TCVN **T I Ê U C H U Ẩ N Q U Ố C G I A**

TCVN ISO 9735-7 : 2004

ISO 9735-7 : 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 LỚP ỨNG DỤNG (SỐ PHIÊN BẢN CÚ PHÁP: 4, SỐ PHÁT HÀNH CÚ PHÁP : 1).

PHẦN 7: QUI TẮC AN NINH CHO EDI LÔ (TÍNH BẢO MẬT)

Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules (Syntax version number:4, Syntax release number: 1)- Part 7: security rules for batch EDI (confidentiality)

HÀ NỘI – 2008

Mục lục

Lời nói đầu

TCVN ISO 9735-7 : 2004 hoàn toàn tương đương với **ISO 9735-7: 2002**.

TCVN ISO 9735-7 : 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

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 hay 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 hay trao đổi.

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.

Trao đổi dữ liệu điện tử trong quản lý hành chính, thương mại và vận tải - 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 an ninh cho EDI lô (tính bảo mật)

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

Part 7: Security rules for batch EDI (confidentiality)

1 Phạm vi áp dụng

Tiêu chuẩn này quy định an ninh về độ tin cậy cho EDIFACT lô tại mức trao đổi, mức nhóm và mức gói/thông điệp phù hợp với các cơ chế an ninh đã được thiết 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*), 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 (sửa đổi và in lại năm 1990): *Số hiệu phiên bản cú pháp: 2*
- ISO 9735 : 1988 (Sửa đổi 1 :1992): *Số hiệu phiên bản cú pháp: 3*
- ISO 9735 : 1998: *Số hiệu phiên bản cú pháp: 4*

Phù hợp với một tiêu chuẩn có nghĩa là tất cả mọi yêu cầu, bao gồm cả các lựa chọn của tiêu chuẩn phải được hỗ trợ. Nếu tất cả các lựa chọn không được hỗ trợ thì phải công bố rõ là phù hợp với lựa chọn nào.

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 (ISO 9735-1), TCVN ISO 9735-2 (ISO 9735-2), TCVN ISO 9735-5 (ISO 9735-5) và TCVN ISO 9735-10 (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 Tài liệu viện dẫn

Những tiêu chuẩn sau đây bao gồm các điều khoản, mà thông qua tham khảo các tiêu chuẩn này tạo thành các điều khoản của tiêu chuẩn này. Đối với bất kỳ tài liệu tham khảo cũ (không phù hợp), các văn bản sửa đổi, hoặc soát xét nào đều không được áp dụng. Các tiêu chuẩn tham khảo có hiệu lực hiện thời:

TCVN ISO 9735-1: 2003 (ISO 9735-1: 2002), *Trao đổi dữ liệu điện tử trong quản lý hành chính, thương mại và vận tải (EDIFACT) - 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 (ISO 9735-2: 2002), *Trao đổi dữ liệu điện tử trong quản lý hành chính, thương mại và vận tải (EDIFACT) - 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 trưng cho EDI Lô.*

TCVN ISO 9735-3: 2003 (ISO 9735- 3: 2002), *Trao đổi dữ liệu điện tử trong quản lý hành chính, thương mại và vận tải (EDIFACT) - Qui tắc mức áp dụng (Số hiệu phiên bản cú pháp: 4, Số hiệu phát hành cú pháp: 1) – Phần 3: Qui tắc cú pháp đặc trưng cho EDI tương tác.*

TCVN ISO 9735-10: 2004 (ISO 9735- 10: 2002), *Trao đổi dữ liệu điện tử trong quản lý hành chính, thương mại và vận tải (EDIFACT) - Quy tắc cú pháp mức ứng dụng (Số hiệu phiên bản cú pháp: 4, Số hiệu phát hành cú pháp: 1). Phần 10 : Danh mục dịch vụ cú pháp.*

ISO/IEC 10181-5:1996*, Công nghệ thông tin – Kết nối các hệ thống mở – Khung an ninh cho các hệ thống mở: Khung bảo mật (Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework).*

4 Thuật ngữ và định nghĩa

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

5 Các quy tắc cho độ tin cậy EDI lô

5.1 Độ tin cậy EDIFACT

5.1.1 Khái quát

Các mối đe dọa an ninh liên quan đến truyền dữ liệu EDIFACT và các dịch vụ an ninh đưa ra nhằm chống lại các mối đe dọa trên được mô tả trong các phụ lục A và B của TCVN ISO 9735-5 (ISO 9735-5).

Điều này trình bày giải pháp cung cấp cấu trúc EDIFACT với dịch vụ an ninh về độ tin cậy.

Độ tin cậy của cấu trúc EDIFACT (thông điệp, gói, nhóm hoặc trao đổi) được cung cấp bằng cách mật mã hóa thân thông điệp, đối tượng, các thông điệp/gói hoặc các thông điệp/gói/nhóm, cùng với bất kỳ nhóm đoạn tiêu đề và đuôi an ninh khác, có sử dụng một thuật toán mật mã hóa thích hợp. Dữ liệu mật mã hóa này có thể được lọc để sử dụng cho các mạng truyền thông có dung lượng hạn chế.

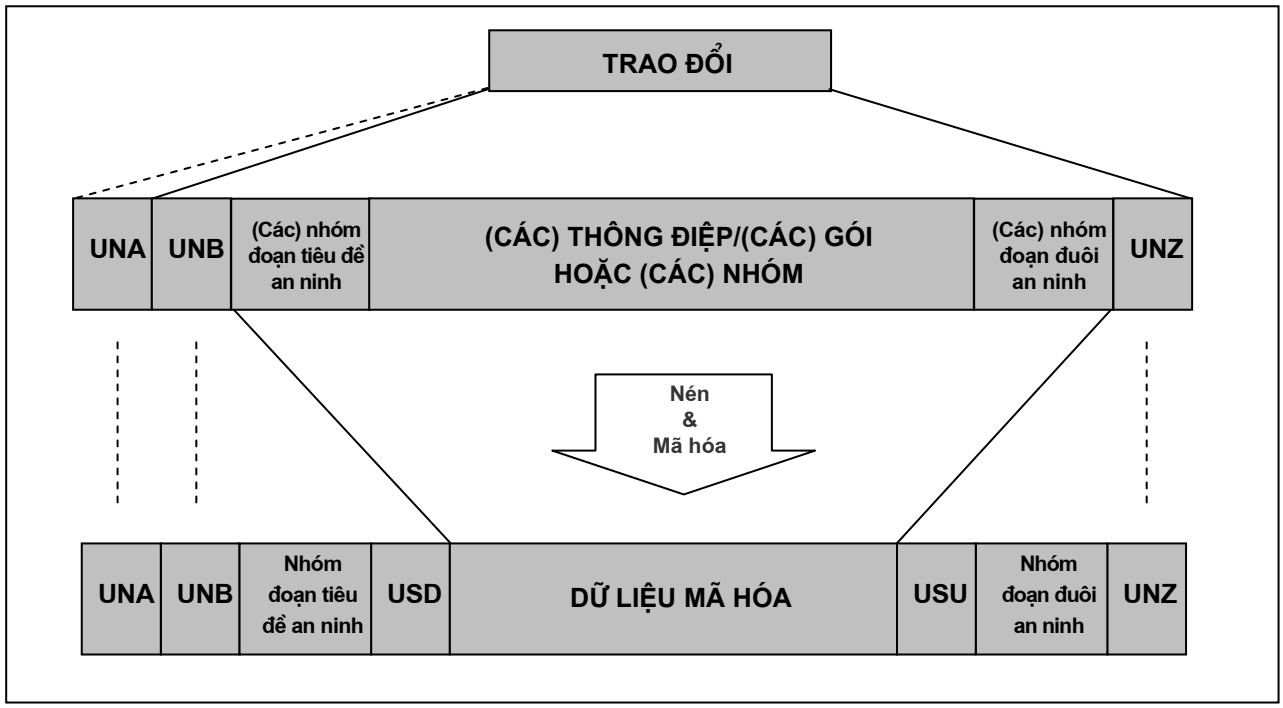
5.1.2 Độ tin cậy EDI lô

5.1.2.1 Độ tin cậy trao đổi

Hình 1 biểu diễn cấu trúc một trao đổi được bảo vệ với dịch vụ an ninh về độ tin cậy. Thông báo chuỗi dịch vụ (UNA), đoạn tiêu đề trao đổi (UNB) và đoạn đuôi trao đổi (UNZ) không bị ảnh hưởng bởi mật mã hóa.

Nếu nén thì phải áp dụng trước khi mật mã hóa.

Thuật toán mật mã hóa, nén và lọc cùng các tham số được quy định trong nhóm đoạn tiêu đề an ninh.



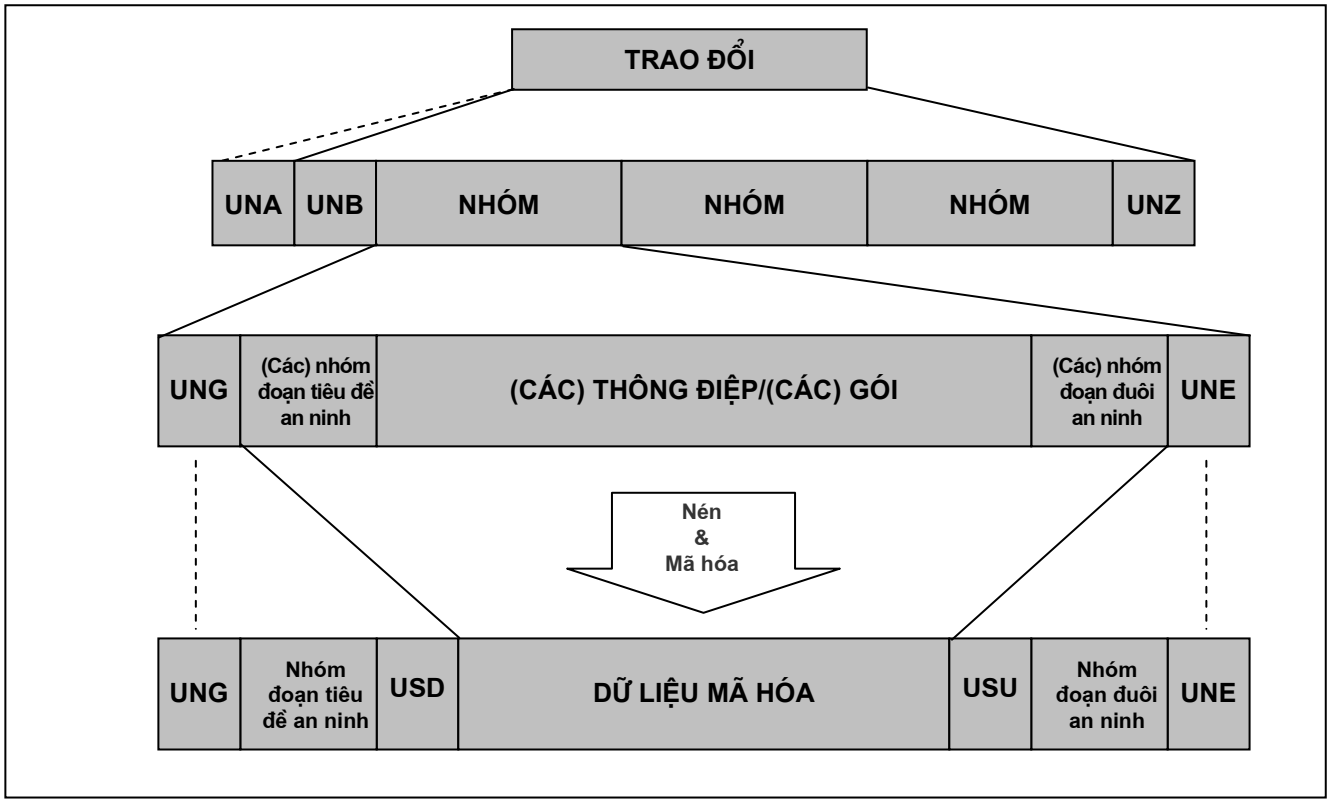
Hình 1 - Cấu trúc một trao đổi có nội dung [(các)thông điệp/(các) gói hoặc (các) nhóm] được mật mã hóa (giản đồ)

5.1.2.2 Độ tin cậy nhóm

Hình 2 biểu diễn cấu trúc một trao đổi gồm một nhóm được mã hóa, và nhóm này đã được bảo vệ bởi các dịch vụ an ninh khác. Đoạn tiêu đề nhóm (UNG) và đoạn đuôi nhóm (UNE) không bị ảnh hưởng do mã hóa.

Nếu nén thì phải áp dụng trước khi mật mã hóa.

Thuật toán mật mã hóa, thuật toán nén và thuật toán lọc cùng các tham số được quy định trong nhóm đoạn tiêu đề an ninh.



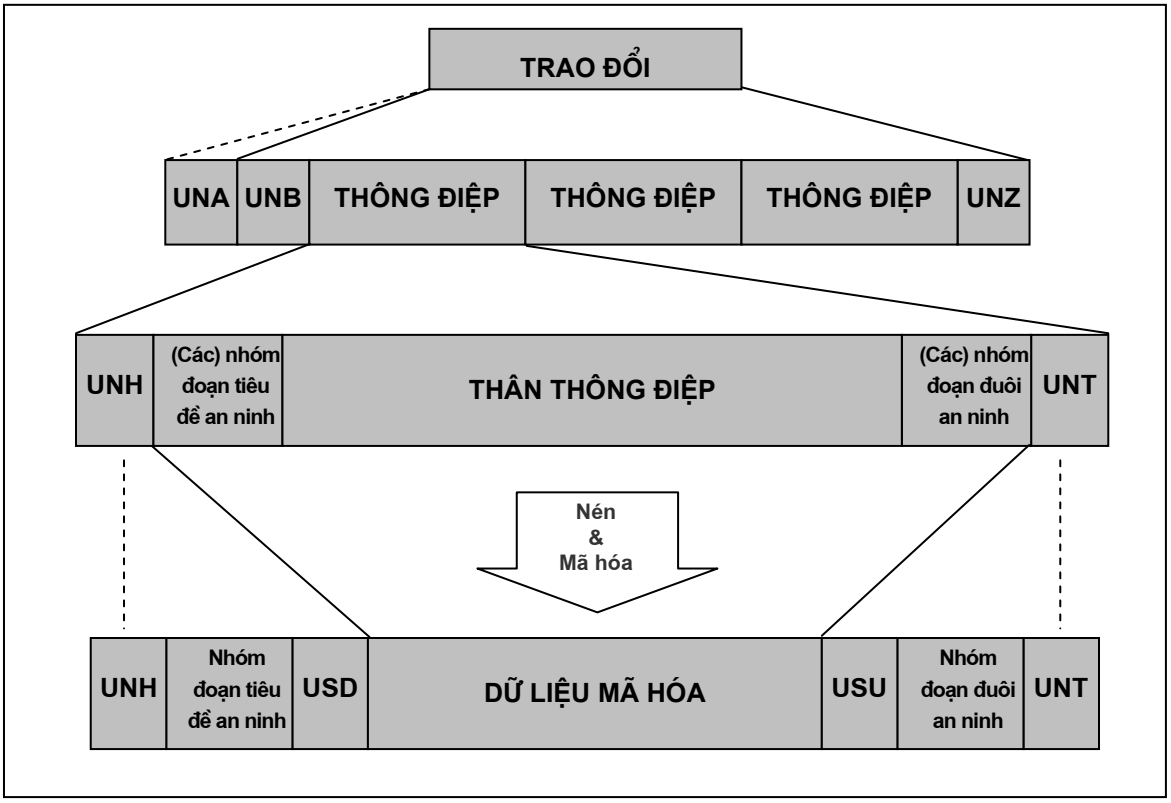
Hình 2 - Cấu trúc một trao đổi gồm một nhóm có nội dung (thân nhóm và các nhóm đoạn tiêu đề và đuôi an ninh liên kết) đã được mật mã hóa (giản đồ)

5.1.2.3 Độ tin cậy thông điệp

Hình 3 biểu diễn cấu trúc một trao đổi gồm một thông điệp đã mật mã hóa và thông điệp này đã được bảo vệ bởi các dịch vụ an ninh khác. Đoạn tiêu đề thông điệp (UNH) và đoạn đuôi thông điệp (UNT) không bị ảnh hưởng do mật mã hóa.

Nếu nén thì phải áp dụng trước khi mật mã hóa.

Thuật toán mật mã hóa, nén và lọc cùng các tham số được chỉ rõ trong nhóm đoạn tiêu đề an ninh.



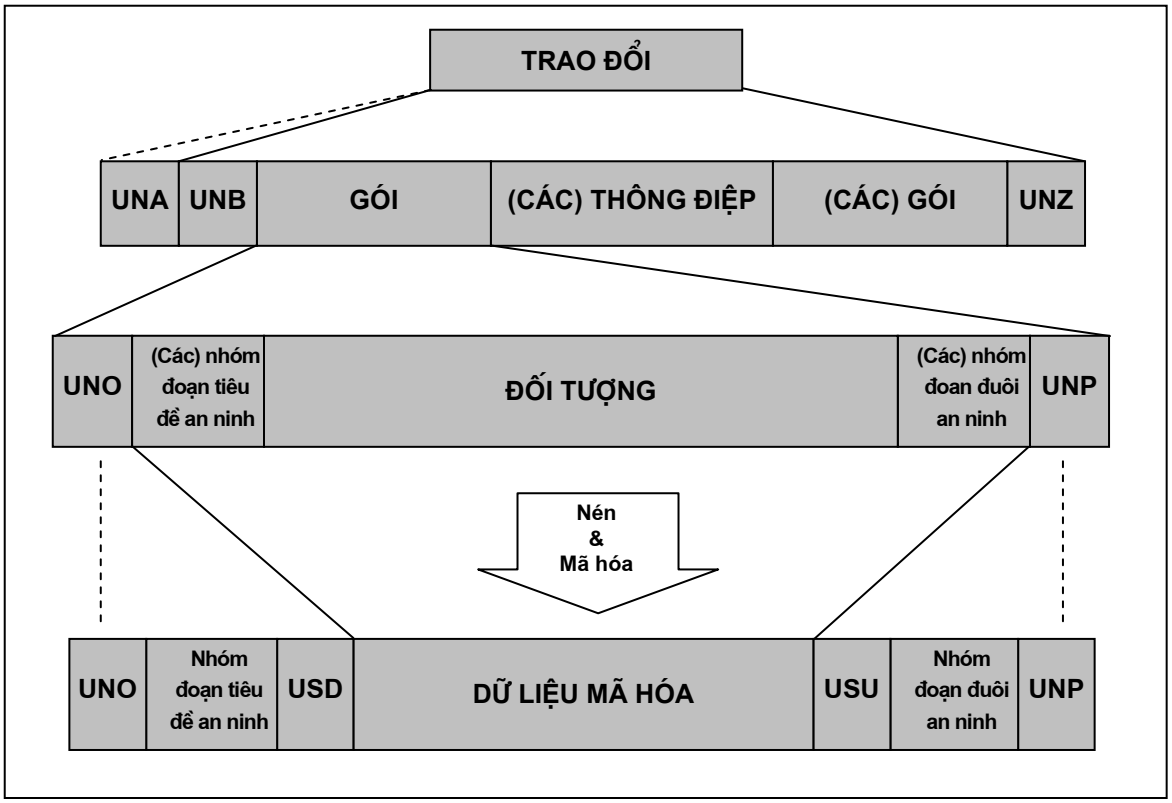
Hình 3 - Cấu trúc một trao đổi gồm một thông điệp có nội dung (thân thông điệp và các nhóm đoạn tiêu đề an ninh và nhóm đoạn đuôi an ninh liên kết) được mật mã hóa (giản đồ)

5.1.2.4 Độ tin cậy gói

Hình 4 biểu diễn cấu trúc một trao đổi gồm một gói đã mật mã hóa và được bảo vệ bằng các dịch vụ an ninh khác. Đoạn tiêu đề gói (UNO) và đoạn đuôi gói (UNP) không bị ảnh hưởng do mã hóa.

Nếu nén thì phải áp dụng trước khi mật mã hóa.

Thuật toán mật mã hóa, thuật toán nén và thuật toán lọc cùng các tham số được quy định trong nhóm đoạn tiêu đề an ninh.



Hình 4 - Cấu trúc một trao đổi gồm một gói có nội dung (đối tượng và các nhóm đoạn tiêu đề an ninh và nhóm đoạn đuôi an ninh liên kết) được mật mã hóa (giản đồ)

5.1.3 Cấu trúc dữ liệu mã hóa đoạn tiêu đề và đoạn đuôi

Bảng 1 - Bảng đoạn các nhóm đoạn tiêu đề và nhóm đoạn đuôi an ninh

THẺ	Tên	S	R
-----	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		3
USR	Kết quả an ninh	C	1
USD	Tiêu đề mã hoá dữ liệu	M	1
	Dữ liệu đã mã hóa		
USU	Đuôi mã hoá dữ liệu	M	1
-----	Nhóm đoạn n ----------	C	99
UST	Đuôi an ninh	M	1
USR	Kết quả an ninh	C	1

CHÚ THÍCH Các đoạn USH, USA, USC, USR và UST không được mô tả trong tiêu chuẩn này mà được qui định trong TCVN ISO 9735-10 (ISO 9735-10).

5.1.4 Phân loại đoạn dữ liệu

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

Nhóm đoạn xác định dịch vụ an ninh, các cơ chế an ninh được áp dụng và dữ liệu cần thiết để tiến hành các tính toán hợp lệ.

Chỉ cần một nhóm đoạn tiêu đề an ninh cho độ tin cậy.

USH, Tiêu đề an ninh

Đoạn quy định dịch vụ an ninh về độ tin cậy áp dụng cho cấu trúc EDIFACT chứa đoạn đó (xem TCVN ISO 9735-5 (ISO 9735-5)).

USA, Thuật toán an ninh

Đoạn xác định thuật toán an ninh, kỹ thuật sử dụng và chứa các tham số kỹ thuật yêu cầu. (Các) thuật toán được áp dụng cho thân thông điệp, đối tượng, thông điệp/gói hoặc thông điệp/ gói/ nhóm. (Các) thuật toán này phải chứa phép đối xứng, phép nén hoặc tính toàn vẹn của phép nén.

Thuật toán không đối xứng không được tham chiếu trực tiếp trong đoạn USA trong nhóm đoạn 1 nhưng có thể xuất hiện chỉ trong nhóm đoạn 2, được khởi tạo bởi đoạn USC.

Nếu sử dụng, phải nén dữ liệu trước khi mật mã hóa, một lần xuất hiện của USA được sử dụng để quy định thuật toán và phương thức hoạt động tùy chọn. Tham số bổ sung, như cây thư mục khởi tạo, có thể được quy định bởi giá trị tham số trong đoạn USA.

Nếu nén và thuật toán nén sử dụng không gắn liền với việc xác minh toàn vẹn thì sự xuất hiện của đoạn USA có thể được sử dụng để chỉ rõ điều này. Giá trị xác minh toàn vẹn được tính toán thông qua văn bản được nén trước khi mật mã hóa. Vị trí (nghĩa là bộ tám dự phòng) của giá trị xác minh toàn vẹn trong dữ liệu được nén có thể được quy định bằng một giá trị tham số. Kích thước (bộ tám bít) của giá trị xác minh toàn vẹn được đưa ra gián tiếp qua thuật toán xác minh toàn vẹn được sử dụng.

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

Nhóm đoạn bao gồm các dữ liệu cần thiết để thông qua các phương pháp an ninh áp dụng cho cấu trúc EDIFACT khi sử dụng các thuật toán không đối xứng (xem TCVN ISO 9735-5 (ISO 9735-5)).

USC, Chứng chỉ

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

USA, Thuật toán an ninh

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

USR, Kết quả an ninh

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

USD, Tiêu đề mã hóa dữ liệu

Đoạn này quy định kích thước trong các bộ tám bít của dữ liệu được nén (tùy chọn), mã hóa và lọc (tùy chọn). Có thể qui định số tham chiếu được sử dụng để nhận biết cấu trúc EDIFACT đã mã. Nếu có số tham chiếu thì phải sử dụng cùng số tham chiếu trong cả hai đoạn USD và USU.

Nếu áp dụng cơ chế đệm trước khi mật mã hóa thì có thể qui định số lượng các bộ tám bít đã đệm.

Dữ liệu mã hóa

Tiêu chuẩn này chứa dữ liệu đã mã hóa nhờ sử dụng các thuật toán và các cơ chế được quy định trong nhóm đoạn tiêu đề an ninh.

USU, Đuôi mã hóa dữ liệu

Đoạn này quy định kích thước trong các bộ tám bít của dữ liệu được nén (tùy chọn), được mã hóa và được lọc (tùy chọn). Có thể qui định số tham chiếu được sử dụng để nhận biết cấu trúc EDIFACT đã mã hóa. Nếu có số tham chiếu thì phải sử dụng cùng số tham chiếu trong cả hai đoạn USD và USU.

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

Một Nhóm đoạn chứa một liên kết với nhóm đoạn tiêu đề an ninh và kết quả của các chức năng an ninh áp dụng cho cấu trúc EDIFACT (xem TCVN ISO 9735-5 (ISO 9735-5)).

UST, Đuôi an ninh

Đoạn thiết lập một liên kết giữa nhóm đoạn tiêu đề và đuôi an ninh, và quy định số lượng đoạn an ninh được chứa trong các nhóm này, cộng với các đoạn USD và USU.

USR, Kết quả an ninh

Đoạn chứa kết quả của các chức năng an ninh áp dụng cho cấu trúc EDIFACT được quy định trong nhóm tiêu đề an ninh liên kết (xem TCVN ISO 9735-5 (ISO 9735-5)). Đoạn này không có mặt trong dịch vụ an ninh về độ tin cậy.

5.1.5 Sử dụng tiêu đề mã hóa dữ liệu và đuôi mã hóa dữ liệu cho bảo mật

Một cấu trúc EDIFACT được gói trong một tiêu đề mã hóa dữ liệu và đuôi mã hóa dữ liệu được biến đổi thành dữ liệu mã hóa. Dữ liệu mã hóa và các nhóm đoạn tiêu đề và đuôi an ninh kết hợp thay cho thân thông điệp gốc, đối tượng hoặc (các) thông điệp/(các) gói/(các) nhóm. Tiêu đề và đuôi của cấu trúc EDIFACT được mã hóa không bị ảnh hưởng khi mã hóa.

Dữ liệu mã hóa phải bắt đầu ngay sau dấu phân tách kết thúc đoạn USD là đoạn chỉ ra độ dài của dữ liệu mã hóa theo các bộ tám bít. Dữ liệu mã hóa được theo sau bởi đoạn USU là đoạn xác định lại độ dài của dữ liệu mã hóa phải giống như trong đoạn USD.

5.1.6 Sử dụng các nhóm đoạn tiêu đề và đuôi an ninh cho bảo mật

Như trong TCVN ISO 9735-5 (ISO 9735-5), một nhóm đoạn tiêu đề an ninh quy định bảo mật và bao gồm một nhóm đoạn đuôi an ninh. Nhóm đoạn đuôi an ninh sử dụng cho bảo mật chỉ chứa đoạn UST.

Không được sử dụng dịch vụ an ninh EDIFACT nào khác cho một cấu trúc EDIFACT đã được mã hóa.

5.2 Nguyên tắc sử dụng

5.2.1 Đa dịch vụ an ninh

Nếu nhiều hơn một dịch vụ an ninh trừ tính bảo mật được yêu cầu cùng một lúc bởi bên gửi cấu trúc EDIFACT trước khi mã hoá thì phải thực hiện theo các quy tắc quy định trong TCVN ISO 9735-5 (ISO 9735-5). Bên nhận phải thực hiện các xác minh liên quan sau khi giải mã.

5.2.2 Độ tin cậy

Độ tin cậy của cấu trúc EDIFACT phải phù hợp với các nguyên tắc đã được quy định trong ISO/IEC 10181-5.

Dịch vụ an ninh về bảo mật phải được chỉ rõ trong nhóm đoạn tiêu đề an ninh, và thuật toán phải được chỉ ra trong đoạn USA trong nhóm đoạn 1. Đoạn USA này cũng có thể chứa dữ liệu cần thiết để thiết lập khóa quan hệ giữa các bên với vai trò là bên khởi tạo an ninh và bên nhận an ninh.

Bên khởi tạo an ninh phải mã hóa cấu trúc EDIFACT, từ ngay sau dấu kết thúc đoạn của đoạn tiêu đề (thông điệp/gói hoặc nhóm trao đổi), tới ngay trước ký tự đầu tiên của đoạn đuôi (thông điệp/gói hoặc nhóm trao đổi), và kết quả là dữ liệu mã hóa. Đối với việc nhận dữ liệu mã hóa, bên nhận an ninh phải giải mã dữ liệu mã hóa và do đó phải khôi phục lại cấu trúc EDIFACT gốc, ngoại trừ các đoạn tiêu đề và đuôi.

5.2.3 Hàm lọc và trình bày bên trong

Kết quả của quá trình mã hóa là một chuỗi bít ngẫu nhiên. Điều này có thể gây khó khăn cho các mạng truyền thông dung lượng hạn chế. Để phòng ngừa vấn đề này, chuỗi bít có thể được ánh xạ ngược lại một bộ ký tự cụ thể bằng một hàm lọc.

Mục đích của việc sử dụng một hàm lọc là làm tăng kích thước của dữ liệu mã hóa. Các hàm lọc khác nhau thường có các hệ số mở rộng hơi khác nhau. Một số có thể cho phép tài liệu lọc chứa bất kỳ ký tự nào của bộ ký tự đích, bao gồm các ký tự dịch vụ như các ký tự kết thúc đoạn, trong khi đó các hàm lọc khác có thể lọc ra các ký tự dịch vụ này.

Độ dài của dữ liệu được truyền trong phần tử dữ liệu "độ dài dữ liệu trong các bộ tám bít" trong các đoạn USD và USU phải biểu diễn độ dài của dữ liệu (được lọc) được mã hóa (và được nén), được sử dụng để xác định kết thúc của dữ liệu mã hóa. Hàm lọc được sử dụng phải được chỉ trong 0505 (hàm lọc, mã hóa) của USH trong nhóm đoạn tiêu đề an ninh tin cậy.

5.2.4 Sử dụng kỹ thuật nén trước khi mã hóa

Chi phí tính toán cho việc mã hóa liên quan trực tiếp đến kích thước của dữ liệu cần mã hóa, nó có thể có ích khi nén dữ liệu trước khi mật mã hóa.

Hầu hết các kỹ thuật nén không ảnh hưởng đến văn bản mã hóa, thậm chí lọc, như vậy nếu việc nén được yêu cầu thì nó được áp dụng trước khi mật mã hóa.

Bởi vậy, khi kỹ thuật nén được sử dụng cho dịch vụ an ninh bảo mật, nhóm đoạn tiêu đề an ninh có thể chỉ ra rằng dữ liệu đã được nén trước khi mật mã hóa, và có thể nhận biết thuật toán nén cùng các tham

số tùy chọn được sử dụng. Sau khi giải mã dữ liệu mã hóa, dữ liệu được giải nén trước khi cấu trúc EDIFACT được khôi phục lại.

5.2.5 Trình tự hoạt động

5.2.5.1 Mã hóa và các hoạt động liên quan

Khi xử lý một cấu trúc EDIFACT để cung cấp bảo mật, các hoạt động phải tiến hành như sau:

1. nén cấu trúc EDIFACT (tùy chọn) và tính toán giá trị toàn vẹn trên dữ liệu nén (tùy chọn);
2. mã hóa cấu trúc EDIFACT (được bảo vệ toàn vẹn và nén);
3. lọc (tùy chọn) dữ liệu mã hóa (được bảo vệ nén và toàn vẹn).

5.2.5.2 Giải mã và các thao tác liên quan

Khi xử lý một cấu trúc EDIFACT đã mã hóa để khôi phục lại một cấu trúc EDIFACT gốc, các hoạt động tiến hành như sau:

1. giải lọc dữ liệu mã hóa được lọc (nếu được lọc);
2. giải mã dữ liệu mã hóa;
3. xác minh giá trị toàn vẹn trên dữ liệu nén (nếu giá trị toàn vẹn có mặt) và triển khai (nghĩa là giải nén) dữ liệu giải mã để khôi phục cấu trúc EDIFACT gốc (nếu được nén).

Phụ lục A

(tham khảo)

Ví dụ bảo vệ thông điệp

A.1 Lời nói đầu

Ví dụ đưa ra ở đây minh họa áp dụng đoạn dịch vụ an ninh.

Ví dụ về bảo mật thông điệp đơn đặt hàng thanh toán EDIFACT tưởng tượng. Các cơ chế an ninh được trình bầy ở đây hoàn toàn độc lập với kiểu thông điệp và có thể áp dụng cho mọi thông điệp EDIFACT.

Ví dụ này trình bầy cách sử dụng các đoạn dịch vụ an ninh khi phương pháp được áp dụng dựa trên một **thuật toán đối xứng**, nhằm cung cấp dịch vụ an ninh về bảo mật thông điệp. Khóa đối xứng được trao đổi trước giữa các bên, và nhóm đoạn tiêu đề an ninh chỉ chứa hai đoạn đơn giản.

A.2 Tình huống

Công ty A yêu cầu Ngân hàng A, dùng mã 603000 để ghi vào sổ nợ số tài khoản 00387806 vào ngày 9 tháng 4 năm 1995 tổng số 54345,10 Bảng Anh. Số tiền này để trả cho Ngân hàng B, dùng mã 201827, với số tài khoản 00663151 của Công ty B, West Dock, Milford Haven. Việc thanh toán theo hóa đơn 62345. Tên liên hệ của Bên được trả nợ là ông Jones thuộc Phòng kinh doanh.

Ngân hàng A yêu cầu đơn đặt hàng thanh toán được bảo vệ bằng dịch vụ an ninh về "bảo mật thông điệp".

Việc này đạt được bằng mã hóa thân thông điệp với "Tiêu chuẩn Mã hóa Dữ liệu" (DES) đối xứng tại gửi thông điệp. Cho rằng khóa - DES bí mật đã được trao đổi trước giữa Công ty A và Ngân hàng A. Để giảm kích thước thông tin truyền, thân thông điệp được nén trước khi mật mã hóa. Thuật toán sử dụng để nén thân thông điệp theo ISO/IEC 12042, Information technology - Data compression for information interchange - Binary arithmetic coding algorithm *(Công nghệ thông tin – Nén dữ liệu cho trao đổi thông tin – Thuật toán mật mã hóa số nhị phân)*.

A.3 Chi tiết an ninh

Dưới đây chỉ đề cập các nhóm đoạn tiêu đề và nhóm đoạn đuôi an ninh bảo mật.

TIÊU ĐỀ AN NINH	
DỊCH VỤ AN NINH	Độ tin cậy thông điệp
SỐ THAM CHIẾU AN NINH	Số tham chiếu của tiêu đề là 1
HÀM LỌC	Tất cả các giá trị nhị phân được lọc với bộ lọc thập lục phân
BỘ KÝ TỰ MÃ HÓA GỐC	Thông điệp được mã hóa thành mã ASCII 8 bít
CHI TIẾT ĐỊNH DANH AN NINH	

Bên gửi thông điệp (bên mã hóa thông điệp)	Ông Smith ở Công ty A
CHI TIẾT ĐỊNH DANH AN NINH Bên nhận thông điệp (bên giải mã thông điệp)	 Ngân hàng A
SỐ THỨ TỰ AN NINH	Số thứ tự an ninh của thông điệp này là 001
NGÀY VÀ GIỜ AN NINH	Thẻ thời gian an ninh là: ngày: 09041995, giờ: 13:59:50
THUẬT TOÁN AN NINH	
THUẬT TOÁN AN NINH Sử dụng thuật toán Phương thức hoạt động mã hoá Thuật toán Cơ chế đệm	 Một thuật toán đối xứng được sử dụng để thông điệp tin cậy Một chế độ tính chuỗi khối được sử dụng Thuật toán DES được sử dụng Số nhị phân 0 được sử dụng cho lược đồ đệm
THÔNG SỐ THUẬT TOÁN Hạn định thông số thuật toán Giá trị thông số thuật toán	 Xác định giá trị thông số thuật toán này bằng tên của khóa đối xứng được trao đổi trước Khóa là ENC-KEY1 được sử dụng
THUẬT TOÁN AN NINH	
THUẬT TOÁN AN NINH Thuật toán sử dụng Thuật toán	 Một thuật toán nén được sử dụng để giảm kích thước thông điệp trước khi mật mã hóa Một thuật toán nén được sử dụng theo ISO 12042
ĐỘ DÀI CỦA DỮ LIỆU BỘ 8 BÍT SỐ THAM CHIẾU MÃ HÓA SỐ LƯỢNG BYTE ĐỆM	Kích thước của thân thông điệp đã được nén, đã được mã hóa và lọc Số tham chiếu là 1 Số lượng byte đệm là 4
Dữ liệu đã mã hóa	
Dữ liệu đã mã hóa	Thân thông điệp đã được nén, đã được mã hóa và đã được lọc
ĐUÔI MÃ HÓA	
ĐỘ DÀI CỦA DỮ LIỆU TRONG BỘ 8 BÍT SỐ THAM CHIẾU MÃ HÓA	Kích thước của thân thông điệp đã được nén, đã được mã hóa và đã được lọc. Số tham chiếu là 1
ĐUÔI AN NINH	
SỐ LƯỢNG ĐOẠN AN NINH	Có giá trị là 6. (USH, USA, USA, USD, USU, UST)
SỐ THAM CHIẾU AN NINH	Số tham chiếu của đuôi an ninh là 1

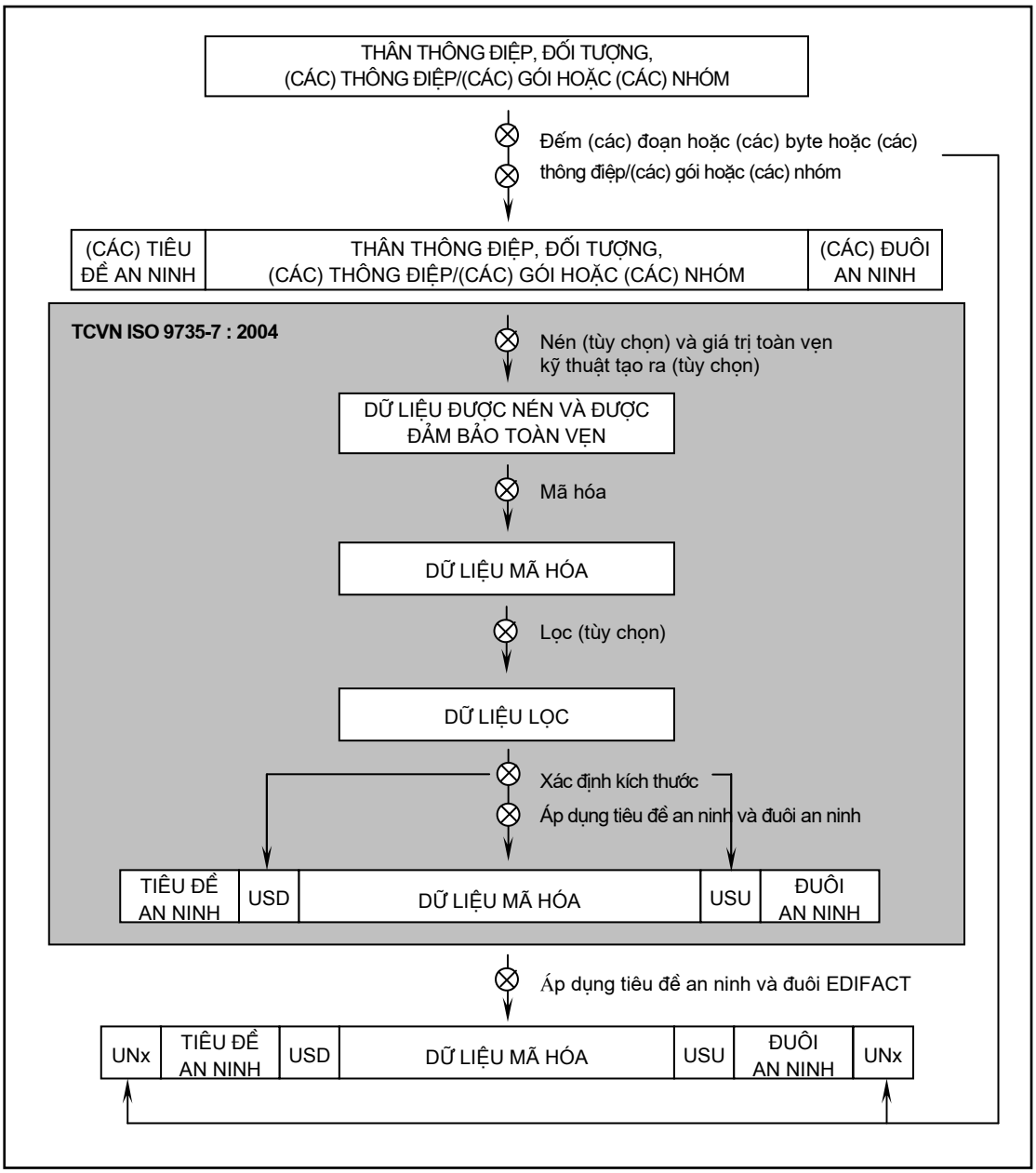
Phụ lục B

(tham khảo)

Ví dụ quá trình xử lý

B.1 Ví dụ mã hóa

Sơ đồ trong hình B.1 là một ví dụ về quá trình xử lý. Việc thực hiện có thể theo trình tự và thành phần liên quan khác nhau.

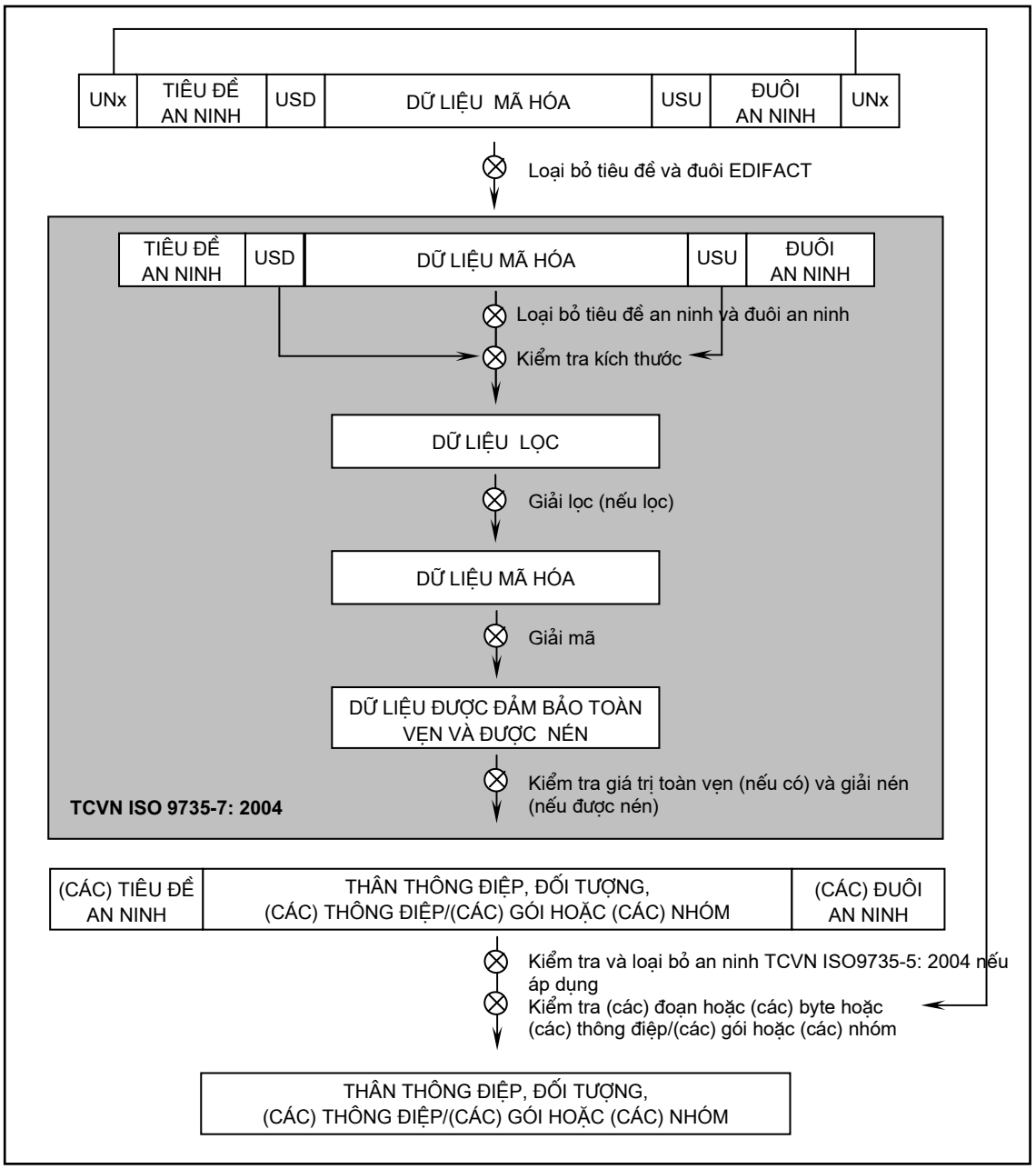


Hình B.1 - Quá trình liên quan đến mã hóa một cấu trúc EDIFACT

.

B.2 Ví dụ giải mã

Sơ đồ ở hình B.2 là một ví dụ về quá trình xử lý. Việc thực hiện có thể theo trình tự khác nhau và các thành phần liên quan khác nhau.



Hình B.2 - Quá trình liên quan đến giải mã một cấu trúc EDIFACT

Phụ lục C

(tham khảo)

Các thuật toán và dịch vụ về bảo mật

C.1 Mục đích và phạm vi áp dụng

Phụ lục này đưa ra các ví dụ về tổ hợp các phần tử dữ liệu và giá trị mã từ nhóm đoạn an ninh. Những ví dụ sau đây minh họa một số kỹ thuật an ninh được sử dụng rộng dãi, dựa trên các Tiêu chuẩn Quốc tế.

Để trình bày tất cả các tổ hợp có thể là quá rộng đối với phụ lục này. Sự lựa chọn ở đây không xem như một sự xác nhận về thuật toán hoặc các phương thức hoạt động. Người sử dụng chọn các kỹ thuật thích hợp để bảo vệ chống lại các với mối đe dọa an ninh.

Mục đích của phụ lục này là cung cấp cho người 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 người sử dụng.

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

0501 Dịch vụ an ninh, đã mã hóa

4	Độ tin cậy

0523 Thuật toán sử dụng, đã mã hóa

3	Ký nhận của Bên phát hành
4	Hàm băm của Bên phát hành
5	Mật mã hóa của bên sở hữu
8	Nén của bên sở hữu
9	Tính toàn vẹn và nén của bên sở hữu

0525 Phương thức hoạt động mã hoá, đã mã hóa

2	CBC (phương thức hoạt động DES)
16	DSMR (hệ thống chữ ký số cho khôi phục thông điệp)
36	CTS (chế độ hoạt động RC5)

0527 Thuật toán, đã mã hóa

1	DES (Tiêu chuẩn Mã hóa Dữ liệu)
4	IDEA (Thuật toán mật mã hóa Dữ liệu Quốc tế)
10	RSA
14	RIPEMD-160 (Hàm băm chuyên dụng #1)
18	ZLIB (Thuật toán nén dữ liệu)
25	CRC-32 (Kiểm tra dư thừa tuần hoàn)
27	ISO12042 (Nén dữ liệu)
29	RC5 (Mã hoá khối đối xứng kích thước khóa-biến đổi)

0531	*Hạn định tham số thuật toán*
5	Khóa đối xứng, được mã hóa dưới một khóa đối xứng
6	Khóa đối xứng, được mã hóa dưới một khóa công bố
9	Tên khóa đối xứng
10	Tên khóa mã hoá khoá
12	Các môđun
13	Số mũ
14	Độ dài các môđun

0563	*Hạn định giá trị hiệu lực*
1	Giá trị hiệu lực duy nhất

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

0591	*Cơ chế đệm,đã mã hóa*
1	Đệm số 0
2	Đệm PKCS #1
4	Đệm TBSS

Các chữ viết tắt được sử dụng

A123, 1, ABC99	=	Biểu diễn một Số Tham chiếu An ninh
CA	=	Tổ chức chứng nhận
CA - Sig	=	Chữ ký CA
Enc - Key	=	Khóa mã hóa
Exp	=	Số mũ chung
Key - N	=	Tên khóa
Len	=	Độ dài trong các bộ 8 bít của dữ liệu được (nén) được mã hóa (và được lọc)
Mod	=	Các môđun chung
Mod - L	=	Độ dài các môđun chung
PK/CA	=	Khóa công bố của Tổ chức chứng nhận.

C.2 Sử dụng kết hợp các thuật toán đối xứng và các đoạn an ninh tích hợp để có được bảo mật của cấu trúc EDIFACT

Ma trận trong bảng C.1 thiết lập các mối quan hệ trong trao đổi;

– tích hợp an ninh mức thông điệp/gói/nhóm trao đổi;

– sử dụng các thuật toán đối xứng để mật mã hoá;

– sử dụng các thuật toán đối xứng và không đối xứng cho trao đổi khóa;

– cung cấp dịch vụ an ninh bảo mật;

– tính bảo mật được cung cấp nhờ sử dụng các thuật toán DES, IDEA và RC5. Có ba ví dụ.

1. DES trong chế độ CBC cùng với một khóa bí mật được bên nhận biết. Khóa bí mật cần được mã hóa dưới một khóa - mã hóa - khóa dùng chung giữa bên gửi và bên nhận. Khóa - mã hóa- khóa này được tham chiếu bởi tên của nó. Không nén dữ liệu. Cơ chế đệm được sử dụng là đệm - Số 0 và yêu cầu thông tin bổ xung số lượng byte đệm.
2. RC5 trong chế độ CTS với một khóa bí mật được bên nhận biết. Khóa bí mật cần được mã hóa dưới một khóa - mã hóa - khóa dùng chung giữa bên gửi và bên nhận. Khóa - mã hóa - khóa này không được tham chiếu bởi tên của nó. Nén theo ISO 12042 trước khi mật mã hóa.
3. IDEA trong chế độ CBC. Khóa bí mật sử dụng cho mã hóa được trao đổi nhờ sử dụng khóa công bố của bên nhận. Khóa công bố được nhúng trong một chứng chỉ. Nén Z - lib và bảo vệ tính toàn vẹn theo CRC-32 trước khi mật mã hóa.

- Mặc dù bên gửi và bên nhận dùng chung khóa, các cơ chế mã hóa hoàn toàn không được thoả thuận trước. Bởi vậy tất cả các thuật toán và phương thức hoạt động sử dụng có tên chính xác;
- Chỉ các trường an ninh liên quan đến các kỹ thuật an ninh, các thuật toán và các phương thức hoạt động sử dụng thực tế được chỉ ra;
- Đoạn USC chứa sự xác định chính xác hàm băm và hàm chữ ký được Tổ chức Chứng nhận sử dụng để ký chứng chỉ. Khóa công bố của Tổ chức Chứng nhận, cần thiết để kiểm tra chữ ký chứng chỉ đã được bên nhận biết. Nó được tham chiếu bằng tên trong đoạn USC.

Bảng C.1 - Ma trận quan hệ

THẺ	Tên	S	R	Độ tin cậy ví dụ 1	Độ tin cậy ví dụ 2	Độ tin cậy ví dụ 3	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	4	4	4	
0534	SỐ THAM CHIẾU AN NINH	M	1	a123	1	ABC99	
S500	CHI TIẾT ĐỊNH DANH AN NINH	C	2	(Bên gửi)			
0577	Hạn định bên an ninh	M		1	1	1	
0511	Định danh bên an ninh	C		Id của bên gửi	Id của bên gửi	Id của bên gửi	
S500	CHI TIẾT ĐỊNH DANH AN NINH	C	2	(Bên nhận)			
0577	Hạn định bên an ninh	M		2	2	2	
0511	Định danh bên an ninh	C		Id của bên nhận	Id của bên nhận	Id của bên nhận	
USA	THUẬT TOÁN AN NINH	C	3	(Thuật toán mật mã hóa)			
S502	THUẬT TOÁN AN NINH	M	1				
0523	**Thuật toán sử dụng, đã mã hóa**	M		5	5	5	
0525	Phương thức hoạt động mã hoá, đã mã hóa	C		2	36	2	
0527	Thuật toán, đã mã hóa	C		1	29	4	
0591	Cơ chế đệm, đã mã hóa	C		1	2	4	2
S503	THAM SỐ THUẬT TOÁN	C	9	Một cho khóa mã hóa			
0531	Hạn định tham số thuật toán	M		5	5	6	
0554	Giá trị tham số thuật toán	M		khóa	khóa	khóa	
S503	THAM SỐ THUẬT TOÁN	C	9	Một cho tên khóa - mã hóa - khóa			
0531	Hạn định tham số thuật toán	M		10	10	-	
0554	**Giá trị tham số thuật toán**	M		Key - N	Key - N	-	
USA	THUẬT TOÁN AN NINH	C	3	(Thuật toán nén)			
S502	THUẬT TOÁN AN NINH	M	1				
0523	Thuật toán sử dụng, đã mã hóa	M		-	8	8	
0525	Phương thức hoạt động mã hoá, đã mã hóa	C		-	-	-	
0527	Thuật toán, đã mã hóa	C		-	27	18	

THẺ	Tên	S	R	Độ tin cậy ví dụ 1	Độ tin cậy ví dụ 2	Độ tin cậy ví dụ 3	Chú thích
USA	THUẬT TOÁN AN NINH	C	3	(Thuật toán nén toàn vẹn)			
S502	THUẬT TOÁN AN NINH	M	1				
0523	Thuật toán sử dụng, đã mã hóa	M		-	-	9	
0525	Phương thức hoạt động mã hoá, đã	C		-	-	-	
0527	Thuật toán, đã mã hóa	C		-	-	25	
SG 2		C	2	Chỉ một: chứng chỉ bên nhận			
USC	CHỨNG CHỈ	M	1				
S500	CHI TIẾT ĐỊNH DANH AN NINH	C	2	(Bên sở hữu chứng chỉ)			
0577	Hạn định bên an ninh	M		-	-	3	
0511	Định danh bên an ninh	C		-	-	Id của bên sở hữu	
S500	CHI TIẾT ĐỊNH DANH AN NINH	C	2	(Bên xác nhận)			
0577	Hạn định bên an ninh	M		-	-	4	
0538	Tên khóa	C		-	-	(Tên PK/CA)	
0511	Định danh bên an ninh	C		-	-	Id của CA	
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	Thuật toán sử dụng, đã mã hóa	M		-	-	4	
0525	**Mã hoá phương thức hoạt động, đã mã hóa**	C		-	-	-	
0527	Thuật toán, đã mã hóa	C		-	-	14	
USA	THUẬT TOÁN AN NINH	C	3	(Hàm chữ ký của CA cho chữ ký của chứng chỉ)			
S502	THUẬT TOÁN AN NINH	M	1				
0523	Thuật toán sử dụng, đã mã hóa	M		-	-	3	
0525	Phương thức hoạt động mã hoá, đã mã hóa	C		-	-	16	
0527	Thuật toán, đã mã hóa	C		-	-	10	
S503	THAM SỐ THUẬT TOÁN	C	9	(Các môđun khóa công bố CA)			
0531	Hạn định tham số thuật toán	M		-	-	12	
0554	Giá trị tham số thuật toán	M		-	-	Mod	

THẺ	Tên	S	R	Độ tin cậy ví dụ 1	Độ tin cậy ví dụ 2	Độ tin cậy ví dụ 3	Chú thích
S503	THAM SỐ THUẬT TOÁN	C	9	(Số mũ khoá công bố của CA)			
0531	Hạn định tham số thuật toán	M		-	-	13	
0554	Giá trị tham số thuật toán	M	-	-	Exp		
S503	THAM SỐ THUẬT TOÁN	C	9	(Độ dài các môđun khóa công bố của CA)			
0531	Hạn định tham số thuật toán	M		-	-	14	
0554	Giá trị tham số thuật toán	M		-	-	Mod - L	
USA	THUẬT TOÁN AN NINH	C	3	(Hàm mã hóa của bên sở hữu chứng chỉ)			
S502	THUẬT TOÁN AN NINH	M	1				
0523	Cách sử dụng thuật toán,đã mã hóa	M		-	-	5	
0525	Phương thức hoạt động mã hoá, đã mã hóa	C		-	-	-	
0527	Thuật toán, đã mã hóa	C		-	-	10	
S503	THAM SỐ THUẬT TOÁN	C	9	(Các môđun khóa công bố của bên sở hữu)			
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 khóa công bố của bên sở hữu)			
0531	Hạn định tham số thuật toán	M		-	-	13	
0554	Giá trị tham số thuật toán	M		-	-	Exp	
S503	THAM SỐ THUẬT TOÁN	C	9	(Độ dài các môđun khóa công bố của bên sở hữu)			
0531	Hạn định tham số thuật toán	M		-	-	14	
0554	Giá trị tham số thuật toán	M		-	-	Mod - L	
USR	KẾT QUẢ AN NINH	C	1				
S508	KẾT QUẢ HỢP LỆ	M	2				
0563	**Hạn định giá trị hiệu lực**	M		-	-	1	
0560	Giá trị hiệu lực	C		-	-	CA - Sig	
USD	TIÊU ĐỀ MÃ HÓA DỮ LIỆU	M	1				
0556	ĐỘ DÀI DỮ LIỆU THEO BỘ TÁM BÍT	M	1	Len	Len	Len	
0518	SỐ THAM CHIẾU MÃ HÓA	C	1	-	A	-	
582	SỐ LƯỢNG ĐỆM	C	1	3	-	-	3

THẺ	Tên	S	R	Độ tin cậy ví dụ 1	Độ tin cậy ví dụ 2	Độ tin cậy ví dụ 3	Chú thích
Cấu trúc dữ liệu được bảo vệ (thân thông điệp, đối tượng, (các) thông điệp/(các) gói)/các (nhóm))							
USU	ĐUÔI MÃ HÓA DỮ LIỆU	M	1				
0556	ĐỘ DÀI DỮ LIỆU THEO BỘ TÁM BÍT	M	1				
0518	SỐ THAM CHIẾU MÃ HÓA	C	1	-	A	-	
SG n		C	99	Một cho mỗi dịch vụ an ninh			1
UST	ĐUÔI AN NINH	M	1				
0534	SỐ THAM CHIẾU AN NINH	M	a	23	1	ABC 99	
0588	SỐ LƯỢNG ĐOẠN AN NINH	M	1	5	6	12	

CHÚ THÍCH

1. Cả hai cấu trúc phải có cùng số lần có xuất hiện;
2. Chỉ áp dụng cơ chế đệm cho đoạn USA quy định thuật toán mật mã hóa;
3. Số lượng các byte đệm được chọn như là ví dụ.