đạt được như dịch vụ phụ của dịch vụ an ninh không từ chối gốc.

Trong đa số trường hợp, càng ít dịch vụ xác thực gốc càng tốt.

A.3.5 Không - từ chối gốc

Không - từ chối gốc bảo vệ bên tiếp nhận một thông điệp/gói, nhóm hoặc trao đổi tránh việc phủ nhận đã gửi thông điệp/gói, một nhóm hoặc trao đổi đó của bên gửi.

Sự bảo vệ có thể thực hiện nhờ một chữ ký số (hoặc bằng việc sử dụng thích hợp chức năng đã được mô tả trong "xác thực gốc" trên cơ sở phần cứng chống giả mạo hoặc sự xác thực của các bên thứ ba). Một chữ ký số thu được khi mã hoá với một thuật toán không đối xứng và một khóa riêng, đối tượng hoặc một giá trị kiểm soát được tạo ra từ dữ liệu này (ví dụ sử dụng một hàm băm).

Chữ ký số có thể được xác minh bằng việc sử dụng khóa công bố được tạo ra từ khóa riêng tương ứng. Khóa công bố này có thể bao gồm trong thỏa thuận trao đổi đã ký bởi các bên tham gia hoặc trong một chứng chỉ số được ký hiệu bởi tổ chức chứng nhận. Chứng chỉ này có thể được gửi như một phần của cấu trúc EDIFACT.

Chữ ký số không chỉ cung cấp dịch vụ không - từ chối gốc mà còn dịch vụ về tính toàn vẹn nội dung và xác thực gốc.

A.3.6 Không - từ chối nhận của bên tiếp nhận

Không - từ chối nhận của bên tiếp nhận bảo vệ bên gửi mộ thông điệp/gói, nhóm hoặc trao đổi trước sự từ chối nhận của bên tiếp nhận.

Sự bảo vệ có thể thực hiện qua việc bên tiếp nhận gửi một báo nhận có chứa một chữ ký số dựa trên dữ liệu trong cấu trúc EDI gốc. Báo nhận này đưa mẫu một thông điệp dịch vụ từ bên tiếp nhận tới bên gửi.

A.3.7 Độ tin cậy về nội dung

Độ tin cậy về nội dung nhằm tránh để lộ, sao chép hoặc đọc trái phép nội dung một nhóm hoặc thông điệp/gói trao đổi.

Sự bảo vệ có thể đảm bảo nhờ mật mã hóa dữ liệu. Mật mã hóa có thể thực hiện bằng cách sử dụng một thuật toán đối xứng với một khóa bí mật được dùng chung bởi bên gửi và bên tiếp nhận.

Tuy nhiên, khóa bí mật có thể được truyền đi an toàn bằng cách mật mã hóa theo một thuật toán không đối xứng dưới dạng khóa công bố của bên tiếp nhận.

Độ tin cậy được trình bày riêng trong TCVN ISO 9735-7.

A.3.8 Mối quan hệ giữa các dịch vụ an ninh

Như đã nói, một số dịch vụ anh ninh bản thân đã bao hàm cả dịch vụ khác, do đó không cần thiết bổ sung các dịch vụ đã đạt được hoàn toàn. Ví dụ, sử dụng cơ chế cung cấp dịch vụ không - từ chối gốc bao gồm dịch vụ về tính toàn vẹn nội dung.

Bảng A.1 Tổng kết mối quan hệ.

Bảng A.1 - Bảng tương quan

Sử dụng	Bao gồm		
	Toàn vẹn nội dung	Xác thực gốc	Không từ chối gốc
Toàn vẹn nội dung	có	-	-
Xác thực gốc	có	có	-
Không - từ chối gốc	có	có	có

Phụ lục B

(tham khảo)

Cách bảo vệ một cấu trúc EDIFACT

B.1 Khái quát

Sau đây là một số bước cơ bản được dùng để thực hiện an ninh cho các cấu trúc EDIFACT: trao đổi, nhóm hoặc thông điệp/gói. Chi tiết và giải thích các nguyên tắc được đề cập đến trong Phụ lục A, ISO 7498 - 2 và ISO/IEC 9594-8/CCITT X.509.

Bước đầu tiên là xác định (kết hợp với các nghiệp vụ liên quan) nhu cầu dịch vụ an ninh. Các dịch vụ an ninh thông dụng của EDIFACT dưới đây là quan trọng để đáp ứng các yêu cầu nghiệp vụ tránh các mối đe dọa an ninh đã được xác định. Các nhu cầu này có thể được xác định thông qua yêu cầu kiểm tra nội bộ cũng như bên ngoài. Các dịch vụ an ninh cơ bản có sẵn tại bên gửi là:

– tính toàn vẹn nội dung;

– xác thực gốc;

– không - từ chối gốc.

Các dịch vụ này không độc lập nhau mà chúng đã hàm chứa lẫn nhau, do đó không cần thiết bổ sung các dịch vụ đã được bao gồm trong dịch vụ khác. Ví dụ, nếu sử dụng dịch vụ không - từ chối gốc thì cũng đạt được dịch vụ về tính toàn vẹn nội dung.

Các mối quan hệ này được tổng kết trong Bảng A.1.

Do đó, bên gửi chỉ cần chọn một trong ba dịch vụ.

Không - từ chối nhận việc nhận là dịch vụ được bắt đầu từ bên tiếp nhận. Nó có thể được yêu cầu bởi bên gửi hoặc được đề nghị trong một thỏa thuận trao đổi. Thông điệp AUTACT được phát triển để mang thông tin về sự nhận được.

B.2 Thỏa thuận song phương/bên thứ ba

Nếu các dịch vụ an ninh được tích hợp, các thỏa thuận bổ sung phải được thiết lập cùng với các bên tham gia nghiệp vụ. Có một số cách tiếp cận khác nhau, ở đây trình bày ngắn gọn hai trường hợp đại diện.

Một yêu cầu tối thiểu về dịch vụ an ninh, thuật toán, mã hóa, phương pháp quản lý khóa, hành động khắc phục lỗi, v.v có thể là một thỏa thuận song phương với mỗi bên tham gia riêng lẻ với nhau. Ví dụ; Một bản dự thảo thỏa thuận có sẵn từ Chương trình TEDIS của Uỷ ban Châu Âu. Trong trường hợp này, cần thiết rất ít thông tin an ninh liên quan trong bản thân thông điệp/gói này.

Trong trường hợp đối với mức độ an ninh cao liên quan đến một bên thứ ba có vai trò như một tổ chức chứng nhận, lưu trữ hồ sơ của tất cả các bên sử dụng và phát hành các chứng chỉ để chứng nhận khóa công bố. Trường hợp này, hoàn toàn là việc ký kết một thỏa thuận với tổ chức chứng nhận. Tổ chức chứng nhận đại diện chịu trách nhiệm ghi vào danh sách đen. Trường hợp này có thể cần bao gồm nhiều thông tin an ninh liên quan.

Các dịch vụ an ninh được tích hợp trong EDIFACT thiết lập theo cách nhằm tạo sự linh hoạt tối đa và phục vụ cho cả hai trường hợp trên cũng như cho bất cứ trường hợp nào.

B.3 Khía cạnh thực tế

Trên thực tế, có một số khía cạnh khác nhau cần thiết để xác định dịch vụ an ninh như tạo khóa, nhu cầu có bộ chuyển dịch có khả năng điều khiển các đoạn an ninh, các thủ tục nội bộ để sử dụng đầy đủ các dịch vụ an ninh, như là lưu trữ thông điệp/gói đến cùng các chữ ký số, sử dụng đa chữ ký, v.v.

Cần nhấn mạnh rằng việc tích hợp các dịch vụ an ninh là hoàn toàn rõ ràng và độc lập với các giao thức truyền thông được sử dụng. Nếu một hệ thống cho phép truyền một thông điệp/gói EDIFACT cũng cho phép truyền một thông điệp/gói EDIFACT an ninh.

B.4 Thủ tục xây dựng một cấu trúc EDIFACT an ninh

Trước tiên, cấu trúc EDIFACT như thông điệp/gói, nhóm hoặc trao đổi được tạo ra. Sau đó, các dịch vụ an ninh thích hợp được xác định và áp dụng. Nếu dịch vụ này dựa trên các chữ ký số thì các cá nhân xử lý khóa riêng phải được liên quan một cách trực tiếp hoặc gián tiếp. Nhưng điều này không cần phải thực hiện ngay lập tức sau khi tạo cấu trúc EDIFACT

Tương tự như hoạt động lưu trữ giấy tờ, bước đầu tiên là xác minh các dịch vụ an ninh cấu trúc EDIFACT, có thể lưu cấu trúc EDIFACT đã đảm bảo an ninh cho việc kiểm tra và làm tài liệu chứng từ sau này.

B.5 Thứ tự các dịch vụ an ninh áp dụng

Thứ tự các dịch vụ an ninh được thực hiện hoàn toàn tùy ý đối với người sử dụng do tất cả các dịch vụ an ninh là độc lập hoàn toàn với nhau. Đặc biệt, nếu sử dụng nhiều chữ ký số, ngoài việc nhúng các nhóm đoạn an ninh và đoạn tiêu đề an ninh còn tính toán và xác minh thứ tự các nhóm đoạn này trong cấu trúc EDIFACT.

B.6 An ninh thông điệp phân tách tại mức thông điệp/gói

B.6.1 Các yêu cầu nghiệp vụ

Có hai yêu cầu nghiệp vụ cho đặc tính này, đó là:

a) cung cấp an ninh cho một hoặc nhiều thông điệp/gói trong một thông điệp riêng từ bên gửi,

b) cung cấp một báo nhận được đảm bảo an ninh cho bên gửi khi nhận được (các) thông điệp/(các) gói gốc mà không trả lại.

Các yêu cầu này có thể đáp ứng bằng xác thực an ninh và thông điệp báo nhận AUTACK, được trình bày trong TCVN ISO 9735- 6.

B.6.2 An ninh thông điệp phân tách được sử dụng bởi bên gửi

Việc sử dụng AUTACK này cho phép bên gửi cung cấp bất kỳ dịch vụ an ninh nào nhưng được tiến hành trong một thông điệp tách biệt. Do đó, các dịch vụ an ninh có thể được truyền vào một thời điểm thích hợp hơn sau đó. Hơn nữa, chúng có thể bảo vệ cho vài thông điệp/gói gốc, khác với sự tích hợp trực tiếp, chúng chỉ bảo vệ một thông điệp/gói tại một thời điểm ở mức thông điệp/gói.

Các nguyên tắc này dành cho các cách tiếp cận tách biệt và tích hợp, nhưng cách sau yêu cầu một tham chiếu duy nhất tới gói/thông điệp gốc đang được bảo vệ.

B.6.3 An ninh thông điệp phân tách được sử dụng bởi bên tiếp nhận

Việc sử dụng AUTACK này đáp ứng yêu cầu cung cấp không - từ chối nhận của bên tiếp nhận. Chi tiết về thông điệp xem phần AUTACK trong TCVN ISO 9735- 6 : 2004.

AUTACK được sử dụng như một báo nhận được đảm bảo an ninh được gửi bởi bên tiếp nhận của một hoặc nhiều trao đổi hoặc một hoặc nhiều gói/thông điệp từ một hoặc nhiều trao đổi đến bên gửi của chúng. Một AUTACK được phát đi tới bên gửi của trao đổi hoặc thông điệp/gói gốc cùng với báo nhận an ninh là cách thức tiêu chuẩn có nghĩa rằng bên bên tham gia đã nhận được trao đổi hoặc thông điệp/gói.

B.7 An ninh thông điệp phân tách tại mức nhóm hoặc mức trao đổi

Kỹ thuật trình bày cho an ninh thông điệp/gói phân tách trong mục D.5 tại mức thông điệp/gói có thể được sử dụng để bảo vệ cho trao đổi hoàn chỉnh hoặc nhóm hoàn chỉnh.

Hai yêu cầu nghiệp vụ đặc trưng là:

a) cung cấp an ninh cho một hoặc nhiều nhóm trao đổi hoặc trong một thông điệp tách biệt từ bên gửi;

b) cung cấp một báo nhận đã được đảm bảo an ninh tới bên gửi về việc nhận được các nhóm hoặc (các) trao đổi gốc mà không gửi lại chúng.

Các yêu cầu này có thể được đáp ứng bằng xác thực an ninh và thông điệp báo nhận AUTACK được trình bày trong TCVN ISO 9735- 6 : 2004.

Phụ lục C

(tham khảo)

Các ví dụ về bảo vệ thông điệp

C.1 Giới thiệu

Ba ví dụ trong phụ lục này minh họa việc áp dụng khác nhau của các đoạn dịch vụ an ninh.

Các ví dụ về an ninh thông điệp này dựa trên cơ sở các hóa đơn thanh toán EDIFACT như trình bày trong sổ tay MIG về các thông điệp tài chính được SWIFT ban hành. Tuy nhiên, những cơ chế an ninh được trình bày ở đây là hoàn toàn độc lập với kiểu thông điệp và có thể áp dụng cho bất kỳ thông điệp EDIFACT nào.

"Ví dụ 1: xác thực nguồn gốc thông điệp" chỉ ra cách các đoạn dịch vụ an ninh có thể được sử dụng khi áp dụng phương pháp dựa trên cơ sở thuật toán đối xứng để cung cấp dịch vụ xác thực nguồn gốc thông điệp. Khóa đối xứng được trao đổi trước đó giữa các bên tham gia và nhóm đoạn tiêu đề an ninh chỉ chứa đúng hai đoạn đơn giản.

"Ví dụ 2: không - từ chối gốc, kỹ thuật thứ nhất" chỉ ra cách các đoạn dịch vụ an ninh có thể được sử dụng khi áp dụng phương pháp dựa trên cơ sở một thuật toán không đối xứng để cung cấp dịch vụ không từ chối gốc. Thuật toán áp dụng trực tiếp cho thông điệp là **một hàm băm**, hàm băm này không yêu cầu bất kỳ trao đổi khoá nào giữa các bên tham gia. Giá trị - băm này được ký hiệu bằng một thuật toán không đối xứng. Khoá công bố mà bên tiếp nhận cần để xác minh chữ ký của thông điệp được chứa trong một đoạn chứng chỉ được truyền trong nhóm đoạn tiêu đề an ninh của thông đIệp. Chứng chỉ này được ký hiệu bởi người phát hành (**"**bên chứng nhận**"** nào đó) và chứa khoá công bố của bên chứng nhận đó, để bên tham gia nào cũng có thể xác minh tính toàn vẹn hoặc tính xác thực của chứng chỉ.

"Ví dụ 3: không - từ chối gốc, kỹ thuật thứ hai" chỉ ra cách các đoạn dịch vụ an ninh có thể được sử dụng khi áp dụng phương pháp dựa trên cơ sở một thuật toán không đối xứng để cung cấp dịch vụ không - từ chối gốc. Thuật toán áp dụng trực tiếp vào thông điệp là một thuật toán đối xứng, thuật toán đối xứng này yêu cầu một trao đổi khoá đối xứng giữa các bên tham gia và cung cấp một **"**giá trị toàn vẹn**"**. Khoá đối xứng này được trao đổi trong nhóm đoạn tiêu đề an ninh của thông điệp, được mã hoá bằng một thuật toán không đối xứng dưới dạng khoá công bố của người nhận.

Giá trị toàn vẹn này được ký hiệu bằng một thuật toán không đối xứng. Khoá công bố cần cho bên tiếp nhận để xác minh chữ ký của thông điệp có trong đoạn chứng chỉ thứ nhất, đoạn này được truyền trong nhóm đoạn tiêu đề an ninh của thông điệp. Chứng chỉ này được ký hiệu bởi bên phát hành nó (**"**bên chứng nhận**"** nào đó) và chứa khoá công bố của bên chứng nhận trong trường hợp một bên tham gia nào đó có thể xác minh tính toàn vẹn hoặc tính xác thực của chứng chỉ.

Một đoạn chứng chỉ thứ hai chứa một tham chiếu đến khoá công bố của bên tiếp nhận, được sử dụng bởi bên gửi thông điệp để bảo vệ khoá đối xứng.

Kỹ thuật này hiện nay được các ngân hàng Pháp sử dụng trong hệ thống ETEBAC 5 (truyền file đã được đảm bảo an ninh giữa các ngân hàng và khách hàng công ty).

Trong hai ví dụ sau, bất kỳ bên tham gia được ủy thác là bên có thẩm quyền nào cũng có thể xác minh chữ ký của thông điệp nhận được mà chỉ cần sử dụng dữ liệu chứa trong thông điệp.

C.2 Ví dụ 1: xác thực nguồn gốc thông điệp

C.2.1 Tình huống

Công ty A yêu cầu Ngân hàng A, dùng mã 603000 để ghi vào sổ nợ số tài khoản 00387806 tổng số 54345,10 bảng Anh vào ngày 09 tháng 04 năm 1996. Tổng số tiền này được trả cho ngân hàng B, dùng mã phân loại 201827 với số tài khoản 00663151 của công ty B, Bến tầu phía tây, Milford Haven. Việc thanh toán theo hoá đơn 62345. Tên liên hệ của bên được trả nợ là ông Jones thuộc Phòng Kinh doanh.

Ngân hàng A yêu cầu thủ tục thanh toán được đảm bảo an ninh bằng chức năng an ninh **"**xác thực nguồn gốc thông điệp**"**. Việc này được thực hiện bằng việc tạo ra một **"**Mã Xác thực Thông điệp**"** (MAC) cùng với **"**Tiêu chuẩn Mã hóa Dữ liệu**"** đối xứng (DES) tuân theo ISO 8731-1 tại bên gửi thông điệp, được kiểm tra tính hợp lệ bởi Ngân hàng A. Giả sử rằng Khóa - DES bí mật đã được trao đổi trước giữa Công ty A và Ngân hàng A.

Lưu ý:

Trong phần sau đây, chỉ những phần liên quan đến an ninh của thông điệp mới được đề đến.

C.2.2 Chi tiết an ninh

TIÊU ĐỀ AN NINH	
DỊCH VỤ AN NINH	Xác thực nguồn gốc thông điệp
SỐ HIỆU THAM CHIẾU AN NINH	Tham chiếu của tiêu đề này là 1.
HÀM LỌC	Tất cả giá trị nhị phân (MAC) được lọc bằng bộ lọc thập lục phân.
MÃ HÓA BỘ KÝ TỰ GỐC	Thông điệp được mã hóa thành mã ASCII 8 bít khi MAC được tạo ra.
CHI TIẾT ĐỊNH DANH AN NINH Bên gửi thông điệp (bên tạo ra Mã Xác thực Thông điệp).	Ông Smith ở Công ty A

CHI TIẾT ĐỊNH DANH AN NINH Bên tiếp nhận thông điệp (bên xác minh Mã Xác thực Thông điệp).	Ngân hàng A
SỐ HIỆU THỨ TỰ AN NINH	Số hiệu thứ tự an ninh của thông điệp này là 001.
NGÀY THÁNG VÀ THỜI GIAN AN NINH	Thẻ thời gian an ninh có dạng: ngày 1996 04 09 thời gian: 13:59:50.
THUẬT TOÁN AN NINH	
THUẬT TOÁN AN NINH Sử dụng thuật toán Phương thức hoạt động mật mã hoá Thuật toán	 Sử dụng một thuật toán đối xứng cho xác thực nguồn gốc thông điệp. Một MAC được tính toán, theo ISO 8731-1. Sử dụng thuật toán DES.
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Xác định giá trị tham số thuật toán sau bằng tên của một khóa đối xứng được trao đổi trước đó. Khóa sử dụng là MAC - KEY1.
ĐUÔI AN NINH	
SỐ HIỆU THAM CHIẾU AN NINH	Số tham chiếu của đuôi là 1.
SỐ LƯỢNG ĐOẠN AN NINH	4
KẾT QUẢ AN NINH	
KẾT QUẢ HỢP LỆ Hạn định giá trị hợp lệ Giá trị hợp lệ	 MAC 4 byte Kết quả hợp lệ (Mã Xác thực Thông điệp)

C.3 Ví dụ 2: Không - từ chối gốc, kỹ thuật thứ nhất

C.3.1 Tình huống

Ngân hàng A muốn sử dụng dịch vụ an ninh không từ chối gốc cho đơn đặt hàng thanh toán từ Công ty A, được thực hiện bởi ông Smith.

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

Chứng chỉ xác nhận khoá công bố của ông Smith được phát hành bởi một cơ quan có thẩm quyền đã được ủy quyền bởi cả hai bên, Bên phát hành chứng chỉ.

C.3.2 Chi tiết an ninh

TIÊU ĐỀ AN NINH	
DỊCH VỤ AN NINH	Không - từ chối gốc
SỐ HIỆU THAM CHIẾU AN NINH	Tham chiếu của tiêu đề này là 1.
HÌNH THỨC ĐÁP ỨNG	Không yêu cầu báo nhận.
HÀM LỌC	Tất cả giá trị nhị phân (các chữ ký) được lọc bằng bộ lọc thập lục phân.
MÃ HÓA BỘ KÝ TỰ GỐC	Thông điệp được mã hóa thành mã ASCII 8 bít khi chữ ký của nó được tạo ra
SỐ HIỆU THỨ TỰ AN NINH	Số hiệu thứ tự an ninh của thông điệp là 202.
NGÀY THÁNG VÀ THỜI GIAN AN NINH	Thẻ thời gian an ninh có dạng: ngày: 1996 01 15,thời gian: 10:05:30.
THUẬT TOÁN AN NINH	Ông Smith sử dụng hàm băm cho chữ ký.
THUẬT TOÁN AN NINH Sử dụng thuật toán Phương thức hoạt động mật mã hoá Thuật toán	 Bên bên sở hữu sử dụng một thuật toán băm Hàm băm ISO/IEC 10118 - 2 các hàm băm sử dụng một thuật toán mã hoá khối n - bít để tạo ra một mã băm có độ dài gấp đôi (128 bít); các giá trị đầu vào: IV = 0F 0F 0F 0F 0F 0F 0F 0F IV’ = F0 F0 F0 F0 F0 F0 F0 F0; các qui tắc đệm như phần biến đầu tiên của B.3 trong ISO/IEC 10118:2000; Phép biến đổi u và u’ như trong phụ lục A của ISO/IEC 10118 -2:2000. Sử dụng thuật toán mã khối DES.
CHỨNG CHỈ	Chứng chỉ của ông Smith
THAM CHIẾU CHỨNG CHỈ	Chứng chỉ này được tham chiếu bởi CƠ QUAN CÓ THẨM QUYỀN: 00000001.
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên tham gia an ninh	 Bên sở hữu chứng chỉ (ông Smith ở Công ty A)
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên tham gia an ninh	 Xác thực bên tham gia (chứng chỉ của ông Smith được phát

Tên khóa	hành bởi một cơ quan chứng nhận gọi là: CƠ QUAN CÓ THẨM QUYỀN) Khóa công bố của CƠ QUAN CÓ THẨM QUYỀN được sử dụng để phát hành chứng chỉ của ông Smith là PK1.
CÚ PHÁP VÀ PHIÊN BẢN CHỨNG CHỈ	Phiên bản chứng chỉ của danh mục đoạn dịch vụ UN/EDIFACT
HÀM LỌC	Tất cả giá trị nhị phân (các chữ ký số và khóa) được lọc bằng bộ lọc thập lục phân.
MÃ HÓA BỘ KÝ TỰ GỐC	Giấy ủy nhiệm về chứng chỉ được mã hóa thành 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 tính toán Ký tự dịch vụ là dấu 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 tính toán 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 tính toán 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 tính toán Ký tự dịch vụ là dấu phân tách lặp lại Giá trị **“ * ”** (dấu hoa thị)
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 tính toán Ký tự dịch vụ là ký tự phát hành Giá trị **“ ? ”** (dấu hỏi)
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày và giờ	Thời gian phát hành chứng chỉ Chứng chỉ ông Smith được phát hành vào 931215 lúc 14:12 :00
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày và giờ	Bắt đầu thời gian hợp lệ của chứng chỉ Thời gian chứng chỉ của ông Smith hợp lệ bắt đầu: 1996 01 01 000000
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày và giờ	Kết thúc thời gian hợp lệ 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 sử dụng để ký
THUẬT TOÁN AN NINH	

Sử dụng thuật toán Phương thức hoạt động mật mã hoá Thuật toán	Bên sở hữu sử dụng một thuật toán để ký Không có phương thức hoạt động 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	 Nhận dạng tham số thuật toán như là một hàm mũ công bố cho việc xác minh chữ ký Khoá công bố của ông Smith
TIÊU ĐỀ AN NINH	
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Định danh tham số thuật toán như một môđun cho việc 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	 định danh tham số thuật toán như độ dài các môđun của ông Smith (bằng bít) Các mô môđun của ông Smith dài 512 bít
THUẬT TOÁN AN NINH	Hàm băm được BÊN CHỨNG NHẬN sử dụng để phát hành chứng chỉ của ông Smith
THUẬT TOÁN AN NINH Sử dụng thuật toán Mật mã hoá phương thức hoạt động Thuật toán	 Bên phát hành sử dụng một thuật toán băm Hàm băm ISO/IEC 10118-2 Hàm băm sử dụng một thuật toán mã khối n-bít để tạo ra một mã băm có độ dài gấp đôi (128 bít); giá trị ban đầu: IV = 0F 0F 0F 0F 0F 0F 0F 0F IV’ = F0 F0 F0 F0 F0 F0 F0 F0; các quy tắc đệm như phần biến đầu tiên của B.3 trong ISO/IEC 10118-2:2000; việc biến đổi u và u’ như được quy định trong phụ lục A của ISO/IEC 10118-2: 2000. Thuật toán mã khối DES được sử dụng
THUẬT TOÁN AN NINH Sự sử dụng thuật toán Mật mã hoá phương thức hoạt động Thuật toán	 Bên phát hành sử dụng một thuật toán để ký Không có phương thức hoạt động 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	 định danh tham số thuật toán như một hàm mũ công bố cho việc xác minh chữ ký Khoá chung của BÊN CHỨNG NHẬN
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán	 định danh tham số thuật toán như một môđun cho việc xác minh

Giá trị tham số thuật toán	chữ ký Các môđun của BÊN CHỨNG NHẬN
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 định danh tham số thuật toán như độ dài môđun của BÊN CHỨNG NHẬN (theo bít) Các mô đul 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 512 bít
ĐUÔI AN NINH	
TIÊU ĐỀ AN NINH	
SỐ HIỆU THAM CHIẾU AN NINH	Số tham chiếu của đuôi an ninh là 1
SỐ LƯỢNG ĐOẠN AN NINH	9
KẾT QUẢ AN NINH	Chữ ký số của thông điệp
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 512 bít

C.4 Ví dụ 3: không từ chối gốc, kỹ thuật thứ hai

C.4.1 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. Công ty A yêu cầu một báo nhận an ninh từ ngân hàng A (không - từ chối việc nhận của bên tiếp nhận) được truyền trong một thông điệp AUTACK.

Dịch vụ an ninh không - từ chối gốc được thiết lập giữa các bên trao đổi để hoàn tất các đơn đặt hàng thanh toán bằng cách sử dụng một chữ ký số.

Cả hai bên đồng ý rằng chữ ký này được tính toán bằng RSA 512 bít (thuật toán không đối xứng) nhờ một giá trị toàn vẹn - 64 bít được tính toán bằng CBC trong chế độ DES (thuật toán đối xứng). Chứng chỉ để định danh khoá công bố của ông Smith được phát hành bởi một bên chứng nhận được cả hai bên tin cậy.

C.4.2 Chi tiết an ninh

TIÊU ĐỀ AN NINH	
DỊCH VỤ AN NINH	Không - từ chối gốc
SỐ HIỆU THAM CHIẾU AN NINH	Số tham chiếu của tiêu đề là 1.
HÌNH THỨC ĐÁP ỨNG	Yêu cầu báo nhận.
HÀM LỌC	Tất cả giá trị nhị phân các (chữ ký) được lọc bằng bộ lọc thập lục phân.
MÃ HÓA BỘ KÝ TỰ GỐC	Thông điệp được mã hóa thành mã ASCII 8 bít khi chữ ký của nó được phát hành.
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên tham gia an ninh	 Bên gửi thông điệp (bên tham gia an ninh thông điệp: ông Smith ở công ty A)
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên tham gia an ninh	 Bên tiếp nhận thông điệp (bên xác minh thông điệp an ninh: Ngân hàng A)
SỐ HIỆU THỨ TỰ AN NINH	Số hiệu thứ tự an ninh của thông điệp là 001
NGÀY THÁNG VÀ THỜI GIAN AN NINH	Thẻ thời gian an ninh có dạng: ngày: 196 01 15, thời gian: 10:05:30.
THUẬT TOÁN AN NINH	Thuật toán đối xứng được sử dụng để tính một giá trị toàn vẹn
THUẬT TOÁN AN NINH Sử dụng thuật toán Phương thức hoạt động mật mã hoá Thuật toán	 Sử dụng một thuật toán băm của bên sở hữu. Chuỗi khối mã; ISO/IEC 10116 (n - bít). Một giá trị toàn vẹn 64 bít được tính toán; giá trị ban đầu là số 0 nhị phân; một khóa - bí mật DES được sử dụng. Nó được truyền và mã hóa dưới khóa công bố của Ngân hàng A. Thuật toán mã khối DES được sử dụng.
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Định danh giá trị tham số thuật toán theo sau như một khóa đối xứng được mã hóa dưới một khóa công bố. Khoá đối xứng được mã hóa dưới khóa công bố của Ngân hàng A.
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 Định danh giá trị tham số thuật toán theo sau như một giá trị văn bản ban đầu. Giá trị văn bản ban đầu (tất cả là số nhị phân 0).
CHỨNG CHỈ	Chứng chỉ của ông Smith (Bên gửi thông điệp)

THAM CHIẾU CHỨNG CHỈ	Chứng chỉ này được tham chiếu: 00000001, bởi BÊN CHỨNG NHẬN
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên tham gia an ninh	 Bên sở hữu chứng chỉ (ông Smith ở Công ty A)
CHI TIẾT ĐỊNH DANH AN NINH Hạn định bên tham gia an ninh Tên khóa	 Xác thực bên tham gia (chứng chỉ của ông Smith được phát hành bởi một tổ chức chứng nhận gọi là: BÊN CHỨNG NHẬN) Khóa công bố của BÊN CHỨNG NHẬN được sử dụng để phát hành chứng chỉ của ông Smith là PK1.
CÚ PHÁP VÀ PHIÊN BẢN CHỨNG CHỈ	Phiên bản chứng chỉ của thư mục đoạn dịch vụ UN/EDIFACT
HÀM LỌC	Tất cả giá trị nhị phân (các chữ ký số và khóa) được lọc bằng bộ lọc thập lục phân
MÃ HÓA BỘ KÝ TỰ GỐC	Thông tin về chứng chỉ được mã hóa thành 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 hoá Ký tự dịch vụ là dấu 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 hoá 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 hoá 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 hoá Ký tự dịch vụ là dấu phân tách lặp lại Giá trị **“ * ”** (dấu hoa thị)
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 hoá Ký tự dịch vụ là ký tự phát hành Giá trị **“ ? ”** (dấu hỏi)
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày và giờ	Thời gian phát hành chứng chỉ Chứng chỉ ông Smith được tạo ra vào 931215 lúc 14:12:00
NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày và giờ	Bắt đầu thời gian hợp lệ của chứng chỉ Quá trình có hiệu lực của ông Smith bắt đầu: 1996 01 01 000000

NGÀY THÁNG VÀ THỜI GIAN AN NINH Ngày và giờ	Kết thúc thời gian hợp lệ 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 sử dụng để ký
THUẬT TOÁN AN NINH Sử dụng thuật toán Phương thức hoạt động mật mã hoá Thuật toán	 Bên sở hữu sử dụng một thuật toán để ký Không có lao động 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	 định danh tham số thuật toán như một hàm mũ công bố việc xác minh chữ ký Khoá công bố của ông Smith
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 định danh tham số thuật toán như một môđun cho việc xác minh chữ ký Môđun của ông Smith
THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 định danh tham số thuật toán như độ dài các môđun của ông Smith (bằng bít) Các mô đun của ông Smith dài 512 bít
THUẬT TOÁN AN NINH	Hàm băm được BÊN CHỨNG NHẬN sử dụng để phát hành chứng chỉ của ông Smith
THUẬT TOÁN AN NINH Sử dụng thuật toán Mật mã hoá phương thức hoạt động Thuật toán	 Bên phát hành sử dụng một thuật toán băm Hàm băm n bình phương đối với RSA; phụ lục D, CCITT X509. ISO/IEC 9594-8. Thuật toán không đối xứng RSA
THUẬT TOÁN AN NINH	Thuật toán không đối xứng được BÊN CHỨNG NHẬN sử dụng để ký
THUẬT TOÁN AN NINH Sự sử dụng thuật toán Mật mã hoá phương thức hoạt động Thuật toán	 Bên phát hành sử dụng một thuật toán để ký Không có phương thức hoạt động 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	 định danh tham số thuật toán này một cách công khai đối với xác minh chữ ký Khoá chung của BÊN THI HÀNH

THAM SỐ THUẬT TOÁN Hạn định tham số thuật toán Giá trị tham số thuật toán	 định danh tham số thuật toán như một hàm mũ công bố cho việc xác minh chữ ký 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 độ dài các mô đul 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 512 bít
CHỨNG CHỈ	Chứng chỉ của Ngân hàng A (Bên tiếp nhận thông điệp)
THAM CHIẾU CHỨNG CHỈ	Khóa công bố của Ngân hàng A được sử dụng liên quan với chứng chỉ được tham chiếu là 00001001
ĐUÔI AN NINH	
SỐ HIỆU THAM CHIẾU AN NINH	Số tham chiếu của đuôi an ninh là 1
SỐ LƯỢNG ĐOẠN AN NINH	10
KẾT QUẢ AN NINH	Chữ ký số của thông điệp
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 512 bít

Phụ lục D

(tham khảo)

Các hàm lọc đối với các kho bộ ký tự A và C của UN/EDIFACT

D.1 Bộ lọc EDA

D.1.1 Cơ sở

Việc lọc thập lục phân tăng gấp đôi số ký tự yêu cầu để biểu diễn dữ liệu nhị phân. Đây là sự lãng phí không gian. Các hàm lọc đã được tiêu chuẩn hóa và đang tồn tại khác hoặc là không thích hợp đối với các kho bộ ký tự A và B của UN/EDIFACT (ISO/IEC 646) bởi vì chúng ánh xạ tới hầu hết bộ ký tự đầy đủ có thể xuất bản của ISO (94 ký tự ngoài 96 ký tự có thể xuất bản), hoặc là do chúng thực sự không hiệu quả về không gian so với lọc thập lục phân (bộ lọc Baudot).

Do đó nên xác định một hàm lọc đủ đơn giản và ánh xạ tới (một tập con của) kho bộ ký tự mức A của UN/EDIFACT, sẽ hiệu quả hơn bộ lọc thập lục phân.

D.1.2 Kho bộ ký tự UN/EDIFACT

Kho bộ ký tự A có 44 ký tự, việc sử dụng nó là không hạn chế. Trường hợp bổ sung thêm vào 44 ký tự đó, một phần của bộ ký tự này gồm bốn ký tự dịch vụ và tám ký tự không cho phép truyền TELEX.

Tất cả các ký tự trên cũng là một phần của kho bộ ký tự B của UN/EDIFACT, các ký tự này không được dùng trong việc truyền TELEX, và nó gồm 82 ký tự thường và ba ký tự dịch vụ không – thể xuất bản được.

D.1.3 Lọc hai thành ba

Để biểu diễn hai ký tự nhị phân bằng ba ký tự được lọc, yêu cầu tối thiểu 41 ký tự trong bộ ký tự này:
41 ** 3 = 68 921 > 65 536 > 64 000 = 40 ** 3.

D.1.4 Đặc tả bộ lọc EDA

Có 44 ký tự được cho phép, tránh sử dụng phần ký tự trống trong 44 ký tự đó và lọc mỗi cặp ký tự đầu vào (nếu là lẻ, lọc ký tự cuối cùng trong hai lần kết quả) bằng:

– việc tính toán giá trị nhị phân của số nguyên không dấu được tạo ra bởi cặp ký tự này (giá trị này phụ thuộc khách quan vào bản chất LITTLE_ENDIAN / BIG_ENDIAN (Byte đầu tiên có nghĩa nhất hoặc ít nghĩa nhất) của máy tính sử dụng. Tiêu chuẩn hóa cho BIG_ENDIAN: byte đầu tiên có nghĩa nhất;

– biểu diễn giá trị bằng một dãy ba số (hai cho byte lẻ cuối cùng), trong khoảng từ 0 đến 42 theo:

- kết quả của phép chia cho 1849 (43 bình phương) (bỏ qua byte lẻ cuối cùng);
- giá trị dư của 1849 chia cho 43;
- giá trị dư 43;

– ánh xạ mỗi số trong bảng chữ cái mức A của UN/EDIFACT bởi bảng tương ứng:

0 tới 9	được biểu diễn bằng	0 tới 9
A tới Z	được biểu diễn bằng	10 tới 35
() , - . / =	được biểu diễn bằng	36 tới 42 theo thứ tự.

D.1.5 Giải lọc

Để giải lọc: ánh xạ trong mỗi ký tự trong 43 ký tự trở lại giá trị của nó giữa 0 và 42,

nếu còn lại ít nhất ba ký tự được lọc, tính toán: cl * 1849 + c2 *43 + c3 = số nguyên ngắn;

còn ít nhất hai ký tự thì tính: c1 * 43 + c2 = giá trị ký tự.

Lưu ý:

a) số nguyên ngắn nên < 65 536;

b) giá trị ký tự nên < 256;

c) trong một máy tính LITTLE_ENDIAN, chuyển hai ký tự của giá trị số nguyên ngắn.

D.2 Bộ lọc EDC

D.2.1 Cơ sở

Bộ lọc EDA được xây dựng để cho phép lọc sang kho mức A hoặc B của UN/EDIFACT. Tất nhiên, do kho ký tự này bị giới hạn theo các ký tự, mức mở rộng = 3/2 là khá tồi, mặc dù đã tốt hơn nhiều so với bộ lọc thập lục phân = 2/1.

Trong các kho mức C,D,E và F, có thể đạt được dễ dàng một mức mở rộng tốt hơn nhiều .

Thực tế, trong các kho ký tự này, chỉ các liên kết không thể cho phép chỉ gồm các giá trị nhị phân từ 0/0 tới 1/15 và các giá trị 8/0 tới 9/15.

Trong 256 giá trị nhị phân có thể thì 192 ký tự được cho phép.

Một bộ lọc mức C, lý tưởng khi mức mở rộng thấp mà không yêu cầu tính toán dài, sẽ cho phép biểu diễn 18 byte nhị phân thành 19 byte được lọc, nhưng không được từ 19 byte sang 20 byte được lọc, bởi vì:

192**19 > 256**18, và

192**20 < 256**19

Mức mở rộng thực tế là 8/7 do sự hạn chế của phép biến đổi các thao tác bít.

D.2.2 Phép biến đổi lọc

Để biến đổi một chuỗi byte nhị phân sang kho ký tự mức C:

– chia nhỏ chuỗi thành các chuỗi con bẩy - byte (chuỗi con cuối cùng có nhiều nhất bẩy byte);

– thêm vào trước mỗi chuỗi con một byte điều khiển với giá trị bắt đầu 64 (bít 1 = 1),

– đặt 1 trong mỗi bít của byte điều khiển, có vị trí 0 hoặc 2 đến 7 phụ thuộc vào phép biến đổi lọc được áp dụng cho byte dữ liệu tương ứng của chuỗi con hoặc không;

– Kiểm tra mỗi byte dữ liệu trong chuỗi con khi phép biến đổi được áp dụng bởi;

– là (byte dữ liệu.and.64 == 0) hoặc không?

– Nếu đúng, thì đặt bít 1 là 1 trong byte dữ liệu và trong bít vị trí của byte điều khiển;

– nếu không, thì giữ nguyên không thay đổi byte dữ liệu và byte điều khiển;

– Tất cả giá trị lọc bắt buộc có bít 1 của mỗi byte = 1;

– Các ký tự dịch vụ mặc định do đó bị loại khỏi kho ký tự lọc đích.

D.2.3 Phép biến đổi giải lọc

Để biến đổi trở lại chuỗi được lọc thành chuỗi nhị phân:

– phân chia chuỗi thành các chuỗi con tám - byte (chuỗi con cuối cùng có nhiều nhất tám byte);

– coi mỗi byte bắt đầu của mỗi chuỗi con như một byte điều khiển, các byte khác là byte dữ liệu;

– kiểm tra các vị trí bít 0 và 2 đến 7 của byte điều khiển;

– các vị trí byte của chuỗi con tương ứng với thứ tự 1 tới 7,

– nếu bít = 0, giữ nguyên byte dữ liệu của vị trí tương ứng;

– nếu bít = 1, đặt bít 1 của byte dữ liệu tương ứng là 0.

Phụ lục E

(tham khảo)

Thuật toán và dịch vụ an ninh

E.1 Phạm vi và mục đích

Phụ lục này đưa ra những ví dụ về khả năng liên kết các phần tử dữ liệu và các giá trị mã từ các nhóm đoạn an ninh. Các ví dụ được chọn nhằm minh họa một số kỹ thuật an ninh được sử dụng rộng rãi dựa trên các Tiêu chuẩn Quốc tế.

Để trình bày tất cả các khả năng liên kết là quá nhiều đối với phụ lục này. Ở đây sự lựa chọn xem như một sự xác định về thuật toán hoặc các phương thức hoạt động. Bên sử dụng chọn các kỹ thuật thích hợp để bảo vệ chống lại mối đe doạ an ninh.

Mục đích của phụ lục này là cung cấp cho bên sử dụng kỹ thuật an ninh đã chọn, với một điểm khởi đầu toàn diện để tìm ra giải pháp phù hợp cho ứng dụng riêng của bên sử dụng.

Để cho dễ đọc và dễ hiểu, vấn đề được chia thành hai phần, mỗi phần tập trung vào những nguyên tắc cơ bản khác nhau đối với việc áp dụng an ninh.
Hai phần đó là:

1. liên kết sử dụng các thuật toán đối xứng và các đoạn an ninh thích hợp;
2. liên kết sử dụng các thuật toán không đối xứng và các đoạn an ninh thích hợp.

Danh sách mã sử dụng trong ma trận (một phần của danh sách mã đầy đủ)

0501 Dịch vụ an ninh, đã mã hoá

1	Không từ chối gốc
2	Xác thực nguồn gốc thông điệp
3	Tính toàn vẹn

0505 Chức năng lọc, đã mã hoá

6	Bộ lọc EDC

0523 Thuật toán sử dụng, đã mã hoá

1	Hàm băm bên sở hữu
2	Hàm đối xứng Bên sở hữu
3	Ký hiệu Bên phát hành(CA)
4	Hàm băm Bên phát hành (CA)
6	Ký hiệu bên sở hữu

0525 Mật mã hoá phương thức hoạt động, đã mã hoá

16	DSMR (Chữ ký Số với khôi phục lại Thông điệp)

0527	*Thuật toán, đã mã hoá*
1	DES (Tiêu chuẩn mật mã hoá Dữ liệu)
8	SHA (Thuật toán Băm An ninh)
10	RSA (Rivest, Shamir, Adleman)
11	DSA (Thuật toán ký Số)
16	SHA1 (Thuật toán Băm An ninh)
37	MAC (Mã Xác thực Thông điệp)
38	DIM1 (Cơ chế Toàn vẹn Dữ liệu)
40	MDC2 (Mã phát hiện Sự thay đổi)
42	HDS (Hàm băm)

0531	*Hạn định tham số thuật toán*
5	Mã hoá khoá đối xứng
9	Tên khoá đối xứng
10	Tên khoá mã hoá khoá
12	Môđun
13	Hàm mũ
14	Độ dài môđun
25	Tham số P của DSA
26	Tham số của Q của DSA
27	Tham số G của DSA
28	Tham số Y của DSA

0563	*Hạn định giá trị hợp lệ*
1	Giá trị hợp lệ duy nhất
2	Tham số r của thuật toán DSA
3	Tham số s của thuật toán DSA

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

Các chữ viết tắt được sử dụng

a, b, c, e	=	Biểu diễn của một số hiệu tham chiếu an ninh
CA	=	Tổ chức chứng nhận
Enc-key	=	Khóa mã hóa
G	=	Tham số khóa công bố G của DSA
Hash	=	Giá trị băm
KEK-N	=	Tên khóa mã hóa khóa
Key-N	=	Tên khóa
KN	=	Tên khóa
MAC	=	Mã xác thực thông điệp
Mod	=	Môđun
Mod-L	=	Độ dài môđun
P	=	Tham số khóa công bố P của DSA
PK/CA	=	Khóa công bố của bên chứng nhận
Pub-K	=	Khóa công bố
Q	=	Tham số khóa công bố Q của DSA
R	=	Kết quả tham số r của chữ ký DAS
S	=	Kết quả tham số s của chữ ký DAS
Sig	=	Chữ ký

Y = Tham số khóa công bố Y của DSA

E.2 Liên kết sử dụng các thuật toán đối xứng và các đoạn an ninh tích hợp

Ma trận trong Bảng E.1 thiết lập các mối quan hệ trong các trường hợp sau:

- an ninh mức trao đổi /gói/nhóm/trao đổi (TCVN ISO 9735 - 5): 2004;
- sử dụng thuật toán đối xứng duy nhất;
- các dịch vụ an ninh đã cung cấp là xác thực nguồn gốc thông điệp và toàn vẹn nội dung.
- Xác thực nguồn gốc thông điệp được cung cấp bằng cách gắn thêm một MAC (Mã Xác thực Thông điệp) vào thông điệp. Hai ví dụ được đưa ra, cùng với một ví dụ về DES ở chế độ CBC với một khóa bí mật mà Bên tiếp nhận thông điệp biết và chỉ được chỉ định bằng một tên khóa. Ví dụ thứ nhất theo ISO 8731-1. Ví dụ thứ hai dựa trên việc sử dụng thuật toán DES phù hợp với phương thức hoạt động được trình bày trong ISO/IEC 9797. Khóa bí mật cần được mã hóa DES để truyền đi dưới một khóa mã hóa - khóa dùng chung cho cả Bên gửi và Bên tiếp nhận. Khóa mã hóa khóa này được chỉ định bằng tên của nó.
- Toàn vẹn nội dung được cung cấp bằng một hàm băm dựa trên thuật toán DES trong chế độ MDC, phù hợp với ISO 10118-2. Trong ví dụ thứ ba này, không có khóa bí mật dùng chung cho cả B và Bên tiếp nhận. Giá trị băm được truyền đi không bảo vệ, do vậy dịch vụ an ninh này có thể không có khả năng đảm bảo an toàn cho thông điệp.
- Mặc dù Bên gửi và Bên tiếp nhận dùng chung các khóa, các cơ chế mã hóa không được thỏa thuận hoàn toàn 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 kỹ thuật an ninh, thuật toán và các phương thức hoạt động được sử dụng trên thực tế.

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

Thẻ	Tên	S	R	Xác thực nguồn gốc thông điệp ISO 8731 -1	Xác thực nguồn gốc thông điệp ISO 9797	Toàn vẹn nội dung ISO/IEC 10118-2	Chú thích
SG1		C	99	Một cho mỗi dịch vụ an ninh			1
USH	TIÊU ĐỀ AN NINH	M	1				
0501	DỊCH VỤ AN NINH, ĐÃ MÃ HÓA	M	1	2	2	3	
0534	SỐ HIỆU THAM CHIẾU AN NINH	M	1	a	b	c	
0505	HÀM LỌC, ĐÃ MÃ HÓA	C	1	6	6	6	
S500	CHI TIẾT ĐỊNH DANH AN NINH	C	2				
0577	Hạn định bên tham gia an ninh	M		1	1	1	2

Thẻ	Tên	S	R	Xác thực nguồn gốc thông điệp ISO 8731 -1	Xác thực nguồn gốc thông điệp ISO 9797	Toàn vẹn nội dung ISO/IEC 10118-2	Chú thích
0538	Tên khóa	C		Key - N	—	—	3
S500	CHI TIẾT ĐỊNH DANH AN NINH	C	2				
0577	Hạn định bên tham gia an ninh	M		2	2	2	4
USA	THUẬT TOÁN AN NINH	C	3				
S502	THUẬT TOÁN AN NINH	M	1				
0523	Sử dụng thuật toán, đã mã hóa	M		2	2	2	
0525	Mật mã hoá phương thức hoạt động, đã mã hóa	C		—	—	—	
0527	Thuật toán, đã mã hóa	C		37	38	40	
S503	THAM SỐ THUẬT TOÁN	C	9		Một cho tên khóa mã hóa khóa		
0531	Hạn định tham số thuật toán	M		—	10	—	5
0554	Giá trị tham số thuật toán	M		—	KEK - N	—	
S503	THAM SỐ THUẬT TOÁN	C	9		Một cho khóa mã hóa		
0531	Hạn định tham số thuật toán	M		—	5	—	6
0554	Giá trị tham số thuật toán	M		—	Enc - Key	—	
Cấu trúc dữ liệu được bảo vệ (các đoạn/đối tượng (các)trao đổi/(các)gói/(các) nhóm của bên sử dụng)							
SGn		C	99	Một cho mỗi dịch vụ an ninh			1
UST	ĐUÔI AN NINH	M	1				
0534	SỐ HIỆU THAM CHIẾU AN NINH	M	1	A	b	c	
0588	SỐ LƯỢNG ĐOẠN AN NINH	M	1				
USR	KẾT QUẢ AN NINH	C	1				
S508	KẾT QUẢ HỢP LỆ	M	2				7
0563	Hạn định giá trị hợp lệ	M		1	1	1	
0560	Giá trị hợp lệ	C		MAC	MAC	Hash	8

Thẻ	Tên	S	R	Xác thực nguồn gốc thông điệp ISO 8731 -1	Xác thực nguồn gốc thông điệp ISO 9797	Toàn vẹn nội dung ISO/IEC 10118-2	Chú thích
CHÚ THÍCH 1. Cả hai cấu trúc phải có số lần xuất hiện như nhau; 2. Bên gửi thông điệp; 3. Tên khóa bí mật dùng chung cho bên gửi và bên tiếp nhận; 4. Bên tiếp nhận thông điệp; 5. Khóa mã hóa khóa dùng chung cho bên gửi và bên tiếp nhận ở đây chỉ đề cập đến tên khoá mã hoá khoá; 6. Khóa bí mật được mã hóa theo với khóa mã hóa khóa; 7. Một số thuật toán ký (như DSA) yêu cầu hai kết quả tham số; 8. Các giá trị kết quả đối với "toàn vẹn" không được bảo vệ và có thể phải tách biệt nhau.							

E.3 Liên kết sử dụng khóa không đối xứng và các đoạn an ninh thích hợp

Ma trận trong Bảng E.2 thiết lập các mối quan hệ trong các trường hợp sau:

- an ninh mức thông điệp/gói trao đổi tích hợp (TCVN ISO 9735- 5 : 2004);
- dịch vụ an ninh được cung cấp là không- từ chối gốc, có hai phương pháp với kỹ thuật tính toán chữ ký khác nhau;
- có hai thuật toán không đối xứng: RSA và DSA;
- hai hàm - băm được chọn: DES trong chế độ MDC cùng với RSA, và SHA-1 cùng với DSA;
- chứng chỉ được thừa nhận không trao đổi trước;
- đoạn USC định danh chính xác hàm băm và hàm ký được tổ chức chứng nhận sử dụng để ký chứng chỉ. Bên tiếp nhận đã biết khóa công bố cần cho việc kiểm tra chữ ký chứng nhận của tổ chức chứng nhân. Khoá công bố này được chỉ định bằng tên trong đoạn USC;
- chỉ bao gồm một chứng chỉ, cần cái thứ hai, nếu chỉ sử dụng một khóa công bố của bên tiếp nhận.

Bảng E.2 - Ma trận tương quan khi sử dụng thuật toán không đối xứng

THẺ	Tên	S	R	Không từ chối gốc (RSA)	Không từ chối gốc (DSA)	Chú thích
SG1		C	99	Một cho mỗi dịch vụ an ninh		1
USH	TIÊU ĐỀ AN NINH	M	1			
0501	DỊCH VỤ AN NINH, ĐÃ MÃ HÓA	M	1	1	1	2
0534	SỐ HIỆU THAM CHIẾU AN NINH	M	1	d	e	
0505	HÀM LỌC, ĐÃ MÃ HÓA	C	1	6	6	
S500	CHI TIẾT ĐỊNH DANH AN NINH	C	2			
0577	Hạn định bên tham gia an ninh	M		1	1	3

THẺ	Tên	S	R	Không từ chối gốc (RSA)	Không từ chối gốc (DSA)	Chú thích
S500	CHI TIẾT ĐỊNH DANH AN NINH	C	2			
0r577	Hạn định bên tham gia an ninh	M		2	2	4
USA	THUẬT TOÁN AN NINH	C	3			
S502	THUẬT TOÁN AN NINH	M	1			
0523	Sử dụng thuật toán, mã hóa	M		1	1	5
0525	Mật mã hoá phương thức hoạt động, đã mã hóa	C		—	—	
0527	Thuật toán, đã mã hóa	C		42	16	
SG2		C	2	Chỉ một: chứng chỉ Bên gửi		
USC		M	1			
0536	THAM CHIẾU CHỨNG CHỈ	C	1	Tham chiếu của chứng chỉ này		
S500	CÁC CHI TIẾT ĐỊNH DANH AN NINH	C	2	(Bên sở hữu chứng chỉ)		
0577	Hạn định bên tham gia an ninh	M		3	3	6
S500	CHI TIẾT XÁC MINH AN NINH	C	2	(bên xác thực)		
0577	Hạn định bên tham gia an ninh	M		4	4	7
0538	Tên khóa	C		Tên (PK/CA)	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	Sử dụng thuật toán, đã mã hóa	M		6	6	8
0525	Sử dụng thuật toá, đã mã hóa	C		16	—	
0527	Thuật toán, mã hóa	C		10	11	
S503	THAM SỐ THUẬT TOÁN	C	9	(độ dài mô đun)	Tham số P của DSA	
0531	Hạn định tham số thuật toán	M		14	25	
0554	Giá trị tham số thuật toán	M		Mod - L	P	
S503	THAM SỐ THUẬT TOÁN	C	9	(mô đun)	Tham số Q của DSA	
0531	Hạn định tham số thuật toán	M		12	26	
0554	Giá trị tham số thuật toán	M		Mod	Q	
S503	THAM SỐ THUẬT TOÁN	C	9	(Hàm mũ công bố)	Tham số G của DSA	
0531	Hạn định tham số thuật toán	M		13	27	
0554	Giá trị tham số thuật toán	M		Pub - K	G	
S503	THAM SỐ THUẬT TOÁN	C	9	—	Tham số Y của DSA	
0531	Hạn định tham số thuật toán	M		—	28	

THẺ	Tên	S	R	Không từ chối gốc (RSA)	Không từ chối gốc (DSA)	Chú thích
0554	Giá trị tham số thuật toán	M		—	Y	
USA	THUẬT TOÁN AN NINH	C	3	(hàm băm của CA cho chữ ký của chứng chỉ)		
S502	THUẬT TOÁN AN NINH	M	1			
0523	Sử dụng thuật toán, đã mã hóa	M		4	4	9
0525	Sử dụng thuật toán, đã mã hóa	C		11	—	
0527	Thuật toán, đã mã hóa	C		1	8	
USA	THUẬT TOÁN AN NINH	C	3	(Chức năng ký của CA cho chữ ký của chứng chỉ)		
S502	THUẬT TOÁN AN NINH	M	1			
0523	Sử dụng thuật toán, mã hóa	M		3	3	10
0525	Sử dụng thuật toán, mã hóa	C		16	—	
0527	Thuật toán, đã mã hóa	C		10	11	
USR	KẾT QUẢ AN NINH	C	1			
S508	KẾT QUẢ HỢP LỆ	M	2			11
0563	Hạn định giá trị hợp lệ	M		1	2	
0560	Giá trị hợp lệ	C		Sig	R	
S508	KẾT QUẢ HỢP LỆ	M	2			11
0563	Hạn định giá trị hợp lệ	M		—	3	
0560	Giá trị hợp lệ	C		—	S	
Cấu trúc dữ liệu được bảo vệ (các đoạn/đối tượng/(các)trao đổi/(các)gói (các) nhóm của bên sử dụng)						
SGn		C	99	Một cho mỗi dịch vụ an ninh		1
UST	ĐUÔI AN NINH	M	1			
0534	SỐ HIỆU THAM CHIẾU AN NINH	M	1	d	e	
0588	SỐ LƯỢNG 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	2	
0560	Giá trị hợp lệ	C		Sig	R	
S508	KẾT QUẢ HỢP LỆ	M	2			11
0563	Hạn định giá trị hợp lệ	M		—	3	
0560	Giá trị hợp lệ	C		—	S	

THẺ	Tên	S	R	Không từ chối gốc (RSA)	Không từ chối gốc (DSA)	Chú thích
CHÚ THÍCH 1. Cả hai cấu trúc phải có cùng số lần xuất hiện; 2. Thừa nhận không - từ chối gốc bao Chức năng xác thực nguồn gốc thông điệp và toàn vẹn; 3. Bên gửi thông điệp; 4. Bên tiếp nhận thông điệp; 5. Bên gửi áp dụng hàm băm trên cấu trúc an ninh; 6. Bên sở hữu chứng chỉ: các chi tiết định danh giống như trong USH S500 cho Bên gửi thông điệp; 7. Bên xác thực: tổ chức chứng nhận (CA); 8. Chức năng chữ ký của Bên gửi; 9. Hàm băm của CA; 10. Chức năng chữ ký của CA; 11. Một số thuật toán ký (như DSA) yêu cầu hai kết quả tham số.						

Tài liệu tham khảo

1. ISO/IEC 646 : 1991, Information technology - ISO 7 - bít coded character set for information interchange *(Công nghệ thông tin – Bộ ký tự mã hóa 7 bít ISO cho trao đổi thông tin);*
2. ISO 8601 : 2000, Data elements and interchange formats - Information interchange - Representation of dates and times *(Phần tử dữ liệu và định dạng trao đổi – Trao đổi thông tin – Biểu diễn ngày và giờ);*
3. ISO 8731-1 : 1987, Banking - Approved algorithms for message authentication - Part 1 : DEA *(Nghiệp vụ quản lý – Thuật toán dành cho xác thực thông điệp – Phần 1 : DEA);*
4. ISO/IEC 9797 : 1994, Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm *(Công nghệ thông tin – Kỹ thuật an ninh – Cơ chế toàn vẹn dữ liệu sử dụng một Chức năng kiểm tra mã hóa với một thuật toán mã khối)*
5. ISO/IEC 10116 : 1997 Information technology - Security techniques - Modes of operation for an n - bít block cipher *(Công nghệ thông tin – Kỹ thuật an ninh – Chế độ thao tác một mã khối n - bít);*
6. ISO/IEC 10118-2 : 2000, Information technology - Security techniques - Hash-functions - Part 2 : Hash - functions using an n - bít block cipher *(Công nghệ thông tin – Kỹ thuật an ninh – Hàm băm – Phần 2 : Hàm băm sử dụng một mã khối n - bít);*
7. ISO/IEC 10181-1 : 1996, Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview *(Công nghệ thông tin – Liên kết hệ thống mở – Cơ cấu an ninh hệ thống mở: Khái quát);*
8. ISO/IEC 10646-1 : 2000, Information technology - Universal Multiple - Octet Coded Character Set (UCS) - Part 1 : Architecture and Basic Multilingual Plane *(Công nghệ thông tin – Bộ ký tự mã hóa bội tám chung (UCS) – Phần 1 : Mức đa ngữ cơ bản và kiến trúc);*
9. ISO/IEC 11770-1 : 1996, Information technology - Security techniques - Key management - Part 1 : Framework *(Công nghệ thông tin – Kỹ thuật an ninh – Quản lý khóa – Phần 1: Cơ cấu).*