# LỜI CẢM ƠN

Em xin được bày tỏ lòng biết ơn sâu sắc tới thầy giáo, TS. Lê Phê Đô. người đã trực tiếp hướng dẫn, tận tình chỉ bảo em trong suốt quá trình làm tốt nghiệp.

Em xin chân thành cảm ơn tất cả các thầy cô giáo trong khoa Công nghệ thông tin - Trường ĐHDL Hải Phòng, những người đã nhiệt tình giảng dạy và truyền đạt những kiến thức cần thiết trong suốt thời gian em học tập tại trường, để em hoàn thành tốt quá trình tốt nghiệp.

Cuối cùng em xin cảm ơn gia đình đã tạo điều kiện giúp đỡ em trong suốt quá trình làm tốt nghiệp. Và em xin cảm ơn tất cả các bạn đã góp ý, trao đổi hỗ trợ cho em trong suốt thời gian vừa qua.

Em xin chân thành cảm ơn!

Hà Nội, ngày 1 tháng 7 năm 2009

Sinh viên

Nguyễn Thị Nguyên

# MỤC LỤC

# LỜI MỞ ĐẦU

Ngày nay, an toàn thông tin đang và sẽ tiếp tục là một điểm nóng trong ngành tài chính - ngân hàng. Các nguy cơ rủi ro trong tài chính được thể hiện hoặc tiềm ẩn trên nhiều khía cạnh: con người, tin tặc, virus,… Để giải quyết vấn đề này cần xây dựng các hệ thống đảm bảo an toàn thông tin cho các hệ thống tài chính trên quy định hiện hành của pháp luật Việt Nam.

Hiện nay Đảng và Nhà nước ta đang rất coi trọng cải cách các thủ tục hành chính sao cho gọn nhẹ và hiệu quả. Để triển khai hệ thống ứng dụng CNTT trong những nhiệm vụ trọng tâm để đẩy nhanh quá trình cải cách hành chính. Ngoài việc chú trọng nghiên cứu xây dựng hệ thống, cần tiến hành song song việc nghiên cứu, xây dựng các hệ thống đảm bảo an toàn thông tin trong lĩnh vực tài chính. Trong khuôn khổ  của khoá luận này em trình bày các vấn đề bảo mật thông tin và xác thực thông tin dựa trên chứng chỉ số. Cấu trúc khoá luận gồm 3 chương:

**Chương 1: An toàn thông tin trong lĩnh vực tài chính**

**Chương 2: Giải pháp an toàn thông tin trong lĩnh vực tài chính**

**Chương 3: Tìm hiểu hoạt động tài chính ở một số đơn vị**

# DANH SÁCH CÁC TỪ VIẾT TẮT

| Các từ viết tắt | Ý nghĩa |
|---|---|
| CNTT | Công nghệ thông tin |
| CSDL | Cơ sở dữ liệu |
| HQ | Hải quan |
| DN | Doanh nghiệp |
| CA | Chứng thực điện tử |
| TCT | Tổng cục thuế |
| TCHQ | Tổng cục Hải quan |
| UBCKNN | Uỷ ban chứng khoán nhà nước |
| KBNN | Kho bạc nhà nước |

# Chương 1:
# AN TOÀN THÔNG TIN TRONG LĨNH VỰC TÀI CHÍNH

## 1.1. Giới thiệu chung về an toàn thông tin.

Khoa học công nghệ ngày càng phát triển, những khái niệm như an ninh mạng, bảo mật, an toàn thông tin, không còn xa lạ với người dân Việt Nam. An toàn thông tin giờ đây được xếp ngang hàng với An toàn thực phẩm, An toàn y tế...và nó quyết định không nhỏ đến vận mệnh quốc gia.

An toàn nghĩa là thông tin được bảo vệ, các hệ thống và những dịch vụ có khả năng chống lại những hiểm hoạ, lỗi và sự tác động không mong đợi, các thay đổi tác động đến độ an toàn của hệ thống là nhỏ nhất. Hệ thống có một trong các đặc điểm sau là không an toàn: Các thông tin dữ liệu trong hệ thống bị người không được quyền truy nhập tìm cách lấy và sử dụng (thông tin bị rò rỉ). Các thông tin trong hệ thống bị thay thế hoặc sửa đổi làm sai lệch nội dung (thông tin bị xáo trộn)…

Thông tin chỉ có giá trị cao khi đảm bảo tính chính xác và kịp thời. Hệ thống chỉ có thể cung cấp các thông tin có giá trị thực sự khi các chức năng của hệ thống đảm bảo hoạt động đúng đắn. Mục tiêu của an toàn, bảo mật thông tin trong công nghệ thông tin là đưa ra một số tiêu chuẩn an toàn. Ứng dụng các tiêu chuẩn an toàn này vào đâu để loại trừ hoặc giảm bớt các nguy hiểm. Do kỹ thuật truyền nhận và xử lý thông tin ngày càng phát triển để đáp ứng các yêu cầu ngày càng cao của cuộc sống đạt tới độ an toàn nào đó. Quản lý an toàn và sự rủi ro được gắn chặt với quản lý chất lượng. Khi đánh giá độ an toàn thông tin cần phải dựa trên phân tích các rủi ro, tăng sự an toàn bằng cách giảm tối thiểu rủi ro. Các đánh giá cần hài hoà với đặc tính, cấu trúc hệ thống và quá trình kiểm tra chất lượng.

***Các yêu cầu an toàn bảo mật thông tin***

Hiện nay các biện pháp tấn công càng ngày càng tinh vi, đe doạ tới độ an toàn thông tin có thể đến từ nhiều nơi theo nhiều cách chúng ta nên đưa ra các chính sách và phương pháp đề phòng cần thiết. Mục đích cuối cùng của an toàn bảo mật là bảo vệ các thông tin và tài nguyên theo các yêu cầu sau:

• Đảm bảo tính tin cậy(Confidentiality): Thông tin không thể bị truy nhập trái phép bởi những người không có thẩm quyền.

• Đảm bảo tính nguyên vẹn(Integrity): Thông tin không thể bị sửa đổi, bị làm giả bởi những người không có thẩm quyền.

• Đảm bảo tính sẵn sàng(Availability): Thông tin luôn sẵn sàng để đáp ứng sử dụng cho người có thẩm quyền.

• Đảm bảo tính không thể chối bỏ (Non-repudiation): Thông tin được cam kết về mặt pháp luật của người cung cấp.

Tại Việt Nam, không gian mạng đã dần trở thành một xã hội thu nhỏ, với đầy đủ các thành phần phức tạp và nguy cơ về an toàn thông tin. Nguyên nhân của tình trạng này là do nhận thức về an toàn thông tin chưa cao và việc triển khai, đầu tư chiến lược an ninh bảo mật chưa hiệu quả. Theo khảo sát của VNISA dựa vào các chuẩn an toàn thông tin của các tổ chức chuyên nghiệp về an ninh và bảo mật quốc tế đối với các doanh nghiệp, 40% doanh nghiệp Việt Nam không có hệ thống tường lửa, 70% doanh nghiệp không có quy trình xử lý sự cố an toàn thông tin, 85% doanh nghiệp không có chính sách an toàn thông tin.

## 1.2.Vai trò ứng dụng công nghệ thông tin trong lĩnh vực tài chính.

Đến nay, ngành tài chính là cơ quan chính phủ đi đầu trong ứng dụng công nghệ thông tin. Theo Cục Tin học thống kê tài chính năm 2008 với trên 90% nghiệp vụ tác nghiệp chính đã được ứng dụng công nghệ thông tin. Mạng hạ tầng truyền thông đã thiết lập được 3541 kênh truyền (MPLS và leased-line) từ cấp trung ương tới cấp quận, huyện. Số lượng máy chủ và máy trạm đã được trang bị cho toàn ngành lần lượt đạt 3894 và 54975 chiếc. Tổng cộng đã có khoảng 6300 cán bộ tham gia vào công tác triển khai ứng dụng tin học, trong đó có 3144 là cán bộ tin học (chiếm 4,9% tổng số cán bộ toàn ngành), số còn lại là cán bộ kiêm nhiệm.

Vì vậy vai trò việc ứng dụng công nghệ thông tin vào công tác chuyên môn nghiệp vụ của Bộ Tài chính thời gian qua có thể đánh giá ngắn gọn bằng các kết quả sau:

+ Các chương trình CNTT đã giúp tin học hóa nhiều quy trình nghiệp vụ của Bộ.

+ Hình thành hạ tầng kỹ thuật từ Bộ tới các Sở trong ngành.

+ Tạo cơ sở dữ liệu tài chính phục vụ chế độ tổng hợp, báo cáo thống kê.

Vai trò của công nghệ thông tin trong một số cơ quan trực thuộc Bộ Tài Chính:

***Trong Kho bạc nhà nước***: KBNN là một cơ quan quản lý nhà nước, phục vụ tất cả các đối tượng có quan hệ với ngân sách nhà nước. Việc ứng dụng CNTT trong các hoạt động nghiệp vụ không chỉ là hiện đại hóa công nghệ quản lý, nâng cao chất lượng và hiệu quả công việc mà còn đem lại những lợi ích đáng kể - những giá trị gia tăng vô hình – cho các khách hàng của KBNN.

- **Với ứng dụng thanh toán chuyển tiền điện tử** (triển khai năm 2006), chất lượng thanh toán giữa các khách hàng thông qua các đơn vị KBNN đã được cải thiện đáng kể: an toàn hơn, chính xác hơn và đặc biệt là nhanh chóng, kịp thời hơn với thời gian thanh toán tính bằng phút.

- **Với ứng dụng quản lý trái phiếu, công trái** (triển khai năm 2002) KBNN đã đáp ứng được nhu cầu thanh toán trái phiếu, công trái vãng lai của khách hàng tại bất kỳ nơi nào trên toàn quốc mà không phụ thuộc vào tờ trái phiếu, công trái được phát hành tại đâu.

- **Trong nội bộ hệ thống KBNN,** việc triển khai hệ thống Intranet (triển khai năm 2006-2007) với các dịch vụ cơ bản ban đầu là Portal, email, chat đã tạo ra một nếp làm việc mới đối với cả lãnh đạo các cấp là người chỉ đạo, điều hành và cán bộ, công chức là người thừa hành công vụ, vừa tiết kiệm chi phí vừa phù hợp với xu hướng cải cách hành chính trong các cơ quan quản lý nhà nước.

***Trong Tổng cục Hải quan*:** Việc áp dụng công nghệ thông tin trong ngành Hải quan được thực hiện toàn diện, đem lại hiệu quả về nhiều mặt. Đối với công tác quản lý, công nghệ thông tin giúp xây dựng cơ sở dữ liệu khoa học, an toàn phục vụ công tác quản lý, ra quyết định của người lãnh đạo. Nhờ ứng dụng cộng nghệ thông tin trong các khu quản lý mà ngành đã đảm bảo tính liêm chính và chuyên nghiệp cao, xây dựng được cơ chế dân chủ bền vững, tạo sức mạnh về nội lực. Đối với doanh nghiệp và các tổ chức xã hội và người dân, ngành đã ứng dụng tốt công nghệ thông tin để xây dựng các kênh thông tin tuyên truyền (báo chí, website, cổng thông tin điện tử tư vấn trực tuyến..) thực hiện chức năng cầu nối giữa cơ quan quản lý với

người sử dụng; xây dựng và áp dụng hệ thống thông quan tiên tiến, giảm giấy tờ, chi phí, thời gian, giảm phiền hà cho doanh nghiệp, triển khai cơ chế một cửa, hình thành mối quan hệ tương tác hai chiều giữa doanh nghiệp với cơ quan qua các dịch vụ hành chính công. Kết quả nổi bật mà ứng dụng CNTT đem lại đó là đã làm thay đổi hình ảnh cơ quan quản lý nhà nước trở thành cơ quan phục vụ mang tính chuyên nghiệp cao, tích cực chủ động cung cấp nhiều dịch vụ hải quan cho doanh nghiệp và người dân khi tham gia các hoạt động thương mại Quốc tế.

***Trong Tổng cục Thuế:*** Thông tin ngành thuế phải xử lý tăng gấp hàng trăm lần so với chục năm trước. Và để hoàn thành được khối lượng công việc khổng lồ này, không có cách nào khác là ngành thuế đã phải không ngừng đẩy mạnh việc ứng dụng công nghệ thông tin vào các khâu quản lý, đặc biệt là các khâu xử lý, phân tích thông tin, dữ liệu.

Tổng cục Thuế cho biết, đến nay hầu hết các chỉ tiêu thông tin về kê khai, nộp thuế quy định trong các quy định pháp luật về thuế đã được nhập và lưu giữ trong hệ thống tin học tại từng cơ quan thuế. Vì vậy, tại những đơn vị mà lãnh đạo sử dụng và khai thác được thông tin quản lý thuế trên hệ thống máy tính đều có thể nắm bắt được nhanh chóng diễn biến tình hình thu, nộp thuế, nợ thuế từng ngày của từng doanh nghiệp, từng hộ, cũng như tình trạng quản lý thu thuế của từng đơn vị trực thuộc. Điều này đã giúp cho lãnh đạo cơ quan thuế có thể đưa ra được những quyết định kịp thời, chính xác và hiệu quả, sát thực nhất. Thực tế cho thấy, những cục trưởng có khả năng sử dụng, khai thác thông tin quản lý thuế trên mạng máy tính thì khả năng điều hành, quản lý tốt hơn nhiều, bởi các quyết định có đầy đủ căn cứ cả về định tính và định lượng nên có tính khả thi cao, tác động tích cực đến tốc độ tăng thu ngân sách và ổn định được bộ máy quản lý.

Không những thế, việc chuyển sang quản lý thuế trên mạng máy tính còn giúp chia sẻ thông tin nhanh chóng giữa các bộ phận, tạo mối liên kết trao đổi công việc chặt chẽ giữa các chức năng, từ đó giúp cho việc kiểm soát chất lượng công việc giữa các bộ phận quản lý trong đơn vị tốt hơn, hiệu quả hơn. Ví dụ: một số đơn vị thực hiện công khai hoá doanh số và tình trạng nợ thuế của từng phòng, đội thuế trên máy tính đã giúp cho các phòng, đội tự đối chiếu, so sánh về tình trạng quản lý, khai thác nguồn thu, tăng doanh số và giảm số thuế còn để nợ của mình so với phòng,

đội khác. Từ đó, tạo ra động lực thi đua hoàn thành nhiệm vụ, tăng nguồn thu cho ngân sách nhà nước.

Việc triển khai rộng ứng dụng tờ khai mã vạch cũng đã giúp cơ quan thuế giảm đáng kể nhân lực nhập tờ khai. Nếu trước đây một cán bộ nhập một tờ khai thuế giá trị gia tăng trung bình mất 3-4 phút thì nay máy đọc mã vạch tờ khai chỉ mất khoảng từ 3-5 giây, tiết kiệm thời gian khoảng 40-60 lần. Vì thế, cơ quan thuế có điều kiện tập trung nhân lực cho các khâu khác như: kiểm tra, thanh tra thuế... từ đó phát hiện và xử lý kịp thời các hành vi khai man, cố tình trốn thuế.

Mặt khác, việc ứng dụng công nghệ thông tin giúp giảm thời gian thực hiện giải quyết thủ tục hành chính về thuế cho người nộp thuế do cơ quan thuế đã theo dõi được chặt chẽ tiến độ xử lý giải quyết các hồ sơ thuế trên mạng máy tính, kịp thời đôn đốc các bộ phận giải quyết các thủ tục theo thời hạn luật thuế quy định. Đồng thời, việc công khai, minh bạch chính sách, thủ tục về thuế trên mạng Internet đã giúp cho người nộp thuế có khả năng khai thác và tìm hiểu tốt những thông tin liên quan về các chính sách, thủ tục thuế. Qua đó giúp doanh nghiệp thực hiện nghĩa vụ của mình được nhanh chóng và thuận tiện.

Có thể nói, ứng dụng công nghệ thông tin vào các khâu quản lý trong ngành thuế đã đem lại những hiệu quả thiết thực cho công tác quản lý, điều hành chung của toàn ngành thuế theo hướng cải cách và hiện đại hoá. Nhận thức rõ tầm quan trọng của công nghệ thông tin, năm 2009, ngành thuế tiếp tục đẩy mạnh ứng dụng này vào công tác điều hành và quản lý thuế, làm cho công cuộc tin học hoá, hiện đại hoá ngành thuế sớm đạt được những thành công tốt đẹp.

## 1.3. An toàn thông tin trong lĩnh vực tài chính.

Ngành tài chính đã triển khai ứng dụng CNTT từ những năm 90 của thế kỷ trước. Cho đến nay, hầu hết hoạt động nghiệp vụ của các đơn vị trong ngành đều dựa trên nền tảng CNTT, mạng WAN của ngành liên thông toàn diện với mạng Internet và có kết nối với các mạng dùng riêng khác (CPnet, hệ thống ngân hàng, các đại lý…) Do đó, ngành nhận thức rõ việc đảm bảo an toàn bảo mật cho hệ thống thông tin là nhiệm vụ cấp bách và cần phải được ưu tiên.

Hệ thống thông tin ngành tài chính hoạt động trên hạ tầng mạng diện rộng của ngành, cho đến nay hầu hết các cơ quan tài chính đều có kết nối với Internet, điều đó đồng nghĩa với việc mạng WAN ngành tài chính liên thông ở rất nhiều điểm với Internet.

An toàn bảo mật cho hệ thống thông tin ngành tài chính được đặt ra từ rất sớm, nhưng để triển khai một cách hệ thống, từ 2002, Cục Tin học thống kê tài chính đã chủ trì xây dựng đề án "thiết kế tổng thể giải pháp an toàn bảo mật hệ thống thông tin thống nhất ngành tài chính", được Bộ Tài chính phê duyệt và triển khai trong 5 năm, 2002-2006.

Bên cạnh những việc đã làm được, những việc chưa thực hiện được là chưa có hệ thống chính sách và các quy định thống nhất trong toàn ngành về an toàn bảo mật thông tin, chưa có hệ thống quản lý rủi ro, việc triển khai cho các cơ quan tài chính địa phương còn hạn chế.

Lúng túng lớn nhất là sự phức tạp và các mối đe doạ về sự mất an toàn bảo mật hệ thống thông tin ngày càng tăng. Tìm được một giải pháp tổng thể với chi phí hợp lý là điều không dễ cho các doanh nghiệp nói chung, trong đó có các doanh nghiệp trong lĩnh vực tài chính. Mặt khác, nhiều dự án về phía Nhà nước triển khai chậm cũng gây khó dễ cho các tổ chức và doanh nghiệp trong lĩnh vực tài chính.

Năm 2008-2009 là những năm bản lề trong việc triển khai các dự án của ngành thuế, kho bạc, hải quan.. Việc xây dựng hệ thống an toàn bảo mật cho các giao dịch nghiệp vụ như thanh toán kho bạc, quản lý và thanh toán tín trái phiếu, khai hải quan điện tử, khai thuế điện tử. Các công ty chứng khoán chuyển mạnh sang giao dịch trực tuyến, các sàn Hà Nội, Tp.HCM chuyển dần sang mô hình giao dịch qua mạng ("giao dịch không sàn"). Cho nên, vấn đề sống còn cho việc triển khai thành công những hoạt động trên là phải đảm bảo an toàn bảo mật cho các giao dịch, cho hệ thống thông tin của ngành, và của các doanh nghiệp.

Vì vậy ngành tài chính xác định rõ vấn đề đảm bảo an toàn thông tin không chỉ thuần tuý về mặt kỹ thuật mà gắn liền với 3 yếu tố: con người; quy trình nghiệp vụ và hạ tầng kỹ thuật. Do đó, giải pháp cho an toàn thông tin chính là các biện pháp tác động lên con người, quy trình nghiệp vụ và hạ tầng kỹ thuật để thông tin đảm

bảo được 3 thuộc tính bảo mật, toàn vẹn và sẵn sàng của nó. Không những thế, việc triển khai an toàn thông tin phải là một quá trình liên tục. Bởi lẽ, hệ thống an toàn thông tin sau khi xây dựng, đi vào hoạt động phải được định kỳ đánh giá, nhằm phát hiện các điểm yếu, mối đe dọa mới để từ đó có kế hoạch nâng cấp, hoàn thiện.

### 1.3.1. Thiếu đồng bộ, nhiều rủi ro

Ngay từ năm 2002, ngành tài chính đã có đề án triển khai hệ thống an toàn thông tin được phê duyệt, bao gồm các hệ thống giám sát an ninh mạng, phòng chống xâm nhập, chống virus, hệ thống xác thực, hệ thống dự phòng với mục tiêu thiết kế tổng thể giải pháp an toàn bảo mật hệ thống thông tin tài chính. Đến nay, ngành đã thiết lập được hệ thống Firewall (FW- tường lửa) cho 100% hệ thống mạng; thiết lập đường truyền giám sát bảo mật mức thiết bị; triển khai hệ thống sao lưu dự phòng cho các máy chủ ứng dụng và máy chủ dữ liệu; xây dựng hệ thống chứng thực điện tử (CA) trong giao dịch thanh toán điện tử kho bạc nhà nước; thiết lập hệ thống phòng, chống, phát hiện và kiểm tra virus. Mặc dù đã có đề án tổng thể, nhưng hiện nay hệ thống đảm bảo an toàn bảo mật thông tin của ngành vẫn còn không ít tồn tại như: chưa có chính sách chung, bao quát những quan điểm về an ninh thông tin của ngành, chưa có tổ chức chuyên trách về an toàn bảo mật thông tin, chưa có hệ thống CA để thực hiện giao dịch điện tử an toàn. Đặc biệt, hệ thống giải pháp đảm bảo an toàn bảo mật thông tin vẫn chủ yếu tập trung vào các giải pháp liên quan đến công nghệ, hạ tầng kỹ thuật, coi nhẹ yếu tố con người và quy trình nghiệp vụ. Ngay cả yếu tố hạ tầng kỹ thuật của hệ thống an ninh thông tin ngành tài chính cũng đang bộc lộ những bất cập. Cụ thể, mặc dù đã áp dụng các biện pháp bảo mật nhưng do mức độ phức tạp của hệ thống truyền thông và đa dạng về ứng dụng, cơ sở dữ liệu nên các biện pháp an toàn bảo mật tuy đã áp dụng nhưng vẫn chưa đầy đủ, thiếu tính nhất quán. Các đơn vị trực thuộc ngành tài chính như: Tổng cục Thuế (TCT), Kho bạc Nhà nước (KBNN), Tổng cục Hải quan (TCHQ), Uỷ ban chứng khoán Nhà nước (UBCKNN)… hiện đang có sự đầu tư cho hạ tầng kỹ thuật đảm bảo an toàn bảo mật thông tin theo kiểu "mỗi nơi một phách". Bên cạnh đó, ngành

tài chính mới chỉ có một số quy định được áp dụng trong nội bộ từng đơn vị trực thuộc ngành.

Do những tồn tại trên nên trong toàn bộ hệ thống thông tin ngành tài chính tiềm ẩn nhiều rủi ro, có nguy cơ bị tấn công cao. Đó là những điểm yếu, rủi ro liên quan đến con người, tổ chức; liên quan đến các quy trình nghiệp vụ, quản lý và liên quan công nghệ, sự phối hợp giữa con người, tổ chức. Đơn cử, hiện nay nhận thức về an ninh thông tin và tính tuân thủ các quy định còn yếu. Mỗi người của đơn vị được cấp 1 tài khoản dịch vụ (1 cặp username và password), để có thể truy cập mạng và sử dụng các dịch vụ đươc phân quyền như mail, dịch vụ tệp, khai thác CSDL, truy cập Internet… Theo quy định thì các đơn vị phải định kỳ cập nhật cho bộ phận CNTT về thay đổi nhân sự trong đơn vị mình để kịp thu hồi các tài khoản dịch vụ, nhưng rất nhiều đơn vị không tuân thủ chế độ báo cáo này. Do đó, ở nhiều cơ quan vẫn xảy ra tình trạng cán bộ của đơn vị chuyển công tác nhưng tài khoản dịch vụ không bị thu hồi và nguy cơ "rò rỉ" thông tin là rất cao.

### 1.3.2. Những biện pháp để đảm bảo an toàn thông tin

Ngành tài chính triển khai đề án An toàn bảo mật hệ thống thông tin tài chính từ năm 2004. Giai đoạn đầu, ngành tài chính chú trọng vào thiết lập hệ thống an ninh mạng. Hiện nay, đã triển khai theo cả 3 hướng: kiện toàn tổ chức chuyên trách về an ninh thông tin, đặt tại phòng Quản trị mạng, nay có tên mới là Phòng quản lý mạng và an ninh thông tin; xây dựng các quy chế sử dụng khai thác mạng LAN cơ quan và mạng WAN toàn ngành, xây dựng các quy trình nội bộ về quản trị, quản lý dữ liệu; tiếp tục đàu tư cho các công cụ an toàn bảo mật mức mạng, ứng dụng, tổ chức hệ thống lưu trữ thông tin có độ an toàn, tính sẵn sàng cao (SAN), thử nghiệm và mua sắm các phần mềm hỗ trợ giám sát mạng. Tìm kiếm chuyên gia tư vấn để giúp xây dựng chính sách về an ninh thông tin và xây dựng hệ thống quản lý an ninh thông tin (ISMS) theo chuẩn ISO 27001/27002.

Từ 2 năm nay Bộ Tài chính muốn tiếp cận 1 cách đồng bộ từ mức chính sách, kiểm soát tính tuân thủ cho đến các giải pháp an toàn bảo mật ở mức vật lý và mức mạng. Ở mức vật lý, đã đưa vào sử dụng Data Center tại cơ quan Bộ Tài chính, với hệ thống kiểm soát truy cập hiện đại, có quy định về việc khai thác, vận hành Datacenter và có bộ phận chuyên trách giám sát việc thực hiện quy định này. Ở mức mạng, hệ thống mạng tại Bộ Tài chính được phân chia theo các vùng khác nhau, mỗi vùng mạng chứa máy chủ ứng dụng phục vụ đối tượng khai thác khác nhau như khai thác mức ngành, khai thác nội bộ,…. đã triển khai những giải pháp/sản phẩm của các hãng uy tín để kiểm soát truy nhập đến các vùng mạng này.

Năm nay Bộ Tài chính tiếp tục nâng cấp hệ thống bằng cách kiến trúc lại phần kiểm soát truy nhập qua hình thức VPN, bổ sung thêm các FireWall mức mạng và mức ứng dụng để tăng độ an toàn cho cácvùng mạng, ứng dụng quan trọng, chuẩn bị đầu tư cho giải pháp End-point Security và tìm kiếm công cụ hỗ trợ giám sát an ninh mức mạng, ứng dụng một cách toàn diện, hiệu quả.

## 1.4. Các cơ sở pháp lý của các giao dịch tài chính online.

Tài chính là ngành bao trùm rất rộng, không chỉ quản lý ngân sách nhà nước mà còn cả lĩnh vực về Thuế, Hải quan, Chứng khoán, Dự trữ quốc gia, Kho bạc. Các khối ngành này trong nhiều năm qua đã và đang đẩy mạnh công tác hiện đại hoá. Hiện nay, việc xử lý, trao đổi thông tin giữa các cơ quan thuộc Bộ đều thực hiện trên mạng nội bộ và mạng diện rộng. Mặc dù vậy, điều cần thiết hiện nay là cần phải có cơ sở pháp lý đảm bảo cho việc giao dịch được thuận lợi, tránh tình trạng vừa thực hiện giao dịch điện tử nhưng vẫn phải in toàn bộ nội dung ra như hiện nay. Chẳng hạn trong lĩnh vực Hải quan, ngoài việc thí điểm thủ tục hải quan điện tử đối với một số doanh nghiệp, còn lại mặc dù nói là khai báo hải quan điện tử, nhưng cơ quan Hải quan vẫn phải in bộ hồ sơ ra giấy, vẫn cần phải có dấu và chữ ký tay của các cấp có thẩm quyền. Một ví dụ khác trong lĩnh vực Kho bạc, hiện nay theo chế độ kế toán hàng ngày vẫn phải in ra rất nhiều bản kê chứng từ, sổ phụ… để lưu lại, rất tốn kém và mất thời gian. Tất cả những tồn tại này đều có thể loại bỏ nếu chúng

ta thực hiện hoàn toàn trên môi trường điện tử. Khi đó, tất cả đều thực hiện bằng các chứng từ điện tử, rất thuận lợi cho cơ quan quản lý cũng như các doanh nghiệp.

Tuy nhiên, muốn thực hiện được cần phải có quy định cụ thể để các bộ ngành khác cùng thực hiện. Vì vậy cần phải tiếp tục đầu tư công nghệ sao cho tất cả các giao dịch được đảm bảo, an toàn và tin cậy. Khi đó mới có thể thay thế được hoàn toàn chứng từ giấy, giúp cắt giảm chi phí và thuận lợi hơn trong hoạt động giao dịch.

Ngày 23/2/2007 thủ tướng chính phủ đã ký duyệt Nghị định thi hành Luật giao dịch điện tử trong lĩnh vực tài chính. Nghị định này có thể chia thành 3 mảng: Giao dịch trong nội bộ ngành Tài chính; Giao dịch giữa ngành Tài chính với các đối tượng ngành Tài chính quản lý, phục vụ; Giao dịch liên quan đến lĩnh vực tài chính giữa các tổ chức, cá nhân. Nghị định này có ý nghĩa hết sức quan trọng, là nền tảng pháp lý vững chắc cho các hoạt động giao dịch điện tử trong lĩnh vực tài chính. Nó đã cụ thể hoá và hệ thống hoá cho các hoạt động giao dịch. Nó sẽ giúp cho các hoạt động giao dịch được thuận lợi hơn rất nhiều. Không những thế, nó còn giúp chỉnh sửa lại các quy định cũ cho phù hợp với môi trường điện tử, đồng thời có cơ sở pháp lý để đầu tư thêm hạ tầng và mạnh dạn triển khai các bài toán giao dịch điện tử trước đây đã đề ra một cách hoàn thiện và tốt hơn.

Giao dịch điện tử trong hoạt động tài chính giữa tổ chức, cá nhân với cơ quan tài chính phải sử dụng chữ ký số và chứng thư số do Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng cung cấp.

Theo Nghị định trên, chứng từ điện tử chỉ được hủy khi có sự đồng ý và xác nhận của các bên tham gia giao dịch, trừ trường hợp pháp luật chuyên ngành có quy định khác; việc tiêu hủy chứng từ điện tử có hiệu lực theo đúng thời hạn do các bên tham gia đã thỏa thuận.

Chứng từ điện tử đã hủy phải được lưu trữ phục vụ việc tra cứu của cơ quan nhà nước có thẩm quyền. Chứng từ điện tử đã hết thời hạn lưu trữ theo quy định, nếu không có quyết định khác của cơ quan nhà nước có thẩm quyền thì được phép tiêu hủy. Việc tiêu hủy chứng từ điện tử không được làm ảnh hưởng đến tính toàn

vẹn của các chứng từ điện tử chưa tiêu hủy và phải đảm bảo sự hoạt động bình thường của hệ thống thông tin.

Chứng từ điện tử bị niêm phong, tạm giữ, tịch thu phải theo đúng quy định của pháp luật. Sau khi cơ quan nhà nước có thẩm quyền quyết định và thực hiện các biện pháp niêm phong, tạm giữ, tịch thu chứng từ điện tử thì tổ chức, cá nhân không được phép khai thác, sử dụng, sửa đổi chứng từ điện tử này trong hệ thống thông tin của mình để giao dịch hoặc sử dụng cho mục đích khác.

Chứng từ điện tử được gửi, nhận và xử lý giữa cá nhân với hệ thống thông tin tự động hoặc giữa các hệ thống thông tin tự động với nhau không bị phủ nhận giá trị pháp lý. Tổ chức, cá nhân chịu toàn bộ trách nhiệm trong việc sử dụng hệ thống thông tin tự động trong các hoạt động tài chính của mình. Khi cần thiết, chứng từ điện tử có thể chuyển sang chứng từ giấy và ngược lại nhưng phải đáp ứng đủ các điều kiện theo quy định. Bộ trưởng Bộ Tài chính quy định giá trị pháp lý của các chứng từ điện tử chuyển sang chứng từ giấy và ngược lại cho từng loại hoạt động tài chính.

Nghị định nêu rõ, cơ quan nhà nước có thẩm quyền có trách nhiệm thanh tra, kiểm tra, kịp thời phát hiện và xử lý theo quy định của pháp luật các vi phạm về giao dịch điện tử trong hoạt động tài chính. Nhà nước khuyến khích các bên có tranh chấp về giao dịch điện tử trong hoạt động tài chính giải quyết thông qua hòa giải. Trong trường hợp các bên không hòa giải được thì thẩm quyền, trình tự, thủ tục giải quyết tranh chấp về giao dịch điện tử trong hoạt động tài chính được thực hiện theo quy định của pháp luật có liên quan.

Tổ chức khi tham gia giao dịch điện tử trong hoạt động tài chính có hành vi vi phạm pháp luật thì tùy theo tính chất, mức độ vi phạm mà bị xử phạt vi phạm hành chính theo quy định của pháp luật hoặc bị đình chỉ hoạt động giao dịch điện tử; cá nhân vi phạm thì bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự. Tổ chức, cá nhân gây thiệt hại cho tổ chức, cá nhân khác khi tham gia giao dịch điện tử trong hoạt động tài chính phải bồi thường theo quy định của pháp luật.

Trước đó, Chính phủ đã ban hành Nghị định 26/2007/NĐ-CP (ngày 15-2-2007) quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số. Theo đó, trong trường hợp pháp luật quy định văn bản cần có chữ ký thì yêu cầu đối với một thông điệp dữ liệu được xem là đáp ứng nếu thông điệp dữ liệu đó được ký bằng chữ ký số.

Trong trường hợp pháp luật quy định văn bản cần được đóng dấu của cơ quan, tổ chức thì yêu cầu đó đối với một thông điệp dữ liệu được xem là đáp ứng nếu thông điệp dữ liệu đó được ký bởi chữ ký số của người có thẩm quyền theo quy định của pháp luật về quản lý và sử dụng con dấu và chữ ký số đó được bảo đảm an toàn theo quy định.

Chữ ký số và chứng thư số nước ngoài được công nhận theo quy định tại Nghị định này có giá trị pháp lý và hiệu lực như chữ ký số và chứng thư do tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng của Việt Nam cấp.

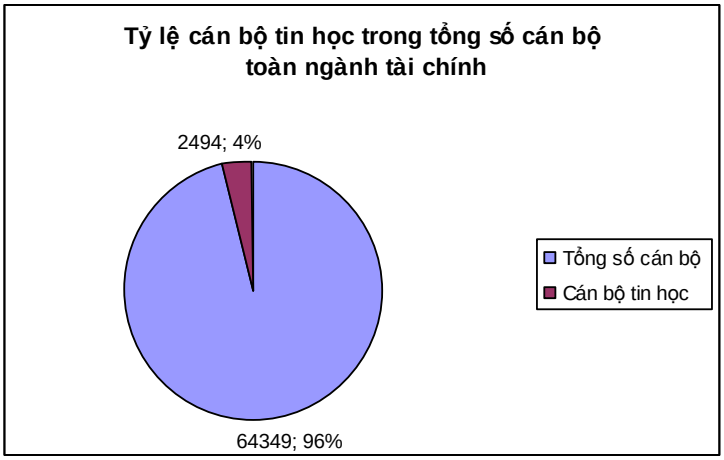
Ngoài ra, dự luật cũng quy định về bảo đảm an ninh, an toàn trong giao dịch điện tử, bảo vệ thông điệp dữ liệu, bảo mật thông tin, trách nhiệm của người cung cấp dịch vụ mạng, trách nhiệm của tổ chức và cá nhân khi có yêu cầu của cơ quan Nhà nước có thẩm quyền, quyền của các cơ quan Nhà nước có thẩm quyền, vấn đề tuân thủ pháp luật sở hữu trí tuệ trong giao dịch điện tử, quyền và nghĩa vụ của người khởi tạo thông điệp dữ liệu, nghĩa vụ của người nhận thông điệp dữ liệu, quyền và nghĩa vụ của người trung gian, vấn đề thanh tra hoạt động giao dịch điện tử, xử lý vi phạm pháp luật trong giao dịch điện tử.

# Chương 2:
# GIẢI PHÁP AN TOÀN THÔNG TIN TRONG LĨNH VỰC TÀI CHÍNH

## 2.1. Giải pháp về chế độ chính sách về nhân sự

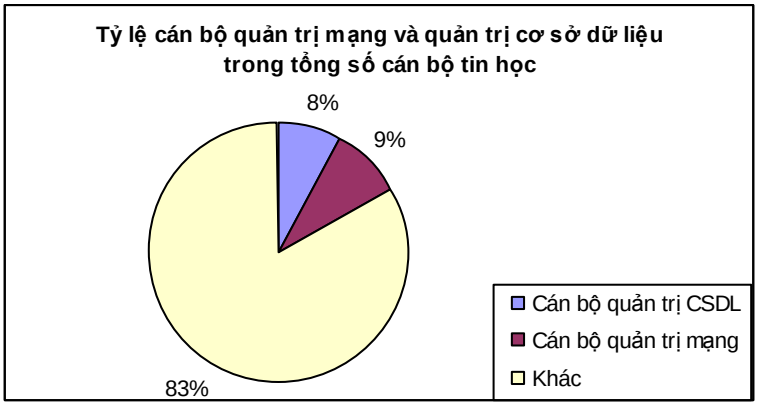
Về tổ chức đội ngũ tin học, xuất phát từ con số 0 từ những năm 90, toàn ngành Tài chính hiện tại có trên 2000 cán bộ tin học, với nòng cốt là các cán bộ kiêm nhiệm, dần chuyển sang làm công tác tin học. Tổ chức bộ máy dần chuyển từ tổ máy tính trực thuộc đến tổ tin học và hiện tại Kho bạc và Thuế đã hình thành Trung tâm tin học thống kê tạo nền tảng vững chắc và đủ khả năng để đảm nhiệm công việc phát triển, triển khai các hệ thống ứng dụng côngn nghệ thông tin tại địa phương.

Hiện tại, toàn ngành tài chính có khoảng 64 vạn cán bộ trong đó số lượng cán bộ tin học là 2494 cán bộ (chiếm 4%)




Trong tổng số 2494 cán  bộ tin học trong toàn ngành thì tỷ lệ cán bộ tin học vẫn ít hơn số cán bộ kiêm nhiệm phục vụ cho lĩnh vực tin học.


Ngoài ra trong số cán bộ tin học toàn ngành mới chỉ có 224 cán bộ quản trị mạng và truyền thông (chiếm 9%) và khoảng 200 cán bộ quản trị cơ sở dữ liệu (chiếm 8 %). So với yêu cầu về cán bộ để quản lý hệ thống lớn thì mới chỉ đáp ứng 30%-40%.




Cùng với việc phát triển đội ngũ cán bộ thì công tác đào tạo tin học trong ngành tài chính được làm thường xuyên và liên tục, bước đầu đã đáp ứng được yêu cầu. Việc đào tạo tin học được phân cấp và thực hiện theo các chương trình phù hợp với từng đối tượng và trình độ khác nhau:

Đào tạo cán bộ tin học trình độ cao để quản lý các dự án tin học, phát triển các ứng dụng lớn của ngành, nghiên cứu nắm bắt các thành tựu tin học mới để áp dụng trong ngành. Đến nay số cán bộ được đào tạo tin học chuyên sâu khoảng 1800 lượt người bao gồm các nội dung về: phân tích, thiết kế dữ liệu sử dụng công cụ ORACLE; Quản trị cơ sở dữ liệu ORACLE; Xây dựng Kho dữ liệu; Quản trị mạng;

Chuyên gia mạng Cisco; An toàn bảo mật; Quản trị hệ thống thư điện tử Lotus Notes; Lập trình Java; Lập trình C#net...

Đào tạo các cán bộ sử dụng các chương trình ứng dụng. Số cán bộ này chủ yếu là các cán bộ nghiệp vụ, không làm chuyên tin học, chỉ sử dụng máy tính để phục vụ cho công tác chuyên môn nghiệp vụ. Việc đào tạo này do các cán bộ tin học đảm nhiệm, có phân cấp cho các đơn vị địa phương. Theo thống kê, toàn ngành đã tổ chức đào tạo tin học cơ bản và sử dụng ứng dụng chuyên ngành cho gần 30.000 lượt cán bộ.

Với mục tiêu đào tạo cán bộ lãnh đạo có nhận thức cao về vai trò của CNTT trong công tác quản lý tài chính để có thể trực tiếp khai thác thông tin phục vụ công tác điều hành quản lý và ra quyết định. Hàng năm các khoá tập huấn trong thời gian ngắn với các nội dung về tin học cơ bản, khái niệm về hệ thống và mạng máy tính, hướng dẫn khai thác thông tin báo cáo từ các cơ sở dữ liệu phục vụ cho công tác quản lý điều hành, hoạch định chính sách và ra quyết định được tổ chức để đào tạo cho các cán bộ lãnh đạo. Hiện tại, 100% cán bộ lãnh đạo trong cơ quan Bộ và cán bộ lãnh đạo tại các đơn vị trực thuộc Bộ đã được đào tạo kiến thức tin học, sử dụng mạng máy tính để khai thác thông tin phục vụ công tác quản lý điều hành.

## 2.2. Giải pháp về công nghệ thông tin

### 2.2.1. Khoá công khai

**Mật mã hóa khóa công khai** là một dạng mật mã hóa cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa chung bí mật trước đó. Điều này được thực hiện bằng cách sử dụng một cặp khóa có quan hệ toán học với nhau là **khóa công khai** và khoá cá nhân(hay khóa bí mật).

Thuật ngữ mật mã hóa khóa bất đối xứng thường được dùng đồng nghĩa với mật mã hóa khóa công khai mặc dù hai khái niệm không hoàn toàn tương đương. Có những thuật toán mật mã khóa bất đối xứng không có tính chất khóa công khai và bí mật như đề cập ở trên mà cả hai khóa (cho mã hóa và giải mã) đều cần phải giữ bí mật.

Trong mật mã hóa khóa công khai, khóa cá nhân phải được giữ bí mật trong khi khóa công khai được phổ biến công khai. Trong 2 khóa, một dùng để mã hóa và khóa còn lại dùng để giải mã. Điều quan trọng đối với hệ thống là không thể tìm ra khóa bí mật nếu chỉ biết khóa công khai.

Hệ thống mật mã hóa khóa công khai có thể sử dụng với các mục đích:

**Mã hoá**: giữ bí mật thông tin và chỉ có người có khóa bí mật mới giải mã được.

**Tạo ch**ữ ký số: cho phép kiểm tra một văn bản có phải đã được tạo với một khóa bí mật nào đó hay không.

**Thoả thuận khoá:** cho phép thiết lập khóa dùng để trao đổi thông tin mật giữa 2 bên.

Thông thường, các kỹ thuật mật mã hóa khóa công khai đòi hỏi khối lượng tính toán nhiều hơn các kỹ thuật mã hoá khoá đối xứng nhưng những lợi điểm mà chúng mang lại khiến cho chúng được áp dụng trong nhiều ứng dụng.

***a. An toàn***

Về khía cạnh an toàn, các thuật toán mật mã hóa khóa bất đối xứng cũng không khác nhiều với các thuật toán mã hóa khóa đối xứng. Có những thuật toán được dùng rộng rãi, có thuật toán chủ yếu trên lý thuyết; có thuật toán vẫn được xem là an toàn, có thuật toán đã bị phá vỡ... Cũng cần lưu ý là những thuật toán được dùng rộng rãi không phải lúc nào cũng đảm bảo an toàn. Một số thuật toán có những chứng minh về độ an toàn với những tiêu chuẩn khác nhau. Nhiều chứng minh gắn việc phá vỡ thuật toán với những bài toán nổi tiếng vẫn được cho là không có lời giải trong thời gian đa thức. Nhìn chung, chưa có thuật toán nào được chứng minh là an toàn tuyệt đối (như hệ thống mật mã sử dụng một lần). Vì vậy, cũng giống như tất cả các thuật toán mật mã nói chung, các thuật toán mã hóa khóa công khai cần phải được sử dụng một cách thận trọng.

***b. Các ứng dụng***

Ứng dụng rõ ràng nhất của mật mã hóa khóa công khai là bảo mật: một văn bản được mã hóa bằng khóa công khai của một người sử dụng thì chỉ có thể giải mã với khóa bí mật của người đó.

Các thuật toán tạo chữ ký số khóa công khai có thể dùng để nhận thực. Một người sử dụng có thể mã hóa văn bản với khóa bí mật của mình. Nếu một người khác có thể giải mã với **khóa công khai** của người gửi thì có thể tin rằng văn bản thực sự xuất phát từ người gắn với khóa công khai đó.

Các đặc điểm trên còn có ích cho nhiều ứng dụng khác như: tiền điện tử, thỏa thuận khóa...

***c. Thuật toán: liên kết giữa 2 khóa trong cặp***

Không phải tất cả các thuật toán mật mã hóa khóa bất đối xứng đều hoạt động giống nhau nhưng phần lớn đều gồm 2 khóa có quan hệ toán học với nhau: một cho mã hóa và một để giải mã  Để thuật toán đảm bảo an toàn thì không thể tìm được khóa giải mã nếu chỉ biết khóa đã dùng mã hóa. Điều này còn được gọi là mã hóa công khai vì khóa dùng để mã hóa có thể công bố công khai mà không ảnh hưởng đến bí mật của văn bản mã hóa. Trong ví dụ ở trên, khóa công khai có thể là những hướng dẫn đủ để tạo ra khóa với tính chất là một khi đã khóa thì không thể mở được nếu chỉ biết những hướng dẫn đã cho. Các thông tin để mở khóa thì chỉ có người sở hữu mới biết.

***d. Những điểm yếu***

Tồn tại khả năng một người nào đó có thể tìm ra được khóa bí mật. Không giống với hệ thống mật mã sử dụng một lần (one-time pad) hoặc tương đương, chưa có thuật toán mã hóa khóa bất đối xứng nào được tuyệt đối là an toàn trước các tấn công dựa trên bản chất toán học của thuật toán. Khả năng một mối quan hệ nào đó giữa 2 khóa hay điểm yếu của thuật toán dẫn tới cho phép giải mã không cần tới khóa hay chỉ cần khóa mã hóa vẫn chưa được loại trừ. An toàn của các thuật toán này đều dựa trên các ước lượng về khối lượng tính toán để giải các bài toán gắn với chúng. Các ước lượng này lại luôn thay đổi tùy thuộc khả năng của máy tính và các phát hiện toán học mới.

Mặc dù vậy, độ an toàn của các thuật toán mật mã hóa khóa công khai cũng tương đối đảm bảo. Nếu thời gian để phá một mã (bằng phương pháp duyệt toàn bộ) được ước lượng là 1000 năm thì thuật toán này hoàn toàn có thể dùng để mã hóa các thông tin về thẻ tín dụng - Rõ ràng là thời gian phá mã lớn hơn nhiều lần thời gian tồn tại của thẻ (vài năm).

Nhiều điểm yếu của một số thuật toán mật mã hoá khoá bất đối xứng đã được tìm ra trong quá khứ. Thuật toán ***đóng gói ba lô*** là một ví dụ. Nó chỉ được xem là không an toàn khi một dạng tấn công không lường trước bị phát hiện. Gần đây, một số dạng tấn công đã đơn giản hóa việc tìm khóa giải mã dựa trên việc đo đạc chính xác thời gian mà một hệ thống phần cứng thực hiện mã hoá. Vì vậy, việc sử dụng mã hóa khóa bất đối xứng không thể đảm bảo an toàn tuyệt đối. Đây là một lĩnh vực đang được tích cực nghiên cứu để tìm ra những dạng tấn công mới.

Một điểm yếu tiềm tàng trong việc sử dụng khóa bất đối xứng là khả năng bị tấn công dạng kẻ tấn công đứng giữa (man in the middle attack): kẻ tấn công lợi dụng việc phân phối khóa công khai để thay đổi khóa công khai. Sau khi đã giả mạo được khóa công khai, kẻ tấn công đứng ở giữa 2 bên để nhận các gói tin, giải mã rồi lại maã hoá với khóa đúng và gửi đến nơi nhận để tránh bị phát hiện. Dạng tấn công kiểu này có thể phòng ngừa bằng các phương pháp trao đổi khoá an toàn nhằm đảm bảo nhận thực người gửi và toàn vẹn thông tin. Một điều cần lưu ý là khi các chính phủ quan tâm đến dạng tấn công này: họ có thể thuyết phục (hay bắt buộc) nhà cung cấp chứng thực số xác nhận một khóa giả mạo và có thể đọc các thông tin mã hóa.

***e. Khối lượng tính toán***

Để đạt được độ an toàn tương đương, thuật toán mật mã hoá khoá bất đối xứng đòi hỏi khối lượng tính toán nhiều hơn đáng kể so với thuật toán mật mã hoá khoá đối xứng. Vì thế trong thực tế hai dạng thuật toán này thường được dùng bổ sung cho nhau để đạt hiệu quả cao. Trong mô hình này, một bên tham gia trao đổi thông tin tạo ra một khóa đối xứng dùng cho phiên giao dịch. Khóa này sẽ được trao đổi an toàn thông qua hệ thống mã hóa khóa bất đối xứng. Sau đó 2 bên trao đổi thông tin bí mật bằng hệ thống mã hóa đối xứng trong suốt phiên giao dịch.

***f. Mối quan hệ giữa khóa công khai với thực thể sở hữu khóa***

Để có thể đạt được những ưu điểm của hệ thống thì mối quan hệ giữa khóa công khai và thực thể sở hữu khóa phải được đảm bảo chính xác. Vì thế các giao

thức thiết lập và kiểm tra mối quan hệ này là đặc biệt quan trọng. Việc gắn một khóa công khai với một định danh người sử dụng thường được thực hiện bởi các giao thức thực hiện hạ tầng khoá công khai (PKI). Các giao thức này cho phép kiểm tra mối quan hệ giữa khóa và người được cho là sở hữu khóa thông qua một bên thứ ba được tin tưởng. Mô hình tổ chức của hệ thống kiểm tra có thể theo phân lớp (các nhà cung cấp chứng thực số-X.509) hoặc theo thống kê (mạng lưới tín nhiệm-PGP, GPG) hoặc theo mô hình tín nhiệm nội bộ (SPKI). Không phụ thuộc vào bản chất của thuật toán hay giao thức, việc đánh giá mối quan hệ giữa khoá và người sở hữu khóa vẫn phải dựa trên những đánh giá chủ quan của bên thứ ba bởi vì khóa là một thực thể toán học còn người sở hữu và mối quan hệ thì không. Hạ tầng khoá công khai chính là các thiết chế để đưa ra những chính sáchcho việc đánh giá này.

### 2.2.2. Hệ mật RSA & Elgamal

#### 2.2.2.1. Hệ mật RSA

***a. Mô tả sơ lược***

Thuật toán RSA có hai khoá: khoá công khai (hay khóa công cộng) và khoá bí mật (hay khóa cá nhân). Mỗi khóa là những số cố định sử dụng trong quá trình mã hóa và giải mã. Khóa công khai được công bố rộng rãi cho mọi người và được dùng để mã hoá. Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng. Nói cách khác, mọi người đều có thể mã hóa nhưng chỉ có người biết khóa cá nhân (bí mật) mới có thể giải mã được.

Ta có thể mô phỏng trực quan một hệ mật mã khoá công khai như sau : Bob muốn gửi cho Alice một thông tin mật mà Bob muốn duy nhất Alice có thể đọc được. Để làm được điều này, Alice gửi cho Bob một chiếc hộp có khóa đã mở sẵn và giữ lại chìa khóa. Bob nhận chiếc hộp, cho vào đó một tờ giấy viết thư bình thường và khóa lại (như loại khoá thông thường chỉ cần sập chốt lại, sau khi sập chốt khóa ngay cả Bob cũng không thể mở lại được-không đọc lại hay sửa thông tin trong thư được nữa). Sau đó Bob gửi chiếc hộp lại cho Alice. Alice mở hộp với chìa

khóa của mình và đọc thông tin trong thư. Trong ví dụ này, chiếc hộp với khóa mở đóng vai trò khóa công khai, chiếc chìa khóa chính là khóa bí mật.

***b. Tạo khóa***

Giả sử Alice và Bob cần trao đổi thông tin bí mật thông qua một kênh không an toàn (ví dụ như Internet). Với thuật toán RSA, Alice đầu tiên cần tạo ra cho mình cặp khóa gồm khóa công khai và khóa bí mật theo các bước sau:

1. Chọn 2 số nguyên tố lớn $p$và $q$với $p \neq q$, lựa chọn ngẫu nhiên và độc lập.
2. Tính: $n = pq$.
3. Tính: giá trị hàm số Ơle $\phi(n) = (p-1)(q-1)$.
4. Chọn một số tự nhiên *e* sao cho $1 < e < \phi(n)$và là số nguyên tố cùng nhau với $\phi(n)$.
5. Tính: *d* sao cho. $de \equiv 1 \pmod{\phi(n)}$

**Khóa công khai** bao gồm:

- *n*, môđun, và
- *e*, số mũ công khai (cũng gọi là *số mũ mã hóa*).

**Khóa bí mật** bao gồm:

- *n*, môđun, xuất hiện cả trong khóa công khai và khóa bí mật, và
- *d*, số mũ bí mật (cũng gọi là *số mũ giải mã*).

Một dạng khác của khóa bí mật bao gồm:

- *p* and *q*, hai số nguyên tố chọn ban đầu,
- *d mod (p-1)* và *d mod (q-1)* (thường được gọi là *dmp1* và *dmq1*),
- *(1/q) mod p* (thường được gọi là *iqmp*)

Dạng này cho phép thực hiện giải mã và ký nhanh hơn với việc sử dụng định lý số dư Trung Quốc (tiếng Anh: *Chinese Remainder Theorem* - CRT). Ở dạng này, tất cả thành phần của khóa bí mật phải được giữ bí mật.

Alice gửi khóa công khai cho Bob, và giữ bí mật khóa cá nhân của mình. Ở đây, *p* và *q* giữ vai trò rất quan trọng. Chúng là các phân tố của n và cho phép tính *d* khi biết *e*. Nếu không sử dụng dạng sau của khóa bí mật (dạng CRT) thì *p* và *q* sẽ được xóa ngay sau khi thực hiện xong quá trình tạo khóa.

***Mã hóa***

Giả sử Bob muốn gửi đoạn thông tin *M* cho Alice. Đầu tiên Bob chuyển *M* thành một số $m < n$ theo một hàm có thể đảo ngược (từ *m* có thể xác định lại *M*) được thỏa thuận trước. Quá trình này được mô tả ở phần #Chuyển đổi văn bản rõ.

Lúc này Bob có *m* và biết *n* cũng như *e* do Alice gửi. Bob sẽ tính *c* là bản mã hóa của *m* theo công thức:

$$c = m^e \mod n$$

Hàm trên có thể tính dễ dàng sử dụng phương pháp tính hàm mũ (theo môđun) bằng (thuật toán bình phương và nhân) Cuối cùng Bob gửi *c* cho Alice.

***Giải mã***

Alice nhận *c* từ Bob và biết khóa bí mật *d*. Alice có thể tìm được *m* từ *c* theo công thức sau:

$$m = c^d \mod n$$

Biết *m*, Alice tìm lại *M* theo phương pháp đã thỏa thuận trước. Quá trình giải mã hoạt động vì ta có

$$c^d \equiv (m^e)^d \equiv m^{ed} \pmod{n}.$$

Do $ed \equiv 1 \pmod{p\text{-}1}$ và $ed \equiv 1 \pmod{q\text{-}1}$, (theo Định lý Fermat nhỏ) nên:

$$m^{ed} \equiv m \pmod{p}$$

và

$$m^{ed} \equiv m \pmod{q}$$

Do *p* và *q* là hai số nguyên tố cùng nhau, áp dụng định lý số dư Trung Quốc, ta có:

$$m^{ed} \equiv m \pmod{pq}.$$

hay:

$$c^d \equiv m \pmod{n}.$$

**Ví dụ**

Sau đây là một ví dụ với những số cụ thể. Ở đây chúng ta sử dụng những số nhỏ để tiện tính toán còn trong thực tế phải dùng các số có giá trị đủ lớn.

Lấy:

$p = 61$ — số nguyên tố thứ nhất (giữ bí mật hoặc hủy sau khi tạo khóa)

$q = 53$ — số nguyên tố thứ hai (giữ bí mật hoặc hủy sau khi tạo khóa)

$n = pq = 3233$ — môđun (công bố công khai)

$e = 17$ — số mũ công khai

$d = 2753$ — số mũ bí mật

Khóa công khai là cặp $(e, n)$. Khóa bí mật là $d$. Hàm mã hóa là:

$$\text{encrypt}(m) = m^e \bmod n = m^{17} \bmod 3233$$

với $m$ là văn bản rõ. Hàm giải mã là:

$$\text{decrypt}(c) = c^d \bmod n = c^{2753} \bmod 3233$$

với $c$ là văn bản mã.

Để mã hóa văn bản có giá trị 123, ta thực hiện phép tính:

$$\text{encrypt}(123) = 123^{17} \bmod 3233 = 855$$

Để giải mã văn bản có giá trị 855, ta thực hiện phép tính:

$$\text{decrypt}(855) = 855^{2753} \bmod 3233 = 123$$

Cả hai phép tính trên đều có thể được thực hiện hiệu quả nhờ giải thuật bình phương và nhân.

***c. Chuyển đổi văn bản rõ***

Trước khi thực hiện mã hóa, ta phải thực hiện việc chuyển đổi văn bản rõ (chuyển đổi từ *M* sang *m*) sao cho không có giá trị nào của M tạo ra văn bản mã không an toàn. Nếu không có quá trình này, RSA sẽ gặp phải một số vấn đề sau:

- Nếu $m = 0$ hoặc $m = 1$ sẽ tạo ra các bản mã có giá trị là 0 và 1 tương ứng
- Khi mã hóa với số mũ nhỏ (chẳng hạn $e = 3$) và *m* cũng có giá trị nhỏ, giá trị $m^e$ cũng nhận giá trị nhỏ (so với *n*). Như vậy phép môđun không có tác dụng và có thể dễ dàng tìm được *m* bằng cách khai căn bậc *e* của *c* (bỏ qua môđun).
- RSA là phương pháp mã hóa xác định (không có thành phần ngẫu nhiên) nên kẻ tấn công có thể thực hiện tấn công lựa chọn bản rõ bằng cách tạo ra một bảng tra giữa bản rõ và bản mã. Khi gặp một bản mã, kẻ tấn công sử dụng bảng tra để tìm ra bản rõ tương ứng.

Trên thực tế, ta thường gặp 2 vấn đề đầu khi gửi các bản tin ASCII ngắn với *m* là nhóm vài ký tự ASCII. Một đoạn tin chỉ có 1 ký tự NUL sẽ được gán giá trị $m = 0$ và cho ra bản mã là 0 bất kể giá trị của *e* và *N*. Tương tự, một ký tự ASCII khác, SOH, có giá trị 1 sẽ luôn cho ra bản mã là 1. Với các hệ thống dùng giá trị *e* nhỏ thì tất cả ký tự ASCII đều cho kết quả mã hóa không an toàn vì giá trị lớn nhất của *m* chỉ là 255 và $255^3$ nhỏ hơn giá trị *n* chấp nhận được. Những bản mã này sẽ dễ dàng bị phá mã.

Để tránh gặp phải những vấn đề trên, RSA trên thực tế thường bao gồm một hình thức chuyển đổi ngẫu nhiên hóa *m* trước khi mã hóa. Quá trình chuyển đổi này phải đảm bảo rằng *m* không rơi vào các giá trị không an toàn. Sau khi chuyển đổi, mỗi bản rõ khi mã hóa sẽ cho ra một trong số khả năng trong tập hợp bản mã. Điều này làm giảm tính khả thi của phương pháp tấn công lựa chọn bản rõ (một bản rõ sẽ có thể tương ứng với nhiều bản mã tuỳ thuộc vào cách chuyển đổi).

***d. Tạo chữ ký số cho văn bản***

Thuật toán RSA còn được dùng để tạo chữ ký số cho văn bản. Giả sử Alice muốn gửi cho Bob một văn bản có chữ ký của mình. Để làm việc này, Alice tạo ra một giá trị băm (hash value) của văn bản cần ký và tính giá trị mũ *d* mod *n* của nó (giống như khi Alice thực hiện giải mã). Giá trị cuối cùng chính là chữ ký điện tử của văn bản đang xét. Khi Bob nhận được văn bản cùng với chữ ký điện tử, anh ta tính giá trị mũ *e* mod *n* của chữ ký đồng thời với việc tính giá trị băm của văn bản. Nếu 2 giá trị này như nhau thì Bob biết rằng người tạo ra chữ ký biết khóa bí mật của Alice và văn bản đã không bị thay đổi sau khi ký.

Cần chú ý rằng các phương pháp chuyển đổi bản rõ giữ vai trò quan trọng đối với quá trình mã hóa cũng như chữ ký điện tử và không được dùng khóa chung cho đồng thời cho cả hai mục đích trên.

***e. An ninh***

Độ an toàn của hệ thống RSA dựa trên 2 vấn đề của toán học: bài toán phân tích ra thừa số nguyên tố các số nguyên lớn và bài toán RSA. Nếu 2 bài toán trên là khó (không tìm được thuật toán hiệu quả để giải chúng) thì không thể thực hiện được việc phá mã toàn bộ đối với RSA. Phá mã một phần phải được ngăn chặn bằng các phương pháp chuyển đổi bản rõ an toàn.

***Bài toán RSA*** là bài toán tính căn bậc *e* môđun *n* (với *n* là hợp số): tìm số *m* sao cho $m^e = c$ mod n, trong đó (*e, n*) chính là khóa công khai và *c* là bản mã. Hiện nay phương pháp triển vọng nhất giải bài toán này là phân tích *n* ra thừa số nguyên tố. Khi thực hiện được điều này, kẻ tấn công sẽ tìm ra số mũ bí mật *d* từ khóa công khai và có thể giải mã theo đúng quy trình của thuật toán. Nếu kẻ tấn công tìm được 2 số nguyên tố *p* và *q* sao cho: *n* = *pq* thì có thể dễ dàng tìm được giá trị (*p*-1)(*q*-1) và qua đó xác định *d* từ *e*. Chưa có một phương pháp nào được tìm ra trên máy tính để giải bài toán này trong thời gian đa thức (*polynomial-time*). Tuy nhiên người ta

cũng chưa chứng minh được điều ngược lại (sự không tồn tại của thuật toán). Xem thêm phân tích ra thừa số nguyên tố về vấn đề này.

Tại thời điểm năm 2005, số lớn nhất có thể được phân tích ra thừa số nguyên tố có độ dài 663 bít với phương pháp phân tán trong khi khóa của RSA có độ dài từ 1024 tới 2048 bít. Một số chuyên gia cho rằng khóa 1024 bít có thể sớm bị phá vỡ (cũng có nhiều người phản đối việc này). Với khóa 4096 bít thì hầu như không có khả năng bị phá vỡ trong tương lai gần. Do đó, người ta thường cho rằng RSA đảm bảo an toàn với điều kiện *n* được chọn đủ lớn. Nếu *n* có độ dài 256 bít hoặc ngắn hơn, nó có thể bị phân tích trong vài giờ với máy tính cá nhân dùng các phần mềm có sẵn. Nếu n có độ dài 512 bít, nó có thể bị phân tích bởi vài trăm máy tính tại thời điểm năm 1999. Vì vậy hiện nay người ta khuyến cáo sử dụng khóa có độ dài tối thiểu 2048 bít.

### *f. Các vấn đề đặt ra trong thực tế*

#### Quá trình tạo khóa

Việc tìm ra 2 số nguyên tố đủ lớn *p* và *q* thường được thực hiện bằng cách thử xác suất các số ngẫu nhiên có độ lớn phù hợp (dùng phép kiểm tra nguyên tố cho phép loại bỏ hầu hết các hợp số).

*p* và *q* còn cần được chọn không quá gần nhau để phòng trường hợp phân tích *n* bằng phương pháp phân tích Fermat. Ngoài ra, nếu *p*-1 hoặc *q*-1 có thừa số nguyên tố nhỏ thì *n* cũng có thể dễ dàng bị phân tích và vì thế *p* và *q* cũng cần được thử để tránh khả năng này.

Bên cạnh đó, cần tránh sử dụng các phương pháp tìm số ngẫu nhiên mà kẻ tấn công có thể lợi dụng để biết thêm thông tin về việc lựa chọn (cần dùng các bộ tạo số ngẫu nhiên tốt). Yêu cầu ở đây là các số được lựa chọn cần đồng thời ngẫu nhiên và không dự đoán được. Đây là các yêu cầu khác nhau: một số có thể được lựa chọn ngẫu nhiên (không có kiểu mẫu trong kết quả) nhưng nếu có thể dự đoán được dù

chỉ một phần thì an ninh của thuật toán cũng không được đảm bảo. Một ví dụ là bảng các số ngẫu nhiên do tập đoàn Rand xuất bản vào những năm 1950 có thể rất thực sự ngẫu nhiên nhưng kẻ tấn công cũng có bảng này. Nếu kẻ tấn công đoán được một nửa chữ số của $p$ hay $q$ thì chúng có thể dễ dàng tìm ra nửa còn lại (theo nghiên cứu của Donald Coppersmith vào năm 1997)

Một điểm nữa cần nhấn mạnh là khóa bí mật $d$ phải đủ lớn. Năm 1990, Wiener chỉ ra rằng nếu giá trị của $p$ nằm trong khoảng $q$ và $2q$ (khá phổ biến) và $d < n^{1/4}/3$ thì có thể tìm ra được $d$ từ $n$ và $e$.

Mặc dù $e$ đã từng có giá trị là 3 nhưng hiện nay các số mũ nhỏ không còn được sử dụng do có thể tạo nên những lỗ hổng (đã đề cập ở phần chuyển đổi văn bản rõ). Giá trị thường dùng hiện nay là 65537 vì được xem là đủ lớn và cũng không quá lớn ảnh hưởng tới việc thực hiện hàm mũ.

**Tốc độ**

RSA có tốc độ thực hiện chậm hơn đáng kể so với DES và các thuật toán mã hóa đối xứng khác. Trên thực tế, Bob sử dụng một thuật toán mã hóa đối xứng nào đó để mã hóa văn bản cần gửi và chỉ sử dụng RSA để mã hóa khóa để giải mã (thông thường khóa ngắn hơn nhiều so với văn bản).

Phương thức này cũng tạo ra những vấn đề an ninh mới. Một ví dụ là cần phải tạo ra khóa đối xứng thật sự ngẫu nhiên. Nếu không, kẻ tấn công (thường ký hiệu là Eve) sẽ bỏ qua RSA và tập trung vào việc đoán khóa đối xứng.

**Phân phối khóa**

Cũng giống như các thuật toán mã hóa khác, cách thức phân phối khóa công khai là một trong những yếu tố quyết định đối với độ an toàn của RSA. Quá trình phân phối khóa cần chống lại được tấn công đứng giữa (*man-in-the-middle attack*). Giả sử Eve có thể gửi cho Bob một khóa bất kỳ và khiến Bob tin rằng đó là khóa

(công khai) của Alice. Đồng thời Eve có khả năng đọc được thông tin trao đổi giữa Bob và Alice. Khi đó, Eve sẽ gửi cho Bob khóa công khai của chính mình (mà Bob nghĩ rằng đó là khóa của Alice). Sau đó, Eve đọc tất cả văn bản mã hóa do Bob gửi, giải mã với khóa bí mật của mình, giữ 1 bản copy đồng thời mã hóa bằng khóa công khai của Alice và gửi cho Alice. Về nguyên tắc, cả Bob và Alice đều không phát hiện ra sự can thiệp của người thứ ba. Các phương pháp chống lại dạng tấn công này thường dựa trên các chứng thực khóa công khai (digital certificate) hoặc các thành phần của hạ tầng khóa công khai (public key infrastructure - PKI).

**Tấn công dựa trên thời gian**

Vào năm 1995, Paul Kocher mô tả một dạng tấn công mới lên RSA: nếu kẻ tấn công nắm đủ thông tin về phần cứng thực hiện mã hóa và xác định được thời gian giải mã đối với một số bản mã lựa chọn thì có thể nhanh chóng tìm ra khóa *d*. Dạng tấn công này có thể áp dụng đối với hệ thống chữ ký điện tử sử dụng RSA. Năm 2003, Dan Boneh và David Brumley chứng minh một dạng tấn công thực tế hơn: phân tích thừa số RSA dùng mạng máy tính (Máy chủ web dùng SSL). Tấn công đã khai thác thông tin rò rỉ của việc tối ưu hóa định lý số dư Trung quốc mà nhiều ứng dụng đã thực hiện.

Để chống lại tấn công dựa trên thời gian là đảm bảo quá trình giải mã luôn diễn ra trong thời gian không đổi bất kể văn bản mã. Tuy nhiên, cách này có thể làm giảm hiệu suất tính toán. Thay vào đó, hầu hết các ứng dụng RSA sử dụng một kỹ thuật gọi là che mắt. Kỹ thuật này dựa trên tính nhân của RSA: thay vì tính $c^d \bmod n$, Alice đầu tiên chọn một số ngẫu nhiên $r$ và tính $(r^e c)^d \bmod n$. Kết quả của phép tính này là $rm \bmod n$ và tác động của r sẽ được loại bỏ bằng cách nhân kết quả với nghịch đảo của r. Đối với mỗi văn bản mã, người ta chọn một giá trị của r. Vì vậy, thời gian giải mã sẽ không còn phụ thuộc vào giá trị của văn bản mã.

**Tấn công lựa chọn thích nghi bản mã**

Năm 1981, Daniel Bleichenbacher mô tả dạng tấn công lựa chọn thích nghi bản mã (adaptive chosen ciphertext attack) đầu tiên có thể thực hiện trên thực tế đối với một văn bản mã hóa bằng RSA. Văn bản này được mã hóa dựa trên tiêu chuẩn PKCS #1 v1, một tiêu chuẩn chuyển đổi bản rõ có khả năng kiểm tra tính hợp lệ của văn bản sau khi giải mã. Do những khiếm khuyết của PKCS #1, Bleichenbacher có thể thực hiện một tấn công lên bản RSA dùng cho giao thức SSL (tìm được khóa phiên). Do phát hiện này, các mô hình chuyển đổi an toàn hơn như chuyển đổi mã hóa bất đối xứng tối ưu (Optimal Asymmetric Encryption Padding) được khuyến cáo sử dụng. Đồng thời phòng nghiên cứu của RSA cũng đưa ra phiên bản mới của PKCS #1 có khả năng chống lại dạng tấn công nói trên.

### 2.2.2.2. Hệ mật Elgamal

***a. Hệ mật El - Gamal***

Hệ mật El - Gamal, ra đời vào năm 1985 và hiệnn nay đã được sử dụng khá rộng rãi . Sự an toàn của hệ mật El - Gamal được dựa trên độ khó của việc tính loga rời rạc.

Việc lập và giải mã của hệ được tiến hành như sau .

B (Bob) chọn một số nguyên tố p và một căn nguyên thuỷ g mod p, tức một phần tử g sao cho các luỹ thừa $g^0$, $g^1$, ..., $g^{p-2}$ đều là những số phân biệt modulo p và bao gồm tất cả những lớp đồng dư khác không modulo p. B cũng chọn một số nguyên a $\in$ { 1, ... , p-2 } và tính h = $g^a$ (mod p).

Khoá công khai của B là (p, g, h) còn số a đựoc giữ bí mật .

A (Alice) cần gửi một bản rõ x cho B với x được mã hoá như một số nguyên dương ≤ p-1. A chọn ngẫu nhiên một số nguyên dương k ≤ p-1, tính $y_1 = g^k \pmod p$ và $y_2 = xh^k \pmod p$ và có được bản mã là cặp $(y_1, y_2)$ .

Chú ý là

- Bản mã dài gấp hai lần bản rõ;

• Với mỗi bản rõ, có thể có p-1 bản mã khác nhau, mỗi bản mã ứng với một phép chọn ngẫu nhiên số k nói ở trên.

Khi nhận được bản mã ($g^k$, $xh^k$) mod p, B tiến hành giải mã như sau. Vì đã biết a là số thoả mãn tính chất $h = g^a$ nên B có thể tính

$$h^k \equiv (g^a)^k \equiv (g^k)^a \bmod p$$

mà không cần biết số bí mật k của A . Bây giờ A có thể tính x bằng việc "chia" $y_2 = xh^k$ cho $h^k$ . Nói một cách chính xác hơn, A dùng thuật toán Euclid suy rộng để tìm nghịch đảo của $h^k$ mod p, rồi nhân $y_2$ với nghịch đảo đó để có được bản rõ x .

Kẻ trộm tin là E (Eve) khi chặn được bản mã, phải đối mặt với bài toán sau :

• Hoặc là phải tìm số a sao cho $h \equiv g^a \pmod p$ để sau đó có thể dùng phương pháp giải mã như B đã làm;

• Hoặc là phải tìm số k sao cho $y_1 = g^k \pmod p$ để sau đó có thể tính trực tiếp $h^k$ và từ đó tìm được x .

Cả hai cách tiếp cận nói trên đều đòi hỏi E phải giải bài toán loga rời rạc, như đã biết là bài toán khó, và cho tới nay chưa có cách nào tốt hơn để phá vỡ hệ mật El - Gamal.

Cũng cần lưu ý là, nếu E có đủ các tài nguyên cần cho việc tính toán (chẳng hạn thời gian và thiết bị) để giải một bài toán loga rời rạc thì E sẽ dùng chúng để giải bài toán thứ nhất (tức tính số a) vì nếu giải được bài toán đó thì E sẽ biết được khoá bí mật của B và có thể đọc được tất cả các thông báo gửi cho B. Còn như nếu giải bài toán thứ hai thì chỉ tìm được số ngẫu nhiên k của A, là số thay đổi theo mỗi thông báo, và như vậy vẫn cùng việc này sẽ phải làm nhiều làn.

Sau đây là một thí dụ minh hoạ. Giả sử B chọn số ngẫu nhiên p = 83, căn nguyên thuỷ g = 2 và số a = 30. Như vậy $h = 2^{30} \bmod 83 = 40$ . Khoá công khai của B là (83, 2, 40). Bây giờ , giả sử bản rõ của A là 54 và số ngẫu nhiên được A chọn là k = 13 . Khi đó bản mã của A sẽ là ($g^k$, $xh^k$) mod p = (58, 71).

Nhận được bản mã trên, B sẽ tính $58^{30} \bmod 83 = 9$. Bằng thuật toán Euclid suy rộng, nghịch đảo của 9 tính được là 37, và như vậy bản rõ là $37.71 \bmod 83 = 54$.

***b. Chữ ký số El - Gamal .***

Vì bản mã trong hệ mật El - Gamal dài gấp đôi bản rõ và phụ thuộc vào việc chọn số ngẫu nhiên k, nên lược đồ El - Gamal cho chữ ký số có phức tạp hơn , chẳng hạn so với việc dùng hệ RSA.

Giả sử khoá công khai El - Gamal của A là (p, g, h), với p là một số nguyên tố, và g là một căn nguyên thuỷ mod p. Khi đó $h \equiv g^a \pmod p$, trong đó chỉ có A là người biết được số a . Để ký một thông báo $x \in \{1, 2, ... , p-1 \}$, A chọn một số ngẫu nhiên k sao cho gcd (k, p-1) = 1. Dùng thuật toán Euclid suy rộng, A tính được nghịch đảo l của k mod (p-1) và sau đó, tính tiếp $z_1 = g^k \bmod p$, $z_2 = ( x - az_1)\ l \bmod (p-1)$ .

Thông báo được ký là $(x, z_1, z_2)$ . Lưu ý là , cũng giống như trong trường hợp mã hoá, thông báo được ký này dài gấp ba lần thông báo chưa được ký và còn phụ thuộc vào số ngẫu nhiên k được chọn. Bây giờ, A mã hoá thông báo được ký này bằng khoá công khai của B và gửi nó cho B.

Nhận đựoc, B giải mã thông báo và tìm được ba thành phần. Thành phần thứ nhất là bản rõ x. Các thành phần thứ hai và thứ ba bao gồm chữ ký. B chấp nhận chữ ký là hợp lệ nếu

Ta cần chứng minh rằng:

1. Nếu A làm đúng theo giao thức, điều kiện trên sẽ được thoả mãn ;
2. E (người trộm tin) không thể giả mạo chữ ký (có nghĩa không thể tạo ra $(x, z_1, z_2)$ thoả mãn điều kiện nêu trên mà không phải giải một bài toán loga rời rạc.

Phần thứ nhất chỉ là việc kiểm tra

Lưu ý là $g^{p-1} \equiv 1 \pmod p$ , nên các luỹ thừa của p có thể được đọc theo mod p-1 . Do có $kl \equiv 1 \pmod{p - 1}$ , nên

Khi đó , với những tính toán đơn giản, có

Phần thứ hai phức tạp hơn và ta không trình bầy ở đây. Rõ ràng là E không thể thực hiện những tính toán như A đã làm khi không biết được số a. Và như vậy, chắc chắn là E không có cách nào khác để có thể giả mạo chữ ký được .

Thí dụ sau đây cho một minh hoạ về cách sử dụng chữ ký số El - Gamal.

Cho khoá công khai của A là (107, 2, 15), với số bí mật a là 11. Như vậy , khi lấy 2 là một căn nguyên thuỷ mod 107, ta có $g^a \equiv 2^{11} = 15 \pmod{107}$. Giả sử A cần gửi thông báo x = 10 cho B và ký thông báo đó . A chọn k = 17, là số nguyên tố cùng p - 1 = 106, và có nghịch đảo bằng 25. Chữ ký số là $(z_1, z_2)$, trong đó

$z_1 = 2^{17} \bmod 107 = 104$ ,

$z_2 = ( 10 - 11.104) .25 \bmod 106 = 58$ .

Sau đó, A mã hoá bản rõ ( 10, 104, 58 ) với khoá công khai của B và gửi nó cho B. Nhận được, B giải mã thông báo và thu được (10, 104, 58). B kiểm tra xem phải chăng $15^{104}. 104^{58} \equiv 2^{10} \pmod{107}$, và thấy là đúng.Khi đó B biết chắc chắn là thông báo được gửi đến từ A.

### *c. Vấn đề tìm căn nguyên thuỷ.*

Hệ mật El - Gamal đòi hỏi mỗi người dùng phải chọn một số nguyên tố p và một căn nguyên thuỷ g mod p. Vậy phải tìm một căn nguyên thuỷ như thế nào?

Có hai cách tiếp cận đã được dùng. Cách tiếp cận thứ nhất xuất phát từ nhận xét là đối với thao tác của phương pháp, việc g phải là một căn nguyên thuỷ không phải là cốt yếu. Điều quan trọng là g phải có nhiều luỹ thừa mod p khác nhau. Như vậy tất cả những gì mà B phải làm là tìm một số g và kiểm tra rằng không có $g^i \equiv 1 \pmod{p}$ với mọi i không quá lớn !

Cách tiếp cận thứ hai dựa trên nhận xét là có những số nguyên tố đặc biệt mà với chúng có thể dễ dàng tìm được một căn nguyên thuỷ. Có một cách làm như sau .

Một cặp số nguyên tố (p, q) được gọi là cặp *Sophie Germain* nếu p = 2q + 1. Những cặp số nguyên tố như vậy có rất nhiều và ý tưởng này do Sophie Germain đưa ra vào năm 1825. Để tìm một cặp số Sophie Germain, có thể tìm trước một số nguyên tố q và sau đó kiểm tra xem p = 2q + 1 có là nguyên tố hay không. Ta có mệnh đề sau:

***<u>Mệnh đề 1</u>. Cho (q, p) là một cặp Sophie Germain. Giả sử rằng 1 < g < p - 2 . Khi đó g là một căn nguyên thuỷ mod p nếu và chỉ nếu $g^q \equiv -1 \pmod p$***

Xem như bài tập trong những ngày Xuân Bính Tuất, độc giả hãy thử chứng minh mệnh đề 1.

Trở lại thí dụ đã xét ở trên, ta thấy (41, 83) là một cặp Sophie Germain. Áp dụng bổ đề 1, để kiểm tra xem 2 có phải là một căn nguyên thuỷ mod 83 không, ta chỉ cần xem $2^{41} \equiv -1 \pmod{83}$ hay không ? Điều này là đúng và có thể được tính trực tiếp hoặc sử dụng một công cụ đã có của lý thuyết số

### 2.2.3. Chữ ký số

Khi nhận được một văn bản bằng giấy, các khía cạnh sau đây thường được xem xét từ phía người nhận:

- Ai là người viết ra, có trách nhiệm với văn bản này?
- Từ khi được gửi đi từ người viết đến khi nhận được từ người đọc, nội dung văn bản có bị thay đổi gì không?
- Người viết văn bản không chối bỏ những nội dung mà mình đã viết ra và gửi đi
- Từ khi được gửi đi từ người viết đến khi nhận được từ người đọc, nội dung văn bản không bị đọc bởi một người thứ ba khác?

Nếu được diễn giải dưới góc độ chuyên môn của an toàn thông tin (Information Security), văn bản này được xem xét dưới các khía cạnh:

- Tính xác thực của người gửi – Authentication
- Tính toàn vẹn của văn bản – Integrity
- Tính chống từ chối, chống chối bỏ - Non-repudiation
- Tính bí mật, tính riêng tư – Privacy

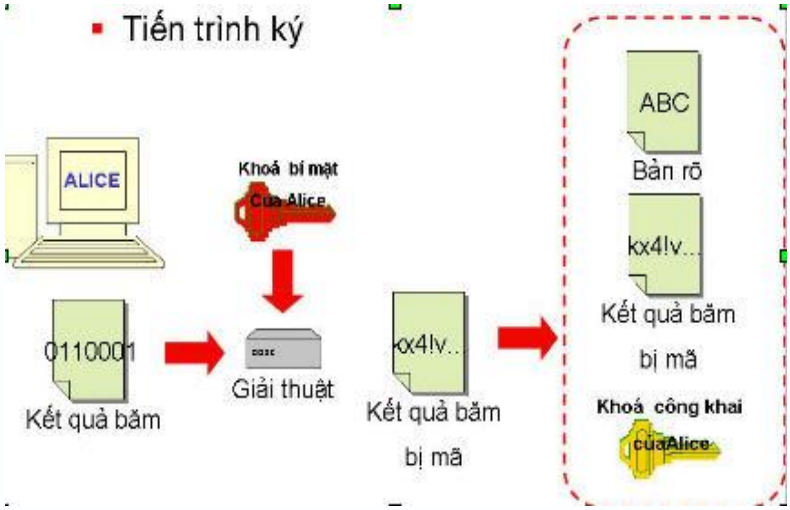
Quay lai một văn bản bằng giấy, các vấn đề trên được giải quyết như thế nào:

- Ai là người viết ra, có trách nhiệm với văn bản này: kiểm tra họ, tên người ký văn bản

- Từ khi được gửi đi từ người viết đến khi nhận được từ người đọc, nội dung văn bản có bị thay đổi gì không: xem xét các chữ kỹ nháy trên từng trang, tính liên tục của đánh số trang,...
- Người viết văn bản không chối bỏ những nội dung mà mình đã viết ra và gửi đi: kiểm tra chữ ký cuối cùng của văn bản là chữ ký hợp lệ của người gửi, so sánh chữ ký này với chữ ký mẫu mà mình đã có
- Từ khi được gửi đi từ người viết đến khi nhận được từ người đọc, nội dung văn bản không bị đọc bởi một người thứ ba khác: kiểm tra phong bì đựng văn bản có còn nguyên trạng không?

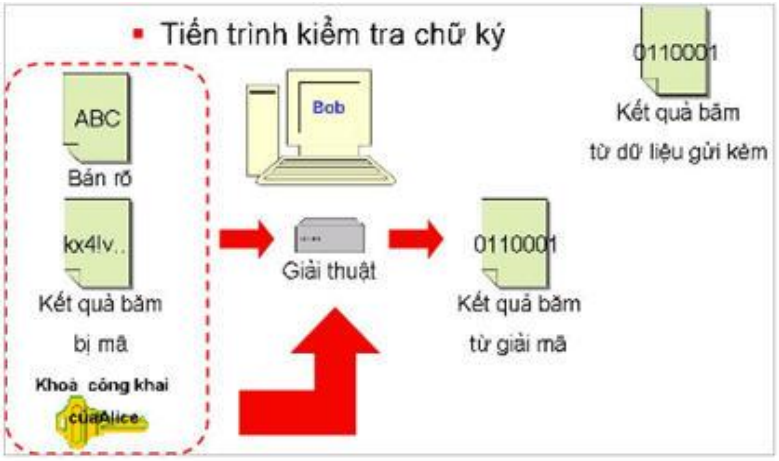
Khi trao đổi một "văn bản" trong môi trường điện tử (một email, một đoạn dữ liệu trong giao dịch, một file dữ liệu,....) cả 4 khía cạnh nêu trên cũng cần được xem xét trong điều kiện không có "chữ ký", "phong bì", ... Tuy nhiên các vấn đề nêu trên đã được giải quyết về mặt công nghệ khi các tiến trình và giải thuật sử dụng khoá đối xứng (asymmetric key) được phát triển và hoàn thiện. Tiến trình xử lý sẽ như sau:

- Đoạn dữ liệu cần được bảo mật được đưa qua hàm băm (hashing), kết quả của hàm băm là một đoạn bit đảm bảo 2 tính chất:
- Tính duy nhất: mỗi một đoạn dữ liệu khác nhau thì sẽ có một đoạn bit khác nhau, không trùng lặp, có độ dài không đổi
- Tính một chiều: từ đoạn bit đặc trưng này, không suy ngược lại được nối dung đoạn văn bản
- Đoạn bit đặc trưng này được mã hoá bằng khoá bí mật của người gửi và được đính kèm vào "văn bản", rồi gửi đến người nhận – **đoạn bit được mã hoá này chính là chữ ký số (digital signature)**




**Hình 1: Minh họa tiến trình chữ ký số**Từ phía người nhận, khi nhận được "văn bản" kèm chữ ký số, tiến trình kiểm tra sẽ như sau:

- Lấy đoạn dữ liệu gốc, đưa qua hàm băm đã nói ở trên, thu được một đoạn bit là kết quả băm
- Lấy đoạn bit được mã hoá (chữ ký số), giải mã bằng khoá công khai của người gửi, thu được đoạn bit đặc trưng
- So sánh đoạn bit vừa thu được với đoạn bit thu được trong bước 1, nếu 2 đoạn trùng nhau và tin rằng khoá công khai chắc chắn là do người gửi phát hành thì kết luận:
- Dữ liệu nhận được có tính toàn vẹn (vì kết quả băm là duy nhất, một chiều)
- Dữ liệu nhận được là do chính người gửi gửi đi vì chỉ duy nhất anh ta mới có khoá bí mật phù hợp với khoá công khai đã được sử dụng để giải mã. Như vậy tính chống từ chối và tính xác thực được kiểm tra và xác nhận. Lúc này người nhận tin rằng, khoá công khai đó đại diện hợp pháp cho người gửi




**Hình 2: Minh hoạ tiến trình kiểm tra chữ ký**

Sau khí ký "văn bản" nếu cần thiết phải cho vào "phong bì" nhằm bảo đảm tính bí mật khi gửi đi, toàn bộ dữ liệu gốc và chữ ký có thể được đưa vào mã hoá bằng khoá đối xứng, chìa khoá của mã khoá đối xứng được mã một lần bởi khoá công khai của người sẽ nhận "văn bản". Khi nhận được, người nhận sẽ sử dụng khoá bí mật mình đang sở hửu để giải mã và lấy được khoá mã, tiếp tục sử dụng khoá mã này sẽ giải mã được văn bản. Như vậy, tính bí mật của giao dịch sẽ được đảm bảo từ người gửi, đến tận người nhận, điều mà các giải pháp mã hoá trên đường truyền như VPN, mã hoá bằng thiết bị cứng không giải quyết được. Tuy nhiên, câu hỏi đặt ra ở đây là: khoá công khai đó có đúng là của người gửi văn bản không, có đại diện cho người gửi văn bản không và khoá công khai này lấy ở đâu để có thể tin cậy được? Trong đó, vai trò của khoá công khai của người gửi có thể được coi như chữ ký mẫu của người gửi khi làm việc với văn bản giấy, chữ ký mẫu này được chấp nhận và phát tán công khai trong toàn hệ thống giao dịch

## 2.3. Chứng chỉ số

Ngày nay, việc giao tiếp qua mạng Internet đang trở thành một nhu cầu cấp thiết. Các thông tin truyền trên mạng đều rất quan trọng, như mã số tài khoản, thông tin mật...Vì vậy giải pháp tài chính đá sử dụng chứng chỉ số để đảm bảo an toàn thông tin.

Tuy nhiên, với các thủ đoạn tinh vi, nguy cơ bị ăn cắp thông tin qua mạng cũng ngày càng gia tăng.

Hiện giao tiếp qua Internet chủ yếu sử dụng giao thức TCP/IP. Đây là giao thức cho phép các thông tin được gửi từ máy tính này tới máy tính khác thông qua một loạt các máy trung gian hoặc các mạng riêng biệt. Chính điều này đã tạo cơ hội cho những "kẻ trộm"công nghệ cao có thể thực hiện các hành động phi pháp. Các thông tin truyền trên mạng đều có thể bị nghe trộm (Eavesdropping), giả mạo (Tampering), mạo danh (Impersonation) .v.v. Các biện pháp bảo mật hiện nay, chẳng hạn như dùng mật khẩu, đều không đảm bảo vì có thể bị nghe trộm hoặc bị dò ra nhanh chóng.

Do vậy, để bảo mật, các thông tin truyền trên Internet ngày nay đều có xu hướng được mã hoá. Trước khi truyền qua mạng Internet, người gửi mã hoá thông tin, trong quá trình truyền, dù có "chặn" được các thông tin này, kẻ trộm cũng không thể đọc được vì bị mã hoá. Khi tới đích, người nhận sẽ sử dụng một công cụ đặc biệt để giải mã. Phương pháp mã hoá và bảo mật phổ biến nhất đang được thế giới áp dụng là chứng chỉ số (Digital Certificate). Với chứng chỉ số, người sử dụng có thể mã hoá thông tin một cách hiệu quả, chống giả mạo (cho phép người nhận kiểm tra thông tin có bị thay đổi không), xác thực danh tính của người gửi. Ngoài ra chứng chỉ số còn là bằng chứng giúp chống chối cãi nguồn gốc, ngăn chặn người gửi chối cãi nguồn gốc tài liệu mình đã gửi.

Chứng chỉ số là một tệp tin điện tử dùng để xác minh danh tính một cá nhân, một máy chủ, một công ty... trên Internet. Nó giống như bằng lái xe, hộ chiếu, chứng minh thư hay những giấy tờ xác minh cá nhân. Để có chứng minh thư, bạn phải được cơ quan Công An sở tại cấp. Chứng chỉ số cũng vậy, phải do một tổ chức đứng ra chứng nhận những thông tin của bạn là chính xác, được gọi là Nhà cung cấp chứng thực số (Certificate Authority, viết tắt là CA). CA phải đảm bảo về độ tin cậy, chịu trách nhiệm về độ chính xác của chứng chỉ số mà mình cấp.

Trong chứng chỉ số có ba thành phần chính:

- Thông tin cá nhân của người được cấp
- Khoá công khai (Public key) của người được cấp

- Chữ ký số của CA cấp chứng chỉ

***a. Thông tin cá nhân:***

Đây là các thông tin của đối tượng được cấp chứng chỉ số, gồm tên, quốc tịch, địa chỉ, điện thoại, email, tên tổ chức .v.v. Phần này giống như các thông tin trên chứng minh thư của mỗi người.

***b. Khoá công khai***

Trong khái niệm mật mã, khoá công khai là một giá trị được nhà cung cấp chứng thực đưa ra như một khóa mã hoá, kết hợp cùng với một khoá cá nhân duy nhất được tạo ra từ khoá công khai để tạo thành cặp mã khoá bất đối xứng. Nguyên lý hoạt động của khoá công khai trong chứng chỉ số là hai bên giao dịch phải biết khoá công khai của nhau. Bên A muốn gửi cho bên B thì phải dùng khoá công khai của bên B để mã hoá thông tin. Bên B sẽ dùng khoá cá nhân của mình để mở thông tin đó ra. Tính bất đối xứng trong mã hoá thể hiện ở chỗ khoá cá nhân có thể giải mã dữ liệu được mã hoá bằng khóa công khai (trong cùng một cặp khoá duy nhất mà một cá nhân sở hữu), nhưng khoá công khai không có khả năng giải mã lại thông tin, kể cả những thông tin do chính khoá công khai đó đã mã hoá. Đây là đặc tính cần thiết vì có thể nhiều cá nhân B,C, D... cùng thực hiện giao dịch và có khoá công khai của A, nhưng C,D... không thể giải mã được các thông tin mà B gửi cho A dù cho đã chặn bắt được các gói thông tin gửi đi trên mạng.

Hiểu một cách nôm na, nếu chứng chỉ số là một chứng minh thư nhân dân, thì khoá công khai đóng vai trò như danh tính của bạn trên giấy chứng minh thư (gồm tên địa chỉ, ảnh...), còn khoá cá nhân là gương mặt và dấu vân tay của bạn. Nếu coi một bưu phẩm là thông tin truyền đi, được "mã hoá" bằng địa chỉ và tên người nhận của bạn, thì dù ai đó có dùng chứng minh thư của bạn với mục đich lấy bưu phẩm này, họ cũng không được nhân viên bưu điện giao bưu kiện vì ảnh mặt và dấu vân tay không giống.

***c. Chữ ký số của CA cấp chứng chỉ*:**

Còn gọi là chứng chỉ gốc. Đây chính là sự xác nhận của CA, bảo đảm tính chính xác và hợp lệ của chứng chỉ. Muốn kiểm tra một chứng chỉ số, trước tiên phải

kiểm tra chữ ký số của CA có hợp lệ hay không. Trên chứng minh thư, đây chính là con dấu xác nhận của Công An Tỉnh hoặc Thành phố mà bạn trực thuộc. Về nguyên tắc, khi kiểm tra chứng minh thư, đúng ra đầu tiên phải là xem con dấu này, để biết chứng minh thư có bị làm giả hay không.

***d. Lợi ích của chứng chỉ số***

***Mã hoá***

Lợi ích đầu tiên của chứng chỉ số là tính bảo mật thông tin. Khi người gửi đã mã hoá thông tin bằng khoá công khai của bạn, chắc chắn chỉ có bạn mới giải mã được thông tin để đọc. Trong quá trình truyền thông tin qua Internet, dù có đọc được các gói tin đã mã hoá này, kẻ xấu cũng không thể biết được trong gói tin có thông tin gì. Đây là một tính năng rất quan trọng, giúp người sử dụng hoàn toàn tin cậy về khả năng bảo mật thông tin. Những trao đổi thông tin cần bảo mật cao, chẳng hạn giao dịch liên ngân hàng, ngân hàng điện tử, thanh toán bằng thẻ tín dụng, đều cần phải có chứng chỉ số để đảm bảo an toàn.

***Chống giả mạo***

Khi bạn gửi đi một thông tin, có thể là một dữ liệu hoặc một email, có sử dụng chứng chỉ số, người nhận sẽ kiểm tra được thông tin của bạn có bị thay đổi hay không. Bất kỳ một sự sửa đổi hay thay thế nội dung của thông điệp gốc đều sẽ bị phát hiện. Địa chỉ mail của bạn, tên domain... đều có thể bị kẻ xấu làm giả để đánh lừa người nhận để lây lan virus, ăn cắp thông tin quan trọng. Tuy nhiên, chứng chỉ số thì không thể làm giả, nên việc trao đổi thông tin có kèm chứng chỉ số luôn đảm bảo an toàn.

***Xác thực***

Khi bạn gửi một thông tin kèm chứng chỉ số, người nhận - có thể là đối tác kinh doanh, tổ chức hoặc cơ quan chính quyền - sẽ xác định rõ được danh tính của bạn. Có nghĩa là dù không nhìn thấy bạn, nhưng qua hệ thống chứng chỉ số mà bạn và người nhận cùng sử dụng, người nhận sẽ biết chắc chắn đó là bạn chứ không phải là một người khác. Xác thực là một tính năng rất quan trọng trong việc thực hiện các giao dịch điện tử qua mạng, cũng như các thủ tục hành chính với cơ quan pháp quyền. Các hoạt động này cần phải xác minh rõ người gửi thông tin để sử dụng tư

cách pháp nhân. Đây chính là nền tảng của một Chính phủ điệntử, môi trường cho phép công dân có thể giao tiếp, thực hiện các công việc hành chính với cơ quan nhà nước hoàn toàn qua mạng. Có thể nói, chứng chỉ số là một phần không thể thiếu, là phần cốt lõi của Chính phủ điện tử.

***Chống chối cãi nguồn gốc***

Khi sử dụng một chứng chỉ số, bạn phải chịu trách nhiệm hoàn toàn về những thông tin mà chứng chỉ số đi kèm. Trong trường hợp người gửi chối cãi, phủ nhận một thông tin nào đó không phải do mình gửi (chẳng hạn một đơn đặt hàng qua mạng), chứng chỉ số mà người nhận có được sẽ là bằng chứng khẳng định người gửi là tác giả của thông tin đó. Trong trường hợp chối cãi, CA cung cấp chứng chỉ số cho hai bên sẽ chịu trách nhiệm xác minh nguồn gốc thông tin, chứng tỏ nguồn gốc thông tin được gửi.

***Bảo mật Website***

Khi Website của bạn sử dụng cho mục đích thương mại điện tử hay cho những mục đích quan trọng khác, những thông tin trao đổi giữa bạn và khách hàng của bạn có thể bị lộ. Để tránh nguy cơ này, bạn có thể dùng chứng chỉ số SSL Server để bảo mật cho Website của mình. Chứng chỉ số SSL Server sẽ cho phép bạn lập cấu hình Website của mình theo giao thức bảo mật SSL (Secure Sockets Layer). Loại chứng chỉ số này sẽ cung cấp cho Website của bạn một định danh duy nhất nhằm đảm bảo với khách hàng của bạn về tính xác thực và tính hợp pháp của Website. Chứng chỉ số SSL Server cũng cho phép trao đổi thông tin an toàn và bảo mật giữa Website với khách hàng, nhân viên và đối tác của bạn thông qua công nghệ SSL mà nổi bật là các tính năng:

+ Thực hiện mua bán bằng thẻ tín dụng
+ Bảo vệ những thông tin cá nhân nhạy cảm của khách hàng
+ Đảm bảo hacker không thể dò tìm được mật khẩu

***Đảm bảo phần mềm***

Nếu bạn là một nhà sản xuất phần mềm, chắc chắn bạn sẽ cần những "con tem chống hàng giả" cho sản phẩm của mình. Đây là một công cụ không thể thiếu trong việc áp dụng hình thức sở hữu bản quyền. Chứng chỉ số Nhà phát triển phần mềm

sẽ cho phép bạn ký vào các applet, script, Java software, ActiveX control, các file dạng EXE, CAB, DLL... Như vậy, thông qua chứng chỉ số, bạn sẽ đảm bảo tính hợp pháp cũng như nguồn gốc xuất xứ của sản phẩm. Hơn nữa người dùng sản phẩm có thể xác thực được bạn là nhà cung cấp, phát hiện được sự thay đổi của chương trình (do vô tình hỏng hay do virus phá, bị crack và bán lậu...).

# Chương 3:
# TÌM HIỂU HOẠT ĐỘNG TÀI CHÍNH Ở MỘT SỐ ĐƠN VỊ

## 3.1. Ứng dụng công nghệ thông tin trong Hải quan

Ứng dụng CNTT hiện nay được coi là một cấu phần chính trong phương pháp quản lý mới. đặc biệt, trong các biện pháp cải cách hành chính như cải cách về thể chế, về hạ tầng cơ sở vật chất, về nguồn lực… thì CNTT là phương tiện tiên quyết để thực hiện, triển khai các phương thức quản lý hiện đại, toàn diện trong các tổ chức hành chính và doanh nghiệp.

Việc áp dụng CNTT trong ngành Hải quan được thực hiện toàn diện, đem lại hiệu quả về nhiều mặt. Đối với công tác quản lý, CNTT giúp xây dựng cơ sở dữ liệu khoa học, an toàn phục vụ công tác quản lý, ra quyết định của người lãnh đạo. Nhờ ứng dụng CNTT trong các khâu quản lý mà ngành cũng đảm bảo tính liêm chính và chuyên nghiệp cao, xây dựng được quy chế dân chủ cơ sở bền vững, tạo sức mạnh về nội lực. Đối với doanh nghiệp và các tổ chức xã hội và người dân, ngành đã ứng dụng tốt CNTT để xây dựng các kênh thông tin tuyên truyền (báo chí, website, cổng thông tin điện tử tư vấn trực tuyến…), thực hiện chức năng cầu nối giữa cơ quan quản lý với người sử dụng; xây dựng và áp dụng hệ thống thông quan tiên tiến, giảm giấy tờ, chi phí, thời gian, giảm phiền hà cho doanh nghiệp; triển khai cơ chế một cửa, hình thành mối quan hệ tương tác hai chiều giữa doanh nghiệp với cơ quan qua các dịch vụ hành chính công.

Kết quả nổi bật mà ứng dụng CNTT đem lại đó là đã làm thay đổi hình ảnh cơ quan quản lý nhà nước trở thành cơ quan phục vụ mang tính chuyên nghiệp cao, tích cực chủ động cung cấp nhiều dịch vụ hải quan cho doanh nghiệp và người dân khi tham gia các hoạt động thương mại Quốc tế

Đầu tư cho CNTT trong ngành Hải quan đã và đang được thực hiện một cách mạnh mẽ và liên tục trong những năm qua. 5 năm tới đây, ứng dụng CNTT cần đạt được những mục tiêu: Thực hiện cải cách hành chính nhà nước trong ngành Hải quan; thực hiện thành công dự án hiện đại hóa của Ngân hàng thế giới, nâng cao năng

lực quản lý của ngành Hải quan; xây dựng thành công hệ thống thông quan điện tử trong toàn ngành.

Song song với thực hiện những nhiệm vụ hiện tại, ngành Hải quan cũng đã xây dựng cho mình một tầm nhìn xa hơn, cùng với đất nước thực hiện thành công công cuộc cải cách, hiện đại hóa đến năm 2020. Đến năm 2020, ngành Hải quan phấn đấu đạt được những chuẩn mực cơ bản của một cơ quan Hải quan hiện đại với những nội dung cơ bản:

- Hệ thống pháp luật Hải quan đầy đủ, minh bạch, phù hợp với chuẩn mực quốc tế
- Lực lượng Hải quan đạt được trình độ chuyên nghiệp, chuyên sâu
- Thủ tục Hải quan đơn giản, hài hòa, thống nhất, đạt chuẩn mực quốc tế, dựa trên nền tảng ứng dụng CNTT, áp dụng kỹ thuật quản lý rủi
- Trang thiết bị kỹ thuật hiện đại và sử dụng công nghệ cao.

### 3.1.1. Thủ tục hải quan điện tử

Thủ tục hải quan điện tử vẫn còn nặng bởi bên cạnh việc kê khai hải quan qua mạng, các doanh nghiệp vẫn phải đáp ứng các yêu cầu giấy tờ khác.

Trong Quy trình thực hiện thí điểm thủ tục hải quan điện tử đối với hàng hoá xuất nhập khẩu vừa được ký ban hành, Bộ Tài chính đã thể hiện sự nỗ lực của các cơ quan chức năng trong việc đơn giản hoá các thủ tục hải quan. Để thực hiện hải quan điện tử, các doanh nghiệp được khai thông tin trên máy tính (theo mẫu sẵn) qua mạng.

Tuy nhiên, trong các thủ tục hải quan điện tử vẫn còn nặng về giấy tờ hành chính. Bởi song song việc kê khai hải quan qua mạng, các doanh nghiệp vẫn phải đáp ứng các yêu cầu giấy tờ khác.

***Vừa điện tử, vừa giấy!***

Cụ thể, song song với việc kê khai qua mạng như trên, doanh nghiệp vẫn phải gửi hồ sơ gồm các thông tin đã khai hải quan điện tử đến chi cục hải quan điện tử (nơi đăng ký tham gia). Sau đó, doanh nghiệp tiếp tục đợi và thực hiện theo các

hướng dẫn của hải quan, sửa đổi các nội dung khi cơ quan hải quan yêu cầu, in 2 bản tờ khai hải quan điện tử ra để... nộp cho hải quan.

Đối với hàng hoá được Chi cục hải quan điện tử chấp nhận thông tin đã khai điện tử và thông quan doanh nghiệp tiếp tục mang tờ khai điện tử (đã in ra) đến bộ phận giám sát của Chi cục hải quan cửa khẩu, nơi có hàng hoá xuất nhập khẩu, để thông quan hàng hoá.

Đối với hàng hoá Chi cục hải quan điện tử yêu cầu phải xuất trình, nộp chứng từ giấy thuộc hồ sơ hải quan trước khi thông quan thì doanh nghiệp phải nộp hoặc xuất trình tờ khai in cùng các chứng từ giấy thuộc hồ sơ hải quan yêu cầu.

Các hàng hoá hải quan điện tử yêu cầu phải xuất trình chứng từ giấy thuộc hồ sơ hải quan và kiểm tra thực tế hàng hoá. Doanh nghiệp phải nộp, xuất trình tờ khai in cùng các chứng từ giấy thuộc hồ sơ hải quan cho chi cục hải quan điện tử và xuất trình hàng hoá cho chi cục hải quan cửa khẩu để kiểm tra theo yêu cầu.

Riêng đối với hàng hoá xuất khẩu, nhập khẩu thuộc danh mục cấm hoặc có điều kiện thì doanh nghiệp phải nộp hoặc xuất trình các loại giấy phép hoặc văn bản cho phép. Ví như giấy đăng ký kiểm tra chất lượng hàng hoá, thông báo miễn kiểm tra, giấy đăng ký kiểm dịch, kết quả giám định phân tích... với hàng hoá.

Nếu hải quan chấp nhận thông quan hàng hoá trên cơ sở thông tin doanh nghiệp đã khai, hàng hoá được xếp vào "luồng xanh". Nếu phải kiểm tra chứng từ giấy thuộc hồ sơ hải quan trước khi thông quan, hàng hoá phải qua "luồng vàng".

Với trường hợp hàng phải kiểm tra chứng từ giấy thuộc hồ sơ hải quan và kiểm tra thực tế hàng hoá trước khi thông quan hàng hoá, xếp hạng "luồng đỏ".

Với "luồng xanh", doanh nghiệp vẫn phải mang 2 tờ khai điện tử (đã in ra) đến bộ phận giám sát để thông quan hàng hoá. Bộ phận này đối chiếu tờ khai in với thông tin trên hệ thống điện tử. Sau đó xác nhận và đóng dấu "đã thông quan điện tử" trên

tờ khai in. Hải quan lại tiếp tục cập nhật kết quả đã xác nhận vào hệ thống xử lý dữ liệu hải quan điện tử.

***Mất 3 ngày để cấp phép hải quan điện tử!***

Trong quy định mới của mình, Bộ Tài chính yêu cầu Chi cục hải quan điện tử trong thời hạn chậm nhất 3 ngày từ ngày nhận được bản đăng ký của doanh nghiệp phải kiểm tra các tiêu chí trên văn bản và trình Cục trưởng phê duyệt. Sau đó, cấp tài khoản truy cập và Giấy công nhận tham gia thủ tục hải quan điện tử cho doanh nghiệp. Nếu từ chối cũng không được quá thời gian trên.

Với hải quan điện tử, hàng hoá nhập khẩu được thực hiện trước ngày hàng hoá đến cửa khẩu hoặc trong 30 ngày. Thông tin khai hải quan điện tử có giá trị làm thủ tục hải quan trong thời hạn 15 ngày, kể từ ngày hải quan chấp nhận thông tin khai hải quan điện tử.

Hàng hoá xuất khẩu được thực hiện chậm nhất là 8 giờ trước khi phương tiện vận tải xuất cảnh. Thông tin khai hải quan điện tử có giá trị làm thủ tục hải quan trong thời hạn 15 ngày.

Doanh nghiệp tham gia hải quan điện tử được đào tạo, cung cấp các văn bản quy định về thủ tục hải quan điện tử được đề nghị cơ quan hải quan giải đáp các vướng mắc liên quan đến quá trình thực hiện thủ tục hải quan điện tử.

Hải quan phải có trách nhiệm giải thích, hướng dẫn cho doanh nghiệp. Mọi thắc mắc, tranh chấp, khiếu nại được lưu tại hệ thống xử lý dữ liệu hải quan điện tử.

Các doanh nghiệp thuộc mọi thành phần kinh tế tự nguyện đăng ký và được cơ quan hải quan chấp nhận tham gia thủ tục hải quan điện tử.

Theo lý giải của hải quan, với hình thức thông quan điện tử, doanh nghiệp chỉ cần sử dụng máy tính có nối mạng trực tiếp với cơ quan hải quan hoặc thông

qua một doanh nghiệp trung gian để thực hiện khai báo và truyền thẳng thông tin khai báo về hàng hoá xuất nhập khẩu tới hải quan.

Sau đó, hải quan sẽ phân luồng hàng hóa và quyết định hình thức kiểm tra thông qua hệ thống xử lý dữ liệu điện tử tự động trên cơ sở phân tích, xử lý thông tin về hàng hoá. Với kết quả xử lý dữ liệu của hệ thống mạng nội bộ và các phần mềm chuyên ngành cung cấp, hải quan sẽ quyết định thông quan hay không với lô hàng.

Cách làm này cũng giúp cơ quan hải quan chuyển từ kiểm tra, kiểm soát từng lô hàng sang quản lý toàn bộ thông tin về quá trình hoạt động xuất nhập khẩu của doanh nghiệp, tăng cường chống buôn lậu, gian lận thương mại và hạn chế thất thu thuế.

Đồng thời, theo Tổng cục hải quan, thực hiện thông quan điện tử sẽ giảm chi phí, thời gian làm thủ tục cho doanh nghiệp; giúp hạn chế tiêu cực giữa cán bộ hải quan và DN. Các nước trong khu vực đã áp dụng hình thức này từ lâu.

### 3.1.2. Mở rộng thủ tục Hải quan điện tử giai đoạn 2009 - 2010

Hệ thống quy trình thủ tục hải quan điện tử đã bao trùm các khâu trước, trong và sau thông quan. Đã mở rộng thủ tục hải quan điện tử cho hàng gia công, nhập nguyên liệu để sản xuất hàng xuất khẩu, hàng hóa xuất nhập khẩu chuyển cửa khẩu. DN được hưởng sự ưu tiên về thủ tục và được cơ quan hải quan hỗ trợ kịp thời trong quá trình khai báo cũng như làm thủ tục. Số lượng giấy tờ phải nộp/ xuất trình giảm hẳn so với thủ tục hải quan truyền thống. Thời gian thông quan trung bình được rút ngắn, chi phí thông quan hàng hóa giảm, đặc biệt với hàng kinh doanh xuất khẩu, thủ tục hải quan điện tử đã thể hiện tính thuận lợi so với thủ tục hải quan truyền thống. DN và cơ quan hải quan có khả năng kiểm soát toàn bộ quá trình luân chuyển của bộ hồ sơ cũng như việc thực hiện thủ tục hải quan của nhân viên cấp dưới. Thông tin khai hải quan cũng trở nên nhất quán, chuẩn hóa cả từ phía DN và HQ, tạo thuận lợi cho công tác quản lý tại khâu thông quan và các khâu sau.

Theo số liệu thống kê từ 2006 đến 2008: đã có 537 DN tham gia, thông quan cho gần 100.000 tờ khai với lưu lượng trung bình năm 2008 đạt 116 tờ khai/ ngày

(tăng 17% so với 2007). Tổng kim ngạch xuất nhập khẩu từ 2006 đến 2008 đạt xấp xỉ 9,853 tỷ USD với số thuế thu được xấp xỉ 9,287 tỷ đồng. Kim ngạch xuất nhập khẩu đối với hàng hóa làm thủ tục tại Chi cục Hải quan điện tử tại Hải Phòng và TP Hồ Chí Minh chiếm lần lượt 3,7%; 6,2% và 7,0% (theo các năm 2006, 9 tháng đầu năm 2007, 9 tháng đầu năm 2008) trên tổng kim ngạch XNK đối với hàng hóa làm thủ tục tại hai Cục Hải quan trên. Tỷ lệ phân luồng tại Hải Phòng: Xanh: 67%, Vàng: 10%, Đỏ: 23%. Tại TP Hồ Chí Minh: Xanh: 39%, Vàng: 49%, Đỏ: 12%. Thời gian thông quan trung bình đối với các lô hàng luồng xanh là 5 – 10 phút, luồng vàng từ 20 – 30 phút, luồng đỏ phụ thuộc vào thời gian kiểm tra hàng hóa.

Tuy nhiên, qua thời gian thực hiện vẫn còn những tồn tại. Một số nội dung trong thủ tục Hải quan điện tử vẫn còn chậm triển khai hoặc chưa thể triển khai, các nội dung đã triển khai mới chỉ áp dụng với số lượng DN tham gia và địa bàn áp dụng còn hạn chế. Mô hình thông quan với giai đoạn đầu nhưng khó mở rộng. Phầm mềm ứng dụng triển khai chưa đạt tiến độ, vẫn còn phải hiệu chỉnh nhiều trong quá trình triển khai. Hạ tầng mạng và thiết bị tuy đã được nâng cấp nhưng chưa hoàn thiện, dịch vụ C-VAN vẫn chưa thực sự hoàn thiện.

Trong thời gian tới, Tổng cục Hải quan sẽ chuyển sang triển khai mở rộng áp dụng thủ tục hải quan điện tử cả theo chiều sâu (mở rộng về đối tượng và loại hình) và chiều rộng (về địa bàn). Giai đoạn từ nay đến tháng 6/2009, tiến hành các bước mở rộng ra các cục Hải quan Đồng Nai, Bình Dương. Giai đoạn từ 6/2009 đến 12/2009: tiến hành các bước triển khai mở rộng cho các chi cục Hải quan Hà Nội, Lạng Sơn, Đà Nẵng. Đối với các cục HQ khác, tiếp tục đẩy mạng tiếp nhận khai hải quan qua mạng, từ xa để làm tiền đề mở rộng sang thủ tục HQ điện tử.

Để đạt được các mục tiêu đề ra, về nội lực, ngành Hải quan sẽ tiến hành cải thiện về cơ sở pháp lý, quy trình nghiệp vụ, với mô hình thông quan và mô hình tổ chức phù hợp, về hệ thống CNTT và các điều kiện đảm bảo khác. Ngoài ra, để công cuộc cải cách thành công, cũng rất cần sự phối hợp giữa các đơn vị thuộc Bộ Tài chính và các bộ, ngành khác trong việc ban hành các chính sách quản lý cũng như chuẩn hóa, mã hóa các danh mục quản lý chuyên ngành; đẩy nhanh quá trình triển khai hạ tầng kỹ thuật và pháp lý liên quan đến giao dịch điện tử; quy hoạch lại

các điểm làm thủ tục HQ, địa điểm kiểm tra hàng hóa tập trung tại các cảng biển, sân bay, khu công nghiệp… để có thể đầu tư trang thiết bị kiểm tra, giám sát.

## 3.2. Ứng dụng công nghệ thông tin trong ngành Thuế

### 3.2.1. Các cơ sở pháp lý cho ứng dụng CNTT trong ngành thuế

Ngày 15/6/2007, Bộ trưởng Bộ Tài chính đã ký Quyết định số 2090/QĐ-BTC về chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục Ứng dụng Công nghệ thông tin trực thuộc Tổng cục Thuế. Theo đó, Cục Ứng dụng Công nghệ thông tin là tổ chức trực thuộc Tổng cục Thuế, có chức năng giúp Tổng cục Trưởng Tổng cục Thuế nghiên cứu, xây dựng và tổ chức triển khai ứng dụng công nghệ thông tin hiện đại hoá công tác quản lý thuế.

Với những bước đi vững chắc, công tác tin học của hệ thống Thuế đã không ngừng phát triển, bước đầu đã đáp ứng được yêu cầu của công tác quản lý thu thuế. Đến nay, công tác tin học hệ thống Thuế đã đạt được những kết quả đáng khích lệ:

- Đã xây dựng được hệ thống các ứng dụng phục vụ cho các nhiệm vụ trọng tâm của hệ thống Thuế. Đó là: Chương trình đăng ký thuế và cấp mã số thuế; Chương trình quản lý thu thuế; Chương trình quản lý ấn chỉ thuế; Trang thông tin Tổng cục Thuế.
- Thiết lập được hệ thống cơ sở dữ liệu (CSDL) thống nhất: Việc ứng dụng CNTT vào công tác quản lý thuế thời gian qua đã tạo lập được các kho cơ sở dữ liệu thông tin phục vụ thiết thực cho việc tra cứu, phân tích thông tin của hệ thống Thuế. Đến nay, ngành Thuế đã thiết lập được các cơ sở dữ liệu chính: CSDL về đối tượng nộp thuế; CSDL quản lý thuế; CSQL quản lý nội bộ; CSDL chính sách thuế.
- Tạo lập hạ tầng kỹ thuật hiện đại, hệ thống mạng xuyên suốt trong ngành: Trung tâm tin học thống kê Tổng cục Thuế đã xây dựng được hệ thống mạng máy tính kết nối, trao đổi thông tin, dữ liệu toàn ngành từ Tổng cục đến 63 Cục thuế và khoản gần 600 Chi cục Thuế quận, huyện. Những thông tin cơ bản về số thu nộp thuế được truyền giữa các cấp và được máy tính xử lý tự động.

- Hình thành bộ máy xử lý thông tin và tin học, xây dựng đội ngũ cán bộ làm CNTT nhiệt tình.

Trong thời gian tới, ngành Thuế sẽ tiếp tục đẩy mạnh công tác ứng dụng CNTT hơn nữa để phục vụ tốt cho công tác cải cách thuế bước hai và nhằm vào những định hướng chính mà công tác tin học hệ thống Thuế đã đặt ra:

- Cục Ứng dụng CNTT Tổng cục Thuế sẽ triển khai các hệ thống ứng dụng hợp nhất phục vụ cho các lĩnh vực quản lý thuế như: quản lý tính thuế, phục vụ thanh tra, kiểm tra thuế và phục vụ đối tượng nộp thuế. Hệ thống ứng dụng của đơn vị sẽ tích hợp với hệ thống ứng dụng của toàn ngành Tài chính. Các đơn vị thuộc hệ ngành Thuế sẽ có thể truy cập các thông tin cần thiết để thực hiện công việc chuyên môn. Các đối tượng nộp thuế sẽ được cơ quan thuế cung cấp thông tin phục vụ cho việc tự kê khai và nộp thuế. Các cơ quan liên quan trong Bộ Tài chính cũng như một số Bộ, ngành liên quan có thể khai thác thông tin từ hệ thống thông tin ngành Thuế.
- Tổng cục Thuế sẽ trở thành trung tâm xử lý, phân tích thông tin phục vụ cho công tác chỉ đạo thu và tuyên truyền chính sách thuế phục vụ đối tượng nộp thuế. Hệ thống tin học cấp Cục thuế, Chi cục Thuế sẽ là các hệ thống xử lý thông tin trực tiếp về các nghiệp vụ quản lý thuế.
- Hệ thống cơ sở dữ liệu thống nhất toàn ngành Thuế được hoàn thiện dần từng bước. Tại từng cấp có cơ sở dữ liệu tác nghiệp riêng và tại Tổng cục Thuế sẽ hình thành Kho dữ liệu trung tâm của toàn ngành. Nghiên cứu hướng hình thành cơ sở dữ liệu cấp vùng.
- Tăng cường tự động hoá việc trao đổi thông tin giữa các cấp trong ngành Thuế, giữa ngành Thuế với cơ quan Kho bạc, Tài chính và các ngành liên quan. Hình thành dần trung tâm xử lý dữ liệu cấp vùng để tăng khả năng xử lý thông tin, đầu tư có trọng điểm, giảm chi phí và đem lại hiệu quả cao. Củng cố hệ thống mạng máy tính thống nhất trong toàn ngành Thuế, đảm bảo tính an toàn, bảo mật hệ thống.

- Bổ sung cán bộ có trình độ chuyên ngành tin học cho cấp Tổng cục thuế và một số Cục thuế đang còn thiếu. Nghiên cứu xây dựng chế độ bối dưỡng để thu hút cán bộ tin học có trình độ làm việc cho ngành thuế.

### 3.2.2. Kê khai thuế điện tử ở Việt Nam

Đến nay về môi trường pháp lý, Nhà nước ta đã ban hành nhiều văn bản pháp luật có liên quan như Luật Giao dịch điện tử, các Nghị định về giao dịch điện tử trong lĩnh vực tài chính, ngân hàng... và đã tương đối đầy đủ về mặt lý thuyết để thực hiện kê khai thuế điện tử ở Việt Nam. Tuy nhiên, đi sâu vào các vấnđề thì chúng ta thấy vẫn còn thiếu các quy định cụ thể, ví dụ như quy định tờ khai thuế điện tử là như thế nào (phải có mẫu để người dân nhìn thấy được), tờ khai thuế điện tử được lưu trữ và quản lý như thế nào tại cơ quan Thuế và tại người nộp thuế để có thể sử dụng và đối chiếu khi cần; thủ tục để người nộp thuế sử dụng phương thức kê khai thuế điện tử và việc sử dụng các giải pháp an toàn bảo mật (mật khẩu, chữ ký điện tử,...) phải được cụ thể hoá.

Chúng ta nhận thấy rằng, quy trình nghiệp vụ cần bổ sung, sửa đổi hoặc thay thế các quy trình nghiệp vụ hiện có vì khi giao dịch điện tử sẽ có nhiều bước thực hiện sẽ không nhìn thấy được như hiện nay. Bên cạnh đó, cơ sở hạ tầng kỹ thuật cần xây dựng các trung tâm xử lý dữ liệu hoạt động liên tục tại Tổng cục Thuế và có các giải pháp đảm bảo an toàn dữ liệu, giải pháp dự phòng khắcấphục sự cố để đảm bảo tính sẵn sàng cao. Đồng thời cần có các tổ chức trung gian với điều kiện đảm bảo về môi trường kỹ thuật để tiếp nhận các giao dịch điện tử, chuyển đổi theo chuẩn quy định và chuyển đến cơ quan quản lý Nhà nước và ngược lại.

Theo kế hoạch, lộ trình kê khai thuế điện tử của Việt Nam dự kiến được chia thành 3 giai đoạn.

Giai đoạn 1, chúng tôi tiến hành xây dựng cơ sở hạ tầng cơ bản cho việc kê khai, tiếp nhận tờ khai thuế điện tử; xây dựng thông tư hướng dẫn giao dịch điện tử trong lĩnh vực thuế; xác định điều kiện cơ sở hạ tầng kỹ thuật của cơ quan Thuế để có thể ứng dụng giao dịchấthuế điện tử cả trong nội bộ ngành Thuế và các bên liên quan

(người nộp thuế và các cơ quan quản lý Nhà nước, ngân hàng,...). Phạm vi thực hiện giai đoạn này dự kiến triển khai thí điểm kê khai và nhận tờ khai thuế giá trị gia tăng, thuế thu nhập doanh nghiệp, thuế tiêu thụ đặc biệt, thuế tài nguyên, thuế môn bài và áp dụng tại 1 Cục Thuế. Trong thời gian dự kiến thực hiện trong 12 tháng

Giai đoạn 2, mở rộng ra các sắc thuế khác nếu điều kiện áp dụng cho phép, đặc biệt là thuế thu nhập cá nhân; đồng thời xem xét khả năng triển khai giao dịch điện tử các dạng hồ sơ liên quan đến thuế. Thời gian dự kiến thực hiện trong 8 tháng.

Còn giai đoạn 3, tiến hành nâng cấp và tích hợp và kết nối với hệ thống các ngân hàng thương mại, kho bạc Nhà nước để triển khai dịch vụ thanh toán điện tử cho hoạt động nộp thuế (nộp thuế điện tử) với điều kiện hệ thống kho bạc, ngân hàng, kết nối tài chính cùng thống nhất tham gia thực hiện.

Trong thời gian từ nay đến cuối năm 2008, Tổng cục Thuế triển khai giai đoạn 1 với phạm vi dự kiến gồm: áp dụng cho tất cả các tờ khai theo thông tư hiện hành của các sắc thuế: Thuế Giá trị gia tăng; Thuế Thu nhập doanh nghiệp; Thuế Tiêu thụ đặc biệt; Thuế Tài nguyên; Thuế Môn bài. áp dụng thí điểm cho các doanh nghiệp đủ điều kiện thực hiện kê khai thuế điện tử trên địa bàn Cục Thuế thí điểm (doanh nghiệp chỉ kê khai thuế điện tử, không nộp tờ khai giấy), sau đó sẽ mở rộng phạm vi tuỳ thuộc vào điều kiện cơ sở hạ tầng. Xây dựng hệ thống ứng dụng CNTT tập trung tại Tổng cục Thuế (phần cứng, phần mềm, an toàn bảo mật,...) để kê khai và tiếp nhận tờ khai thuế. Xây dựng hệ thống ứng dụng công nghệ thông tin xử lý dữ liệu tờ khai thuế điện tử được triển khai tại Tổng cục để chuyển/trao đổi dữ liệu với Cục Thuế thông qua hạ tầng truyền thông ngành Tài chính. Như vậy có thể nói, trước mắt việc kê khai thuế điện tử mới chỉ thí điểm đối với doanh nghiệp.

Các hoạt động chính để chuẩn bị thí điểm kê khai thuế điện tử không chỉ bó gọn trong việc chuẩn bị hệ thống công nghệ mà còn bao gồm rất nhiều phần việc: Xây dựng kế hoạch và phân tích thiết kế: Khảo sát, phân tích yêu cầu nghiệp vụ; Thiết kế tổng thể hệ thống kê khai thuế qua mạng; Thiết kế và xây dựng ứng dụng tiếp nhận, lưu trữ tờ khai thuế điện tử; Đề xuất hệ thống thiết bị phần cứng, an ninh hệ thống phù hợp với thực tế; Tư vấnxây dựng căn cứ pháp lý: Thuê tư vấnxây dựng các căn cứ pháp lý để triển khai thành công các giao dịch điện tử trong lĩnh

vực thuế; Xây dựng ứng dụng và tổ chức triển khai: Xây dựng chuẩn giao tiếp và định dạng chuẩn giao tiếp thông tin nghiệp vụ về thuế; Xây dựng hệ thống quản lý người dùng tập trung; Xây dựng ứng dụng kê khai thuế điện tử; Cung cấp định dạng để ứng dụng Quản lý thuế Cục Thuế có thể nâng cấp để nhận dữ liệu từ tờ khai điện tử; Lựa chọn doanh nghiệp đủ điều kiện tham gia thí điểm kê khai thuế qua mạng Internet.

Hệ thống ứng dụng phải được thiết kế theo mô hình kiến trúc hướng dịch vụ (SOA), có hệ thống trao đổi dữ liệu trong phạm vi ngành Thuế; Tích hợp dữ liệu về đăng ký thuế, kê khai nộp thuế và cung cấp dữ liệu tờ khai thuế điện tử cho ứng dụng quản lý thuế có thể nâng cấp để nhận và xử lý. Hệ thống cũng phải đảm bảo an toàn, bảo mật tờ khai thuế điện tử, dữ liệu kê khai thuế để phân xử được khi có tranh chấp xảy ra.

Những điểm thuận lợi khi sử dụng CNTT trong hoạt động kê khai thuế như: Độ chính xác của thông tin cũng sẽ được tăng lên. Cụ thể: trong quá trình kê khai thuế trên phần mềm kế toán của doanh nghiệp, do số lượng hoá đơn đầu vào và đầu ra tương đối lớn, nhưng phần mềm kế toán không có cơ chế tự kiểm tra tính chính xác của mã số thuế, do đó đôi khi kế toán kê khai chưa được chính xác. Tuy nhiên, khi triển khai ứng dụng phần mềm kê khai thuế 1.3.0, phần mềm sẽ tự động giúp kế toán doanh nghiệp kiểm tra lại thông tin liên quan đến mã số thuế của doanh nghiệp xuất hoá đơn theo những chuẩn mới nhất về kê khai hoá đơn.

Phần mềm kê khai thuế cũng sẽ giúp các doanh nghiệp giảm thiểu thời gian kê khai và nộp báo cáo thuế: Thông qua việc tự động kiểm tra tính chính xác của các thông tin kê khai của phần mềm kế khai thuế giúp doanh nghiệp giảm thiểu thời gian kiểm tra và thẩm định lại thông tin trên báo cáo thuế. Bên cạnh đó, sử dụng CNTT trong hoạt động kê khai thuế sẽ giúp tự động hóa quy trình kê khai thuế.

***Một số khó khăn trong việc ứng dụng:***

- Tính bảo mật thông tin: Phần mềm hoàn toàn không đặt ra yêu cầu về cấp user và mật khẩu khi sử dụng nên rõ ràng thông tin về tờ khai rất dễ bị xâm nhập và bị xóa

bỏ cũng như làm sai lệch nếu người sử dụng không dùng chức năng sao lưu kịp thời; trong một số trường hợp khi chạy chương trình còn gặp phải lỗi; phần đăng ký danh mục hệ thống trong ứng dụng đôi chỗ còn rất cứng...

- Tính tự động hoá của dữ liệu: khi tích hợp vào phần mềm kê khai thuế, hầu như các phần mềm đều phải chuyển sang file dạng xls (excel), trên thực tế có rất nhiều kế toán bị hạn chế về việc xử lý các file excel chính vì thế trong quá trình chuyển đổi và phần mềm kê khai thuế hay bị vướng.

- Chưa đồng bộ hoá được khâu nộp các báo cáo thuế: hiện tại doanh nghiệp sau khi chuyển đổi file từ phần mềm kế toán vào phần mềm kê khai thuế của Tổng cục thuế vẫn phải thêm một công đoạn là in ra giấy để nộp cho cơ quan thuế nên dễ gây ra sai sót và bất tiện. Trong quá trình chuyển đổi dữ liệu từ phần mềm kế toán vào phần mềm kê khai thuế hoặc nhập trực tiếp thông tin vào phần mềm kê khai thuế, nhiều lúc bị trục trặc do phần mềm không đọc được dữ liệu nên không in được.

### 3.2.3. Ứng dụng CNTT ở cục Thuế Hải Phòng

Thời gian qua, Cục thuế Hải Phòng đã triển khai công tác cải cách thủ tục hành chính và hiện đại hoá ngành thuế. Các hoạt động tập trung vào các lĩnh vực: rà soát lại các thủ tục hành chính về thuế của tất cả các đơn vị, bộ phận trực thuộc; xoá bỏ các thủ tục chưa đúng quy định, rút ngắn thời gian làm các thủ tục về đăng ký thuế, mua bán hoá đơn, thủ tục hoàn thuế.

Sau một thời gian thực hiện cải cách thủ tục hành chính và thực hiện cơ chế "một cửa", thời gian đăng ký thuế, cấp hoá đơn, hoàn thuế được rút ngắn xuống còn 2 đến 3 ngày. Số lượng tổ chức, cá nhân tìm đến cơ quan thuế để được giải thích, hướng dẫn tăng lên rõ rệt, nhiều doanh nghiệp không chỉ tìm hiểu chính sách chế độ về thuế qua cán bộ quản lý thuế mà còn chủ động tìm hiểu qua bộ phận tuyên truyền hỗ trợ.

Mối quan hệ giữa cơ quan thuế và các tổ chức, cá nhân nộp thuế đã có chuyển biến rõ rệt theo chiều hướng cơ quan thuế tạo điều kiện tốt nhất để các tổ chức cá nhân thực hiện nghiêm túc các chính sách pháp luật thuế.

Trong lĩnh vực cấp mã số thuế, Cục thuế Hải Phòng thực hiện đúng theo quy định về thủ tục, hồ sơ kê khai đăng ký thuế, không qui định hoặc hướng dẫn thêm các thủ tục ngoài thông tư số 80/2004/ TT- BTC của Bộ tài chính. Cục thuế cũng dã bố trí một bộ phận của Phòng Tuyên truyền, hỗ trợ thường trực các ngày làm việc để tiếp nhận hướng dẫn giải thích và cấp tờ khai cho các tổ chức cá nhân đến làm thủ tục đăng ký thuế.

Chính vì vậy, mọi vướng mắc về hồ sơ đều được thông báo tại chỗ để người đến đăng ký thuế nắm được thủ tục bổ sung, hoàn chỉnh, không mất thời gian đi lại. Những trường hợp đủ hồ sơ, Cục thuế cấp đăng ký trong vòng từ 5 đến 7 ngày.

Trong thủ tục mua bán hoá đơn: Hồ sơ mua hoá đơn lần đầu của tổ chức kinh doanh hoặc hộ kinh doanh nộp ngay tại Phòng Quản lý ấn chỉ, sau khi xem xét nếu đủ thủ tục thì cấp bán ngay. Việc cấp bán hoá đơn lần đầu Cục thuế thực hiện theo đúng thời gian không quá 5 ngày kể từ khi tổ chức cá nhân có đầy đủ thủ tục theo qui định.

Trong các lần tiếp theo, tổ chức, cá nhân trực tiếp mang hồ sơ mua hoá đơn đến Phòng Quản lý thuế để kiểm tra, xác nhận tình hình sử dụng hoá đơn trước khi cấp bán, sau đó chuyển hồ sơ sang Phòng Quản lý ấn chỉ ngay để bán hoá đơn.

Trong hoàn thuế giá trị gia tăng, hồ sơ được tiếp nhận tại Phòng Hành chính ghi sổ nhận hồ sơ và chuyển hồ sơ cho Phòng Quản lý thuế ngay trong ngày. Phòng Quản lý thuế kiểm tra thủ tục hồ sơ, phân tích đối chiếu số liệu nếu đủ điều kiện và thủ tục thì hoàn thuế theo thời gian qui định.

Nếu hồ sơ cần bổ sung hoặc làm lại, Phòng Quản lý thuế trực tiếp chuyển hồ sơ cho doanh nghiệp để hoàn chỉnh. Với thủ tục miễn, giảm thuế thu nhập doanh nghiệp,

Phòng Hành chính tiếp nhận hồ sơ và chuyển cho Phòng Quản lý Thuế ngay trong ngày. Nếu hồ sơ chưa đủ thủ tục được thông báo lại trong vòng 3 ngày. Nếu doanh nghiệp có đầy đủ thủ tục, đã xác định được số thuế miễn giảm trong thời hạn 3 ngày phải lập xong hồ sơ miễn giảm.

# KẾT LUẬN

Nhà nước ta đã bắt đầu quan tâm và khuyến khích ứng dụng công nghệ thông tin và truyền thông trong các cơ quan nhà nước. Do đó việc giữ an toàn thông tin là quan trọng, nhất là đối với Bộ tài chính.

Qua quá trình tìm hiểu, phân tích và tổng hợp các tài liệu đã có, khoá luận đã trình bày được các vấn đề  sau:

1. Tìm hiểu và nghiên cứu về chứng chỉ số, chữ ký số và hạ tầng khoá công khai.
2. An toàn thông tin trong lĩnh vực tài chính
3. Tìm hiểu về Hải quan điện tử và Thuế điện tử

Vấn đề của khoá luận: tìm hiểu các mô hình ứng dụng CNTT và đảm bảo an toàn thông tin trong lĩnh vực tài chính.

Do thời gian nghiên cứu có hạn, nội dung đề tài khá rộng nên khoá luận này còn chưa bao quát hết vấn đề và còn nhiều thiếu sót. Em rất mong nhận được sự quan tâm, góp ý của thầy cô, bạn bè và những người quan tâm đến lĩnh vực này.

# CÁC TÀI LIỆU THAM KHẢO

[1]: Lý thuyết mật mã & An toàn thông tin: Phan đình diệu – NXB ĐHQGHN – 2002

[2]: An toàn tính toán : Charles Pheeger

Các trang web tham khảo

www.nhandan.com.vn

www.tinhoctaichinh.vn

www.ven.vn

www.ictnews.vn

http://vi.wikipedia.org