Chương trình KC-01:
Nghiên cứu khoa học phát triển công nghệ thông tin và truyền thông

Đề tài KC-01-01:
Nghiên cứu một số vấn đề bảo mật và an toàn thông tin cho các mạng dùng giao thức liên mạng máy tính IP

Báo cáo kết quả nghiên cứu

MÔ HÌNH BẢO MẬT THÔNG TIN CHO CÁC MẠNG MÁY TÍNH

Quyển 2B: "Tổng quan về thương mại điện tử và an toàn Internet"

HÀ NỘI-2002

Báo cáo kết quả nghiên cứu

MÔ HÌNH BẢO MẬT THÔNG TIN CHO CÁC MẠNG MÁY TÍNH

Quyển 2B: "Tổng quan về thương mại điện tử và an toàn Internet"

Chủ trì nhóm thực hiện:
TS. Lê Mỹ Tú và
TS. Đào Văn Giá

MỤC LỤC

CHƯƠNG 1. AN TOÀN INTERNET

Nhiều ứng dụng thương mại điện tử sử dụng Internet cho việc truyền thông của chúng. Không thể phủ nhận được, Internet với các chi phí thấp và tồn tại ở mọi nơi đã làm cho nhiều ứng dụng này trở nên khả thi. Đáng tiếc, các rủi ro khi sử dụng Internet có thể thể gây ra hiện tượng nản chí .

Phần này khai thác các tính năng của Internet như thế nào để tránh được các rủi ro không mong muốn. Chúng ta bắt đầu với một cuộc thảo luận về 3 mảng chính : An toàn mạng được chia thành - an toàn mạng, an toàn ứng dụng và an toàn hệ thống.

Sau đó trình bày một số giải pháp kỹ thuật an toàn cụ thể dành cho Internet, bao gồm an toàn giao thức tầng mạng, bức tường lửa, an toàn gửi tin, an toàn Web, EDI an toàn và giao thức thanh toán bằng thẻ tín dụng giao dịch điện tử an toàn (***Secure Electronic Transaction***- viết tắt ***SET***) .Trong phần này chúng ta trình bày một yếu tố quan trọng trong việc cung cấp tính an toàn cho người dùng Internet từ một hình phối cảnh hợp pháp - hợp đồng của nhà cung cấp dịch vụ Internet.

1. Phân loại vấn đề

An toàn Internet phụ thuộc vào các cung cấp an toàn trong 3 mảng : an toàn mạng, an toàn ứng dụng và an toàn hệ thống. Việc sử dụng các cung cấp an toàn này được kết hợp với các kiểu bảo vệ an toàn như an toàn cục bộ, an toàn cá nhân, an toàn phương tiện và như vậy thoả mãn được các đòi hỏi của một chính sách an toàn tổng thể.

a. An toàn mạng

Với an toàn mạng, chúng tôi muốn nói đến việc bảo vệ xử lý bằng các mục dữ liệu được truyền thông giữa các hệ thống cuối mạng. Đặc biệt, phần này loại ra bất kỳ những gì xảy ra trong các hệ thống cuối - cả các hệ thống client và server.

Nếu một hệ thống cuối (***end-system***) được kết nối trực tiếp với Internet, dữ liệu bất kỳ mà nó nhận được:

+ có thể bị sửa đổi trong quá trình chuyển tiếp.
+ có thể không phải từ dữ liệu nguồn.
+ có thể là một phần của tấn công chủ định chống lại hệ thống.

Do vậy, gói bất kỳ được gửi tới:

+ có thể không tới được nơi mà nó được đánh địa chỉ.
+ có thể bị sửa đổi trên lộ trình.
+ có thể bị những người vô danh hoặc các hệ thống đọc được.

Khi gặp tình trạng rắc rối, an toàn ứng dụng và an toàn hệ thống có xu hướng cho rằng hệ thống không hoàn toàn tin cậy. Các biện pháp có khả năng bảo vệ. An toàn mạng, nói cách khác, được trang bị nhằm nêu bật các đặc điểm an toàn vốn có của mạng, điều này có nghĩa là sự ít tin cậy được thay thế bằng các biện pháp bảo vệ trong các hệ thống cuối. Thỉnh thoảng, điều này có thể có lợi, đặc biệt với các hệ thống cuối không được kiểm soát chặt chẽ bởi những người tỉnh táo và có đủ trình độ về an toàn;ví dụ, máy tính để bàn trong môi trường ở nhà hoặc một công việc kinh doanh đặc trưng. Tính hấp dẫn của an toàn mạng là ở chỗ nó làm việc cho mọi ứng dụng.

Các dịch vụ an toàn mạng, hoặc các bảo vệ, có thể bao gồm:

 Authentication and integrity - Xác thực và toàn vẹn : cung cấp cho hệ thống nhận sự tin cậy về gói nguồn và đảm bảo rằng gói này không bị sửa đổi từ khi rời khỏi nguồn.

 Confidentiality - Sự tin cẩn : Bảo vệ các nội dung của một gói không bị lộ cho bất cứ ai ngoại trừ người được chỉ định nhận gói đó.

 Access control - Kiểm soát truy nhập : Hạn chế truyền thông với một hệ thống cuối riêng biệt, chỉ truyền thông với các ứng dụng riêng biệt hoặc các nguồn và đích của gói từ xa riêng biệt.

Việc cung cấp các dịch vụ xác thực, toàn vẹn, và tin cẩn được trình bày trong mục 2. Việc cung cấp các dịch vụ kiểm soát truy nhập được trình bày trong mục 3.

b. An toàn ứng dụng

An toàn ứng dụng có nghĩa là các bảo vệ an toàn được gắn vào trong một ứng dụng riêng biệt và tiến hành các biện pháp an toàn của một mạng bất kỳ một cách độc lập. Một số dịch vụ an toàn ứng dụng có thể lựa chọn (luân phiên) hoặc nhân đôi các dịch vụ an toàn mạng. Ví dụ, nếu một ***Web browser*** và một ***Web server*** mã hoá, tại tầng ứng dụng, tất cả các thông báo lưu chuyển giữa chúng, có thể thu được cùng một kết quả bằng cách mã hoá tại tầng mạng (IP). Tuy nhiên, nhiều ứng dụng có các đòi hỏi riêng về an toàn vì vậy không thể đáp ứng một cách đơn giản bằng các dịch vụ an toàn mạng.

Ví dụ, khi thực hiện thư tín điện tử (***e-mail***). Một thông báo *e-mail* có thể được truyền đi trên một loạt các phiên mạng khác nhau, được lưu trữ trên hàng loạt các hệ thống không được biết đến trong quá trình chuyển tiếp. An toàn mạng không thể cung cấp các bảo vệ chống lại việc xáo trộn thông báo mà có thể xảy ra tại một cổng e-mail, cổng này thực hiện chức năng lưu giữ và chuyển tiếp thư tín điện tử. Hơn nữa, chẳng có lý do gì để bắt buộc các hệ thống trung gian như vậy có được sự tin cậy trong an toàn - khi bạn tin tưởng vào tính toàn vẹn của các nhà cung cấp dịch

vụ của hệ thống, nhưng khó có thể nói trước được là các hệ thống của họ không bị một người nào đó bất kỳ thâm nhập vào. Hơn nữa, thư tín điện tử cần được bảo vệ trên cơ sở từng cá nhân- không trên cơ sở từng hệ thống. Khi một người gửi thư tín điện tử mã hoá một thông báo cho một người nhận riêng biệt, chỉ người nhận này có khả năng biết được nội dung của thông báo - không người sử dụng nào có thể chia xẻ sử dụng của một hệ thống với người nhận này. Vì vậy, thư tín điện tử đòi hỏi được bảo vệ tin cậy từ đầu này đến đầu kia (***end-to-end***) hoặc từ người viết đến người đọc (***writer to reader***), điều này không chỉ đơn giản là được các dịch vụ an toàn mạng cung cấp mà còn hơn thế nữa.

Các giao thức chi trả điện tử an toàn riêng biệt thậm chí còn có thể phức tạp hơn nhiều. Ví dụ, một thông báo chi trả từ người mua gửi tới cho nhà cung cấp, rồi tới nhà băng, các trường khác nhau trong thông báo bắt buộc phải được giữ bí mật để tôn trọng các thành viên khác. Một số trường có thể được mã hoá, do vậy nhà cung cấp không thể dịch được các nội dung nhưng khi nhà băng nhận được các trường chuyển tiếp, họ có thể dịch được. (Xem mục 6).

Tính phức tạp của các yêu cầu về an toàn trong các giao thức ứng dụng mới, cho thấy xu hướng sử dụng các biện pháp an toàn ứng được ưu tiên hơn các biện pháp an toàn mạng. Sau này, chúng vẫn có vị trí riêng, nhưng nói chung chúng không được áp dụng để phục vụ như là các biện pháp chính nhằm bảo vệ các ứng dụng thương mại điện tử.

Các biện pháp an toàn ứng dụng mở ra nhiều dịch vụ an toàn như : xác thực, kiểm soát truy nhập, tính tin cậy, toàn vẹn dữ liệu, không bác bỏ. Các biện pháp an toàn ứng dụng riêng biệt sẽ được thảo luận chi tiết hơn trong các mục sau chủ yếu về phần an toàn dịch vụ báo tin, an toàn Web , và an toàn dành cho các ứng dụng thương mại điện tử.

c. An toàn hệ thống

An toàn hệ thống quan tâm đến việc bảo vệ một hệ thống cuối riêng biệt và môi trường cục bộ của nó, không quan tâm đến bảo vệ truyền thông được tạo ra thông qua các biện pháp an toàn mạng và an toàn ứng dụng. An toàn hệ thống bao gồm các biện pháp như sau:

 Đảm bảo rằng không có các yếu điểm về an toàn trong các phần mềm được cài đặt. Một người phải đảm bảo rằng tất cả bổ xung phần mềm của nhà cung cấp liên quan đến an toàn phải được cài đặt nhanh chóng và không được cài đặt các phần mềm nghi ngờ có thể chứa virut hoặc con ngựa thành Tơroa.

 Đảm bảo rằng một hệ thống phải định cấu hình để giảm tối thiểu các rủi ro thâm nhập. Hệ thống phải được định cấu hình để theo dõi các gói của Internet trên các cổng được gán cho các ứng dụng, các ứng dụng này được sử dụng tích cực trên

hệ thống. Nói chung, các modem không được định cấu hình cho quay số vào (nếu có một yêu cầu quay số, thì ở đây phải là một phương tiện kiểm soát truy nhập mà xác thực toàn bộ những người gọi mới).

 Đảm bảo rằng một hệ thống được quản trị nhằm giảm tối thiểu các rủi ro thâm nhập. Việc lưu hành của tất cả các dữ liệu kiểm soát truy nhập phải được duy trì thường xuyên. Các mật khẩu phải được thay đổi thường xuyên và không sử dụng các mật khẩu dễ dàng đoán được. Các ***account*** của người dùng quá hạn phải được xoá đi, vì đối tượng thâm nhập trái phép để lấy dữ liệu bằng cách sử dụng một account hầu như khó có thể phát hiện được.

 Đảm bảo rằng các thủ tục kiểm tra thích hợp được tiến hành nhằm duy trì sự tin cậy, đảm bảo phát hiện các thâm nhập thành công và cài đặt các biện pháp mới một cách thích hợp.

Tóm lại, hầu hết các đe doạ hệ thống mà bị coi là các tấn công nguyên thuỷ xuất hiện trên Internet, có thể được ngăn chặn bằng cách tập trung sự chú ý đầy đủ vào an toàn hệ thống. Tất cả các nhà quản trị hệ thống Internet và những người sử dụng cần được đào tạo liên quan đến an toàn và cần nhận thức được sự phát triển có liên quan đến an toàn Internet.

Phần này không trình bày chi tiết hơn về an toàn hệ thống. Hoàn toàn tự nhiên, an toàn hệ thống phụ thuộc vào kiểu nền phần cứng đặc trưng và phần mềm hệ điều hành được sử dụng. Trong khuôn khổ của phần này, chúng ta đơn giản chỉ nhắc lại rằng an toàn hệ thống là một yếu tố chủ yếu trong việc đảm bảo an toàn thương mại điện tử. Không một ứng dụng thương mại điện tử nào được coi là an toàn nếu hệ thống mà nó chạy trên đó lại không an toàn.

2. An toàn giao thức mạng

Giao thức tầng mạng được sử dụng trên Internet là ***Internet Protocol*** (***IP - giao thức mạng***). IP định nghĩa một cách chuẩn để định dạng một tập các mục dữ liệu được gọi là các ***headers*** và gắn chúng vào gói dữ liệu sẽ được truyền đi, tạo ra một thứ được gọi là ***IP datagram***. *Header* thực hiện các nhiệm vụ như nhận dạng địa chỉ hệ thống nguồn và đích và số các cổng. IP là một giao thức không kết nối - mỗi gói dữ liệu được xử lý độc lập. Do sử dụng chuyển mạch gói Internet, nên thỉnh thoảng các gói có thể bị mất hoặc bị sắp xếp lại trong khi chuyển tiếp. Việc sửa chữa vấn đề này không phải là mối quan tâm của IP, nhưng nó là mối quan tâm của một giao thức tầng cao hơn, thường là ***Transmission Control Protocol*** (***TCP - Giao thức kiểm soát truyền***), nó có thể đổi chỗ các gói nhận được theo một thứ tự thích hợp và yêu cầu truyền lại các gói đã bị mất. Vai trò của IP rất đơn giản, nó lấy một gói dữ liệu từ hệ thống nguồn chuyển tới hệ thống đích.

IP vốn đã không an toàn. Ví dụ, bắt đầu vào năm 1994, nhiều hệ thống Internet là mục tiêu của một tấn công được biết đến như ***IP spoofing***. Tấn công này như sau : một kẻ tấn công tạo ra các gói có chứa một địa chỉ nguồn sai lệch. Một số ứng dụng, ví dụ như ứng dụng thiết bị đầu cuối từ xa ***X windows*** dành cho UNIX, phụ thuộc vào địa chỉ nguồn của IP như là một cơ sở để xác thực. Các tấn công chứng tỏ đã thành công khi cho phép những kẻ thâm nhập thực hiện các lệnh có đặc quyền (truy nhập gốc - ***root access***) trên nhiều hệ thống. Khi được phép thực hiện các lệnh này, kẻ tấn công có thể kiểm soát trọn vẹn một hệ thống và dữ liệu được lưu giữ trên đó.

Vào năm 1994, một dự án được giới thiệu bởi *Internet Engineering Task Force*, dự án này nhằm bổ xung thêm các đặc tính an toàn cho IP. Bạn có thể tưởng tượng được, đây đúng là một thách thức. Các vấn đề được đưa ra bao gồm :

 Các thành phần của một mạng đang tồn tại vẫn phải duy trì chức năng, mặc dù nhiều thành phần không bao giờ được nâng cấp các đặc tính an toàn.

 Đưa ra các giới hạn trong kỹ thuật mật mã, điều này có thể làm cho việc triển khai các giải pháp kỹ thuật hiệu quả trở nên khó khăn trên các phần của thế giới.

Điều này dẫn đến hai kỹ thuật an toàn IP - kỹ thuật ***Authentication Header*** và việc mã hoá gói hoặc kỹ thuật ***Encapsulating Security Payload***. Chúng ta tìm hiểu các đặc tính của các kỹ thuật này. Khi việc bảo vệ an toàn ở mức IP chỉ đóng một vai trò hạn chế trong bảo vệ thương mại điện tử, người đọc cần nhận thức được các rào cản bảo vệ, các rào cản này có thể được tạo ra bằng cách sử dụng các công cụ này.

a. Authentication Header

Authentication Header cung cấp các bảo vệ xác thực và toàn vẹn cho các ***IP datagram***, nó không cung cấp dịch vụ tin cậy. Sự vắng mặt của dịch vụ tin cậy được xem như là một đặc tính, nó làm cho việc phát triển *Authentication Header* trở nên thuận tiện hơn bằng cách ngừa hầu hết các kiểm soát trong nhập khẩu, xuất khẩu hoặc sử dụng mã hoá. Nếu tính tin cậy được yêu cầu tại mức IP, kỹ thuật mã hoá gói, được mô tả trong mục sau, phải được sử dụng kết hợp hoặc thay thế cho *Authentication Header*.

Kỹ thuật *Authentication Header* cho phép người nhận của một *IP datagram* có được tính tin cậy trong tính xác thực và toàn vẹn của nó. Không giống với một số phương pháp xác thực Internet trước đây, chúng phụ thuộc vào việc kiểm tra địa chỉ nguồn của IP (Nó dễ dàng bị làm giả , như các tấn công *IP spoofing*), kỹ thuật này phụ thuộc vào bằng chứng trong đó người khởi tạo sở hữu một khoá bí mật riêng.

Sinh ra một *Authentication Header* bao gồm các việc sau: tính toán một giá trị kiểm tra toàn vẹn (hoặc chữ ký số) trên các phần của IP datagram, những phần này thông thường không thay đổi như datagram di chuyển trên mạng. Điều này xác thực nguồn của datagram và xác nhận rằng nó không bị sửa đổi trong quá trình chuyển tiếp.

Các thuật toán khác nhau có thể được sử dụng trong tính giá trị kiểm tra toàn vẹn (***integrity check - value***). Một kiểu thuật toán thông dụng nhất là hàm băm bởi hiệu năng của nó khá cao, ví dụ như *MD5*.

Người khởi tạo và người sử dụng *Authentication Header* phối hợp chọn lựa và sử dụng các thuật toán và các khoá riêng bằng một kết hợp an toàn (***a security association***). Kết hợp an toàn là một bộ các tham số được hai hệ thống sử dụng trong việc bảo vệ dữ liệu được truyền đi giữa hai hệ thống. Với mục đích hỗ trợ kỹ thuật *Authentication Header* (một kết hợp an toàn cũng có thể hỗ trợ kỹ thuật bảo vệ), các tham số gồm có một bộ chỉ báo của thuật toán giá trị kiểm tra và các giá trị của khóa được sử dụng. Mỗi kết hợp an toàn có một nhận dạng, được gọi là một chỉ mục tham số an toàn (***Security Parameter Index***), đòi hỏi phải được sự đồng ý trước của các hệ thống. Nhận dạng có trong mọi *Authentication Header*. Các cách, trong đó kết hợp an toàn được thiết lập, được trình bày trong phần *Key Management*.

b. Mã hoá gói

Việc mã hoá tại mức IP gồm có kỹ thuật ***Encapsulating Security Payload (ESP)***- là một kỹ thuật độc lập với *Authentication Header*, nó được tạo ra nhằm cung cấp cho một *IP datagram* tính tin cậy, chẳng khác gì tính toàn vẹn.

Ở đây có hai chế độ mã hoá khác nhau như sau :

 Tunnel-mode encryption : Một *IP datagram* không có bảo vệ của một thực thể được mã hoá và kết quả này được chứa trong một *datagram* mới cùng với các ***IP header*** của bản rõ mà nó sở hữu. Thông tin địa chỉ có trong datagram cuối cùng có thể khác với thông tin địa chỉ có trong datagram không được bảo vệ, điều này làm cho việc xử lý thông qua các ***getway*** an toàn trở nên thuận tiện hơn.

 Transport- mode encrytion : Việc bảo vệ bằng mã hoá chỉ được áp dụng cho dữ liệu ở tầng cao hơn, dữ liệu này được IP vận chuyển (thông thường là một đơn vị dữ liệu của giao thức TCP), và không được áp dụng cho bất kỳ thông tin *IP header* nào.

Thuật toán mã hoá được sử dụng gọi là một ***transform*** (biến đổi). Nói chung, các *transform* khác nhau là các lựa chọn có hiệu lực. Tuy nhiên, về cơ bản, tất cả các thiết lập yêu cầu sử dụng một *transform* dựa vào thuật toán DES. Tất nhiên trong thực tế, một rào cản, mà bất cứ ai cũng mong muốn có được trong việc sử dụng các

quá trình mã hoá thuộc phạm vi hoạt động quốc tế, là các kiểm soát xuất khẩu (đôi khi là nhập khẩu), chúng được các chính phủ của mỗi quốc gia áp dụng.

Giống như kỹ thuật *Authentication Header*, việc mã hoá gói sử dụng một khái niệm kết hợp an toàn để xác định thuật toán, các khoá và các tham số khác. Một chỉ mục tham số an toàn (***A Security Parameter Index***) chỉ ra một kết hợp an toàn được thiết lập trước chứa trong ***Encapsulation Security Payload header***. Trường này trỏ tới thông tin cần thiết cho một hệ thống nhận để giải mã một phần datagram đã được mã hoá.

c. Quản lý khoá

Công nhận rằng, một hệ thống cuối Internet có thể hỗ trợ tốt hơn một người sử dụng. Định nghĩa hai phương pháp khoá thay thế nhau là : khoá hướng máy chủ (***host-oriented keying***) và khoá hướng người dùng (***user -oriented keying***). Với khoá hướng máy chủ, tất cả những người sử dụng trên một hệ thống máy chủ chia xẻ cùng một kết hợp an toàn, và vì vậy, có cùng một khoá khi truyền thông với một hệ thống cuối khác. Với khoá hướng người dùng, mỗi người sử dụng có thể có một hoặc nhiều kết hợp an toàn mà người dùng sở hữu và vì vậy, các khóa này được sử dụng trong quá trình truyền thông với bất kỳ một hệ thống cuối khác. Với khoá hướng máy chủ, tất nhiên là một người sử dụng có thể giải mã dữ liệu đã được mã hoá của người sử dụng khác, hoặc thậm trí có thể đóng giả (giả dạng) người sử dụng khác. Do vậy, khoá hướng người dùng là tốt hơn cả, đặc biệt nếu khi nhiều người sử dụng chia xẻ một hệ thống máy chủ có thể bị những người sử dụng khác nghi ngờ.

Không có chuẩn đơn lẻ nào đóng vai trò chủ đạo trong việc quản lý các khoá nhằm hỗ trợ cho các kỹ thuật an toàn IP. Một số các giải pháp khác cũng được đề xuất.

Một giải pháp là phân phối khoá thủ công, khi một người định cấu hình cho một hệ thống với khoá của nó và các khoá của các hệ thống khác, các hệ thống này mong đợi truyền thông an toàn. Trong thực tế chỉ dành cho các nhóm nhỏ và khép kín.

Với một giải pháp tổng thể hơn, nó thực sự cần thiết, để sử dụng các giao thức thiết lập khoá và xác thực trực tuyến. Các giao thức như vậy thường phụ thuộc vào việc sử dụng kỹ thuật khoá công khai để xác thực (ví dụ, việc sử dụng các chữ ký số RSA hoặc DSA) và để thiết lập khoá (ví dụ, việc sử dụng thoả thuận truyền tải khoá RSA hoặc khoá Diffie-Helman). *Internet Engineering Task Force* làm việc trên một chuẩn dành cho một giao thức như vậy.

Việc sử dụng bất kỳ một trong các hệ thống quản lý khoá này trên một phạm vi lớn là đòi hỏi tất yếu, tại mức khác, sử dụng cơ sở hạ tầng khoá công khai để phân phối an toàn các khoá công khai cho các hệ thống này. Internet Engineering Task

Force xây dựng một cơ sở hạ tầng khoá công khai vào trong *Internet Domain Name System (DNS)*. Điều này cho phép các khoá công khai xác thực được lưu giữ trong các máy chủ trực tuyến DNS và có thể đáp ứng nhiều đòi hỏi của an toàn tầng mạng và cả an toàn của DNS.

3. Các bức tường lửa

Trong một toà nhà, ***firewall*** (bức tường lửa) bảo vệ chống lại một tình trạng nguy hiểm trong một phần của toà nhà mà có thể lan rộng ra các phần khác. Trong một mạng máy tính, bức tường lửa bảo vệ một phần của mạng khỏi bị nguy hiểm do các nguy hiểm này có thể xuất hiện (thậm chí có thể lan rộng mà không kiểm soát được) vào các phần khác của mạng. Thông thường, một bức tường lửa được xây dựng giữa mạng nội bộ của một tổ chức và xương sống của Internet, thận trọng với các nguy hiểm có thể xảy ra, ví dụ do những kẻ thâm nhập trái phép để lấy tin hoặc người nghe trộm gây ra.

Các bức tường lửa của mạng có thể mang lại các hình thức vật lý khác nhau và cung cấp các chức năng khác nhau. Mục đích chính của chúng là thiết lập một chính sách an toàn cho một tổ chức. Các chính sách an toàn của mỗi tổ chức khác nhau. Các chức năng được bức tường lửa cung cấp bao gồm :

 Hạn chế một tập hợp các ứng dụng mà lưu lượng của nó có thể nhập vào mạng nội bộ từ Internet, và hạn chế các địa chỉ nội bộ mà thông qua đó lưu lượng dành cho các ứng dụng khác nhau có thể đến. Đặc biệt, chỉ thông tin đến được phép tới một hệ thống, nó được trang bị đặc biệt nhằm đối phó với các đe doạ có thể xảy ra. Ví dụ, chỉ có các yêu cầu của ***incoming file transfer (FTP)*** hoặc ***Web HTTP*** được phép đi qua để tới một máy chủ nội bộ, máy này có các các kiểm soát kỹ thuật và quản trị hỗ trợ cho truy nhập bên ngoài. Tuy nhiên, những yêu cầu như vậy sẽ không được phép tới bất kỳ địa chỉ mạng nội bộ nào khác.

 Xác thực nguồn gốc của một số kiểu thông tin đến. Ví dụ, tất cả những người sử dụng bên ngoài cố gắng truy nhập vào một hệ thống mạng nội bộ bất kỳ thông qua giao thức TELNET có thể được phép vào khi họ xác nhận sử dụng thẻ bài cá nhân và được cung cấp, bức tường lửa xác nhận họ là người đã được uỷ quyền.

 Hạn chế khả năng của các hệ thống mạng nội bộ để thiết lập các kết nối cho Internet bên ngoài, dựa vào ứng dụng được sử dụng và thông tin có liên quan khác.

 Hoạt động như là một ***security gateway*** (cổng an toàn), mã hoá và/hoặc kiểm tra tính toàn vẹn của tất cả các thông tin trên xương sống của Internet, đến hoặc đi từ cổng an toàn khác. Thỉnh thoảng , một cấu hình như vậy được gọi là một ***virtual private network*** (mạng riêng ảo).

a.Xây dựng bức tường lửa

Việc xây dựng một bức tường lửa nói chung đòi hỏi phải kết hợp nhiều yếu tố sau : quyết định chính sách, lên kế hoạch về kỹ thuật, mua sản phẩm hoặc định cấu hình, và chế tạo theo yêu cầu khách hàng. Hiện nay có hàng loạt các sản phẩm bức tường lửa thương mại có thể đáp ứng được nhu cầu của nhiều tổ chức. Tuy nhiên, không phải tất cả các yêu cầu của mọi tổ chức có thể được thỏa mãn bằng các giải pháp có sẵn. Các yếu tố trong một giải pháp bức tường lửa có thể bao gồm:

 Screening routers : Một router ngăn chặn có chọn lựa các gói, thông thường, khi định tuyến chúng từ mạng này sang mạng khác. Một *screening router* sử dụng một tập hợp các quy tắc được thiết lập trước, các quy tắc này định nghĩa các kiểu của gói có thể được đi qua (ví dụ, các gói đến hoặc đi từ một địa chỉ IP riêng biệt và cổng). Quá trình này được biết đến như là ***packet filtering*** (lọc gói).

 Proxy servers : ứng dụng là các chương trình phục vụ cụ thể, chúng thực hiện các yêu cầu của người sử dụng về các dịch vụ Internet, ví dụ như Web HTTP hoặc FTP, và chúng chuyển các yêu cầu này (chúng thích hợp với chính sách an toàn cục bộ) cho các máy chủ hiện tại bên ngoài. Một ***proxy server*** (máy chủ uỷ quyền) về cơ bản là trong suốt đối với cả client mạng cục bộ và máy chủ Internet bên ngoài. Thay vào việc phải truyền thông trực tiếp với mỗi hệ thống khác, cả hai hệ thống trong thực tế truyền thông với một máy chủ uỷ quyền. Lưu ý rằng, phần mềm máy khách phải nhận thức được cấu hình uỷ quyền này, vì vậy nó sẽ gửi một lần nữa các yêu cầu uỷ quyền hơn là cố gắng truyền thông trực tiếp với một máy chủ bên ngoài.

 Perimeter network : Một mạng mới được cài vào giữa hai mạng, mạng ngoài và mạng nội bộ. Thậm trí nếu một hệ thống máy chủ trên *perimeter network* (mạng vành đai) bị một kẻ thâm nhập trái phép thoả hiệp (hệ thống máy chủ này nói chung sẽ là một phần của cấu hình bức tường lửa), nó không đưa ra truy nhập vào mạng nội bộ một cách trực tiếp, ví dụ, nó sẽ không cho phép kẻ thâm nhập trái phép giám sát các gói giữa hai hệ thống nội bộ trên một mạng nội bộ.

b.Các mạng riêng ảo

Mục đích của một mạng riêng ảo (***virtual private network***) là có được một tập hợp các ***site*** của mạng, từ đó có thể truyền thông an toàn với mỗi mạng khác, sử dụng xương sống Internet để đáp ứng các nhu cầu truyền thông cơ bản, và đảm bảo rằng thông tin trên mạng riêng không dễ dàng bị tấn công bởi các tấn công bên ngoài. Bức tường lửa có thể cung cấp một khả năng như vậy.

Một cách có được các mạng ảo riêng, trên cơ sở độc lập của một ứng dụng, là sử dụng các ***IP tunnel*** đã được mã hoá. Một hệ thống bức tường lửa tại một *site* - mã hoá tất cả các thông tin dành cho *site* khác mà sử dụng mã hoá gói chế độ *tunnel*. Một hệ thống bức tường lửa tại *site* nhận - giải mã thông tin và định tuyến nó trên mạng nội bộ tại *site* này tới đích cuối cùng.

Các mạng riêng ảo cụ thể có thể được xây dựng bằng nhiều cách, như định cấu hình truyền thông thích hợp cho một hệ thống ở mức ứng dụng, nó cung cấp các dịch vụ mã hoá và an toàn cần thiết tại mức ứng dụng.

4. An toàn dịch vụ gửi tin

Các ứng dụng gửi tin, bao gồm các ứng dụng thư tín điện tử (***e-mail***) và các ứng dụng cho phép gửi thư tín (***mail-enable***) có thể đáp ứng được các yêu cầu về an toàn mà riêng các biện pháp an toàn mạng không thể đáp ứng được. Gửi tin an toàn đòi hỏi sự bảo vệ từ người viết đến người đọc trong một môi trường trong đó các thông báo có thể vượt qua nhiều kết nối mạng và được lưu giữ và chuyển tiếp qua nhiều hệ thống cổng mức ứng dụng không được biết đến. Hơn nữa, các thông báo này có thể được các hệ thống cuối xét duyệt và nhận, các hệ thống này hỗ trợ nhiều người dùng khác nhau.

Trước khi thảo luận về an toàn gửi tin, chúng ta đưa ra một số các từ vựng phổ biến dành cho các hệ thống gửi tin. Các thông báo được tạo ra và được nhận bởi các ***User*** (người dùng), nó có thể là con người hoặc các chương trình ứng dụng cho phép gửi tin. Một thông báo có một ***originator*** (người khởi tạo) và một hoặc nhiều ***recipient*** (người nhận). Một người dùng được phần mềm hỗ trợ được gọi là ***user agent*** (tác nhân người dùng), nó thực hiện các nhiệm vụ như chuẩn bị, xem xét các thông báo, nhận và tiền xử lý các thông báo nhận được cho người dùng. Một *user agent* có thể là một ứng dụng phần mềm độc lập (đôi khi còn được gọi là một ***mailer***), hoặc nó có thể được tích hợp vào nhiều ứng dụng khác như là Web browser. Xương sống chuyển thông báo gồm có nhiều hệ thống được gọi là các ***message transfer agent*** (tác nhân chuyển thông báo, viết tắt MTA). Một thông báo được đưa ra để xem xét tại một ***originating MTA*** và sau đó được chuyển tiếp dọc theo đường dẫn bất kỳ của MTAs tới một ***delivering MTA***, nó phân phối thông báo cho *user agent* của một người nhận. Các MTA có thể là các chuyển mạch thông báo lưu giữ và chuyển tiếp của một kỹ thuật gửi tin cho trước, hoặc chúng có thể là các cổng thư tín giữa các kỹ thuật khác nhau. Khi một thông báo có nhiều người nhận, nội dung của thông báo có thể được sao chép và gửi đi theo nhiều đường dẫn tại hàng loạt các điểm khi vượt qua mạng.

Trong phạm vi của phần này, chúng ta sẽ chia chúng thành hai loại - các dịch vụ cơ bản và các dịch vụ tăng cường.

Các dịch vụ bảo vệ thông báo cơ bản là các biện pháp bảo vệ áp dụng cho một thông báo đơn lẻ như là một đối tượng dữ liệu đơn lẻ. Nói chung, chúng độc lập với các kỹ thuật xem xét, chuyển tiếp, và phân phối dữ liệu, và chúng có thể được thiết lập toàn bộ trong các *user agent*. Các dịch vụ bảo vệ thông báo cơ bản bao gồm :

 Message origin authentication : Xác thực nguồn gốc của thông báo - Đảm bảo với người nhận rằng một thông báo đến từ người khởi tạo. Ví dụ, bộ phận nhận đơn đặt hàng của Tập đoàn thép Sharon nhận được một thông báo về yêu cầu thép của Danielle's Machine Markers, nhân viên của bộ phận này muốn đảm bảo chắc chắn rằng thông báo không phải do một kẻ thâm nhập trái phép tạo ra. Điều này không khó gì đối với một kẻ tấn công, bằng cách khởi tạo trường ***From*** của thông báo bằng một giá trị mong muốn. Dịch vụ xác thực nguồn gốc thông báo xác nhận người khởi tạo trên cơ sở xử lý một khoá mật mã riêng.

 Content integrity : Toàn vẹn nội dung - Bảo vệ các nội dung của thông báo, chống lại việc sửa đổi giữa người khởi tạo và người nhận, và việc sửa đổi này do một người thâm nhập trái phép gây ra. Dịch vụ an toàn này gắn liền với xác thực nguồn gốc của thông báo.

 Content confidentiality : Sự tin cậy của nội dung - Bảo vệ các nội dung của thông báo, chống lại việc bị lộ bởi những kẻ nghe trộm. Sharon và Danielle điều khiển tất cả các công việc kinh doanh của họ bằng các thoả thuận bí mật và cần kỹ thuật để hỗ trợ cho các thoả thuận này.

 Non-repudiation of origin : Chống chối bỏ nguồn gốc - Cung cấp cho người nhận các bằng chứng về nguồn gốc của một thông báo và các nội dung của nó. Khi Nola's E-Market nhận được một yêu cầu từ một khách hàng chưa từng nghe thấy trước đó và yêu cầu vận chuyển các hàng hoá rất đắt, Nola muốn có được sự đảm bảo rằng khách hàng sau đó sẽ không chối bỏ yêu cầu đã đặt trước và phản đối chi trả. (Nola dành một phòng nhỏ để xử lý các yêu cầu trả lại hoặc các vấn đề tranh chấp, vì vậy cô mong muốn có nhiều bằng cớ đủ sức thuyết phục ngay lập tức đối với bất cứ ai có yêu cầu đã đặt trước).

Các dịch vụ bảo vệ thông báo tăng cường tiến hành đơn giản hơn nhiều, nó bảo vệ một thông báo đơn lẻ như là một đối tượng đơn lẻ. Các dịch vụ xác nhận (***confirmation service***) cung cấp các thông báo ngược trở lại cho người khởi tạo thông báo, rằng thông báo đã được phân phối cho một người nhận hoặc, ít nhất, thông báo đã đến một điểm nào đó trên đường dẫn của nó. Các dịch vụ xác nhận có thể khác với giao thức an toàn gửi tin riêng biệt đã sử dụng nhưng có thể bao gồm như sau, ví dụ :

 Proof of delivery : Chứng minh sự chuyển giao - Cung cấp cho người gửi thông báo sự đảm bảo rằng: thông báo đã được chuyển giao cho một người nhận có chủ định mà không bị sửa đổi trong quá trình chuyển tiếp.

 Proof of submission : Chứng minh sự xem xét - Cung cấp cho người gửi thông báo sự đảm bảo rằng: thông báo đã được ***originating MTA*** chấp thuận chuyển tiếp cho người nhận (hoặc nhiều người nhận) theo yêu cầu. Các dịch vụ này hữu ích nhất khi *user agent* của người khởi tạo thuộc về một tổ chức tách ra từ một *user*

agent của originating MTA; ví dụ, một *user agent* riêng lẻ kết nối với một nhà cung cấp dịch vụ thư tín công cộng.

 Non-repudiation of delivery : Chống chối bỏ sự chuyển giao - Cung cấp cho người gửi thông báo các chứng cớ thuyết phục, cho thấy thông báo đã được chuyển giao cho một người nhận có chủ định mà không bị sửa đổi trong quá trình chuyển tiếp.

 Non-repudiation of submission: Chống chối bỏ sự xem xét - Cung cấp cho người gửi thông báo các chứng cớ thuyết phục, cho thấy thông báo đã được originating MTA chấp nhận chuyển tiếp cho một người nhận (hoặc nhiều người nhận) đã yêu cầu.

Các dịch vụ an toàn tăng cường khác có thể được các giao thức an toàn gửi tin riêng biệt cung cấp, nhằm đáp ứng các nhu cầu riêng của các môi trường trong đó chúng được sử dụng. Ví dụ, các giao thức được thiết kế để sử dụng trong các môi trường quân sự có thể bao gồm một dịch vụ dán nhãn an toàn, tiến hành dán một nhãn an toàn vào một thông báo để chỉ ra sự phân loại an toàn của thông báo/ hoặc thông tin khác về điều khiển cấp phép.

Hàng loạt các giao thức an toàn gửi tin được định nghĩa và được sử dụng kết hợp với thư tín Internet hoặc các dịch vụ gửi tin điện tử khác, ghép nối với thư tín Internet thông qua các cổng (getway). Trong thực tế, sự tồn tại của nhiều giao thức là một vấn đề, bởi vì các giao thức không cùng phối hợp hoạt động. Điều này gây khó khăn cho người sử dụng khi mua các sản phẩm được hỗ trợ trao đổi thông báo an toàn với tất cả những người sử dụng khác mà họ kết nối truyền thông. Trong các mục tiếp theo, chúng ta đưa ra các đặc điểm chính của các giao thức gửi tin an toàn được biết đến một cách rộng rãi.

a. *Privacy Enhanced Mail (PEM)*

Privacy Enhanced Mail (PEM) là kết quả của sự kết hợp giữa *Internet Engineering Task Force* và *Internet Research Task Force*, đưa ra vào cuối những năm 1980. Đây là một trong những nỗ lực đầu tiên nhằm thực hiện an toàn thư tín trên Internet. PEM đưa ra 4 phần *Proposed Internet Standards* vào năm 1993. Các đặc tính của PEM rất rõ ràng. Đặc biệt, phần I (RFC 1421) định nghĩa giao thức gửi tin an toàn và phần II (RFC 1422) định nghĩa một cơ sở hạ tầng khoá công khai hỗ trợ.

Từ một tập hợp các dịch vụ an toàn được đưa ra trong các mục trước đó, giao thức gửi tin an toàn PEM được thiết kế nhằm hỗ trợ riêng cho các dịch vụ bảo vệ thông báo cơ bản. PEM hoạt động như sau: nó lấy một thông báo không được bảo vệ và dồn toàn bộ nội dung của thông báo này vào một thông báo PEM - sau đó, các thông báo PEM này được chuyển tiếp trên lộ trình gửi tin thông thường giống như

các thông báo khác. Vì vậy, PEM có thể được thiết lập một cách đơn giản là: chỉ cần nâng cấp các *user agent* có yêu cầu các chức năng an toàn mới.

Đặc tính của PEM chấp nhận hai giải pháp thay thế nhau cho mạng là xác thực và quản lý khoá - một tuỳ chọn đối xứng (***a symmetric alternative***) và một tuỳ chọn khoá công khai (***a public-key alternative***). Tuy nhiên, chỉ có tuỳ chọn khoá công khai được thực thi.

PEM tiếp tục một bước ngoặt quan trọng việc phát triển các giao thức gửi tin an toàn, cũng vẫn quan tâm đến thiết kế kỹ thuật vững chắc. Tuy nhiên, PEM chưa bao giờ được công nhận là thành công trong các giới hạn về phát triển thương mại. Một trong các lý do chính cho việc không được chấp nhận là không tương hợp với MIME - dạng thư tín đa phương tiện Internet được phát triển trong cùng thời gian này.

b. MIME Security Multiparts và các dịch vụ an toàn đối tượng

Một thông báo Internet gồm có một tập hợp các *header* và thân của một thông báo (*a message body*). ***Multipurpose Internet Mail Extensions (MIME)*** là một tập hợp các đặc tính hỗ trợ cho việc hình thành cấu trúc thân của một thông báo - theo các giới hạn của các phần thân. Các phần thân có hàng loạt các kiểu khác nhau, ví dụ như văn bản, ảnh, audio, hoặc các thông báo được gói hoàn chỉnh. Một thông báo hoặc phần thân có một kiểu nội dung (***content type***) - nó định nghĩa kiến trúc và kiểu của thông báo.

Sau khi công bố các đặc tính của PEM vào năm 1993, *Internet Engineering Task Force* tiếp tục nghiên cứu phát triển PEM - như các dịch vụ an toàn được sử dụng kết hợp với các thông báo đã được định dạng của MIME. Công việc này được hoàn thành vào năm 1995, cho ra đời hai đặc tính riêng biệt, nó giải quyết hai phần khác nhau của vấn đề an toàn MIME :

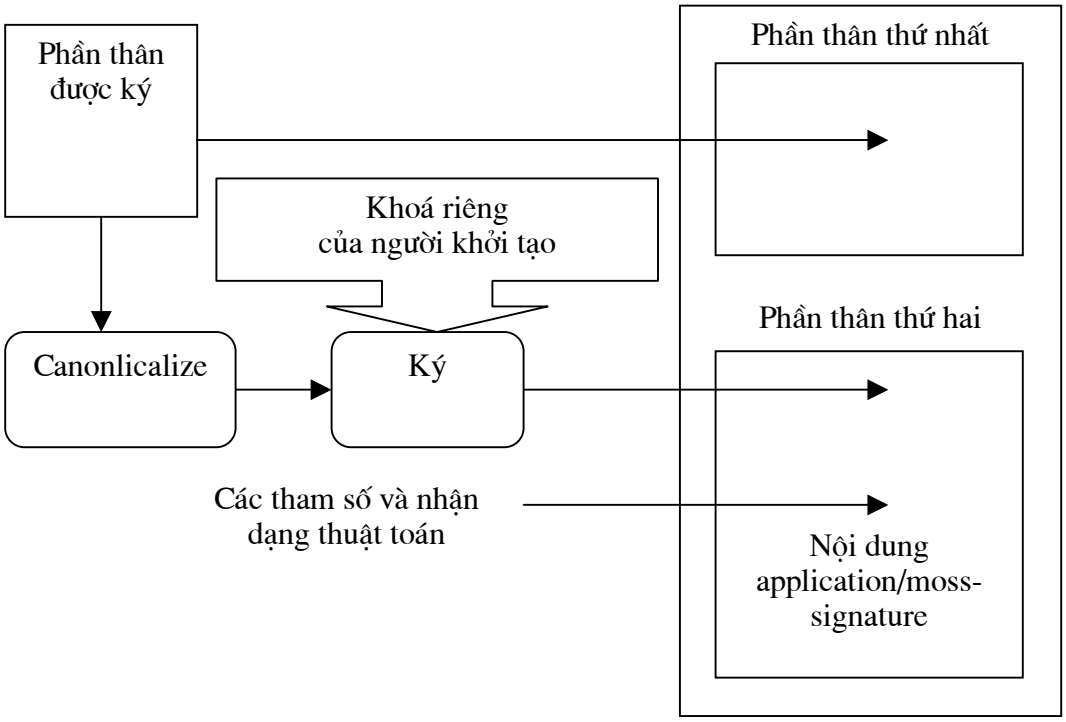
 Security Multiparts for MIME : Đặc tính này định nghĩa hai khung cấu trúc thông báo (kiểu nội dung MIME), nó hỗ trợ chữ ký số và việc mã hoá một thông báo hoặc một phần của thông báo. Hai kiểu nội dung này, được gọi là ***multipart/signed*** và ***multipart/encrypted***, chúng là các kiểu phụ của một kiểu nội dung MIME được gọi là ***multipart***, nó được sử dụng để cấu trúc các thông báo gồm có nhiều phần thân.

 MIME Object Security Services (MOSS): Đặc tính này định nghĩa một tập hợp các thủ tục và khuôn dạng dành cho việc tạo chữ ký số và mã hoá các phần thân MIME, được sử dụng kết hợp với các kiểu nội dung kiến trúc được định nghĩa trong *Security Multiparts for MIME*.

Việc sử dụng kết hợp các đặc tính này với nhau có thể cung cấp cùng một nhóm các dịch vụ an toàn như PEM, là các dịch vụ bảo vệ thông báo cơ bản.

Kiểu nội dung *multipart/signed* định nghĩa một cấu trúc gồm có hai phần thân. Phần thân thứ nhất có thể chứa một nội dung MIME bất kỳ, như một đoạn văn bản, sound clip, hoặc kiểu được kiến trúc (biến thể nào đó của multipart). Chữ ký số được tính toán trên phần thân đầu tiên, gồm có các *MIME header* của nó. Phần thân thứ hai chứa chữ ký số và bất kỳ thông tin điều khiển nào mà một *user agent* của người nhận cần đến để xác nhận chữ ký. Đặc tính MOSS định nghĩa một kiểu nội dung MIME được gọi là ***application/moss-signature***, nó có thể được sử dụng trong phần thân thứ hai của *multipart/signed*.

Đặc tính MOSS cũng mô tả một thủ tục dành cho việc sinh một thông báo được đánh dấu sử dụng *multipart/signed* và *application/moss-signature* . Thủ tục này được minh hoạ trong hình 1.1.



Hình 1.1. Tạo chữ ký số MOSS

Bước đầu tiên là ***canonicalize*** thông báo, hoặc biến đổi nội dung thông báo thành một ***canonical form*** (dạng thức hợp quy). Bước này rất cần thiết vì môi trường gửi tin của Internet được xây dựng dựa vào một hệ thống truyền *text-based* (dựa vào văn bản), nó được thiết kế để chuyển các thông báo mã ký tự, hơn là một hệ thống truyền ***binary*** (nhị phân) - hệ thống này có thể chuyển bất kỳ mục dữ liệu nào được mã hoá

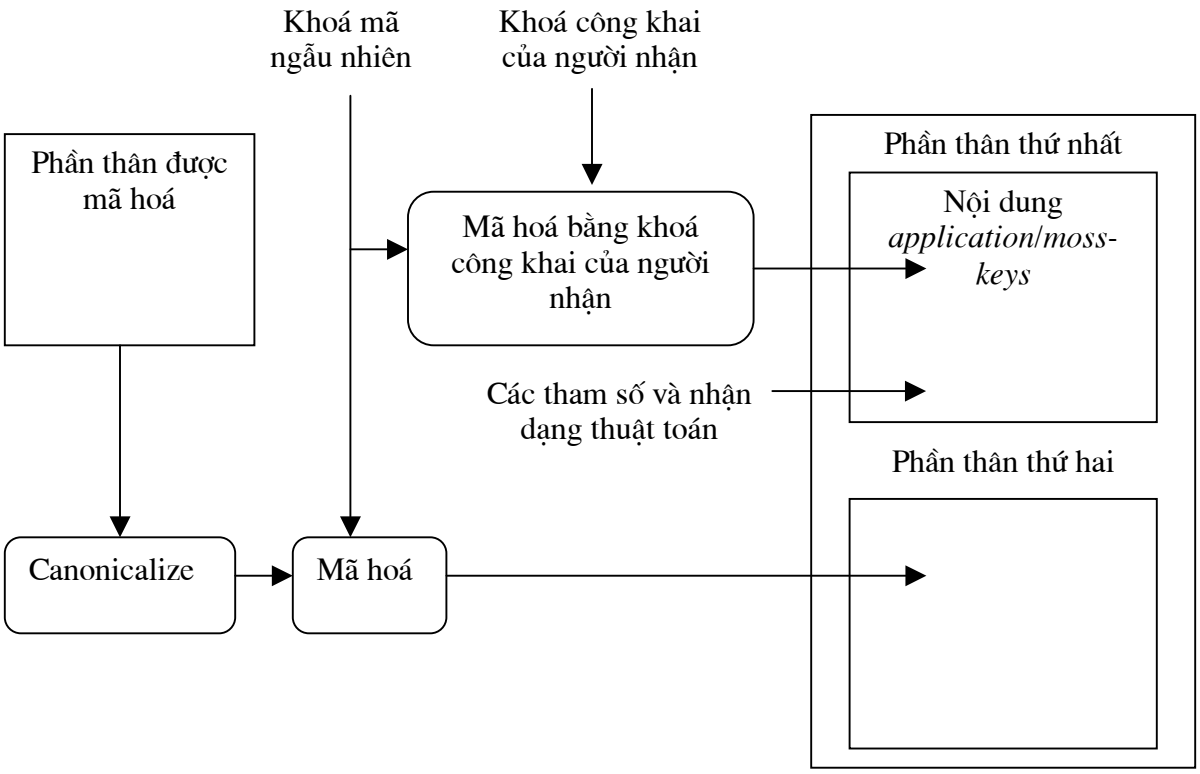
như một chuỗi các bit. Thông thường, trong quá trình thông báo đi theo đường dẫn của nó từ người khởi tạo đến người nhận, việc biểu diễn văn bản của thông báo có thể thay đổi. Các hệ thống khác nhau sử dụng các lược đồ mã ký tự khác nhau. Tương tự, các hệ thống khác nhau sử dụng các quy ước khác nhau để biểu diễn kết thúc của một dòng văn bản, ví dụ, ký tự CR (phím xuống dòng), ký tự LF (tín hiệu xuống dòng). Một thông báo có thể được chuyển đổi để sử dụng các mã ký tự khác nhau và /hoặc một quy ước ký tự kết thúc khác nhau. Khi các quy ước này không thay làm đổi nghĩa của một thông báo, chúng gây ra một rủi ro là : một chữ ký số hợp lệ không được xác nhận nghiêm chỉnh. Để ngăn ngừa những vấn đề như vậy, điều mà tất cả các hệ thống cần phải làm là tính toán các chữ ký số trên biểu diễn thông báo dựa vào thoả thuận (*agreed -upon representation of a message*), sử dụng một mã ký tự dựa vào thoả thuận và một quy ước ký tự kết thúc dựa vào thoả thuận.

Việc biểu diễn chuẩn một thông báo được gọi là dạng thức hợp quy của một thông báo.

Việc biểu diễn hợp quy một thông báo được xử lý thông qua một hàm băm và tạo chữ ký số. Chữ ký số và thông tin điều khiển hỗ trợ được xây dựng trong phần thân mới, nó có kiểu nội dung *application*/*moss-signature* . Phần thân này bao gồm một chữ ký và các ký hiệu nhận dạng của hàm băm riêng biệt và thuật toán chữ ký đã sử dụng. Sau đó, nội dung *multipart*/*signed* được cấu thành, hợp nhất cả hai phần: phần thân gốc (nguyên bản) được đánh dấu và phần thân *application*/*moss-signature*.

Việc mã hoá thực hiện một quá trình khác và sử dụng các kiểu MIME khác. Kiểu *multipart*/*encrypted* định nghĩa một cấu trúc gồm có hai phần thân. Trong trường hợp này, phần thân thứ hai chứa một phiên bản đã được mã hoá của phần thân MIME khác (ví dụ, văn bản, một sound clip, hoặc một cấu trúc đa thành phần). Phần thân thứ nhất chứa thông tin điều khiển cần thiết để giải mã phần thân thứ hai, ví dụ, các ký hiệu nhận dạng của thuật toán mã hoá và thông tin trên khoá được sử dụng. Đặc tính của MIME định nghĩa một kiểu nội dung MIME, *application*/*moss-keys* , được sử dụng trong phần thân thứ nhất của *multipart*/*encrypted*.

Đặc tính MOSS cũng mô tả một thủ tục dành cho việc sinh một thông báo được mã hoá bằng cách sử dụng *multipart*/*encrypted* và *application*/*moss-keys* . Thủ tục này được trình bày trong hình 1.2.



Hình 1.2. Quá trình mã hoá MOSS

Quá trình này được tiến hành như sau :

 Bước 1: Phần thân đã được mã hoá có thể được chuyển đổi thành một dạng thức hợp quy MIME, tất cả các hệ thống đều có thể xử lý nó được.

 Bước 2: Một khoá mã dữ liệu ngẫu nhiên mới cho mỗi người nhận. Các bản sao được mã hoá của khoá mã dữ liệu và thông tin điều khiển hỗ trợ được đưa vào trong một phần thân mới của kiểu *application/moss-keys* .

 Bước 3: Phần thân từ bước 1 được mã hoá với thuật toán mã đối xứng.

 Bước 4: Nội dung *multipart/encrypted* được hình thành, gồm có phần thân *application/moss-keys* và phần thân đã được mã hoá từ bước 3.

Phần thân *application/moss-keys* gồm có các bản sao đã được mã hoá của khoá mã dữ liệu dành cho mọi người nhận, và một ký hiệu nhận dạng thuật toán mã hoá riêng đã được sử dụng.

Không giống với PEM, đặc tính MOSS không định rõ một cách thức chuẩn - cho việc nhận dạng những người nắm giữ các cặp khoá công khai hoặc cho việc quản lý các cặp khoá này. Tuy nhiên, MOSS định nghĩa các kiểu nội dung MIME - dành cho việc chuyển tải một yêu cầu về thông tin khoá công khai từ một thành viên từ xa và dành cho việc chuyển tải thông tin khoá công khai, bao gồm các chứng chỉ khoá công khai, giữa hai thành viên. Các kiểu nội dung này có thể được sử dụng như các công cụ cho việc xây dựng một hệ thống quản lý khoá đặc trưng đầy đủ.

c. S/MIME

Song song với việc phát triển các đặc tính MOSS của Internet Engineering Task Force, một nhóm cá nhân dẫn đầu là RSA Data Sercurity, Inc đã phát triển đặc tính khác dành cho việc tải thông tin được ký hiệu số hoặc mã hoá trong SIME. Các đặc tính này được biết đến như S/SIME. Các mục tiêu của MOSS và S/MIME phần lớn là giống nhau, các giải pháp cơ bản có khác nhau một chút, bởi vì S/MIME được xây dựng dựa vào sự tồn tại của các chuẩn ***defacto*** -được gọi là *Public-Key Cryptography Standards (PKCS*), và cũng được RSA Data Security,Inc phát triển.

Các chuẩn PKCS, đầu tiên được đưa ra vào năm 1993, chỉ gồm có một đặc tính, đó là PKCS#7, nó định nghĩa các cấu trúc dữ liệu và các thủ tục dành cho việc ký hiệu số và mã hoá các cấu trúc dữ liệu khác. Cách thức tiến hành trong SIME, đơn giản chỉ xác định nên áp dụng PKCS#7 như thế nào để bảo vệ được phần thân của MIME, tạo ra một cấu trúc dữ liệu mới, cấu trúc này tự trở thành nội dung của MIME. Điều này tạo ra một nền móng cho các dịch vụ an toàn như đã được PEM và MOSS cung cấp, đó là các dịch vụ bảo vệ thông báo cơ bản.

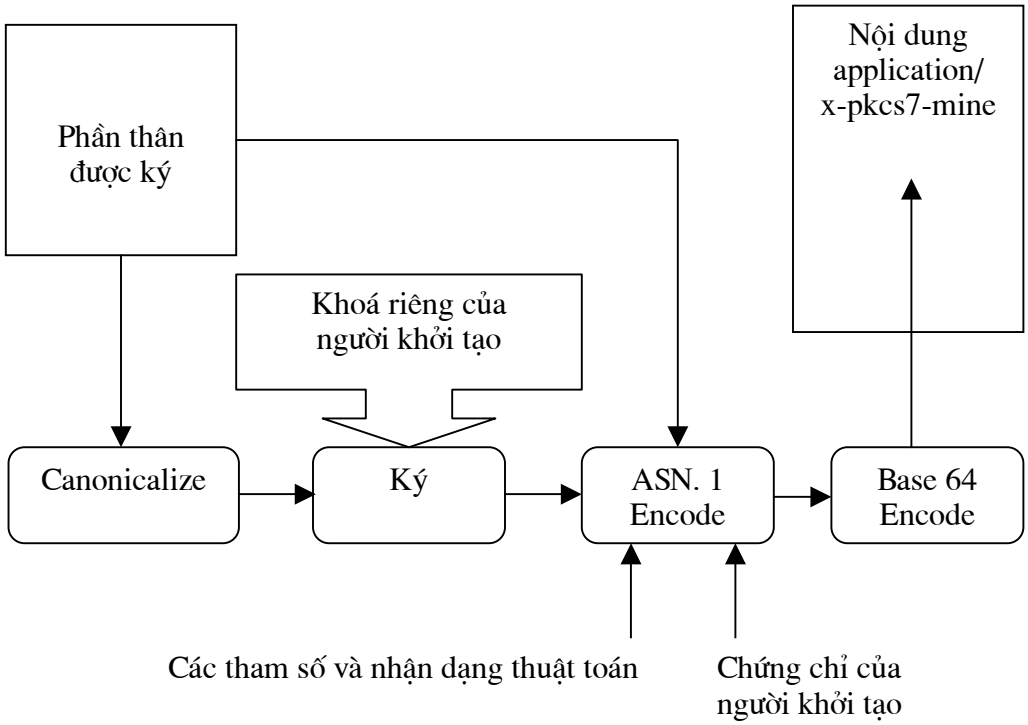
S/MIME định nghĩa một kiểu nội dung của MIME, được gọi là kiểu ***application/x-pkcs7-mine***. Mục đích của kiểu nội dung này là cung cấp một biểu diễn an toàn đối với bất kỳ phần thân MIME không được bảo vệ. Với S/MIME, các trường hợp khác như chữ ký số, mã hoá, hay kết hợp cả hai (mã hoá cộng với chữ ký số) thực chất chỉ là các biến thể của chuyển đổi dữ liệu cơ bản hoặc quá trình ***enveloping***. Các biến thể khác nhau tương ứng với các kiểu dữ liệu được cấu trúc khác nhau (được định nghĩa trong PKCS#7):

 Signed data : Dữ liệu được ký - Biểu diễn phần thân cần được bảo vệ, tạo thành một cấu trúc dữ liệu, trong đó gồm có một chữ ký số bao trùm lên toàn bộ dữ liệu, cùng với các nhận dạng thuật toán cần thiết và các chứng chỉ khoá công khai (tuỳ chọn) và các thông tin liên quan về người ký.

 Enveloped data : Dữ liệu được bao bọc - Biểu diễn phần thân cần được bảo vệ, được mã hoá bằng thuật toán mã đối xứng và sau đó hợp thành một cấu trúc dữ liệu. Cấu trúc dữ liệu này bao gồm một bản sao khoá mã dành cho mỗi người nhận, được mã hoá dựa vào khoá công khai có trong một cặp khoá mã RSA dành cho người nhận này, kết hợp với các nhận dạng người nhận và các nhận dạng thuật toán.

 Signed and Enveloped data : Cấu trúc này kết hợp xử lý cả kiểu dữ liệu được ký và bao bọc.

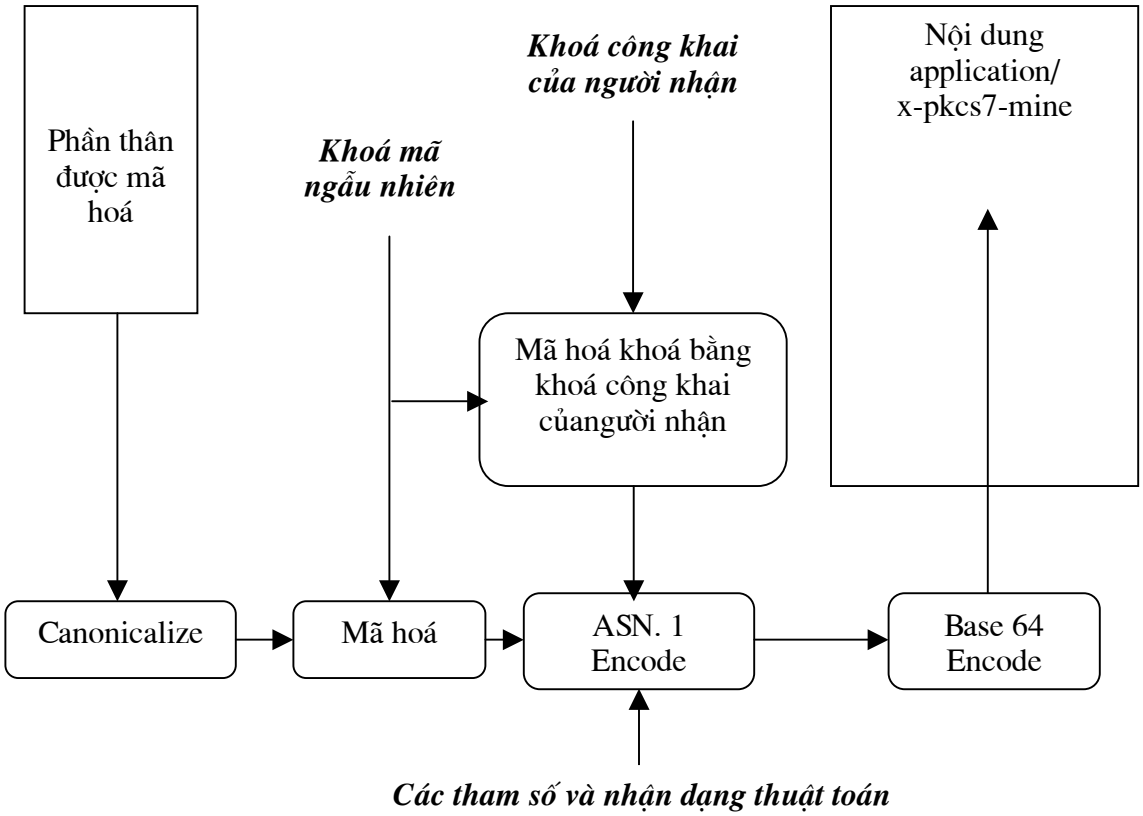
Hình 1.3 minh hoạ quá trình sinh ra nội dung S/MIME dành cho phần thân MIME được ký.



Hình 1.3. Sinh chữ ký số S/MIME

Quá trình sinh chữ ký số S/MIME bao gồm nhiều bước chính tắc các biểu diễn phần thân đưa vào, chuyển đổi mật mã, và chuyển đổi chuỗi dữ liệu nhị phân thành một khuôn dạng, khuôn dạng này có thể đi ngang qua một hệ thống truyền thông báo hướng chuỗi văn bản. (Bước tiếp theo là một quá trình được gọi là *Base 64 endoding*, đây là một cách thông thường dùng để tải dữ liệu nhị phân với MIME). Một cách, mà trong đó S/MIME khác với PEM và MOSS, là PKCS#7 sử dụng kiểu dữ liệu được chuẩn hoá quốc tế và ký hiệu cấu trúc - được gọi là ***Abstract Syntax Notation One (ASN.1)***, hơn là kiểu giao thức mã ký tự mà PEM và MOSS sử dụng.

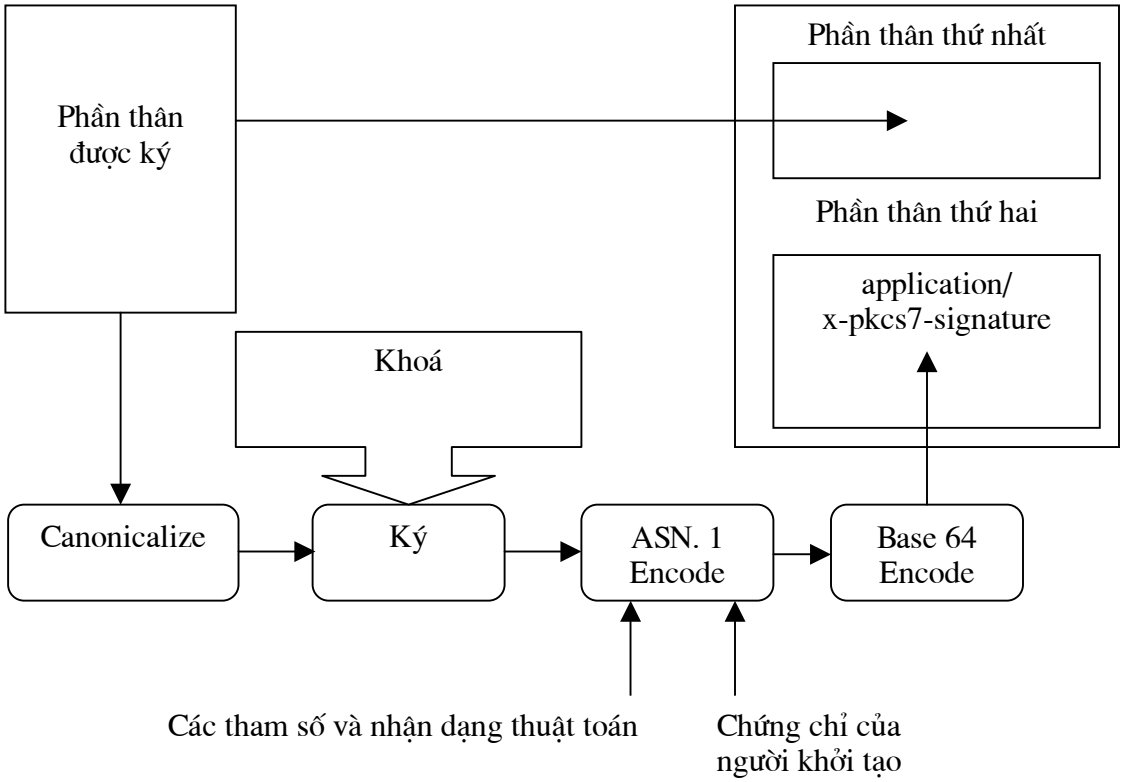
Quá trình sinh nội dung S/MIME để mã hoá được minh hoạ trong hình 1.4. Toàn bộ quá trình này tương tự như quá trình dành cho chữ ký số S/MIME, ngoại trừ biến thể dữ liệu được bao bọc (*enveloped data variant*) của PKCS#7 được sử dụng thay thế cho biến thể dữ liệu được ký (*signed data variant*), dẫn đến sự chuyển đổi mật mã khác nhau.



Hình 1.4. Quá trình mã hoá S/MIME

So sánh với PEM và MOSS, quá trình tạo chữ ký số S/MIME được minh hoạ trong hình 1.3 có một thiếu sót nào đó. Một ***mailer*** - không phải là một S/MIME, không có khả năng đọc được các nội dung phần thân nguyên thuỷ của một thông báo, nó được ký nhưng không được mã hoá. Những người nhận mà không có *mailer* được trang bị an toàn, có thể lợi dụng để đọc được các thông báo đã được ký, thậm chí nếu họ không thể xác nhận được các chữ ký.

S/MIME đưa ra thiếu sót này với một cấu trúc đan xen, sử dụng kiểu *multipart/signed MIME*, đã được giới thiệu trong phần trước, cùng với một kiểu S/MIME khác, được gọi là *application /x-pkcs7-signature*, nó được sử dụng trong phần thân thứ hai của *multipart/signed* . Kết quả được minh hoạ trong hình 1.5. Các nội dung của phần thân thứ hai là trường hợp đặc biệt của biến thể dữ liệu được ký (*signed data variant*) của PKCS#7, nó bỏ qua bản sao của dữ liệu được ký của bản rõ.



Hình 1.5. Sinh chữ ký số S/MIME với multipart/signed

Thêm vào các hình thức bảo vệ thông báo được thảo luận ở trên, S/MIME định nghĩa một hình thức dùng để chuyển một yêu cầu đòi hỏi chứng chỉ khoá công khai đã phát ra. Điều này kéo theo một kiểu nội dung MIME khác, nó được gọi là *application /x-pkcs10* , nó mang một thông báo yêu cầu chứng chỉ, như đã được định nghĩa trong các chuẩn PKCS khác, PKCS#10.

d. Pretty Good Privacy (PGP)

PGP là một sản phẩm phần mềm bảo vệ thông báo, phổ biến và được nhiều người biết đến, nó được sử dụng rộng rãi thông qua nhóm những người sử dụng Internet thông thường. Nó phổ biến ở chỗ hầu hết mọi người có được nó miễn phí. PGP được *Phil Zimmerman* viết, ông là một nhà nghiên cứu máy tính nổi tiếng, vừa là nhà hoạt động chính trị vừa là nhà kinh doanh. PGP được *MIT (Massachussetts Institute of Technology)* phân phối miễn phí trong phạm vi Bắc Mỹ. Một phiên bản hỗ trợ thương mại cũng đã được mang ra sử dụng.

Theo hướng kỹ thuật, PGP tương tự như PEM, MOSS hoặc S/MIME. Nó sử dụng các chức năng chữ ký số và mã hoá, cung cấp cho các dịch vụ bảo vệ thông báo cơ bản. PGP định nghĩa hình thức bảo vệ thông báo của riêng mình, nó có thể được gắn với phần thân của một MIME nếu cần. Một đề xuất về chuẩn Internet cũng được

phát triển, định rõ việc sử dụng một bảo vệ PGP kết hợp với các kiểu cấu trúc *multipart/signed* và *multipart/encrypted* theo cách tương tự như trong MOSS.

Một khía cạch quan trọng của PGP, điều này giúp cho việc phân biệt nó với các giao thức bảo vệ thông báo khác đã được mô tả trong mục 2, là ở chỗ PGP định nghĩa hệ thống quản lý cặp khoá công khai mà nó sở hữu, bao gồm các dạng chứng chỉ khoá công khai. Đáng tiếc là, hệ thống quản lý khoá này không tương thích với các chuẩn cơ sở hạ tầng khoá công khai đã được công nhận. Việc quản lý khoá PGP dựa vào các mối quan hệ nới lỏng, không dự tính trước (***loose , ad hoc relationships***) giữa các thành viên, người dùng sở hữu các cặp khoá PGP, hơn là dựa vào một cơ sở hạ tầng được tổ chức tốt, được thiết kế nhằm hỗ trợ *account*, Thông thường, PGP chứng tỏ mình là một hệ thống đạt hiệu quả cao trong việc bảo vệ thư tín điện tử thông thường giữa những người sử dụng Internet, nhưng nói chung nó không được quan tâm thích đáng cho việc hỗ trợ thương mại điện tử diện rộng.

e. X.400 Security

X.400 có cùng một họ với các giao thức gửi tin điện tử đã được chuẩn hoá quốc tế, được phát triển nhờ sự hợp tác của *International Telecommunication Union (ITU), International Organization for Standardization (ISO), và International Electrotechnical Commission (IEC)*. Các chuẩn X.400 được phát hành đầu tiên vào năm 1984. Chúng được các nhà cung cấp dịch vụ thư tín điện tử thương mại sử dụng. Khi X.400 không được coi là một giao thức Internet, X.400 được định cấu hình để thực hiện gửi tin Internet thông qua các cổng thư tín.

Vào năm 1998, tái bản lại các chuẩn X.400, một bộ các đặc tính an toàn mềm dẻo được bổ xung thêm. Các đặc tính này không chỉ hỗ trợ cho các dịch vụ bảo vệ thông báo cơ bản, mà còn hỗ trợ cho các dịch vụ chứng thực và các dịch vụ an toàn tăng cường.

Rất tiếc là, các đặc tính an toàn của X.400 (năm 1998) có một nhược điểm chính, thay vì việc thiết kế chúng đơn giản như là một tập hợp các khuôn dạng nội dung thông báo, chúng lại kết hợp một cách rắc rối các giao thức xét duyệt, chuyển và phân phối. Điều này có nghĩa là các thông báo tin cậy X.400, không giống các thông báo không được bảo vệ, không thể được sử dụng thông qua các cổng thư tín và vì vậy không được chuyển trên hệ thống thư tín Internet.

f. Message Security Protocol (MSP)

Vào cuối những năm 1980, chính phủ Mỹ phát triển giao thức gửi tin an toàn của riêng mình, được gọi là ***Message Security Protocol (MSP)***. Giao thức này được chấp thuận và được sử dụng trong Bộ quốc phòng Mỹ, đặc biệt là dành cho dự án *Defence Messaging System (DMS)*. Nó là một giao thức - dự định được sử dụng trong các lĩnh vực khác của chính phủ và rất có thể là trong lĩnh vực thương mại.

MSP là một giao thức bảo vệ thông báo, không giống với PKCS#7 hoặc S/MIME, nó gói gọn nội dung của một thông báo không được bảo vệ để tạo ra một nội dung mới của thông báo được bảo vệ. Nó cung cấp các dịch vụ bảo vệ thông báo cơ bản cùng với các dịch vụ bảo vệ thông báo tăng cường - các dịch vụ chứng thực (yêu cầu và đáp lại một xác nhận thông báo đã được ký), và các dịch vụ kết hợp với việc chuyển các nhãn thông báo dành cho các mục đích điều khiển truy nhập. MSP có thể được tải hoặc trên X.400 hoặc trên các phương tiện gửi tin Internet.

Một thông báo MSP mang các nội dung thông báo nguyên thuỷ (có thể được mã hoá, nếu tính tin cậy được yêu cầu) cộng với hàng loạt các tham số an toàn do những người nhận yêu để giải mã và/hoặc phê chuẩn thông báo nhờ xác nhận. Các tham số xác định các thuật toán được dùng trong mã hoá, kiểm tra tính toàn vẹn, và chữ ký số.

Từ một triển vọng về mặt kỹ thuật, MSP là một giao thức an toàn mềm dẻo hơn S/MIME, MOSS, hoặc PEM. Khó khăn chính của nó là thiếu sự chấp thuận trong thương mại và Bộ quốc phòng Mỹ phát triển nó một cách riêng lẻ.

g. So sánh các tuỳ chọn

Có một điều rõ ràng là Internet không cần tất cả các giao thức gửi tin an toàn khác nhau, mà chỉ cần một hoặc hai. Tất cả các giao thức được thảo luận trong mục này cung cấp một mức bảo vệ thích hợp và tất cả sử dụng kỹ thuật có thể so sánh được. Các điểm phân biệt chính- các điểm này có thể khuyến khích hoặc hạn chế bớt việc sử dụng mỗi giao thức - có thể được tóm tắt như sau :

 S/MIME : Được các nhà cung cấp thương mại chấp nhận nhiều hơn cả.

 PGP : Có được miễn phí, nhưng không thích hợp với các chuẩn cơ sở hạ tầng khoá công khai đã được công nhận;

 MSP : Có một bộ đặc tính mềm dẻo nhất sau X.400, nhưng không được ủng hộ nhiều trong thương mại.

 MOSS : Có một số thiếu sót trong việc tương thích với các cơ sở hạ tầng khoá công khai; không thuyết phục được các nhà cung cấp thương mại.

 PEM : Không thích hợp với MIME; không có một cách thức chuẩn áp dụng cho các thông báo có cấu trúc;

 X.400 security : Có một bộ đặc tính mềm dẻo nhất, nhưng không thích hợp với gửi tin Internet.

5. An toàn Web

World Wide Web mang lại vô số các cơ hội trong việc truyền thông tin. An toàn trên Web chia thành hai loại cơ bản : Loại đầu tiên liên quan đến các rủi ro ảnh hưởng đến một ***Web server site***, ví dụ, các tài liệu có thể bị lộ cho những người không được uỷ quyền hoặc những kẻ tấn công có khả năng thực hiện mã không có lợi trên *server*. Mặc dù, những vấn đề như vậy có khuynh hướng trở thành đặc trưng riêng của Web, nhưng về bản chất chúng là một vấn đề về an toàn hệ thống. Để có được lời khuyên trong lĩnh vực này, xem *Stein* hoặc các sách hướng dẫn do *National Computer Security Association* xuất bản. Loại thứ hai liên quan đến các rủi ro ảnh hưởng đến việc truyền thông của những người sử dụng, ví dụ như số thẻ tín dụng bị phát hiện thông qua việc nghe trộm, hoặc thông qua việc thiết lập các *Web site* của những nhà cung cấp không có thực . Những vấn đề như vậy cần được giải quyết - thông qua các giao thức an toàn ứng dụng chuẩn được các sản phẩm *Web server* và *browser* hỗ trợ - có thể tìm được chúng thông qua hàng loạt các nhà cung cấp.

Đây là một lĩnh vực phát triển nhanh chóng. Tại thời điểm công bố, giao thức với mục đích an toàn Web được sử dụng rộng rãi nhất là giao thức ***Secure Sockets Layer (SSL)***. Tiếp theo là giao thức ***Secure HTTP (S-HTTP)***. Các giao thức khác được phát triển với các mục đích riêng, ví dụ như giao thức Secure Electronic Transaction (SET) dành cho mục đích chi trả thẻ ngân hàng.

a. Secure Sockets Layer (SSL)

Giao thức SSL được *Netscape Communication Corporation* phát triển, có thể tăng cường việc bảo vệ truyền thông cho hàng loạt các giao thức ứng dụng Internet. Nguyên thuỷ SSL là một giao thức an toàn Web, trên thực tế nó là một tầng mới - hoạt động trên giao thức Internet TCP. Nó có thể được sử dụng để bảo vệ truyền thông cho bất kỳ giao thức ứng dụng nào mà hoạt động trên TCP, ví dụ, HTTP, FTP, hoặc TELNET. SSL được sử dụng phổ biến nhất trong việc bảo vệ truyền thông HTTP - đặc biệt, một URA khởi đầu với "https://" cho biết việc sử dụng HTTP được SSL bảo vệ.

SSL cung cấp hàng loạt các dịch vụ an toàn cho các ***client-server session***. Để tìm hiểu lợi ích của các dịch vụ này, xem xét chúng trong ví dụ bảo vệ ***Web session*** của Vera, trong đó cô yêu cầu một máy tiện từ Danielle's Machine Makers. Vera sẽ biết *session* là SSL được bảo vệ - do có một chỉ dẫn xuất hiện trên màn hình hiển thị của cô. Các dịch vụ an toàn bao gồm :

 Server authentication : Xác thực máy chủ - Máy chủ được xác thực thông qua máy khách, bằng cách chứng minh quyền sở hữu của một khoá riêng. Điều này rất quan trọng đối với Vera, để đảm bảo rằng thực tế cô đang liên lạc với Danielle's site, và không có một site nào khác đóng giả Danielle's site để lấy được các số thẻ tín dụng hoặc các thông tin cá nhân khác từ những người mua tin cậy.

 Client authentication : Xác thực máy khách - Dịch vụ an toàn tuỳ chọn này xác thực máy khách tới máy chủ, bằng cách chứng minh quyền sở hữu một khoá riêng. Danielle's mong muốn có được bằng chứng - chứng tỏ người ngồi tại máy khách đích thực là Vera, đưa ra số thẻ tín dụng hợp lệ và như vậy việc xác thực đã thành công. Lưu ý rằng, dịch vụ này không bắt buộc đối với nhà cung cấp, và các khách hàng quen thuộc không thể chiếm hữu các cặp khoá của họ, dịch vụ này có thể tìm ra những hạn chế sử dụng khi mua bán trên Internet. Tuy nhiên, đối với các ứng dụng khác, như giao dịch và tiến hành các công việc ngân hàng trên Interent, nó có thể rất quan trọng đối với server site khi xác thực client.

 Integrity: Tính toàn vẹn - Các mục dữ liệu được chuyển đi trên một phiên - được bảo vệ thông qua một giá trị kiểm tra tính toàn vẹn (*integrity - check value*) để đảm bảo rằng mọi cố gắng nhằm sửa đổi dữ liệu trong quá trình chuyển tiếp đều bị phát hiện. Điều này bảo vệ cả Vera và nhà cung cấp chống lại những kẻ ăn cắp thông tin, những người này có thể gây ra thiệt hại bằng cách thay đổi phiếu đặt hàng mua một máy tiện thành phiếu đặt hàng mua 50 máy tiện và /hoặc thay đổi địa chỉ giao hàng.

 Confidentiality : Sự tin cậy - Các mục dữ liệu được chuyển đi trên một phiên - được mã hoá nhằm bảo vệ chống lại những người nghe trộm. Điều này đặc biệt quan trọng, nó có thể bảo vệ chống lại kẻ người nghe trộm tìm hiểu số thẻ tín dụng của Vera hoặc thông tin khác về tài khoản cá nhân khi nó được truyền tới máy chủ.

SSL gồm có hai giao thức nhỏ - ***SSL Record Protocol*** và ***SSL Handshake Protocol***. *SSL Record Protocol* định nghĩa khuôn dạng cơ bản cho tất cả các mục dữ liệu trong phiên. Nó tiến hành nén dữ liệu, sinh ra một giá trị kiểm tra tính toàn vẹn (một MAC), mã hoá dữ liệu, và đảm bảo rằng người nhận có thể xác định chính xác độ dài dữ liệu (lưu ý rằng, dữ liệu đầu vào có thể được đệm thêm để tạo ra một số nguyên các khối, dùng cho thuật toán mã hoá khối). Giá trị kiểm tra tính toàn vẹn được đặt vào trước dữ liệu như một phần của *SSL Record Protocol* trước khi mã hoá. Số thứ tự của một bản ghi được tính đến nhằm bảo vệ chống lại những kẻ lấy tin trái phép ghi chép các mục dữ liệu. Để *SSL Record Protocol* tính toán được giá trị kiểm tra tính toàn vẹn - dùng khi mã hoá, các khoá mã phải được thiết lập hoàn toàn trên máy chủ và máy khách. Giao thức hỗ trợ việc biến đổi thành một tập hợp các thuật toán và các khoá bảo vệ khác nhau tại mọi thời điểm.

SSL Handshake Protocol được sử dụng để :

+ thoả thuận các thuật toán bảo vệ nào sẽ được sử dụng để xác thực máy khách và máy chủ tới mỗi máy khách khác.
+ truyền các chứng chỉ khoá công khai được yêu cầu.

+ thiết lập các khoá phiên dùng trong các quá trình kiểm tra tính toàn vẹn và mã hoá của *SSL Record Protocol*.

Các thuật toán thiết lập khoá khác nhau có thể được hỗ trợ, gồm có truyền tải khoá RSA, thoả thuận khoá Diffie-Hellman, và thuật toán KEA của chính phủ Hoa kỳ.

Khi một phiên mới được thiết lập, nó có thể tái sử dụng lại các khoá phiên đã có từ các cuộc truyền thông trước. Các khóa phiên có một nhận dạng phiên kết hợp (*an associated session identifier*) dành cho mục đích này.

SSL Handshake Protocol là một giao thức mức cao hơn *SSL Record Protocol* theo nghĩa là cái sau tải cái trước. Trong hai cặp thông báo đầu tiên được trao đổi trong một phiên, *SSL Record Protocol* không thể mã hoá hoặc tính toán các giá trị kiểm tra tính toàn vẹn bởi vì các khoá hoàn toàn không được biết đến.

Đối với các thuật toán mã hoá, SSL được thiết kế sao cho có khả năng thiết lập cả trong phạm vi nội địa Hoa kỳ và xuất khẩu. Cả hai kiểu thiết lập sử dụng cùng thuật toán mã hoá có độ dài khoá đặc trưng là 128 bit. Sự khác nhau giữa hai kiểu thiết lập nằm trong việc thiết lập *SSL Handshake Protocol*. Trong thiết lập có khả năng xuất khẩu, độ dài khoá có hiệu lực là 40 bit - khoá mã hoá thực tế có nguồn gốc từ một giá trị bí mật 40 bit, cộng với thông tin công khai. Trong phiên bản nội địa, độ dài khoá có hiệu lực có thể dài hơn, chẳng hạn 128 bit.

Bạn đọc cần được cảnh báo trước rằng, SSL là một đặc tính tiến hoá, là một đối tượng thay đổi nhanh chóng.

b. HTTP an toàn (S-HTTP)

S-HTTP đưa ra một tập hợp các yêu cầu tương tự như SSL, nhưng xuất phát từ một nền móng khác và đưa ra một kiểu giải pháp khác. *S-HTTP* được *Enterprise Integration Technologies* thiết kế nhằm đáp ứng các yều cầu từ phía *CommerceNet*, là một ***consortium*** tập trung vào việc xúc tiến thiết lập các kỹ thuật mà cần thiết cho thương mại điện tử dựa vào Internet.

S-HTTP được thiết kế như là một mở rộng an toàn cho HTTP, về bản chất nó là một giao thức giao dịch yêu cầu - đáp ứng. Điều này làm cho S-HTTP khác so với SSL, nó là một giao thức bảo vệ phiên. Chức năng ban đầu của S-HTTP là bảo vệ các thông báo yêu cầu -đáp ứng của giao dịch cá nhân, ở một mức độ nào đó nó hơi giống giao thức gửi tin an toàn bảo vệ các thông báo thư tín điện tử. Trong thực tế, S-HTTP được xây dựng dựa vào các giao thức gửi tin an toàn đã được nói đến trong mục trước.

Các dịch vụ an toàn được S-HTTP cung cấp cũng giống với các dịch vụ an toàn được SSL cung cấp, như là xác thực thực thể, tính toàn vẹn (thông qua một giá trị kiểm tra tính toàn vẹn), và sự tin cậy (thông qua mã hoá), cộng với một tuỳ chọn dành cho các chữ ký số, nó có thể cung cấp một nền móng cho các dịch vụ an toàn thêm vào.

S-HTTP tạo ra một độ mềm dẻo khi bảo vệ các thông báo và quản lý các khoá. Các hình thức bảo vệ thông báo được hỗ trợ gồm có: PEM(RFC 1421) và PKCS#7. Tuy nhiên, việc quản lý khoá không bị rằng buộc bởi cơ sở hạ tầng bắt buộc của PEM, mà cũng không phải là một tập hợp các quy tắc khắt khe bất kỳ. Các khoá mã hoá có thể được thiết lập thông qua việc truyền tải khoá RSA trong phạm vi PEM hoặc PKCS#7, có thể được tái thiết lập thông qua các phương pháp thủ công, hoặc thậm trí có thể được thiết lập từ các ***Kerberos tickets***. Một URA khởi đầu với "shttp://" cho biết việc sử dụng S-HTTP.

Như với SSL, người đọc cần được cảnh báo trước rằng S-HTTP là một đặc tính tiến hoá, là một đối tượng thay đổi nhanh chóng.

c.Phần mềm có khả năng tải xuống

Web là một thế giới tương đối tĩnh của các trang và liên kết siêu văn bản cho đến khi Sun Microsoft đưa ra ngôn ngữ lập trình ***Java***. Các chương trình Java, được gọi là các ***applet***, được tải xuống một cách tự động từ một máy chủ thông qua việc truy nhập vào các trang Web có sẵn, sau đó được các *browser* của các máy khách thông dịch và biểu diễn. Các ví dụ về Java, như văn bản cuộn tròn (*spining text*) và các biểu tượng hoạt ảnh (*animated icon*), có thể được tìm thấy ở khắp nơi trên Web. Java cũng hỗ trợ truyền thông ngược trở lại máy chủ nguồn của nó, cho phép các ứng dụng như chích dẫn chỉ số chứng khoán lên xuống (*srolling stock quotes*) hoặc các chương trình tán ngẫu qua lại.

Java khám phá ra nhiều rủi ro mới mà người sử dụng Web gặp phải. Thay vào việc chạy phần mềm trên một máy chủ ở xa, việc thực hiện các *Java applet* xảy ra trên hệ thống của máy khách, nó chuyển rủi ro an toàn từ máy chủ sang máy khách. Việc thực hiện mã thực thi từ một nguồn không được biết đến trên một máy tính của một cá nhân nào đó thường làm tăng các quan tâm an toàn chính đáng.

Các *Java applet* chạy trên một môi trường thực thi tin cậy - được gọi là ***sandbox***. Thông qua việc thiết kế, một *applet* không có khả năng kiểm tra hoặc sửa đổi hệ thống file của máy khách, chạy các lệnh hệ thống, hoặc tải các thư viện phần mềm hệ thống. Một *Java applet* chỉ có khả năng liên lạc với máy chủ, nó được máy chủ này tải xuống đầu tiên. Với các hạn chế này, các *applet* phải có khă năng giảm thiệt hại cho các hệ thống máy chủ hoặc máy khách. Tuy nhiên, trong Java còn có nhiều thiếu sót.

Trong tương lai không xa sẽ xuất hiện các ***hostile applet*** (*applet thù địch*). Một *hostile applet* , khi được tải xuống, có thể cố gắng khai thác các nguồn tài nguyên hệ thống của một máy khách theo một cách nào đó. Ví dụ, một *applet* có thể truy nhập vào cổng thư tín của một máy chủ của nó; vì vậy, nó có thể gửi một thư tín được làm giả từ máy khách. Các mối lo ngại ở đây là các *hostile applet* có thể xâm nhập vào các *browser* , làm hỏng các applet khác đang chạy, hoặc lạm dụng các nguồn tài nguyên thừa trong hệ thống của máy khách. Hàng loạt các giải pháp nhằm chống lại các tấn công như vậy cũng đã được đề xuất.

Các mối lo ngại trên chưa phải đã kết thúc cho Java, nhưng chúng lại liên quan đến mảng đối tượng chung hơn đó là phần mềm có khả năng tải xuống. Ví dụ, hệ thống ***ActiveX*** của Microsoft làm tăng các kiểu lo ngại như vậy.Các kiểm soát *ActiveX* là các thành phần phần mềm tái sử dụng được các nhà cung cấp phần mềm phát triển. Các kiểm soát này có thể được sử dụng để làm tăng thêm chức năng xác định cho các Web site, các ứng dụng bàn giấy, và các công cụ phát triển. Ví dụ, một kiểm soát giá trị cổ phiếu (***stock ticker control***) có thể được sử dụng để làm tăng thêm một giá trị cổ phiếu động (***live stock ticker***) cho một trang Web, hoặc một kiểm soát hoạt ảnh có thể được sử dụng nhằm làm tăng thêm các đặc tính hoạt ảnh.

Cách bảo vệ tốt nhất cho lĩnh vực này là có kiến thức xác thực về nguồn của phần mềm bất kỳ, phần mềm này đã được tải xuống một hệ thống nào đó. Các *applet* và phần mềm khác từ các nguồn đáng ngờ không nên được tải về. Hơn nữa, người sử dụng nên biết nguồn gốc của phần mềm để thao tác với tài nguyên.

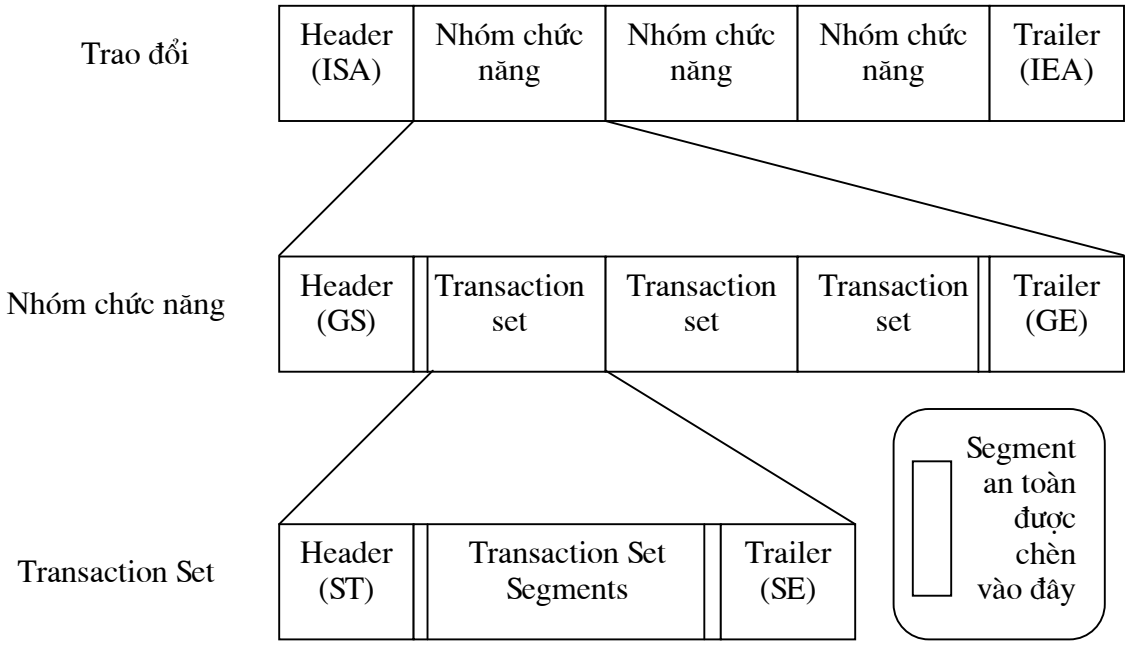
Các hệ thống dành cho việc xác thực nguồn của phần mềm có khả năng tải xuống cũng đã và đang được phát triển , ví dụ , hệ thống ***Authenticode*** của Microsoft Corporation. *Authenticode* cho phép các nhà phát triển gán mã cho với mã phần mềm của họ, cho phép các máy khách xác nhận lại những người phát hành phần mềm được tải xuống trước khi thực hiện nó. Việc xác nhận lại chữ ký số cũng đảm bảo rằng phần mềm không bị làm giả trong quá trình tải xuống. *Authenticode* sử dụng các chuẩn dữ liệu được ký hiệu của PKCS#7. Các chữ ký có thể xác nhận được bằng cách sử dụng các chứng chỉ khoá công khai được những người có thẩm quyền đưa ra.

6. An toàn đối với các ứng dụng thương mại điện tử

Các ứng dụng thương mại điện tử có thể sử dụng các đặc tính an toàn của gửi tin điện tử và các giao thức Web đã được trình bày ở trên. Tuy nhiên, các yêu cầu bổ xung phát sinh trong các viễn cảnh thương mại điện tử cụ thể. Trong mục nhỏ này, chúng tôi trình bày 2 mảng trong đó cần đến các giao thức an toàn tầng cao hơn liên quan đến thương mại - đầu tiên là EDI, thứ hai là các thanh toán thẻ ngân hàng dựa vào Internet.

a. An toàn EDI

Do EDI trao đổi các cấu trúc phức tạp, các phần cố định của nhiều giao dịch thương mại khác nhau, cả ANSI X12 và EDIFACT EDI trao đổi các khuôn dạng, các khuôn dạng này định nghĩa các biện pháp an toàn nội bộ của chúng. Ví dụ, một ***ANSI X12 interchange*** được định nghĩa là một cấu trúc lồng đôi, dựa vào một dãy các ***data segment*** (các đoạn dữ liệu), được trình bày trong hình 1.6. Một trao đổi gồm có một hoặc nhiều ***functional group*** (nhóm chức năng), mỗi nhóm chức năng biểu diễn một tập hợp các hình thức thương mại liên quan. Một nhóm chức năng gồm có một hoặc nhiều ***transaction set*** , mỗi *transaction set* biểu diễn một hình thức thương mại. Chuẩn ANSI X12.58 xác định rõ an toàn được cung cấp như thế nào cho một trong hai, hay cả hai *functional group* và *transaction set*. Các dịch vụ an toàn được cung cấp gồm có: xác thực nguồn gốc dữ liệu, sự tin cậy, và/ hoặc tính toàn vẹn, với một hỗ trợ tuỳ chọn dành cho việc chấp thuận (nếu chữ ký số được sử dụng). ANSI X12.58 định nghĩa các *segment* an toàn được chèn vào các nhóm chức năng và/hoặc *transaction set* như đã được chỉ ra trong hình 1.6. Các đoạn này vận chuyển dữ liệu như: các nhận dạng khoá, các giá trị kiểm tra tính toàn vẹn, các chữ ký số, và các tem thời gian.



Hình 1.6. Cấu trúc trao đổi của ANSI X12.

Một bảo vệ bất kỳ - được cung cấp như là một trao đổi nội bộ- không phụ thuộc vào việc trao đổi có được truyền qua Internet hoặc các phương tiện truyền thông khác hay không. Không quan tâm đến các phương tiện truyền, kiểu bảo vệ này có thể rất quan trọng bởi vì các *transaction set* khác nhau có thể cần được bảo vệ

theo nhiều cách khác nhau, ví dụ, được ký hoặc mã hoá cho nhiều thành viên khác nhau.

Thêm vào đó, khi một trao đổi EDI được truyền qua Internet, có thể áp dụng các giao thức an toàn gửi tin chuẩn của Internet cho các thông báo hoặc các phần thân của chúng. Ví dụ, các kiểu nội dung EDI MIME được giới thiệu tương thích hoàn toàn với các giao thức an toàn MIME như S/MIME. Nói chung cần sử dụng các bảo vệ xác thực và tính toàn vẹn tại mức này và phụ thuộc vào ứng dụng, nó cũng có thể cần bảo vệ tin cậy. Việc sử dụng các dịch vụ an toàn như vậy được khuyến nghị bởi vì toàn bộ trao đổi nội bộ chưa chắc đã được bảo vệ đầy đủ, chúng được thiết kế với một môi trường truyền thông ít rủi ro hơn Internet. Hơn nữa, việc bảo vệ một thông báo Internet không nhất thiết phải thay thế bằng việc bảo vệ các ***transaction set*** hoặc nhóm chức năng cách sử dụng các tuỳ chọn an toàn của X12 hoặc EDIFACT.

b. Các thanh toán thẻ ngân hàng - Giao thức SET

Các tổ chức *Visa* và *MasterCard* cùng nhau phát triển ***SET*** - đây là một giao thức mềm dẻo và đặc tính cơ sở hạ tầng hỗ trợ cho các thanh toán thẻ ngân hàng như một phần của việc mua bán điện tử hoặc cung cấp dịch vụ dựa vào Internet.

Những đối tượng tham gia ban đầu trong môi trường SET gồm có:

(a) ***issuer*** : Một cơ quan tài chính phát hành các thẻ ngân hàng (các thẻ tín dụng hoặc các thẻ nợ), đặc biệt sinh ra một ***brand*** đặc trưng (ví dụ về các *brand* là *Visa* và *Mastercard*).

(b) ***Cardholder*** : (Người nắm giữ thẻ) Một người nắm giữ uỷ quyền một thẻ ngân hàng. Đây là người được đăng ký với *issuer* tương ứng nhằm tiến hành thương mại điện tử.

(c) ***Merchant*** : (Nhà buôn) Một người bán hàng hoá, dịch vụ, hoặc thông tin, người chấp nhận thanh toán điện tử.

(d) ***Acquirer*** : Một cơ quan tài chính hỗ trợ các *merchant* bằng cách cung cấp một dịch vụ dùng trong việc xử lý các giao dịch thẻ ngân hàng.

Những đối tượng tham gia tiếp theo tạo thành một phần của cơ sở hạ tầng SET gồm có:

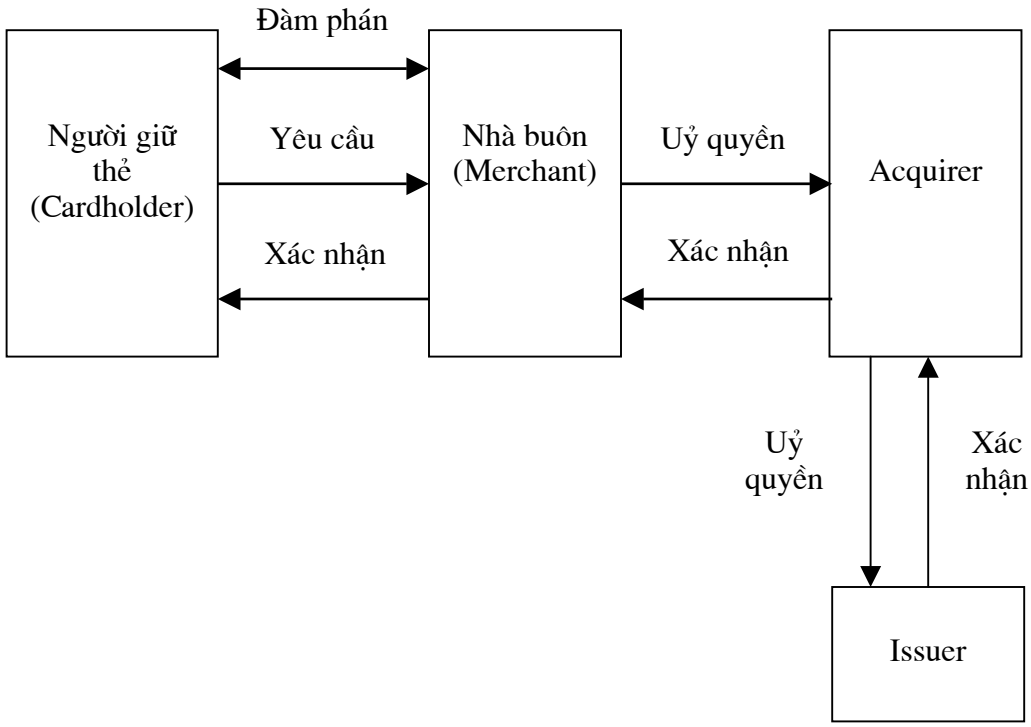
(e) ***Payment gateway*** : (Cổng thanh toán) Một hệ thống mà cung cấp các dịch vụ thương mại trực tuyến cho các *merchant*. Như vậy, một hệ

thống được một *acquirer* hoặc thành viên khác (thành viên này hỗ trợ các *acquirer*) điều hành.

(f) ***Certification authorities*** : Các thành phần của cơ sở hạ tầng mà chứng thực các khoá công khai của *cardholder*, *merchant*, và/hoặc *acquirer* hoặc các *getway* của họ.

Trong khi tiến hành một giao dịch thanh toán điện tử, những đối tượng tham gia ban đầu tác động qua lại lẫn nhau, như được minh hoạ trong hình 1.7.

Sau khi một người nắm giữ thẻ đồng ý tiến hành mua từ nhà buôn, người nắm giữ thẻ gửi một chỉ dẫn thanh toán trực tuyến cho nhà buôn. Nhà buôn liên lạc trực tuyến với *acquirer* của mình thông qua các cổng thanh toán, đặc biệt gửi chuyển tiếp tất cả hoặc một phần chỉ dẫn thanh toán của người nắm giữ thẻ, để uỷ quyền và nắm bắt được giao dịch. Khi việc nắm bắt được *acquirer* tiến hành. Việc cấp phép yêu cầu một giao dịch hỏi ngược trở lại *issuer* - vì thế điều này được thực hiện thông qua việc sử dụng các mạng tài chính - không phải là Internet.



Hình 1.7. Dây chuyền mua sử dụng SET

Trong môi trường này, kỹ thuật khoá công khai được sử dụng nhằm hỗ trợ các chức năng, gồm có :

 Mã hoá các chỉ dẫn thanh toán theo một cách mà có thể đảm bảo rằng số thẻ ngân hàng của người sử dụng không bao giờ bị lộ trong quá trình chuyển tiếp trên Internet, mà cũng không bị các hệ thống nhà buôn phát hiện được (nơi có thể bị lộ - do rủi ro từ việc thoả hiệp gây ra).

 (Tuỳ chọn) Việc xác thực những người nắm giữ thẻ cho các nhà buôn và các *acquirer* nhằm chống lại việc sử dụng các thẻ đã bị lấy cắp thông qua các cá nhân không được uỷ quyền, những người khởi đầu các giao dịch điện tử.

 Xác thực các nhà buôn cho những người nắm giữ thẻ và các *acquirer*, nhằm chống lại những kẻ mạo danh thiết lập các Internet site, nơi họ tự cho mình là các nhà buôn hợp pháp và thực hiện các giao dịch gian lận.

 Xác thực các *acquirer* cho các nhà buôn và những người nắm giữ thẻ, nhằm chống lại một cá nhân nào đó giả mạo thành một *acquirer* để thực hiện mã hoá thông tin chỉ dẫn thanh toán nhạy cảm.

 Bảo vệ toàn vẹn đối với thông tin giao dịch, nhằm ngăn chặn việc giả mạo trên Internet không được bảo vệ.

Cơ sở hạ tầng khoá công khai hỗ trợ môi trường SET được mô tả trong chương 7.

c. Các mô hình thanh toán an toàn khác trên Internet

Hàng loạt các lược đồ khác nhau đã được thực hiện hoặc được đề xuất nhằm bảo vệ các thanh toán trên Internet. Đây là một lĩnh vực phát triển nhanh chóng nên chúng ta không thể gói gọn trong quyển sách này. Một số ví dụ về các lược đồ trực tuyến hiện tại đang được sử dụng , với các thông tin triển vọng, như sau :

 Cyber Cash: *Cyber Cash* đóng vai trò như là một người trung gian giữa các nhà buôn dựa vào Web và các nhà băng thẻ tín dụng. Cả các nhà buôn và các khách hàng đăng ký như là các máy khách của *Cyber Cash*. Các giao dịch của *Cyber Cash* được bảo vệ bằng mật mã khoá công khai. *Cyber Cash* quản lý khoá như là một hệ thống kín.

 CheckFree: *CheckFree* thiết lập một phiên bản trực tuyến dựa vào Internet của hệ thống thanh toán kiểm tra giấy tờ.

 First Virtual: Hệ thống *First Virtual* hỗ trợ các thanh toán thẻ tín dụng dựa vào Internet mà sử dụng các thông báo thư tín điện tử. Không sử dụng mã hoá.

Thêm vào đó, một vài đề xuất tiền điện tử (***electronic cash)*** được đưa vào thử nghiệm hoặc hoạt động sản xuất, gồm có ***DigiCash*** và ***Mondex***.

Thậm chí có một lĩnh vực mới hơn trong đó các hệ thống được phát triển là các hệ thống ***micropayment*** (hệ thống thanh toán cực nhỏ). ở đây có các hệ thống được thiết kế nhằm hỗ trợ cho một số lượng lớn các thanh toán nhỏ; các đồng xu qua các cuộc giao dịch, thay cho đồng đôla. Tại thời điểm hiện tại, việc mua thanh toán cực nhỏ mang tính chất cá nhân - không đủ lớn để được xử lý hiệu quả chi phí như là một giao dịch thanh toán với các giải pháp truyền thống thông qua một tổ chức tài chính. Nhiều giao dịch nhỏ có thể được điều tiết nhưng trước tiên chúng cần tích đống lại với nhau và được bó lại khi tổ chức tài chính xử lý. Các quá trình tập hợp và bó lại không thích hợp với thời gian thực, các yêu cầu giao dịch ngay lập tức của thương mại Internet. Các hệ thống thanh toán cực nhỏ và các thẻ giá trị được lưu giữ cố gắng khắc phục được những nhược điểm này.

7. Các thoả thuận của các nhà cung cấp dịch vụ Internet

Không những áp dụng các kỹ thuật và công nghệ an toàn thích hợp vào các ứng dụng dựa vào Internet, mà còn phải đưa ra các khía cạnh hợp pháp trong việc sử dụng chúng cũng tốt như vậy. Cần chú ý tập trung vào luật pháp vì điều này đã được chứng minh qua các cuộc tranh chấp quyền tác giả. Có một điều rõ ràng là , Internet càng phát triển thì các thành viên tham gia càng phải có trách nhiệm. Một trong các cố gắng nhằm làm tăng trách nhiệm đó chính là thỏa thuận giữa những người sử dụng Internet (gồm có những nhà kinh doanh và tất cả các cá nhân) và các nhà cung cấp dịch vụ Internet của họ (ISP).

Các thoả thuận ISP định nghĩa các quyền và nghĩa vụ của các ISP và những người sử dụng hàng loạt các kiểu dịch vụ Internet. Không giống với các thoả thuận của các nhà cung cấp thương mại truyền thống EDI và VAN, thỏa thuận này đáp ứng các yêu cầu của các hệ thống kín một cách tương đối, còn các thoả thuận ISP cần đưa ra các nội dung và các phát hành an toàn liên quan đến Internet.

Các mục tiếp theo trình bày việc cung cấp các thoả thuận ISP.

a. Sử dụng và chấp nhận

Các hệ thống đăng ký trực tuyến được sử dụng rộng rãi nhằm cung cấp thông cáo về các mục thoả thuận ISP cho các khách hàng. Nó có ý định cho các khách hàng bày tỏ các kiến thức của họ phê chuẩn các mục này thông qua các hệ thống trực tuyến nêu trên. Việc cung cấp chỉ đơn giản là nhấn vào nút ***accept*** hoặc sử dụng dịch vụ "tạo ra sự chấp nhận đối với các mục và điều kiện này".

Các ISP thiết lập các dịch vụ được chuẩn hoá, chúng được kê khai trong các thoả thuận có dạng chuẩn không thương lượng được. Đối với các thoả thuận không

thể thương lượng được, trong đó nội dung của các thoả thuận là bắt buộc tuân theo. Sự cần thiết cho một số lượng lớn những người sử dụng ký giao kèo trong thời gian thực - nhằm bênh vực cho các nhu cầu hợp pháp (và sự chấp nhận của pháp luật).

b. Các định nghĩa dịch vụ

Các thoả thuận ISP mô tả các dịch vụ mà nó cung cấp, đặc biệt bao gồm các truy nhập Internet, các dịch vụ của máy chủ (như thư tín điện tử và các trang chủ), và các dịch vụ cơ sở dữ liệu/thông tin. Ví dụ, một thoả thuận ISP có thể cung cấp cho "các dịch vụ trên các hệ thống tính toán máy chủ [của ISP], bao gồm các dịch vụ tính toán, dịch vụ truyền thông, dịch vụ phần mềm, dịch vụ thông tin, cũng như truy nhập vào các dịch vụ tương tự được các thoả thuận khác cung cấp thông qua Internet".

c. Sử dụng hợp pháp và kiểm soát của nhà cung cấp dịch vụ thông qua nội dung thông tin

Truyền hoặc các cách khác làm cho thông tin có thể sử dụng được - bắt buộc người khởi tạo phải có trách nhiệm pháp lý hợp pháp dựa trên cơ sở nội dung của thông tin đó. Ba lý do liên quan đến trách nhiệm pháp lý - dựa vào nội dung có liên quan đến thương mại điện tử là : sự bôi nhọ, xâm phạm bản quyền tác giả (hoặc cản trở đăng ký nhãn hiệu hoặc các quyền vận dụng chất xám khác), khiêu dâm.

 Defamation : Sự xuyên tạc - một người bị kiện sẽ phải chịu trách nhiệm pháp lý cho việc xuyên tạc nếu người này truyền đạt sai lệch và kết quả là làm tổn thất danh dự của người kiện. Sự xuyên tạc có thể xảy ra qua phương tiện truyền thông liên quan đến thị giác hoặc viết, trong trường hợp này bị coi là ***libel*** (xuyên tạc), hoặc xảy ra qua phương tiện truyền miệng hoặc tai nghe, trong trường hợp này nó được gọi là ***slander*** (vu khống).

 Copyright infringement: Xâm phạm quyền tác giả - Để thắng thế được trong các tranh chấp về quyền tác giả, người đi kiện phải chứng minh được (a) quyền sở hữu của một quyền tác giả hợp lệ và (b) người bị kiện đã "sao chép" một nội dung đã được bảo vệ.

 Obscenity: Sự khiêu dâm - Hàng loạt các luật của các bang và chính phủ Hoa Kỳ ngăn cấm phổ biến các tài liệu "khiêu dâm" hoặc "không đứng đắn" khác.

Bởi vì ISP đóng vai trò trong việc truyền và phân phối nội dung, vì vậy : một ISP có thể phải chịu trách nhiệm pháp lý cho việc gây ra thiệt hại hoặc vi phạm, nội dung được gửi đi từ những người đăng ký. Các toà án đã bắt chịu trách nhiệm pháp lý này trong hàng loạt các trường hợp. Tuy nhiên, các cơ quan lập pháp và các toà án vẫn đang cố gắng để định nghĩa mở rộng và các trường hợp trong đó các ISP có thể phải chịu trách nhiệm như vậy.

Vào năm 1991, trường hợp của *Cubby* tranh chấp với *CompuServe.Inc*, toà án miễn cho *CompuServe* phải chịu trách nhiệm đối với một thông báo xuyên tạc được gửi đi từ một trong những người đăng ký của nó. Bởi vì *CompuServed* đã không thực hiện kiểm soát thu thập và xuất bản trên các thông báo được gửi đi trên dịch vụ của nó. Toà án cho rằng *CompuServe* giống như là một quầy bán báo hay một thư viện hơn là một nhà xuất bản và vì vậy không phải chịu trách nhiệm về nội dung xuyên tạc được gửi đi từ những người đăng ký. Nói cách khác, trường hợp của *Stratton Oakmont* tranh chấp với *Prodigy Service Co* vào năm 1995, đã tìm ra rằng dịch vụ *Prodigy* có thể phải chịu trách nhiệm pháp lý cho các thông báo gửi đi xuyên tạc bởi vì nó đã phổ biến và cung cấp các hướng dẫn và thủ tục trình chiếu nội dung.

Với việc chống xâm phạm quyền tác giả, một toà án liên bang vào năm 1993 đã bắt người điều hành tập san phải chịu trách nhiệm pháp lý về việc xâm phạm bản quyền tác giả trên cơ sở là đã phát hành nội dung mà *Playboy Magazine* đã đăng ký bản quyền, thậm chí người điều hành này không biết rằng mình đã xâm phạm bản quyền hay chỉ vô tình xâm phạm tính nguyên bản của nội dung và thực hiện không đúng vai trò trong việc hiển thị và soạn thảo nội dung.

Vào cuối năm 1995, một toà án khác đã không đồng ý với quyết định của *Playboy*. Trong trường hợp này, toà án không bắt *Netcom*, một ISP phải chịu trách nhiệm pháp lý cho việc xâm phạm bản quyền dựa trên cơ sở là Netcom không tiến hành kiểm soát thu thập và xuất bản trên nội dung bị gửi đi. Tuy nhiên, toà án đã nới lỏng trách nhiệm pháp lý thứ hai do vậy Netcom có thể đã góp phần vào việc xâm phạm bản quyền - thông qua những người đăng ký của mình cung cấp các hình thức xâm phạm bản quyền.

Tuy nhiên, các ISP phải đối mặt với một tình thế tiến thoái lưỡng nan là nếu họ hiển thị nội dung, họ có thể phải chịu trách nhiệm pháp lý đối với nội dung mà họ quên xoá hoặc hạn chế, nhưng nếu họ chọn không hiển thị nội dung, họ có thể phải chịu trách nhiệm pháp lý cho việc không làm như vậy. Tất nhiên, nhiều người đăng ký và các lời bào chữa biểu thị các chống đối về việc các ISP soạn thảo nội dung hoặc các nhà cung cấp dịch vụ thành viên thứ ba.

Sự mập mờ của luật pháp đối với trách nhiệm pháp lý thứ hai đối với các ISP - được dàn xếp do tính không chặt chẽ của luật pháp liên quan đến ***underlying*** nguyên nhân của các hành động bạo lực, ví dụ như liên quan đến sự khiêu dâm. Luật pháp còn lâu mới xử lý hết những gì liên quan đến tài liệu khiêu dâm. Ví dụ, Quốc hội Hoa Kỳ thông qua *Communications Decency Act of 1996*, nó được *Bill Clinton* ký thành điều luật vào tháng 2.1996. Mục 223 (a)(1)(B) của Act cung cấp các sắc lệnh chống lại một thành viên, người này "thông qua một thiết bị viễn thông tiến hành, tạo ra, hoặc thu hút và bắt đầu truyền đi bình luận bất kỳ, yêu cầu, giả định, đề xuất, ảnh hoặc tin tức khác về khiêu dâm hoặc thiếu đứng đắn, và những người nhận thông tin này dưới 18 tuổi". Mục 223 (d)(1) của Act cho rằng sẽ trở thành tội ác nếu sử dụng "dịch vụ máy tính tương tác để gửi đi hoặc hiển thị bằng

mọi cách có thể được cho những người dưới 18 tuổi về bình luận bất kỳ, yêu cầu, giả định, đề xuất, ảnh hoặc thông tin khác mà nội dung của nó liên quan đến sex".

Nhiều bang của Hoa kỳ nói đến khiêu dâm thông qua đạo luật. Các luật của bang được sắp xếp theo thứ tự - từ việc mở rộng các luật đã tồn tại dùng ngăn cấm khiêu dâm trẻ em đến việc giới hạn các cuộc truyền điện tử trong một số bang nhằm ngăn chặn các thông báo "với mục đích quấy rối, xúc phạm hoặc làm người khác hoảng sợ". Tại bang Floria, cơ quan lập pháp ban hành một đạo luật - mở rộng luận khiêu dâm trẻ em nhằm bắt các ISP phải chịu trách nhiệm pháp lý đối với việc cho phép người đăng ký của mình vi phạm. Một luật của bang Georgia ban hành năm 1996, phải chịu tội nếu tiến hành các cuộc truyền mạo danh và ký biệt hiệu. Rất tiếc là những ban hành này một lần nữa lại bị dàn xếp do mâu thuẫn về luật. Ví dụ, một người đăng ký tại California có thể gửi một ảnh, được coi là hợp pháp tại California nhưng lại coi là bất hợp pháp tại Georgia. Một người đăng ký và ISP của anh ta hoặc chị ta , cũng như người chủ của anh ta hoặc chị ta có thể tự nhận thấy trách nhiệm pháp lý tại Georgia. Vào tháng 12 năm 1995, *CompuServer* ngừng không cho những người đăng ký truy nhập vào các nhóm tin *Usenet* (như nhóm tin *alt.sex.binaries*.*) do kết quả của sự đe doạ khởi kiện tại Đức cho rằng CompuServer đã vi phạm bộ luật chống khiêu dâm của Đức. Bởi vì *CompuServer* không thể giới hạn các dịch vụ của mình, Đức ngăn cấm toàn bộ những người sử dụng của *CompuServer*. Những điều này làm cho các ISP phải chịu trách nhiệm pháp lý ở hàng loạt các quốc gia và các bang.

Các ISP cố gắng hạn chế khả năng họ có thể phải chịu trách nhiệm pháp lý, như những người tham dự thứ hai, đối với các vi phạm xuyên tạc, xâm phạm bản quyền, phân phối các tài liệu khiêu dâm, hoặc gây tổn hại hoặc xúc phạm thông qua một người đăng ký. Các ISP đối phó lại những rủi ro này bằng cách hạn chế bị vạch trần thông qua thoả thuận ISP. Vì vậy, nhiều thoả thuận ISP tuyên bố rằng các dịch vụ ISP "chỉ có thể được sử dụng cho các mục đích hợp pháp" và "việc truyền các tài liệu bất kỳ mà vi phạm luật phải bị ngăn cấm, gồm có tài liệu đã đăng ký bản quyền, khiêu dâm, hoặc tài liệu được bảo vệ không công khai kinh doanh". Hầu hết các thoả thuận ISP đều có các tuyên bố rõ ràng, ví dụ như *America Online's Services Agreement* (Thỏa thuận về các dịch vụ của America Online) liên quan đến các dịch vụ độc quyền của tổ chức này, gồm có truy nhập Internet :

"AOL,Inc, là một nhà phân phối (không phải là một nhà xuất bản) nội dung, nội dung này được các thành viên thứ ba và hội viên. Cho nên, AOL,Inc không có quyền kiểm soát thu thập và xuất bản đối với nội dung này hơn một thư viện công cộng, hiệu sách, hoặc quầy bán báo".

Trong lĩnh vực này, luật tất nhiên phải trải qua hàng loạt các đề xướng và sửa đổi trước khi các thành viên tham gia thương mại điện tử có thể có được sự tin cậy. Cho tới lúc đó, các thành viên phải tiếp tục thận trọng với 3 mảng đã nêu và tìm hiểu các quyền và trách nhiệm pháp lý cần thiết.

d. Chất lương của thông tin

Các thoả thuận thường quy định rằng việc sử dụng "thông tin, chương trình hoặc dữ liệu bất kỳ thu được từ hoặc thông qua ISP là rủi ro xuất phát từ người đăng ký. Nói chung ISP từ chối trách nhiệm bất kỳ đối với độ chính xác hoặc chất lượng thông tin có được từ các dịch vụ".

e. Việc sử dụng các mạng khác

Hầu hết các thoả thuận ISP uỷ nhiệm cho những người sử dụng- những người này truy nhập vào các mạng khác (các mạng này được kết nối với ISP) phải tuân theo các quy ước của các mạng khác. Do dó, một số thoả thuận ISP nắm giữ trách nhiệm của những người sử dụng đối với việc quyết định xem dữ liệu mà họ tạo ra sẽ được chuyển đi trên các mạng khác hay không.

f. Sử dụng mang tính chất thương mại và bán lại các dịch vụ

Khi Internet trở nên thương mại hoá , các thoả thuận có khuynh hướng là "việc sử dụng [ISP] cho các mục đích thương mại được thừa nhận (cấp phép) và khuyến khích". Tuy nhiên, các thoả thuận cũng cho rằng "kết nối chỉ được cung cấp cho tổ chức của bạn" và "việc bán lại kết nối IP trực tiếp cho đối tượng khác phải bị ngăn chặn". Các ranh giới trong dịch vụ thương mại và khách hàng trên Internet tiếp tục được đưa ra.

g. An toàn

Như đã trình bày từ trước, tính an toàn được cung cấp thông qua xương sống Internet bị giới hạn rất nhiều; tuy nhiên, các ISP càng ngày càng cố gắng thoái thác trách nhiệm của mình đối với các thoả hiệp an toàn. Nhận thấy nghĩa vụ của người sử dụng cuối đối với an toàn ngày càng trở nên quan trọng - nên các phát hành an toàn thông tin phải được đưa ra thật chi tiết trong các thoả thuận ISP.

Một số thoả thuận ISP gồm có kiến thức hiểu biết của một khách hàng về "Internet vốn đã không an toàn và [ISP] không thể bảo vệ chống lại sự vi phạm về an toàn, sự vi phạm an toàn này do một con người tạo ra trên Internet (bên ngoài ISP)". Mặc dù, không rõ ràng lắm đối với phạm vi trong đó một ISP có thể thoái thác trách nhiệm pháp lý của mình bằng cách sử dụng các kiến thức hiểu biết như vậy, chúng trở nên phổ biến và các ISP trở nên thận trọng khi tính đến chúng. Một số thoả thuận ISP đồng ý cung cấp an toàn tại "mức công nghiệp được quy định hiện thời". Bởi vì (1): nó giả thiết ở đây có một chuẩn như vậy; và (2) : ở đây chỉ có một mức an toàn là đủ nếu nó tồn tại.

Các ISP yêu cầu các khách hàng duy trì một mật khẩu an toàn - mật khẩu an toàn này được sử dụng để truy nhập vào các ***account*** của họ và thay đổi mật khẩu của họ định kỳ. Các khách hàng ngăn chặn việc sử dụng các dịch vụ của ISP để thu được các mật khẩu của họ và từ đó thực hiện các cố gắng trái phép nhằm truy nhập vào các hệ thống và các mạng khác. Một số ISP linh hoạt đồng ý kiểm tra các file mật khẩu của họ định kỳ - nếu ISP phá vỡ thành công một mật khẩu bất kỳ, nó sẽ cảnh báo cho khách hàng và đề nghị hoặc yêu cầu khách hàng thay đổi nó. Các khách hàng thường được yêu cầu hạn chế chia xẻ mật khẩu của mình cho người khác. Tương tự, nếu phát hiện ra hoạt động khả nghi, một số ISP thay đổi mật khẩu của khách hàng một cách đơn phương và cảnh báo cho khách hàng.

Cuối cùng, mặc dù sớm tìm ra cơ sở hạ tầng khoá công khai được đưa ra trong các thoả thuận ISP, thì việc tạo, bảo đảm, sử dụng, ngừng và huỷ bỏ các chứng chỉ khoá công khai sẽ được đưa ra một ngày gần đây trong các thoả thuận ISP bởi vì các dịch vụ quản lý chứng chỉ sẽ được gắn liền với phần mềm và dịch vụ ISP.

h. Sự lạm dụng

Hàng loạt các hoạt động, củng cố thêm cho phạm trù "lạm dụng", được ngăn chặn thông qua các thoả thuận ISP. Những hoạt động này rõ ràng là bất hợp pháp. Các ví dụ về các kiểu tác động gồm có : không gửi một thông báo mà chất thành đống (bao gồm việc buộc chặt các bức thư) để thay đổi linh tinh các nhóm tin tức và danh sách thư tín (***spamming***), gửi từng đoạn thư tín điện tử, gửi các quảng cáo không thích hợp, gửi các tài liệu không thích hợp vào một danh sách thư tín, sinh nhiều quá trình không cần thiết, chúng tiêu phí bộ nhớ thừa hoặc các nguồn tài nguyên của bộ vi xử lý cho các giai đoạn dài và, đối với các hệ thống phi thương mại, việc lãng phí gắn liền khi không sử dụng mạng.

Các cung cấp lạm dụng trong các thoả thuận ISP thông thường tập trung vào các hoạt động quấy nhiễu, phá hoại, hoặc các hoạt động bất hợp pháp bất kỳ (hoặc thử hoặc thành công), gồm có :

- Truy nhập thông tin mà không cần sự cho phép.
- Áp dụng hoặc sử dụng một mật khẩu lừa đảo.
- Có được một mức cao hơn của đặc quyền truy nhập mà không cần quyền riêng.
- Sao chép các file hệ thống.
- Tạo, sử dụng, hoặc phân phối phần mềm chủ tâm gây hại.
- Giải mã các file mật khẩu của người sử dụng hoặc hệ thống.

 Xoá, khảo sát, sao chép, hoặc sửa đổi các file và/hoặc dữ liệu thuộc sở hữu của những người sử dụng khác mà không được đồng ý trước.

 Tránh hoặc thay đổi hạn nghạch (***quota***) của các nguồn tài nguyên.

 Làm giả các thông báo.

  Phá huỷ các chương trình hoặc các hệ thống mạng.

 Gửi hoặc sử dụng tài liệu có đăng ký bản quyền mà không được sự cho phép.

 Chia xẻ, làm lộ, hoặc thoả hiệp các mật khẩu hoặc các xác thực khác.

i. Các cung cấp khác

Các cung cấp khác trong một thoả thuận ISP có thể bao gồm như sau :

 Availablity : Tính sẵn sàng - Một số ISP không đảm bảo được tính sẵn sàng của các dịch vụ của mình và thường cung cấp dứt khoát do vậy các gián đoạn ứng dụng không làm ảnh hưởng các khách hàng mà họ cung cấp.

 Access to user's private data : Truy nhập vào dữ liệu riêng của người sử dụng - Một số thoả thuận ISP ngăn cấm ISP truy nhập vào các file riêng của người sử dụng bất kỳ trừ khi các file này đe doạ tính toàn vẹn ISP của hệ thống mà ISP sở hữu hoặc Internet. Trong các trường hợp như vậy, thoả thuận ISP thường cho phép ISP truy nhập vào các file riêng chỉ sau khi đã (ít nhất) thực hiện liên lạc với khách hàng.

 Account termination*:* Kết thúc *account* - Thỉnh thoảng một số thoả thuận ISP quy định rằng việc sử dụng của Internet là một đặc quyền, không phải là một quyền, và việc sử dụng không thích hợp này có thể bị mất đặc quyền này. Trong các trường hợp này, ISP sẽ thấy được những gì bị coi là sử dụng không thích hợp và quyết định cuối cùng là ở nó. Một số thoả thuận ISP cho phép ISP đóng hoặc đình chỉ một *account* của người sử dụng xác định, có thể hoặc không báo trước hoặc giải thích nguyên nhân. Các thỏa thuận ISP thường quy định như sau : một khách hàng kết thúc một *account* bằng cách gửi một yêu cầu cho ISP. Khách hàng chịu trách nhiệm về tất cả các phí phát sinh cho tới thời hạn kết thúc, trừ khi ISP không có khả năng cung cấp các dịch vụ do sự xơ suất của khách hàng.

 Term: Mục - Các thoả thuận ISP thường quy định rằng họ sẽ giữ nguyên hiệu lực cho đến khi khách hàng kết thúc *account* của anh ta hoặc chị ta, hoặc cho đến khi ISP đình chỉ *account*.

 Amendments: Các bổ xung - Hầu hết các thoả thuận ISP cho phép bổ xung vào các mục và các điều kiện, gồm có các thay đổi trong giá cả, thay đổi các dịch vụ yêu cầu, chỉ dẫn cho người đăng ký (xuất bản trực tuyến và bằng dạng văn bản). Thời hạn có hiệu lực của các thay đổi như vậy được khách hàng chấp nhận và sử dụng.

 Fees: Các chi phí phát sinh - Những người đăng ký thường được gửi hóa đơn thanh toán hàng tháng. Việc chi trả (thường dựa trên một cơ sở được uỷ quyền trước) thông qua thẻ tín dụng và các chuyển nhượng quỹ điện tử là điều không còn là mới nữa.

 Disclaimer of warranties: Từ chối các bảo đảm - Phù hợp với việc lớn mạnh không ngừng tập trung vào nội dung thông tin, nhiều thoả thuận ISP có chứa các từ chối đảm bảo ví dụ như sau :

" Các dịch vụ cũng như các tài liệu và thông tin bạn tìm thấy trong các cơ sở dữ liệu của ISP được cung cấp mà không có đảm bảo, gồm có : không có giới hạn đảm bảo đối với thông tin, các dịch vụ và các sản phẩm mà được cung cấp thông qua hoặc trong kết nối với các dịch vụ của ISP và các đảm bảo bất kỳ về khả năng bán được, sự phù hợp đối với một mục đích riêng, mong đợi của cá nhân hoặc sự không vi phạm ."

Như vậy, cách thức tốt nhất của một khách hàng trong trường hợp không thoả mãn là sự kết thúc.

 Limitation of liability : Giới hạn của trách nhiệm pháp lý- Cũng phù hợp với ISP tập trung vào các phát hành nội dung trong các từ chối đảm bảo, một thoả thuận ISP có thể từ chối trách nhiệm đối với :

"bất kỳ thiệt hại hoặc tổn thương nào bị gây ra do sai lầm khi thực thi, lỗi, bỏ quên, ngắt, xoá bỏ, sai sót, trì hoãn trong điều hành hoặc truyền, virut máy tính, lỗi đường truyền, trộm hoặc phá hoại hoặc truy nhập trái phép, sửa đổi, hoặc sử dụng các bản ghi, hoặc không liên lạc, tác động không trung thực, sơ xuất, hoặc các nguyên nhân hoạt động khác. Khách hàng nhận thức được rằng ISP không chịu trách nhiệm pháp lý đối với việc mất danh dự của khách hàng, đối với các tài liệu bất hợp pháp và ISP cho phép mình có quyền loại bỏ các tài liệu như vậy mà không phải chịu trách nhiệm pháp lý. "

 Indemnification: Sự bồi thường - Các cung cấp này nói rõ rằng khách hàng đồng ý bồi thường hoặc bảo vệ ISP khỏi các mất mát bất kỳ hoặc có quyền đòi bồi

thường từ việc sử dụng các dịch vụ của khách hàng mà gây ra thiệt hại cho khách hàng hoặc thành viên thứ ba.

8. Tổng kết

An toàn Internet gồm có các giải pháp an toàn có tính chất kỹ thuật trong 3 mảng khác nhau : an toàn mạng, an toàn ứng dụng và an toàn hệ thống. An toàn mạng là hình thức bảo vệ quá trình thông qua các mục dữ liệu được truyền thông từ một hệ thống cuối mạng tới một hệ thống cuối mạng khác. An toàn ứng dụng gồm có các bộ phận bảo vệ an toàn, được xây dựng thành một ứng dụng riêng và hoạt động độc lập với các biện pháp an toàn mạng bất kỳ. An toàn hệ thống liên quan đến hình thức bảo vệ của một mạng cuối và nó là môi trường cục bộ không quan tâm đến bảo vệ truyền thông được tạo ra thông qua các biện pháp an toàn mạng và an toàn ứng dụng.

Như một phần của an toàn mạng, giao thức tầng mạng Internet (IP) mở rộng thêm hai kỹ thuật. Kỹ thuật *Authentication Header* cung cấp bảo vệ xác thực và tính toàn vẹn cho một *IP datagram*. Kỹ thuật mã hoá gói (được gọi là *Encapsulating Security Payload*) cung cấp bảo vệ tin cậy và tính toàn vẹn. Các tuỳ chọn quản lý khoá khác nhau đã có sẵn và theo thứ tự từ phân phối khoá thủ công đến cơ sở hạ tầng khoá công khai.

Một bức tường lửa (*firewall*) bảo vệ một mạng khỏi các đe doạ xuất hiện trong kết nối từ mạng này sang mạng khác. Thông thường, một bức tường lửa được xây dựng giữa mạng cục bộ của một tổ chức và xương sống Internet. Các bức tường lửa có thể hạn chế và kiểm soát khả năng tải trên mạng. Chúng có hàng loạt các kỹ thuật bảo vệ như là : các hệ thống lọc gói mức mạng và các hệ thống uỷ quyền mức ứng dụng. Có thể xây dựng được một mạng ảo trong đó các *site* của mạng truyền thông với các *site* khác, thông qua xương sống Internet, cùng với sự tin tưởng rằng khả năng tải của mạng riêng không phải là điểm yếu dễ bị tấn công bởi các tấn công bên ngoài.

Gửi tin Internet, gồm có thư tín điện tử, có thể được bảo vệ bằng cách sử dụng hàng loạt các giao thức bảo vệ mức ứng dụng, ví dụ như : *Privacy Enhanced Mail (PEM), MIME Object Security Services (MOSS, S/MIME, Pretty Good Privacy (PGP), X400 Security, và Message Security Protocol (MSP) của chính phủ Hoa kỳ*. Tất cả các giao thức cung cấp các dịch vụ bảo vệ cơ bản như xác thực nguồn gốc thông báo, tính tin cậy nội dung, tính toàn vẹn nội dung, hỗ trợ cho việc chấp nhận nguồn gốc thông qua một chữ ký số. Một số giao thức cung cấp thêm các dịch vụ an toàn. S/MIME có vẻ như được chấp nhận về mặt thương mại lớn nhất.

Các truyền thông World Wide Web cũng yêu cầu bảo vệ mức ứng dụng, nhằm bảo vệ chống lại các đe doạ như số thẻ tín dụng bị phát hiện thông qua nghe trộm hoặc thiết lập các Web site của các nhà cung cấp giả mạo. Hai giao thức Web

an toàn chiếm ưu thế là giao thức *Secure Sockets Layer (SSL)* và giao thức *Secure HTTP (S-HTTP)*. Các giao thức này cung cấp bảo vệ xác thực thực thể, bảo vệ tin cậy, tính toàn vẹn của các truyền thông máy khách-máy chủ trên Web (trong một trường hợp, với một tuỳ chọn cho các dịch vụ chấp nhận). Tập trung đặc biệt vào việc sử dụng phần mềm có thể tải xuống được, như xảy ra với các hệ thống ActiveX và Java; phần mềm này có thể được ký hiệu số và phê chuẩn trước khi sử dụng.

Các giao dịch EDI gửi đi qua Internet có thể được bảo vệ bằng cách sử dụng các tuỳ chọn an toàn có trong khuôn dạng thông báo EDI và /hoặc một giao thức gửi tin an toàn Internet.

Các đặc tính *Secure Electronic Transaction (SET)* , được Visa và MasterCard phát triển, định nghĩa một giao thức và cơ sở hạ tầng hỗ trợ cho các thanh toán thẻ ngân hàng như là một phần bảo vệ dịch vụ hoặc mua bán điện tử trên Internet. Kỹ thuật khoá công khai được sử dụng để xác thực hàng loạt các thành viên, gồm có (*cardholder*) người nắm giữ thẻ, (*merchant*) các nhà buôn và các tổ chức *acquier* , và để bảo vệ thông tin thanh toán nhạy cảm khỏi bị lộ trên Internet hoặc trong các hệ thống nhà buôn.

Thêm vào việc áp dụng các cung cấp an toàn mang tính chất kỹ thuật thích hợp, những người sử dụng Internet phải chú trọng vào các bảo vệ hợp pháp của họ như đã được đưa ra trong các thoả thuận của nhà cung cấp dịch vụ Internet. Các thoả thuận này thay đổi đáng kể trong các mục cung cấp đã đưa ra. Các cung cấp này bao gồm sử dụng và chấp nhận, các định nghĩa dịch vụ, sử dụng hợp pháp và nhà cung cấp kiểm soát trên nội dung thông tin, sử dụng các mạng khác, sử dụng mang tính chất thương mại, bán lại các dịch vụ, an toàn, lạm dụng, sẵn sàng, truy nhập vào dữ liệu riêng của người sử dụng, kết thúc, giới hạn, thay đổi các mục, phí phát sinh, từ chối đảm bảo, và các giới hạn trách nhiệm pháp lý.

CHƯƠNG 2. NHU CẦU THỰC TẾ VỀ BẢO MẬT

1. Về tình hình phát triển của CNTT trên thế giới

Về hệ thống thông tin: chưa có thời kỳ nào trong lịch sử mà những biến động trong xã hội loài người lại mạnh mẽ, sâu sắc và nhanh chóng như hiện nay. Nhiều khái niệm, cũng như quy tắc hoạt động, ứng xử đang thay đổi; buộc con người phải đổi mới tư duy, phải hành động nhanh, "làm việc theo tốc độ của tư duy".

Công nghệ thông tin được ứng dụng rộng rãi trong mọi lĩnh vực, mạng thông tin đa phương tiện phủ khắp nước, nối với hầu hết các tổ chức, các gia đình. Thông tin trở thành tài nguyên quan trọng nhất của nền kinh tế. Để tận hưởng được cơ hội, vượt qua thách thức, rút ngắn khoảng cách với các nước phát triển, hầu hết quốc gia đã hoạch định và thực hiện các chiến lược phát triển kinh tế tri thức, trong đó đổi mới và số hoá bộ máy nhà nước, làm cho bộ máy hoạt động nhanh nhạy hơn, linh hoạt hơn và có trách nhiệm hơn là một trong những nhiệm vụ ưu tiên.

Nhiều nước gọi quá trình đổi mới và số hoá bộ máy điều hành, quản lý và dịch vụ của nhà nước là quá trình xây dựng chính phủ điện tử (e-Government) hay chính quyền điện tử (e-Governance). Quá trình này nhằm tạo ra một nhà nước phù hợp với xu thế phát triển mới, có khả năng điều hành nhanh, nhạy và hiệu quả hơn; ra quyết định kịp thời và chính xác hơn; hoạt động minh bạch, tiết kiệm và dân chủ hơn; đặc biệt là có hệ thống dịch vụ công tốt hơn, thuận tiện hơn và bình đẳng hơn đối với mọi người dân.

Xây dựng chính phủ điện tử, tin học hoá quản lý nhà nước trước tiên nhằm phục vụ việc nâng cao hiệu quả của các hoạt động bên trong của các cơ quan nhà nước (tin học hoá hướng vào trong). Song tin học hoá không chỉ đơn giản là sử dụng công nghệ thông tin để tự động hoá các quá trình đang tồn tại. Công nghệ thông tin đã tạo ra khả năng trao đổi và liên kết các tổ chức, các cá nhân lại với nhau và từ đó có thể hỗ trợ cho việc tổ chức lại các quá trình hoạt động.

Như vậy, tin học hoá tạo điều kiện cho nhà nước tiến hành những thay đổi trong cấu trúc tổ chức và xây dựng các dịch vụ phục vụ công cộng, nhằm hoàn thiện mối quan hệ của chính phủ với cộng đồng bên ngoài, đặc biệt là với các doanh nghiệp và nhân dân. Mục tiêu của tin học hoá không chỉ là tin học hoá các cơ quan nhà nước, mà điều quan trọng là nó sẽ mang lại một mô hình mới của chính phủ (một phần quan trọng của cải cách hành chính) hiệu quả hơn thông qua việc ứng dụng công nghệ thông tin.

Nhiều nước coi quá trình đổi mới và điện tử hoá chính phủ là nhiệm vụ ưu tiên hàng đầu, có ý nghĩa đột phá, thậm chí có ý nghĩa sống-còn đối với quốc gia nên đã tập trung đầu tư, thực hiện quyết liệt những kế hoạch chiến lược, quyết sách quốc gia, xây dựng chính phủ điện tử, đưa đất nước đi nhanh vào quá trình hội nhập và kinh tế tri thức.

Tuy nhiên, do mục tiêu chính trị, kinh tế, xã hội và điều kiện, hoàn cảnh cụ thể về lịch sử, văn hoá, truyền thống, phong tục tập quán, phương thức điều hành quản lý của các quốc gia rất khác nhau nên việc tiếp cận, ứng dụng công nghệ thông tin để đổi mới, tin học hoá bộ máy quản lý điều hành cũng rất khác nhau. Không thể rập khuôn các mô hình đã thành công, hay đơn giản chỉ mua công nghệ rồi áp dụng một cách máy móc, thực hiện việc "chuyển giao công nghệ" là xong. Càng không thể kỳ vọng một ai đó đi trước, phát triển hơn, nhiều kinh nghiệm hơn đến "làm thay", "làm hộ". Điều quan trọng hơn là các quốc gia phải tự tìm cho mình chiến lược riêng, lựa chọn cách tiếp cận phù hợp với điều kiện, hoàn cảnh của đất nước mình, phát huy trí tuệ sáng tạo, và năng lực nội sinh để chuyển hoá, thích nghi, cải tiến những kết quả, thành tựu khoa học công nghệ của thế giới thành những sản phẩm phục vụ cho chính mình, đáp ứng thực sự có hiệu quả những nhu cầu của quá trình đổi mới, cải cách quản lý hành chính nhà nước, phục vụ đúng, trúng, hiệu quả mục tiêu xây dựng một nhà nước trong sạch, vững mạnh, đủ sức ra những quyết sách thông minh đưa đất nước vượt qua những thử thách, khó khăn, tận dụng thời cơ của quá trình hội nhập, đi nhanh vào kinh tế tri thức. Vì vậy, việc nghiên cứu phát triển hoàn thiện các hệ thống thông tin

phục vụ điều hành quản lý nhà nước theo đặc thù, bản sắc riêng của mỗi quốc gia có ý nghĩa hết sức quan trọng và cấp thiết.

Về công nghệ: Những công nghệ phục vụ cho quá trình hình thành và phát triển chính phủ điện tử công phát triển rất nhanh: công nghệ truyền thông, Internet, các phần mềm xây dựng cơ sở dữ liệu, phần mềm quản lý và tự động hoá công tác văn phòng, công nghệ GIS, multimedia, teleconferencing, công nghệ nén truyền dữ liệu, công nghệ an toàn, bảo mật thông tin, đặc biệt là thương mại điện tử... chỉ trong thời gian ngắn đã có những bước tiến rất dài và vẫn đang tiếp tục phát triển rất nhanh.

Sự phát triển nhanh chóng của kỹ thuật truyền thông đã đưa đến những chuyển biến cơ bản trong công nghệ thiết lập các mạng tin học và hình thành siêu lộ thông tin. Từ thập niên 90 đến nay, mạng Internet đã có sự phát triển bùng nổ với tốc độ trên 12% mỗi tháng. Các dịch vụ trao đổi và cung cấp thông tin ngày càng thuận tiện và phong phú. Việc quản trị và khai thác các hệ thống thông tin, các cơ sở dữ liệu ngày càng phát triển không chỉ theo hướng hoàn thiện các chức năng sắp xếp, lựa chọn tìm kiếm dữ liệu mà còn đang phát triển rất mạnh các chức năng thông minh hơn như tổng hợp, phân tích, khai phá dữ liệu để kết xuất thông tin với hàm lượng trí tuệ ngày càng cao, hỗ trợ các quá trình ra quyết định ngày càng hiệu quả. Theo hướng này, những phần mềm quản trị cơ sở dữ liệu như SQL, Oracle, Informic,... vẫn đang được phát triển với những chức năng, công dụng ngày càng phong phú và hiệu quả. Cùng với sự phát triển như vũ bão của máy tính, những công nghệ liên quan đến các hệ thống thông tin dữ liệu bản đồ (GIS-geographical information system), đa phương tiện (multimedia), hội nghị từ xa (teleconferecing), học tập từ xa (distance learning) cũng được ứng dụng khá rộng rãi và hiệu quả trong các hoạt động điều hành, quản lý.

Cuối những năm 1980 công ty Digital Equipment đưa ra sản phẩm phần mềm ứng dụng trong công tác văn phòng đóng gói chung tất cả (all-in-one) nhằm gộp các chức năng xử lý văn bản, thư tín điện tử và cơ sở dữ liệu vào một ứng dụng. Thế hệ sau của các phần mềm văn phòng tập trung vào các tiêu chuẩn mở và các nhà cung cấp cố

gắng để chiếm thị trường trên cơ sở đưa ra những phần mềm ứng dụng theo chuẩn chung, vì vậy khả năng trao đổi thông tin, sử dụng những phần mềm ứng dụng giữa các chủng loại máy có những bước tiến đáng kể.

Những phần mềm làm việc theo nhóm (Groupware) là công nghệ hiệu suất hoạt động của nhóm, tăng cường và tạo điều kiện cho quá trình hợp tác của một tổ chức. Groupware giúp cho các nhóm làm việc tốt hơn về mọi phương diện, cho dù nhóm công tác ở cùng một chỗ, hay khác chỗ, khác thời gian. Những phần mềm groupware tương đối phổ cập cho công tác tự động hoá văn phòng là: Teamware Office, Microsoft O ffice, Lottus Smartsuite, Novell Groupwise, Microsoft Exchangr, Lotus Note, Eudora Pro... Những phần mềm này càng ngày càng quen thuộc với người sử dụng và luôn luôn được phát triển với mức độ thuận tiện ngày càng cao, với tính năng ngày càng nhiều và cuộc chạy đua bất phân thắng bại vẫn đang tiếp tục diễn ra sôi nổi trên thế giới do mỗi loại phần mềm chỉ phù hợp tốt nhất một số mục tiêu, yêu cầu cụ thể.

Những công nghệ GIS, multimedia, teleconferencing, distant learning cùng với sự phát triển mạnh mẽ của công nghệ viễn thông, Internet 2 và những công nghệ nén, truyền đang tạo ra những khả năng mới trong hệ thống điều hành quản lý của nhà nước không chỉ dựa trên những loại hình thông tin văn bản truyền thống mà cả những loại hình thông tin mới rất đa dạng, phong phú như bản đồ, âm thanh, hình ảnh, tiếng nói...

Những công nghệ quét, nhận dạng chữ viết, tiếng nói, dịch tự động... cũng đang ngày càng hoàn thiện tạo khả năng hoàn toàn hiện thực cho một văn phòng không giấy.

Những công nghệ liên quan đến an toàn, bảo mật thông tin như tường lửa (firewwall), chữ ký điện tử, mã hoá dữ liệu, mạng dùng riêng ảo (VPN - Virtual Private Network), chống virus, lưu cất... cũng đang được coi là hướng quan trọng được ưu tiên đầu tư nghiên cứu và đang phát triển hết sức phong phú, đa dạng.

2. Tình hình phát triển CNTT trong nước

Về hệ thống thông tin: Năm 1993 chính phủ ra Nghị quyết 49/CP nhằm xác định chính sách phát triển và ứng dụng công nghệ thông tin ở nước ta trong những năm 90.

Kế hoạch tổng thể phát triển công nghệ thông tin ở nước ta giai đoạn 1996-2000 tập trung vào hai nội dung chủ yếu là phát triển các nguồn tiềm lực và xây dựng kết cấu hạ tầng về công nghệ thông tin và thực hiện các dự án tin học hoá chủ chốt trong quản lý nhà nước và trong các lĩnh vực phát triển kinh tế xã hội, ứng dụng công nghệ thông tin trong sự nghiệp công nghiệp hoá và hiện đại hoá nền sản xuất và kinh tế của nước ta.

Nhờ kết quả thực hiện các dự án này trong thời gian qua chúng ta đã bước đầu xây dựng được cơ sở hạ tầng kỹ thuật cho việc ứng dụng trong quản lý nhà nước và các hoạt động chuyên ngành. Trên cơ sở đó đã tổ chức triển khai từng bước xây dựng các hệ thống thông tin phục vụ cho các hoạt động quản lý nhà nước. Qua quá trình triển khai này, nhận thức của toàn xã hội trong việc phát triển và ứng dụng công nghệ thông tin đã được nâng cao một bước. Một số kết quả chính đã đạt được trong lĩnh vực này là:

Các dự án ứng dụng công nghệ thông tin trong các cơ quan Đảng:

Các hoạt động tin học hoá hệ thống thông tin của các cơ quan Đảng được bắt đầu triển khai từ năm 1998. Để triển khai các ứng dụng công nghệ thông tin trong các cơ quan Đảng, các công việc sau đã được tiến hành:

Đã thiết kế và triển khai kết nối mạng thông tin diện rộng của hệ thống các cơ quan Đảng. Tới nay đã xây dựng hạ tầng kỹ thuật công nghệ thông tin tối thiểu cho hệ thống các cơ quan Đảng, kết nối và trao đổi thông tin thường xuyên giữa 61 tỉnh, thành uỷ và 16 cơ quan Đảng trực thuộc Trung ương trên cơ sở ứng dụng phần mềm Lotus Notes.

Đã xây dựng hệ thống các phần mềm ứng dụng (gửi nhận văn bản, lưu trình xử lý văn bản, quản lý cán bộ, quản lý tài chính, tài sản...) và hệ thống cơ sở dữ liệu (CSDL văn kiện, CSDL cán bộ, CSDL lưu trữ...) dùng chung thống nhất trong hệ thống các cơ quan Đảng. Xây dựng và phát hành thường xuyên trên Internet Website Đảng cộng sản Việt Nam, đến nay đã có khoảng 7 vạn trang tin.

Tổ chức thường xuyên đào tạo phổ cập và nâng cao kiến thức, năng lực ứng dụng công nghệ thông tin cho các cán bộ lãnh đạo, chuyên viên và cán bộ quản trị mạng trong hệ thống các cơ quan Đảng. Đã đào tạo nên 2000 lượt người tại khu vực Trung ương.

Xây dựng hệ thống quy chế, quy trình công tác, chuẩn thông tin và bảo mật thông tin. Đã ban hành thống nhất quy chế sử dụng và khai thác thông tin trên mạng thông tin diện rộng của Đảng.

Các dự án ứng dụng công nghệ thông tin tại Văn phòng Quốc hội:

Từ năm 1996 đến năm 2000, Văn phòng Quốc hội đã bước đầu xây dựng được hạ tầng cơ sở công nghệ thông tin bao gồm:

Thực hiện Dự án xây dựng mạng máy tính tại trụ sử Văn phòng Quốc hội do Liên minh Quốc hội thế giới và tổ chức SIDA Thụy Điển tài trợ (Dự án IPU/SIDA).

Đã xây dựng được một mạng máy tính trung tâm tại trụ sở Văn phòng Quốc hội 35 Ngô Quyền và một mạng máy tính nhỏ tại Hội trường Ba Đình.

Xây dựng mạng thông tin nội bộ (Intranet) của Văn phòng Quốc hội.

Xây dựng một số chương trình ứng dụng và cơ sở dữ liệu phục vụ các hoạt động của Quốc hội

Dự án Tin học hoá Hệ thống thông tin Văn phòng Chính phủ:

Mục tiêu của Dự án này là ứng dụng công nghệ thông tin nhằm hiện đại hoá hệ thống thông tin tại Văn phòng Chính phủ. Dự án

được triển khai sớm ngay từ đầu những năm 90 đạt được một số kết quả tốt, bước đầu xây dựng mạng thông tin tại Văn phòng Chính phủ. Một số phần mềm ứng dụng như các phần mềm quản lý hồ sơ công việc Chính phủ, gửi nhận văn bản, quản lý đơn thư khiếu tố, các cơ sở dữ liệu về văn bản quy phạm pháp luật, về các dự án đầu tư, về thông tin chính phủ... hoạt động tốt trên mạng này.

Cuối năm 1997, đã tiến hành xây dựng mạng thông tin diện rộng của Chính phủ nhằm kết nối mạng của Văn phòng chính phủ với các mạng tại văn phòng Uỷ ban nhân dân các tỉnh và các cơ quan chính thức đưa vào hoatj động từ 1-1-1998 kết nối đến văn phòng Uỷ ban nhân dân 61 tỉnh và 33 cơ quan bộ, ngành. Qua mạng đã tiến hành trao đổi các loại văn bản quy phạm pháp luật của chính phủ, các báo cáo văn bản từ các địa phương và bộ, ngành. Đồng thời, Trung tâm tin học Văn phòng chính phủ đã cho vận hành một số chương trình ứng dụng tren mạng. Sau hai năm hoạt động đã có hơn 7000 văn bản quy phạm pháp luật được cập nhật vào cơ sở dữ liệu công báo của chính phủ, hơn 20.000 văn bản do văn phòng chính phủ phát hành được quản lý trên mạng của văn phòng chính phủ. Trong năm 1988 đã có gần 3000 báo cáo, văn bản từ các Bộ, ngành, địa phương gửi đến mạng văn phòng chính phủ và qua mạng diện rộng được chuyển tải đến tất cả các cơ quan hành chính đã kết nối vào mạng này.

Các dự án tin học hoá quản lý nhà nước tại các bộ, ngành, các tỉnh, thành phố:

Nội dung chủ yếu của các Dự án tin học hoá quản lý nhà nước tại các Bộ, Ngành, các tỉnh, thành phố trực thuộc trung ương là xây dựng các hệ thống thông tin phục vụ quản lý nhà nước trên cơ sở trang bị kiến trúc tối thiểu ban đầu về cơ sở hạ tầng kỹ thuật công nghệ thông tin và tiến hành đào tạo cán bộ, kể cả cán bộ chủ chốt, theo các chương trình thích hợp nhằm cung cấp các kiến thức tin học cần thiết, để tuỳ theo chức năng mà thực hiện các nhiệm vụ chỉ đạo, quản lý, sử dụng hoặc vận hành các hệ thống thông tin đó. Các dự án được tiến

hành thực hiện đồng thời tại hầu hết các Bộ, Ngành, Cơ quan thuộc Chính phủ và tại tất cả 61 tỉnh, thành phố trực thuộc Trung ương.

Đến nay từ các dự án tin học hoá quản lý nhà nước đã có hơn 100 mạng máy tính cục bộ (mạng LAN) với quy mô lớn nhỏ khác nhau được thiết lập hoặc nâng cấp tại 61 văn phòng Uỷ ban nhân dân các Tỉnh, thành phố và 52 Bộ, Ngành, đoàn thể với hơn 600 máy chủ và trên 10.000 máy trạm. Đã có 94 mạng LAN kết nối vào Mạng diện rộng của chính phủ, khoảng trên 30 mạng diện rộng (mạng WAN) địa phương (nối Văn phòng Uỷ ban nhân dân Tỉnh với các Sở, huyện), gần 20 mạng diện rộng chuyên ngành nối cơ quan Bộ với các đơn vị trực thuộc. Nhiều cơ quan đang thực hiện thường xuyên công việc trao đổi thông tin trong nội bộ qua mạng LAN, hoặc với các cơ quan khác qua mạng WAN. Các mạng LAN được sử dụng để trao đổi thư tín và chia sẻ tài nguyên, thông tin chung dưới những hình thức đơn giản.

Trên cơ sở trang bị kỹ thuật, các cơ quan quản lý nhà nước tại các Tỉnh, thành phố, các Bộ, Ngành đã triển khai một số chương trình phần mềm với các chức năng quản lý khác nhau như: hệ điều hành tác nghiệp (quản lý văn bản vào-ra, hồ sơ công việc), quản lý nhân sự, cơ sở dữ liệu tổng hợp về tình hình kinh tế xã hội của Tỉnh, một số cơ sở dữ liệu theo các chuyên môn nghiệp vụ... Hiệu quả sử dụng các phần mềm này tại các đơn vị ở các mức độ khác nhau.

Các dự án xây dựng cơ sở dữ liệu quốc gia:

Hệ thống các cơ sở dữ liệu quốc gia là một bộ phận cấu thành đặc biệt quan trọng của cơ sở hạ tầng thông tin để từng bước hình thành một xã hội thông tin. Từ năm 1996, Ban chỉ đạo chương trình quốc gia về công nghệ thông tin đã tiến hành xây dựng dự án tổng thể phân tích tính khả thi để lựa chọn xây dựng 6 cơ sở dữ liệu quốc gia trong giai đoạn 1996-2000. Đó là: cơ sở dữ liệu quốc gia Thống kê kinh tế - xã hội; Cơ sở dữ liệu quốc gia Tài chính - Ngân sách; Cơ sở dữ liệu quốc gia Tài nguyên đất; cơ sở dữ liệu quốc gia công chức, viên chức và các đối tượng hưởng chính sách; Cơ sở dữ liệu quốc gia Dân cư và Cơ sở dữ liệu quốc gia Luật và các văn bản pháp quy. Cuối

năm 1998, cả 6 dự án khả thi đã được Hội đồng thẩm định kỹ thuật đánh giá và xếp loại đạt yêu cầu, và được các Bộ, Ngành chủ trì phê duyệt. Từ tháng 6/1999 đã có 4 đơn vị (Tổng cục thống kê, Bộ Tư pháp, Tổng cục địa chính , Uỷ ban dân số và kế hoạch hoá gia đình đã thử tích hợp kỹ thuật và tổ chức khai thác.

Nhờ kết quả thực hiện các dự án này trong thời gian qua đã bước đầu xây dựng được cơ sở hạ tầng kỹ thuật cho việc ứng dụng CNTT trong quản lý nhà nước và các hoạt động chuyên ngành. Trên cơ sở đó đã tổ chức triển khai từng bước xây dựng các hệ thống thông tin phục vụ cho các hoạt động quản lý nhà nước.

Qua quá trình triển khai này, nhận thức của toàn xã hội trong việc phát triển và ứng dụng CNTT đã được nâng cao một bước, tạo thói quen soạn thảo, tra cứu văn bản và trao đổi thông tin qua mạng trong một bộ phận cán bộ, công chức. Một số CSDL và phần mềm chuyên ngành bước đầu đã giúp cho việc nâng cao hiệu suất công tác nghiệp vụ.

Tuy nhiên các hệ thống thông tin được xem xét, phân tích, thiết kế, xây dựng độc lập, trong khi giữa các hệ thống thông tin quốc gia nêu trên đòi hỏi phải thực hiện được những mối liên kết ngang để trao đổi, chia sẻ thông tin, vừa có những mối liên kết dọc theo cấu trúc phân cấp của hệ thống chức năng quản lý nhà nước, hơn nữa trong toàn hệ thống chưa có các chuẩn thông tin cũng như chuẩn CNTT thống nhất để đảm bảo tính đồng bộ và khả năng trao đổi thông tin. CSDL quốc gia vẫn còn đang trong giai đoạn thử nghiệm, còn nhiều vấn đề phải tiếp tục nghiên cứu giải quyết.

Ngoài ra, do các hệ thống thông tin tiếp cận riêng biệt, nên kết quả không chỉ là các hệ thống không trao đổi, chia sẻ thông tin được với nhau mà việc xây dựng các phần mềm có tính năng giống nhau cũng bị trùng lặp nhau, gây lãng phí và do đầu tư tản mạn, không đủ ngưỡng nên cũng khó kiếm được những phần mềm hoàn thiện. Một vấn đề nữa cần nhấn mạnh là triển khai xây dựng một hệ thống thông tin không chỉ đơn thuần là xây dựng và cài đặt phần mềm, mà vấn đề khó khăn hơn là tổ chức lại, thay đổi các quy trình hoạt động trong

đơn vị cho phù hợp với việc tin học hoá để nâng cao hiệu suất hoạt động của đơn vị. Tin học hoá phải gắn với quá trình đổi mới các quy trình hoạt động, cải cách hành chính.

Về công nghệ: Riêng hệ thống các cơ quan Đảng và Nhà nước, như đã trình bày ở trên, bước đầu đã có mạng thông tin diện rộng nối kết đến các Bộ, ngành, uỷ ban nhân dân tỉnh, thành phố và tỉnh, thành uỷ. Công nghệ sử dụng cho việc kết nối chủ yếu dựa trên phần mềm Lotus note của công ty Lotus Note (ngày nay thuộc công ty IBM). Các phần mềm dùng chung phục vụ công tác điều hành tác nghiệp, quản lý văn phòng và các cơ sở dữ liệu cũng như các phương thức an toàn, bảo mật cũng chủ yếu được thực hiện trên nền Lotus Note. Phần mềm Lotus Note có những hạn chế nhất định trong việc bảo mật và khai thác thông tin, vì vậy, về lâu dài cần có một chiến lược tiếp cận, lựa chọn và phát triển công nghệ cho hệ thống điều hành quản lý của Đảng và Nhà nước, trong đó cần tính ngay đến những nhu cầu chuyển đổi sang những công nghệ mới phù hợp hơn, tiện lợi hơn, phần mềm dùng chung, cơ sở dữ liệu đến các Website, các bộ trình duyệt, các phương án an toàn, bảo mật thông tin, chữ ký điện tử,... Cần tổ chức thống nhất, xây dựng chuẩn chung để tránh tình trạng lặp lại "sự kiện Y2K" gây những hậu quả khó lường.

Với một số thông tin trên đây, mặc dù còn chưa đầy đủ song cũng đã đủ thấy sự quan trọng và cần thiết phải tập trung lực lượng, nghiên cứu sớm đưa ra những kết quả và sản phẩm có cơ sở khoa học và thực tiễn phục vụ cho việc triển khai xây dựng hệ thống thông tin điều hành và quản lý của Đảng và Nhà nước, đặc biệt là hệ thống chuẩn thông tin, phần mềm dùng chung và cơ sở dữ liệu thông tin chiến lược, góp phần thực hiện thắng lợi mục tiêu do Đại hội Đảng toàn quốc lần thữ IX và Chỉ thị 58 CT/TW của Bộ chính trị đề ra, đảm bảo cho đất nước sẵn sàng tham gia quá trình hội nhập và từng bước phát triển kinh tế tri thức.

3. Khảo sát mô hình mạng máy tính của Bộ Tài Chính

Hệ thống mang:

Hiện tại sử dụng hệ thống FAST SWITCH và FAST HUB tại Trung tâm để nối với máy chủ. Tại các Vụ của Bộ, đặt các SWITCH 10/100 nối về trung tâm bằng cấp UTP Cat 5, tốc độ 100Mbps. Riêng một số Vụ, do khoảng cách xa hơn 100m, cho nên nối về trung tâm bằng cáp béo, tốc độ 10 Mbps. Các máy trạm nối vào cổng 10 Mbps của SWITCH.

Hệ thống máy chủ

Máy chủ 1: NCR 2 Intel P5 166 Mhz, 1 MB cache procesor, 64 MB ECC RAM, 2 x4.3 GB HDD.

Cài hệ điều hành Sun Solaris Intel 2,5. Cơ sở dữ liệu Oracle 7,3, dùng cho ứng dụng Công sản, Quản lý cán bộ.

Máy chủ 2: NCR 1 Intel P5 166 Mhz, 1 MB cache, 64 MB ECC RAM, 2 x 2.1 GB HDD, RAID controller.

Cài hệ điều hành Windows NT 4.0, Microsoft Internet Information Server, chạy Web + FTP, Chương trình Law Data, Chương trình NSNN trên Fox.

Máy chủ 3: IBM Intel p6 200 Mhz, 512 KB Cache, 256 MB ECC RAM, 4 x4.5 GB HDD, RAID controller.

Cài hệ điều hành Windows NT 4.0, Lotus Notes 4.5, dùng cho ứng dụng văn bản pháp quy, Note Mail và Công văn nội bộ.

Máy chủ 4: IBM 2 Intel P6 200 Mhz, 412 cache, 256 MB ECC RAM, 4 x 4.5 GB HDD, RAID controller.

Cài hệ điều hành Windows NT 4.0, Lotus Notes 4.5, dùng cho ứng dụng Báo cáo nhanh phục vụ lãnh đạo và Công văn chính phủ,

Hệ thống truyền thông:

Mạng LAN Bộ tài chính được nối ra ngoài (với mạng LAN của các phân hệ Thuế, Đầu tư, Doanh nghiệp, Kho bạc và mạng LAN

các Sở Tài chính) thông qua router (Cisco 2500 Access Server). Môi trường truyền là PSTN, sử dụng các asynchronous modem (V34, 28.8 Kbps) kết nối vào các cổng asynchronous của router.

Phần mềm Lotus Notes:

Lotus Notes là sản phẩm cùa hàng Lotus. Lotus Notes cung cấp nhiều mẫu ứng dụng đáp ứng cho những yêu cầu làm việc khác nhau. Có thể xây dựng các ứng dụng khác một cách dễ dàng dựa trên các công cụ mà Lotus Notes cung cấp. Cơ sở dữ liệu (CSDL) hướng văn bản của Lotus Notes là CSDL lý ưởng cho việc lưu trữ và xử lý dữ liệu dạng văn bản, có sẵn nhiều chức năng trợ giúp mạnh mẽ mà người dùng có đầy đủ khả năng truy cập, dò tìm, lưu trữ và tổ chức thông tin. Lotus Notes là giải pháp tốt để tự động hoá dòng công việc quản lý CSDL hướng văn bản. Document của Lotus có thể chứa đựng nhiều các đối tượng và kiểu dữ liệu bao gồm Text, Richtext, dữ liệu số, hình ảnh, âm thanh,.... CSDL của Notes cũng chứa các form dành nhập dữ liệu, các view cho việc tìm kiếm và truy nhập thông tin, các chương tình cho hiển thị tự động hoá các tiến trình công việc có liên quan. Sự tích hợp giữa CSDL Notes và các CSDL truyền thống làm tăng thêm hiệu quả trong tổ chức và khai thác thông tin trên mạng. Notes có một công nghệ riêng - công nghệ sao chứp (Replication) dùng để sao chép tự động các CSDL Notes trên các Server phân tán, đồng bộ mọi thay đổi đồng thời và liền mạch. Do vậy mà mọi người dùng đều làm việc với cùng một thông tin mới nhất ngay cả khi họ chỉ thỉnh thoảng mới kết nối vào mạng. Server kế nối với mọi người dùng trong khoảng thời gian định trước, sao chép mọi thay đổi về document, ACL và các phần thiết kế như View, Form, Notes cũng cung cấp các khả năng Replication giữa trạm client và server. Notes chạy trên các mạng, các phần cứng và phần mềm phổ dụng như Novell Netware, Windows NT, Windows 95, OS2, UNIX, Macintosh. Notes cũng hỗ trợ phần mềm mã hoá bằng RSA, các tài liệu trong Notes có thể được mã hoá toàn bộ hoặc từng trường_ tuỳ theo yêu cầu. Các chế độ bảo vệ được thiết lập ở mức server, database, view, form, document, section và field. Notes còn cung cấp công cụ cho phép người sử dụng xác nhận và chứ ký điện tử.

4. Hiện trạng mạng truyền thông ngành tài chính

Chúng tôi đã khảo sát về mô hình mạng truyền thông trang thiết bị và yêu cầu trao đổi dữ liệu hiện thời của các đơn vị trong Ngành tài chính, cơ chế trao đổi thông tin thực tế tại các đơn vị đã kết nối mạng và chưa được kết nối mạng.

Cơ quan Bô tài chính:

Hiện tại đã thiết lập mạng cục bộ trong toàn bộ khu vực cơ quan Bộ.

Máy chủ để chạy ứng dụng là máy NCR S40 và IRM 704 dùng hệ điều hành Windows NT với ứng dụng trên môi trường Lotus Notes.

Việc kết nối với bên ngoài (KBNN, TCT, TCĐTPT, TCDN, các Sở tài chính) thực hiện thông qua router với 2 đường kết nối với đường điện thoại công cộng PSTN (Public Service Telephone Network) sử dụng modem.

Việc truyền số liệu đã được thực hiện tuy nhiên thao tác kết nối chưa được tự động hoá và yêu cầu chủ động kết nối mới chỉ được thực hiện một chiều (từ các đơn vị về cơ quan Bộ).

Số liệu trên đường truyền bao gồm các báo cáo trong hệ thông tin phục vụ Lãnh đạo và một số báo cáo nhanh cho Vụ NSNN, trao đổi hàng ngày, 5 ngày, 15 ngày và đồng bộ dữ liệu văn bản pháp quy.
Tổng cục Doanh nghiệp

Tại Tổng cục dùng máy PC Server IBM 320 làm máy chủ truyền tin, hệ điều hành WindowsNT và ứng dụng trên môi trường Lotus Notes. Các Cục gửi báo cáo về dưới dạng file, gắn lèm thư điện tử e-mail.

Đánh giá chung, hệ thống thông tin Tổng cục chưa được thiết lập đầy đủ, việc xử lý dữ liệu thường bằng phương pháp thủ công, việc trao đổi thông tin giữa các Cục và Tổng cục thường trên cơ sở các báo cáo bằng giấy tờ khiến Tổng cục, với chức năng tổng hợp số liệu trên

địa bàn cả nước, tổng hợp số liệu bằng phương pháp thủ công gặp rất nhiều khó khăn.

Tổng cuc Đầu tư phát triển:

Hiện tại đã thiết lập mạng LAN mới chỉ ở văn phòng Tổng cục và 6 Cục Đầu tư phát triển.

Hệ thống truyền tin báo cáo qua PSTN đã thiết lập cho 28 cục. Tại Tổng cục dùng máy chủ truyền tin Compaq Proliant 1500, chạy Solaris. Phần mềm truyền dựa trên ứng dụng truyền file của Unix, chỉ cho phép truyền file đơn thuần.

Hiệu suất sử dụng của ứng dụng truyền file đạt 40 - 50%. Hầu hết thông tin báo cáo còn lại thu thập từ các Cục Đầu tư phát triển trong cả nước thực hiện trên giấy tờ chuyển qua đuờng FAX. Ngoài ra một số thông tin nhập dưới dạng bảng tính, chuyển về Tổng cục bằng đĩa mềm qua đường điện thoại.

Đã xây dựng và triển khai tại một số vụ như Vụ Kế toán, Văn phòng hệ thống chương trình nghiệp vụ cho phép thực hiện xử lý thông tin báo cáo từ các Cục gửi lên Tổng cục, hiện nay chỉ thông qua đĩa mềm bằng đường điện thoại. Tuy nhiên khi có sai sót dữ liệu cần phải thực hiện lại dẫn đến sự tốn phí cũng như không đảm bảo được thời gian thực hiện tổng hợp báo cáo. Vì vậy nhu cầu đòi hỏi phải xây dựng hệ thống truyền tin tự động cho phép gửi thông tin trực tiếp qua viễn thông và tại Tổng cục, thông tin sẽ được cập nhật và xử lý bằng các chương trình nghiệp vụ.

Kho bạc Nhà nước

Ngoài kho bạc trung ương, đã có 53 văn phòng KBNN tỉnh có mạng cục bộ (dùng hệ điều hành mạng Novel Netware 4.x). Riêng KBNN Hà Nội đã kết nối mạng cục bọ tại văn phòng và 11 quận huyện. Các mạng cục bộ cũng được kết nối với nhau tạo thành một mạng diện rộng trên địa bàn thành phố thông qua đường điện thoại leased line thường trực thuê bao 24/24, ứng dụng đã hoạt động theo cơ

chế xử lý truy nhập trực tuyến (11 quận có 11 đường truyền kết nối với máy chủ tại Trung tâm).

Giữa các KBNN đều có đường truyền điện thoại và gắn MODEM truyền tin điểm-điểm theo định kỳ (truyền bảng kê thanh toán hàng ngày, truyền báo cáo hàng tháng). Việc liên lạc giữa các đơn vị KBNN (trừ Hà Nội) đều theo chế độ nhân công, cần có người ngồi trên máy tính ở hai đầu chứ chưa thiết lập được chế độ truyền tự động.

Tổng cuc Thuế:

Hiện tại đã thiết lập 2 trung tâm tập hợp số liệu ở Hà Nội và TPHCM (dành cho các tỉnh từ Đà Nẵng trở vào). Môi trường truyền là đường điện thoại công cộng PSTN (với 2 đường tại Thành phố HCM, 5 đường tại Hà Nội), trong đó có một đường tại Hà Nội để báo cáo lên cơ quan Bộ, còn các đường kia để nối trong nội bộ ngành. Máy chủ truyền thông là IBM DX2/66, SCO Unix, dùng multiport để nối modem.

Hiện đã xây dựng được hệ thống nhận thông tin từ Chi cục lên Cục cho hai cục, chủ yếu là nhận báo cáo kế toán thu. Các cục thuế nhỏ khác chỉ trao đổi thông tin với Tổng cục theo cơ chế truyền File gắn kèm thư điện tử (E-mail), chương trình chạy trên Unix do CSE phát triển).

Khối lượng thông tin trao đổi ước tình khoảng: 2KB báo cáo hàng ngày (từ mỗi cục lên Tổng cục, với định dạng file cơ sở dữ liệu DBF của Foxpro), tổng cộng là 180KB cho tất cả các cục. Ngoài ra còn có khoảng 500-1000 KB cập nhật chương trình từ Tổng cục chuyển cho các Cục.