TÓM TẮT NỘI DUNG

Hiện nay, với sự phát triển của công nghệ thông tin và truyền thông, các giao dịch điện tử ngày càng được áp dụng rộng rãi trong mọi lĩnh vực. Trong đó việc áp dụng Giao dịch điện tử trong các cơ quan nhà nước đang được Đảng và nhà nước ta quan tâm rất lớn. Việc áp dụng thành công Giao dịch điện tử trong các cơ quan nhà nước, đặc biệt là trong cải cách hành chính sẽ mang lại nhiều lợi ích như giảm các thủ tục hành chính, minh bạch hóa các thủ tục, đem lại sự thuận tiện cho người dân cũng như các cơ quan nhà nước. Để xây dựng thành công hệ thống giao dịch điện tử trong cơ quan nhà nước, bên cạnh việc phát triển cơ sở hạ tầng thì việc đảm bảo an toàn thông tin cho hệ thống là một điều hết sức quan trọng, có tính quyết định cho sự thành công của hệ thống. Đảm bảo an toàn thông tin cho hệ thống là đảm bảo các yêu cầu về an toàn thông tin như tính bí mật, tính toàn vẹn, tính xác thực, tính chống chối bỏ và tính sẵn sàng.

Nội dung của khóa luận này tập trung vào vấn đề các công nghệ trong đảm bảo an toàn thông tin trong giao dịch hành chính, các yêu cầu đảm bảo an toàn thông tin, nghiên cứu thực trạng ứng dụng CNTT tại một số địa phương và đưa ra một số giao dịch khả thi.

LỜI CẢM ƠN

Em xin được bày tỏ lòng biết ơn sâu sắc tới thầy giáo TS. Lê Phê Đô – giảng viên trường Đại Học Công Nghệ - ĐHQGHN đã tận tình hướng dẫn và tạo mọi điều kiện thuận lợi để em hoàn thành báo cáo tốt nghiệp của mình.

Em xin chân thành cảm ơn tất cả các thầy cô giáo trong khoa Công nghệ thông tin – Trường Đại Học Dân Lập Hải Phòng đã nhiệt tình giảng dạy và cung cấp những kiến thức quý báu để em có thể hoàn thành tốt báo cáo tốt nghiệp và khóa học này.

Cuối cùng em xin cảm ơn tất cả các bạn đã động viên, góp ý và trao đổi hỗ trỡ cho em trong suốt thời gian vừa qua.

Vì thời gian có hạn và trình độ bản thân còn nhiều hạn chế, cho nên đề tài không tránh khỏi những thiếu sót, em rất mong nhận được sự góp ý quý báu của tất cả các thầy cô cùng toàn thể các bạn để đề tài của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

Hải Phòng, tháng 07 năm 2009

Sinh viên

Phạm Thị Mai Anh

MỤC LỤC

LỜI MỞ ĐẦU

Ngày nay, khi mà nhu cầu giao dịch trực tuyến ngày càng tăng thì mối đe dọa và hậu quả tiềm ẩn với thông tin trong giao dịch ngày càng lớn. Các nguy cơ rủi ro trong giao dịch điện tử 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 giao dịch điện tử trên cơ sở 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. Triển khai hệ thống ứng dụng Giao dịch điện tử trong các giao dịch hành chính công là một trong những nhiệm vụ trọng tâm để đẩy nhanh quá trình cải cách hành chính. Để triển khai xấy dựng các ứng dụng Giao dịch điện tử thực sự hiệu quả và tiến tới xây dựng thành công Chính phủ điện tử theo đúng nghĩa của nó, thì bên cạnh chú trọng nghiên cứu xây dựng hệ thống cần tiền hành song song việc nghiên cứu xây dựng các hệ thống đảm bảo an toàn thông tin trong giao dịch điện tử. Trong khuôn khổ của khóa luận này em trình bày các vấn để bảo mật và xác thực thông tin dựa trên chứng chỉ số, các loại giao dịch điện tử và đưa ra một số giao dịch khả thi trong cơ quan nhà nước. Cấu trúc khóa luận gồm 3 chương:

Chương 1: GIỚI THIỆU AN TOÀN THÔNG TIN

Chương 2: AN TOÀN THÔNG TIN TRONG GIAO DỊCH HÀNH CHÍNH

Chương 3: TÌM HIỂU THỰC TIỄN ỨNG DỤNG CNTT TRONG GIAO DỊCH HÀNH CHÍNH TẠI MỘT SỐ ĐỊA PHƯƠNG

CHƯƠNG 1: GIỚI THIỆU AN TOÀN THÔNG TIN

I. Vấn đề an toàn thông tin

1.1 Khái niệm an toàn thông tin

An toàn là giảm thiểu các điểm yếu dễ bị tấn công đối với các tài sản và tài nguyên.

An toàn thông tin nghĩa là thông tin được bảo vệ, các hệ thống và những dịch vụ có khả năng chống lại những hiểm họa, 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 đây 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)...

Về cơ bản, đối với mọi tổ chức, việc có thông tin chính xác và kịp thời có tác động rất quan trọng đến hoạt động, khả năng phát triển và thu lợi của tổ chức đó. An toàn thông tin giúp kiểm soát và bảo vệ thông tin khỏi bị rò rỉ, mất mát, sai lệch do vô tình hoặc cố ý.

An toàn thông tin phải đảm bảo 3 thuộc tính quan trọng:

- Tính bảo mật: đảm bảo rằng chỉ những người được phép mới được truy cập thông tin, tránh cho thông tin không bị rỏ rỉ trái phép cho đối thủ hay công chúng.

- Tính toàn vẹn: bảo vệ tính chính xác và đầy đủ của thông tin và các phương pháp xử lý, tránh cho thông tin bị thay đổi trái phép.

- Tính sẵn sàng: đảm bảo những người được phép có thể truy cập thông tin và các tài sản tương ứng khi cần.

An toàn thông tin bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm đảm bảo cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính

xác và tin cậy. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

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 trong công nghệ thông tin là đưa ra một số tiêu chuẩn an toàn và ứng dụng các tiêu chuẩn an toàn này để loại trừ hoặc giảm bớt các nguy hiểm cho các hệ thống. Do kỹ thuật truyền nhận và xử lý thông tin ngày càng phát triển đáp ứng cácyêu cầu ngày càng cao nên hệ thống chỉ có thể 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.

Việc xây dựng một hệ thống an toàn thông tin không chỉ đơn thuần có ý nghĩa về mặt vật chất và kỹ thuật, về cơ bản nó mang đến nhiều lợi ích ảnh hưởng trực tiếp đến hoạt động của một tổ chức:

- Tài sản thông tin được quản lý chặt chẽ và có hệ thống.
- Nắm bắt và kiểm soát các rủi ro có thể xảy ra.
- Bảo mật thông tin trong nội bộ tổ chức, cũng như giữa tổ chức với bên ngoài.
- Thể hiện sự cam kết của tổ chức với đối tác và khách hang bằng hành động cụ thể.
- Bảo đảm khả năng hoạt động của hệ thống khi có sự cố khẩn cấp xảy ra.

1.2 Nhu cầu an toàn thông tin

Sự phụ thuộc của chúng ta vào các máy tính nối mạng ngày càng tăng và chúng ta phải bảo vệ chống lại nhiều loại hiểm hoạ khác nhau. Các tổ chức đang hướng tới các trung tâm tính toán và dữ liệu phân tán. Ngày nay, các tổ chức thường sử dụng một hoặc nhiều mạng cục bộ (LAN) kết nối tới các vị trí từ xa thông qua mạng diện rộng (WAN). Hơn nữa, các tổ chức sử dụng mọi cách để kết nối và tận dụng những thuận lợi của Internet.

Động cơ của việc kết nối Internet là để có thể thâm nhập vào một thị trường có hàng chục triệu người sử dụng và khách hàng.

Mối quan tâm đối với một kết nối Internet là người dùng cần ngăn chặn truy nhập trái phép vào các hệ thống và ứng dụng trên mạng của của mình.

Chúng ta không chỉ phụ thuộc vào các mạng LAN trong đó có chứa dữ liệu và ứng dụng chạy trên nền Novell, UNIX, hoặc Windows Server, mà còn phụ thuộc vào mạng WAN trong đó có các ứng dụng như Web, thư điện tử, truyền tệp hoặc đăng nhập từ xa.

Ngày nay, các hệ thống có rất nhiều điểm yếu dễ bị tấn công và Virus thì có rất nhiều. Một phần nguyên nhân là do có nhiều cá nhân được phép truy nhập vào các hệ thống thông tin của tổ chức. Hơn nữa, khi các tổ chức kết nối vào Internet thường xuyên, các hiểm hoạ an toàn không chỉ xuất phát từ bên trong mà còn ở bên ngoài - các hiểm hoạ ngày nay mang tính toàn cầu. Sự cần thiết nên và phải tiến hành là hỗ trợ quản lý và kinh phí đầy đủ nhằm đảm bảo an toàn cho tài nguyên và hoạt động của tổ chức.

1.3 Các hiểm hoạ an toàn thông tin

Các hệ thống trong Giao dịch điện tử, đặc biệt khi được kết nối với mạng Internet luôn tiềm ẩn những hiểm họa có khả năng gây nên mất mát và tổn hại tới ATTT của hệ thống. Có 4 kiểu hiểm họa đối với hệ thống: sự ngắt, sự chặn bắt, sự thay đổi và sự giả mạo. Cả 4 hiểu họa đều khai thác khả năng bị tổn thương của những tài sản của hệ thống.

- Hiểm họa ngắt: tài sản của hệ thống sẽ bị mất đi không ở trạng thái sẵn sàng hoặc không thể dung được. Ví dụ như phá hoại cố ý thiết bị phần cứng, xóa bỏ tệp chương trình hay tệp dữ liệu.
- Hiểm họa chặn bắt: một đối tượng không được phép nào đó có thể truy nhập vào tài sản. Đối tượng đó có thể là người, là chương trình hoặc có thể là hệ tính toán. Những ví dụ về kiểu vi phạm này là việc sao chép chương trình, dữ

liệu, việc nghe trộm để lấy dữ liệu qua mạng. Nếu sự chặn bắt lặng lẽ nó sẽ không để lại dấu vết để bị phát hiện.

- Hiểm họa sự biến đổi: Nhóm không được phép không những xâm nhập trái phép mà còn sửa đổi trái phép tài sản của hệ thống. Ví dụ ai đó có thể sửa đổi giá trị của cơ sở dữ liệu, sửa đổi chương trình, hoặc thay đổi dữ liệu đang được truyền qua các phương tiện điện tử như mạng Internet. Một số trường hợp có thể bị phát hiện bằng phương pháp đơn giản, nhưng một số khác tinh vi hơn hầu như không thể phát hiện được.
- Hiểm họa giả mạo: Nhóm không được phép có thể bịa ra những đối tượng giả trên hệ thống. Kẻ xâm nhập có thể đưa ra giao dịch giả mạo vào mạng truyền thống hoặc thêm các bản ghi vào cơ sở dữ liệu hiện có.

Các hiểm họa có thể từ phía người dung, hay một chương trình máy tính, một tai nạn vô ý hoặc từ bản thân hệ thống. Các hiểm họa có thể là cố ý, như phá hủy một hệ thống có chủ ý, hay vô ý như làm đổ cốc cafe lên máy tính. Các hiểm họa có thể đến từ những người trong và hoặc ngoài tổ chức. Các hiểm họa có thể là chủ động, như phá hủy các thao tác trên máy chủ web, hoặc thụ động như việc nghe trộm giao tiếp giữa các bên trong giao dịch.

- Mối hiểm họa từ phía người dùng: xâm nhập bất hợp pháp vào hệ thống, ăn cắp dữ liệu, phần mềm, ăn cắp các dịch vụ máy tính, phá hoại hay làm thay đổi phần mềm hoặc dữ liệu, truy nhập bất hợp pháp có thể gây từ chối dịch vụ với người dùng hợp pháp. Hiểm họa rò rỉ thông tin (dữ liệu, thông tin cá nhân, các thông tin bí mật khác) từ những người dùng trong hệ thống.
- Nguy cơ rủi ro tiềm ẩn trong kiến trúc hệ thống CNTT: tổ chức hệ thống kỹ thuật không có cấu trúc bảo mật thông tin, tổ chức khai thác cơ sở dữ liệu, cơ chế truy nhập từ xa, sử dụng phần mềm ứng dụng. Nếu tổ chức hệ thống thông tin không có cấu trúc bảo mật tốt, tin tặc có thể lợi dụng các lỗ hổng an ninh của hệ thống (như qua các lỗ hổng của các trình duyệt web…) để xâm nhập trái phép vào hệ thống.

- Nguy cơ mất ATTT tiềm ẩn trong chính sách đảm bảo ATTT: đó là sự chấp hành các chuẩn an toàn, tức là xác định rõ cái được phép và không được phép trong khi vận hành hệ thống thông tin; thiết lập trách nhiệm bảo vệ thông tin không rõ ràng; không chấp hành sử dụng chuẩn bảo mật thông tin đã được cấp, chuẩn an toàn mạng, truy cập từ bên ngoài, chuẩn an toàn bức tường lửa; chính sách an toàn Internet, v.v.
- Thông tin trong Giao dịch điện tử dễ bị tổn thương nhất nếu công cụ quản lý của tổ chức vận hành hệ thống không được thiết lập như: quy định mang tính hành chính duy trì kiểm tra tiêu chuẩn bảo mật thường xuyên, các công cụ phát hiện âm mưu xâm nhập nhằm báo trước ý đồ tiếp cận trái phép và giúp phục hồi những sự cố, công cụ mang tính toàn vẹn dữ liệu.
- Ngoài ra, hệ thống tồn tại những hiểm họa từ phần cứng do con người gây ra hoặc do những hiểm họa tự nhiên như: cháy, mất điện, hạ tầng mạng…
- Trong tất cả các mối hiểm họa trên thì con người vẫn là những điểm yếu quyết định về sự an toàn thông tin trong Giao dịch điện tử.

II. Các dịch vụ an toàn

Trong mô hình OSI/RM (Open System Interconnection/ Reference Model) có 7 tầng. Khi chức năng của các tầng được định nghĩa, các giao thức (thông qua các header) thực hiện các yêu cầu chính cũng được xác định. Các giao thức được định nghĩa trên từng tầng của mô hình.

Các dịch vụ an toàn được định nghĩa trong kiến trúc an toàn ISO 7498-2. Khi chức năng của các tầng được định nghĩa, các dịch vụ cũng được xác định trong kiến trúc an toàn. Các dịch vụ có thể được đặt vào các tầng thích hợp của OSI/RM. Các dịch vụ an toàn được định nghĩa như sau:

Dịch vụ an toàn	**Mô tả**
Xác thực	Xác thực là bước đầu tiên trong quá trình truy nhập hệ thống. Gõ tên người dùng và mật khẩu là một ví

	dụ về việc ta tự xác thực như một người sử dụng của hệ thống. Kerberos là một ví dụ về hệ thống xác thực. *Xác thực là quá trình chứng minh định danh của người sử dụng.*
Kiểm soát truy nhập	Dịch vụ này chống lại việc sử dụng trái phép các tài nguyên do truy nhập thông qua các giao thức mạng. *Kiểm soát truy nhập liên quan đến các tài nguyên có trong một hệ thống hoặc mạng mà người sử dụng hoặc dịch vụ có thể truy nhập.*
Bảo mật dữ liệu	Dịch vụ này chống lại các sửa đổi trái phép. Dịch vụ bảo mật dữ liệu bao gồm: bảo mật kết nối, bảo mật không kết nối, bảo mật các trường được chọn và bảo mật dòng thông tin. *Bảo mật dữ liệu liên quan đến sự bí mật của dữ liệu trên một hệ thống hoặc mạng. Bảo mật dữ liệu là bảo vệ dữ liệu khỏi các hiểm hoạ thụ động.*
Toàn vẹn dữ liệu	Dịch vụ này bao gồm: toàn vẹn kết nối có khôi phục, toàn vẹn kết nối không khôi phục, toàn vẹn kết nối các trường được chọn và toàn vẹn không kết nối các trường được chọn. *Toàn vẹn dữ liệu chống lại các hiểm hoạ chủ động.*
Chống chối bỏ	Chối bỏ được được định nghĩa là sự không thừa nhận của một trong các thực thể tham gia truyền thông rằng, anh ta không tham gia tất cả hoặc một phần cuộc truyền thông. *Dịch vụ chống chối bỏ có thể là một trong 2 dạng sau: chống chối bỏ nguồn gốc hoặc chống chối bỏ bằng chứng bàn giao*.

2.1. Các cơ chế an toàn

Các cơ chế an toàn thực hiện các dịch vụ an toàn. Cơ chế an toàn có 2 kiểu như sau:

1) Cơ chế an toàn xác định
2) Cơ chế an toàn toả khắp

Các cơ chế an toàn xác định

Các cơ chế an toàn xác định thường được gắn với một tầng thích hợp nhằm cung cấp các dịch vụ an toàn được mô tả ở trên. Các cơ chế an toàn xác định bao gồm:

- Mã hoá
- Chữ ký số
- Các cơ chế kiểm soát truy nhập
- Các cơ chế toàn vẹn dữ liệu
- Xác thực
- Đệm lưu lượng
- Chứng thực

Mã hoá được sử dụng để đảm bảo tính bí mật cho dữ liệu hoặc thông tin về luồng lưu lượng.

Chữ ký số có các thuộc tính sau:

- Có khả năng kiểm tra tác giả của chữ ký, thời gian ký;
- Có khả năng xác thực các nội dung tại thời điểm ký;
- Các thành viên thứ 3 có thể kiểm tra chữ ký trong trường hợp xảy ra tranh chấp.

Các cơ chế kiểm soát truy nhập có thể được thực hiện tại điểm gốc hoặc điểm trung gian bất kỳ, nhằm xác định người gửi có được phép truyền thông với người nhận hoặc sử dụng các tài nguyên hay không. Các cơ chế kiểm soát truy nhập có thể dựa vào thông tin xác thực như: mật khẩu, nhãn an toàn, khoảng thời gian truy nhập, thời điểm truy nhập, hoặc hình thức truy nhập.

Các cơ chế toàn vẹn dữ liệu bao gồm: gán nhãn thời gian, đánh số thứ tự, hoặc chuỗi mật mã; chúng có thể được sử dụng để đảm bảo tính toàn vẹn cho một đơn vị dữ liệu hoặc một trường; một chuỗi các đơn vị dữ liệu hoặc các trường.

Thông tin xác thực chẳng hạn như mật khẩu, các đặc điểm của thực thể, chữ ký số, hoặc có thể áp dụng một kỹ thuật khác như chứng thực. *Đệm lưu lượng* có thể chống lại các phân tích lưu lượng.

Mỗi cuộc truyền thông có thể sử dụng chữ ký số, mã hoá và các cơ chế toàn vẹn phù hợp với dịch vụ được đưa ra. Các thuộc tính như nguồn gốc dữ liệu, thời gian và đích có thể được đảm bảo thông qua điều khoản của một cơ chế *chứng thực*.

Các cơ chế an toàn toả khắp

Các cơ chế này không xác định cho một dịch vụ an toàn cụ thể nào và nói chung, chúng liên quan trực tiếp đến mức an toàn được yêu cầu. Các cơ chế an toàn toả khắp bao gồm:

- Chức năng tin cậy
- Các nhãn an toàn
- Vết kiểm toán
- Khôi phục an toàn

Chức năng tin cậy có thể được sử dụng để mở rộng phạm vi hoặc thiết lập hiệu lực của các cơ chế an toàn khác.

Nhãn an toàn có thể được sử dụng để chỉ ra mức độ nhạy cảm. Nhãn là thông tin bổ sung vào dữ liệu được truyền đi hoặc có thể được ngầm định thông qua việc sử dụng một khoá xác định để mã hoá dữ liệu.

Vết kiểm toán cho phép phát hiện và điều tra các lỗ hổng an toàn.

Ghi nhật ký cũng được xem là một cơ chế an toàn.

Khôi phục an toàn giải quyết các yêu cầu xuất phát từ cơ chế – ví dụ, các chức năng xử lý hoặc quản lý biến cố – và khôi phục được xem là kết quả của việc áp dụng một tập các quy tắc.

Quản lý an toàn

An toàn cho tất cả chức năng quản lý hệ thống và mạng, truyền thông an toàn đối với tất cả các thông tin quản lý thực sự quan trọng. Lĩnh vực quản lý an toàn bao gồm:

1) Quản lý an toàn hệ thống.
2) Quản lý dịch vụ an toàn.
3) Quản lý cơ chế an toàn.

Quản lý an toàn hệ thống là quản lý toàn bộ môi trường tính toán phân tán. Quản lý này bao gồm duy trì và quản lý toàn bộ các chính sách an toàn của tổ chức; tương tác với quản lý dịch vụ an toàn và quản lý cơ chế an toàn. Quản lý an toàn hệ thống cũng liên quan đến quản lý kiểm toán an toàn và quản lý khôi phục an toàn.

Quản lý dịch vụ an toàn là quản lý các dịch vụ an toàn xác định. Dịch vụ này đảm bảo gọi đến các cơ chế an toàn xác định bằng cách sử dụng chức năng quản lý cơ chế an toàn thích hợp.

Quản lý cơ chế an toàn là quản lý các cơ chế an toàn. Các chức năng quản lý cơ chế an toàn bao gồm:

- Quản lý khoá;

- Quản lý mã hoá;
- Quản lý chữ ký số;
- Quản lý kiểm soát truy nhập;
- Quản lý toàn vẹn dữ liệu;
- Quản lý xác thực;
- Quản lý đệm lưu lượng;
- Quản lý kiểm soát định tuyến
- Quản lý chứng thực

III. Mật mã hóa khóa công khai và hạ tầng khóa công khai

3.1 Giới thiệu mật mã khóa công khai

Trong hầu hết lịch sử mật mã học, khóa dùng trong các quá trình mã hóa và giải mã phải được giữ bí mật và cần được trao đổi bằng một phương pháp an toàn khác (không dùng mật mã) như gặp nhau trực tiếp hay thông qua người đưa thư tin cậy. Vì vậy quá trình phân phối khóa trong thực tế gặp rất nhiều khó khăn, đặc biệt là khi số lượng người sử dụng rất lớn. Để giải quyết vấn đề này, năm 1976 Diffie và Hellman đã đề xuất một loại mật mã mới: với một hệ thống mã khóa công khai, mỗi người dùng sẽ có một khóa không cần giữ bí mật. Bản chất công khai của nó không làm tổn hại tới tính an toàn của hệ thống. Phép biến đổi khóa công khai về cơ bản là phép mã một chiều với cách giải mã bí mật.

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 khóa 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 (dùng cho mã hóa và giải mã) đề cần phải giữ bí mật.

Trong mật mã 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 hóa: giữ bí mật thông tin và chỉ có người có khóa bí mật mới giải mã được.
- Tạo chữ ký số: cho phép kiểm tra một văn bản có phải đã được tạo với một khóa bí mật nào đó hay không.
- Thỏa thuận khóa: cho phép thiết lập khóa dùng để trao đổi thông tin mật giữa 2 bên.

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

An toàn

Về khía cạnh an toàn, các thuật toán mật mã khóa bất đối xứng cũng không khác nhiều với các thuật toàn mã hóa khóa đối xứng. Có những thuật toán được dùng rộng rãi, có thuật toán chủ yếu trên lý thuyết; có thuật toán 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 toàn 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 toàn 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. 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.

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 xác nhận. Nếu một người khác có thể giải mã với khóa công khai của người gửi thì 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…

Thuật toán liên kết giữa 2 khóa trong cặp

Không phải tất cả các thuật toán mật mã 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 để 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. 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 thong tin mở khóa thì chỉ có người sở hữu mới biết.

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 lân hoặc tương đương, chưa có thuật toán mã hóa khóa bất đối xứng nào được chứng minh 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 đẻ giải các bài toán gắn với chúng. Các ước lượng này luôn thay đổi tùy thuộc khả năng của máy tính và các biện pháp 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 lương là 1000 năm thì thuật toán này hoàn toàn có thể dùng để mã hóa các thông tin về thẻ tín dụng. Rõ rang là thời gian phá mã lớn hoen nhiều lần thời gian tồn tại của thẻ.

Những điểm yếu của một số thuật tón mật mã hóa khóa công 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 cũng 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 hóa. 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: 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 giữa 2 bên để nhận các gói tin, giải mã rồi lại mã hóa với khóa đún 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 khóa an toàn nhằm đảm bảo xác thực được 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.

Khối lượng tính toán

Để đạt được độ an toàn tương đương, thuật toán mật mã hóa khóa bất đối xứng đòi hỏi khối lượng tính toán nhiều hơn đáng kể so với thuật toán mật mã hóa khóa 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, 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.

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 giao thức thiết lập và kiểm tra mối quan hệ này là đặc biệt quan trong. 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 khóa 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 phân theo lớp (các nhà cung cấp chứng thực số) hoặc theo thống kê (mạng lưới tín nhiệm) hoặc theo mô hình tín nhiệm nôi bộ (SPKI). Không phụ thuộc vào bản chất của thuật toán hay giao thức, việc đánh giá mối quan hệ giữa khóa và người sở hữu khóa vẫn phải dựa trên những đánh giá chủ quan của bên thứ 3 bởi vì khóa là một thực thể toán học còn người sở hữu và mối quan hệ thì không. Hạ tầng khóa công khai chính là các thiết chế để đưa ra những chính sách cho việc đánh giá này.

3.2 Hạ tầng khóa công khai (PKI)

3.2.1 Khái niệm

Cơ sở hạ tầng khóa công khai (Public Key Infrestructure - PKI) là một tập hợp phần cứng, phần mềm, chính sách, thủ tục cần thiết để tạo, quản lý và lưu trữ, phân phối và thu hồi các chứng chỉ số dựa trên công nghệ mã hóa khóa công khai. Mã hóa và chữ ký số đã trở thành một phần không thể thiếu được đối với thương mại điện tử, giao dịch điện tử cũng như các lĩnh vực đòi hỏi an toàn và bảo mật. PKI cung cấp cơ sở hạ tang giúp cho việc sử dụng mã hóa và chữ ký số một cách dễ dàng và trong suốt đối với người sử dụng.

PKI là một khái niệm mô tả toàn bộ nền tảng cơ sở nhằm cung cấp các dịch vụ quản lý truy cập, tính toàn vẹn, tính xác thực, tính bí mật và tính chống chối bỏ. Nền tảng này bao gồm các hệ thống phần mềm như nhà phát hành chứng chỉ, kho chứa dữ liệu, các chính sách... PKI đảm bảo cho các giao dịch điện tử cũng như những phiên kết nối bí mật được an toàn dựa trên công nghệ mã hóa khóa công khai.

3.2.2 Các thành phần trong hệ thống PKI

Một hệ thống PKI gồm 4 thành phần như sau:

- Cơ quan chứng thực (CA):

Là cơ quan có quyền cấp phát và thu hồi chứng chỉ. Đồng thời áp đặt những chính sách với những chứng chỉ mà nó đã phát hành. Trong một hệ thống PKI tồn tại một hệ thống CA quan hệ với nhau theo cấu trúc ngang hàng hoặc phân cấp.

- Cơ quan đăng ký chứng chỉ (Registration Authỏities - RA):

RA là một đại diện cho CA có nhiệm vụ xác nhận những thông tin người dùng cho CA. Đồng thời, RA cũng có thể thay mặt người sử dụng yêu cầu CA cấp phát, thu hồi, thay đổi thông tin trên chứng chỉ.

Các RA có chức năng:

- ✓ Nhận các yêu cầu cấp phát chứng chỉ từ phía người dùng, chứng nhận các thông tin trên yêu cầu đó.
- ✓ Gửi yêu cầu phát hành chứng chỉ đến CA. Nhận các chứng chỉ từ CA và trao nó cho chủ thể chứng chỉ.
- ✓ Nhận yêu cầu thu hồi chứng chỉ từ phía người dùng, kiểm tra yêu cầu thu hồi và gửi những yêu cầu này cho CA.

- Thực thể cuối (End Entities) - ứng dụng sử dụng chứng chỉ, clients

Thực thể cuối trong PKI có thể là con người, thiết bị, hay một chương trình phần mềm nhưng thường là người sử dụng hệ thống. Thực thể cuối sẽ thực hiện những chức năng mật mã (mã hóa, giải mã và ký số).

- Kho chứa chứng chỉ (Certificate/CRL Repository)

Hệ thống (có thể phân tán) lưu trữ chứng chỉ và danh sách các chứng chỉ bị thu hồi. Nó cung cấp cơ chế phân phối chứng chỉ phục vụ nhu cầu tra cứu, lấy khóa công khai của đối tác cần thực hiện giao dịch chứng thực số. Kho chứa chứng chỉ

còn đảm bảo những thông tin được lưu trữ trên nó là hoàn toàn chính xác và tính nhất quán.

3.2.3. Chức năng cơ bản của PKI

3.2.3.1 Chứng thực (Certification)

Chứng thực là chức năng quan trọng nhất của hệ thống PKI. Đây là quá trình ràng buộc khóa công khai với định danh của thực thể. CA là thực thể PKI thực hiện chức năng chứng thực. Có 2 phương pháp chứng thực:

- Cơ quan chứng thực tạo ra cặp khóa bí mật- công khai và tạo ra chứng chỉ cho phần khóa công khai của cặp khóa.
- Người sử dụng tự tạo cặp khóa và đưa khóa công khai cho CA để CA tạo chứng chỉ cho khóa công khai đó. Chứng chỉ đảm bảo tính toàn vẹn của khóa công khai và các thông tin gắn cùng.

3.2.3.2 Thẩm tra (Validation)

Quá trình xác định liệu chứng chỉ đã đưa ra có thể được sử dụng đúng mục đích thích hợp hay không được xem như là quá trình kiểm tra tính hiệu lực của chứng chỉ. Quá trình này bao gồm một số bước sau:

Kiểm tra xem liệu có đúng CA được tin tưởng đã ký số lên chứng chỉ hay không (xử lý theo đường dẫn chứng chỉ).

Kiểm tra chữ ký số của CA trên chứng chỉ để kiểm tra tính toàn vẹn.

Xác định xem chứng chỉ còn ở trong thời gian có hiệu lực hay không.

Xác định xem chứng chỉ đã bị thu hồi hay chưa.

Xác định xem chứng chỉ đang được sử dụng có đúng mục đích hay không bằng cách kiểm tra những trường hợp mở rộng, cụ thể như mở rộng chính sách chứng chỉ, hay mở rộng việc sử dụng khóa.

3.2.3.3 Quản lý khóa

Thông thường việc quản lý khóa do CA thực hiện thông qua quản lý chứng chỉ. Chức năng này gồm các chức năng ký, sinh khóa, thu hồi khóa khi không còn hiệu lực và khôi phục cặp khóa khi xảy ra sự cố trong hệ thống.

a. Đăng ký

Đăng ký là quá trình đăng ký các thông tin xin cấp chứng chỉ với các tổ chức, trung tâm tin cậy. RA và CA là những thực thể trong quá trình đăng ký. Quá trình đăng ký phụ thuộc vào chính sách của tổ chức. Nếu chứng chỉ được cấp cho các mục đích dùng cho những hoạt động bí mật thì sử dụng phương pháp gặp mặt trực tiếp. Nếu chứng chỉ sử dụng cho mục đích hoạt động thường thì có thể đăng ký qua những ứng dụng viết sẵn hoặc các ứng dụng điện tử.

b. Sinh khóa

Khóa sinh ra phải đảm bảo về chất lượng (khó tấn công bằng phương pháp vét cạn), tính duy nhất trong hệ thống và tính bí mật. Việc sinh khóa phụ thuộc vào chính sách của PKI. Dưới đây là 3 cách mà hệ thống sử dụng để khởi tạo khóa:

Người sử dụng tự sinh cặp khóa cho mình sau đó gửi khóa công khai cho CA quản lý. Ưu điểm của phương pháp này là khóa bí mật của người sử dụng không bao giờ bị bên thứ ba biết đến. Tuy nhiên để đảm bảo an toàn trong quá trình sinh khóa thì đòi hỏi hệ thống phía người dùng phức tạp.

Cặp khóa được sinh bởi một hệ thống chuyên chịu trách nhiệm sinh khóa. Khóa công khai được gửi cho CA quản lý. Còn khóa bí mật gửi lại cho người dùng theo một kênh truyền an toàn (ví dụ như sử dụng smart card để lưu khóa bí mật).

Cặp khóa được sinh bởi CA: đây là một trương hợp riêng của trường hợp trên.

c. Phân phối, thu hồi, treo và lưu trữ khóa

Các chức năng này đồng nhất với chức năng quản lý chứng chỉ của CA. Tuy nhiên chức năng quản lý khóa trong một số trường hợp có những điểm khác biệt. Ví dụ như một cặp khóa được sử dụng trong nhiều chứng chỉ khác nhau. Rõ ràng chỉ cần quản lý một cặp khóa nhưng lại quản lý nhiều chứng chỉ.

- Lưu trữ, phân phối khóa: Các khóa công khai được lưu trữ phân phối cho các ứng dụng thông qua các hệ thống không cần đảm bảo bí mật. Còn khóa bí mật được phân phối cho người dùng thông qua các kênh truyền an toàn như smart card, hoặc được mã hóa bởi một thành phần bí mật khác.

- Thu hồi, treo khóa: Quá trình thu hồi khóa biểu hiện thông qua việc thu hồi chứng chỉ, chứng chỉ bị thu hồi bao hàm hai ý nghĩa là thông tin định danh không còn chính xác hoặc khóa bị thỏa hiệp. Khi phát hiện khóa bị thỏa hiệp hoặc do yêu cầu từ người dùng, các thành phần PKI có chức năng yêu cầu CA thu hồi các chứng chỉ tương ứng. Còn quá trình treo khóa là quá trình thu hồi khóa tạm thời, khóa đó hoàn toàn có thể được sử dụng lại, tùy thuộc vào kết quả kiểm tra của CA xem nó đã bị thỏa hiệp chưa.

d. Khôi phục khóa

Trong bất kỳ hệ thống nào rủi ro luôn luôn có thể xảy ra. Hệ thống PKI phải lường trước tình trạng khóa mã hóa bị mất. Đối với khóa công khai thì việc phân phối khóa là đơn giản, vì nó được lưu trữ trên server công cộng, mọi đối tượng sử dụng đều có quyền truy cập vào lấy thông tin. Nhưng đối với khóa bí mật thì khác, nguyên nhân mất có thể là do mất mật khẩu truy nhập vào hệ thống lưu trữ, hoặc hệ thống lưu trữ bị hỏng hóc, việc hệ thống sinh khóa có lưu trữ khóa bí mật này không tùy thuộc vào chính sách của PKI. Nếu việc lưu trữ khóa bí mật được thực hiện thì khóa bí mật sẽ khôi phục được, tuy nhiên lại nảy sinh vấn đề tính riêng tư bị xâm phạm vì một bên thứ 3 có thể xem toàn bộ thông tin bí mật của bạn. Nếu khóa bí mật không được lưu trữ riêng thì tính riêng tư của tài liệu mã hóa không bị vi phạm, nhưng nếu khóa bí mật bị mất thì đồng nghĩa với việc toàn bộ dữ liệu đã mã hóa của bạn sẽ bị mất theo.

3.2.3.4 Quản lý thời gian

Thời gian trong hệ thống PKI phải có tính nhất quán, bởi rất nhiều thành phần chỉ có được sự tin tưởng trong một thời gian cụ thể. Rõ ràng PKI phải quản lý cả vấn đề thời gian trong hệ thống. Nếu dịch vụ thời gian của PKI không được đảm

bảo thì bất kỳ thành phần nào trong hệ thống PKI đều có thể lạm dụng sử dụng những thành phần phụ thuộc vào thời gian, thực hiện những hành động không an toàn và chối bỏ về mặt thời gian trong các phiên kết nối.

3.2.3.5 Đảm bảo an toàn

Hệ thống PKI sử dụng công nghệ mã hóa khóa công khai để cung cấp các dịch vụ đảm bảo bí mật cho người sử dụng, bên canh đó nó phải đảm bảo rằng các dịch vụ mà nó sử dụng phải an toàn cho người sử dụng. Tức là phải đảm bảo tính bí mật, toàn vẹn và tính sẵn sàng của các dịch vụ PKI. Bên cạnh đó các hệ thống PKI còn phải đảm bảo các chính sách giải quyết các vấn đề nảy sinh khi các rủi ro trong hệ thống xảy ra.

Ví dụ: Bob và Alice muốn liên lạc với nhau qua Internet, dùng PKI để chắc chắn rằng thông tin trao đổi giữa họ được bảo mật. Bob đã có chứng nhận kỹ thuật số, nhưng Alice thì chưa. Để có nó, cô phải chứng minh được với Tổ chức cấp giấy chứng nhận cô thực sự là Alice. Một khi các thông số nhận dạng của Alice được Tổ chức thông qua, họ sẽ phát hành cho cô một chứng nhận kỹ thuật số. Chứng nhận điện tử này có giá trị thực sự, giống như tấm hộ chiếu vậy, nó đại diện cho Alice và gồm những chi tiết nhận dạng Alice, một bản sao chìa khóa công cộng của cô và thời hạn của giấy chứng nhận cũng như chữ ký số của Tổ chức chứng nhận. Alice cũng nhận được chìa khóa cá nhân kèm theo chìa khóa công cộng. Chìa khóa cá nhận này được lưu ý là phải giữ bí mật, không được san sẻ với bất kỳ ai.

Bây giờ Alice đã có chứng nhận kỹ thuật số, Bob có thể gửi cho cô những thông tin quan trọng được số hóa. Bob có thể xác nhận với cô là thông điệp đó xuất phát từ anh ta cũng nhu đảm bảo rằng nội dung thông điệp không bị thay đổi và không có ai khác ngoài Alice đọc được nó.

Bảng sau đây minh họa cho tiến trình của chữ ký điện tử và độ tin cậy cao đáp ứng cho yêu cầu giao dịch điện tử an toàn của Bob và Alice.

Bob muốn chuyển một thư điện tử đến cho Alice, với yêu cầu rằng giao dịch phải chứng minh được chính anh đã gởi nó đi và nội dung bức thư không bị thay đổi.	Phần mềm PKI dùng chìa khóa cá nhân của Bob tạo ra một chữ ký điện tử cho bức thư
Bob muốn chắc chắn rằng không ai ngoài Alice đọc được bức thư này	Phần mềm PKI của Bob dùng chìa khóa công cộng của Alice để mã hóa thông điệp của Bob.
Alice muốn đọc thư do Bob gởi	Phần mềm PKI dùng chìa khóa cá nhân của Alice để để giải mã thông điệp.
Alice muốn kiểm chứng rằng chính Bob đã gởi đi thông điệp đó và nội dung thông điệp không bị chỉnh sửa.	Phần mềm PKI của Alice dùng chìa khóa công cộng của Bob để kiểm chứng chữ ký điện tử của anh ta.

Chương 2: AN TOÀN THÔNG TIN TRONG GIAO DỊCH HÀNH CHÍNH

2.1 Giao dịch điện tử

Giao dịch điện tử là giao dịch được thực hiện thông qua các phương tiện điện tử và cũng có giá trị pháp lý như nó được ghi chép hoặc mô tả bằng văn bản theo phương pháp truyền thống. Có thể coi văn bản pháp lý đầu tiên ở Việt Nam về giao dịch điện tử là Quyết định của Thủ tướng Chính phủ số 44, năm 2002 về chấp nhận chữ ký điện tử trong thanh toán liên ngân hang. Hiện nay, ngành Ngân hang đang ứng dụng một số giao dịch điện tử như gửi, nhận, cung cấp thông tin qua mạng, xử lý chứng từ kế toán, giao dịch giữa ngân hang với khách hàng…

Giao dịch điện tử gồm các hình thức thông điệp dữ liệu, chữ ký điện tử, chứng thực điện tử, giao kết và thực hiện hợp đồng điện tử…

- Thông điệp dữ liệu là thông tin được tạo ra, được gửi đi, được nhận và được lưu trữ bằng phương tiện điện tử. Nó được thể hiện dưới hình thức trao đổi dữ liệu điện tử, chứng từ điện tử, điện báo, fax và các hình thức tương tự.

- Chữ ký điện tử là chữ ký được tạo lập dưới dạng từ, số, ký hiện, âm thanh hoặc các hình thức khác bằng phương tiện điện tử, gắn liền hoặc kết hợp một cách logic với thông điệp dữ liệu. Chữ ký điện tử có giá trị xác nhận người ký thông điện dữ liệu và xác nhận sự chấp thuận của người đó đối với nội dung thông điệp dữ liệu được ký.

- Hợp đồng điện tử được giao kết bằng các phương tiện điện tử cũng có giá trị pháp lý và cũng được thực hiện như các hợp đồng được giao kết bằng phương tiện văn bản truyền thống.

2.2 Ứng dụng Công nghệ thông tin trong giao dịch hành chính

Giao dịch hành chính là dịch vụ trao đổi thông tin giữa các cơ quan tổ chức nhà nước; giữc cơ quan, tổ chức nhà nước với công dân, người lao động và các doanh nghiệp. Hiện nay với sự pháp triển của khoa học công nghệ, cùng với sự phát triển hạ tầng cơ sở CNTT trong các cơ quan nhà nước, việc ứng dụng CNTT và truyền thông trong giao dịch hành chính công là một bộ phận quan trọng trong mô hình Chính phủ điện tử.

2.2.1 Chính phủ điện tử

Chính phủ điện tử (E-gov) hiện nay còn được hiểu theo nhiều nghĩa, điều đó phụ thuộc vào mức độ ứng dụng công nghệ thông tin vào hoạt động quản lý công, khả năng ưu tiên về chính sách và khả năng ứng dụng công nghệ thông tin của từng Chính phủ cụ thể. Theo nghĩa rộng thì E-gov là việc sử dụng Internet (online trực tuyến) trong các hoạt động tương tác giữa Chính phủ với các bộ phận khác nhau trong xã hội hoặc chỉ đơn giản là nâng cao năng lực ứng dụng công nghệ thông tin của nhân viên hành chính trong bộ máy công. Theo nghĩa cụ thể hơn thì "Chính phủ điện tử là việc sử dụng công nghệ thông tin, mà đặc biệt là Internet như là một công cụ để hỗ trợ nhằm đạt đến một Chính phủ hoạt động hiệu quả nhất". Mô hình Chính

phủ điện tử hiệu quả sẽ bao gồm các mô thức giải quyết quan hệ tương tác về thông tin giữa ba chủ thể: Chính phủ, doanh nghiệp và người dân.

Các loại GDĐT trong cơ quan nhà nước

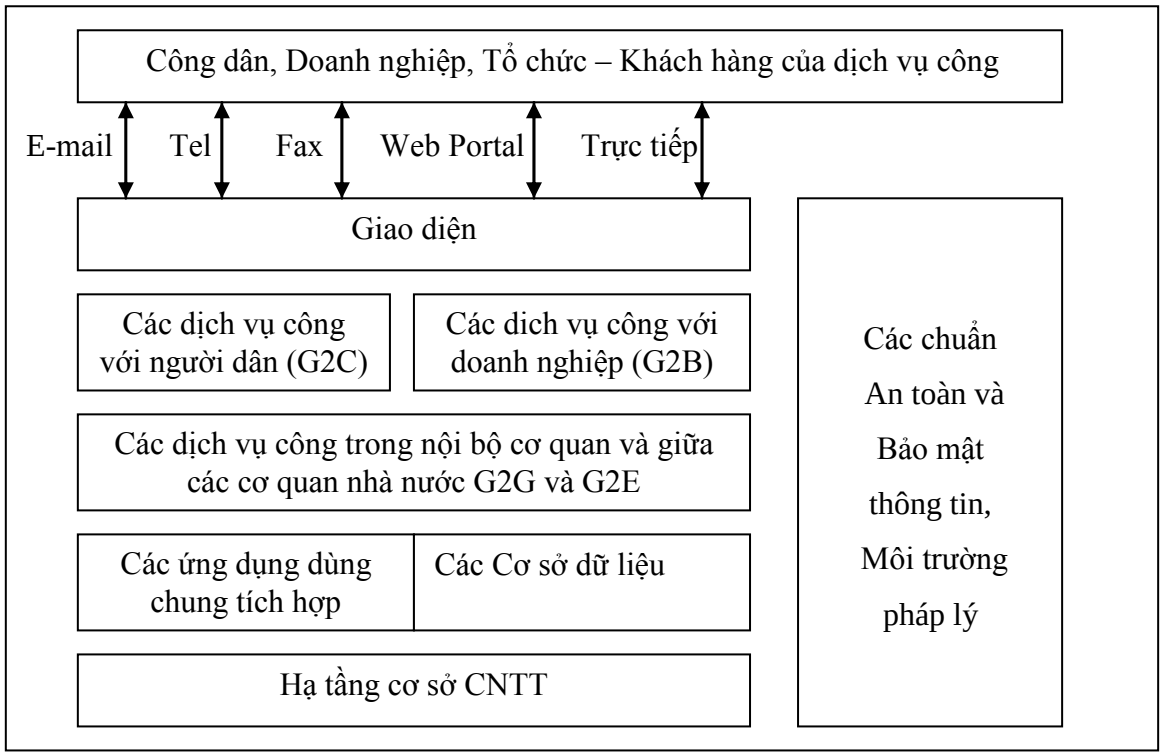
Theo điều 39 chương V của luật Giao dịch điện tử quy định 3 loại Giao dịch điện tử trong cơ quan nhà nước đó là:

- Giao dịch điện tử trong nội bộ cơ quan nhà nước
- Giao dịch điện tử giữa các cơ quan nhà nước với nhau
- Giao dịch điện tử giữa cơ quan nhà nước với cơ quan, tổ chức, cá nhân.

Dưới góc độ kỹ thuật, các hoạt động trong Giao dịch điện tử trong các cơ quan nhà nước gồm các nội dung cơ bản sau:

- Lưu trữ thông điệp
- Gửi, nhận thông điệp
- "Ký điện tử" và chứng thực "Chữ ký điện tử"
- Giao kết và thực hiện hợp đồng điện tử.

Vai trò và mối quan hệ của việc đảm bảo ATTT trong Giao dịch điện tử của cơ quan nhà nước trong kiến trúc chung của Chính quyền điện tử được mô tả trong hình sau:



Hình : Mô hình kiến trúc tổng quát của Chính phủ điện tử

Trong đó

- G2C: Government – to – Citizen (Chính phủ với công dân)
- G2B: Government – to – Business (Chính phủ với doanh nghiệp)
- G2E: Government – to – Employees (Chính phủ với công chức)
- G2G: Government – to – Government (Chính phủ với chính phủ)

Chi tiết các dịch vụ bao gồm trong các loại giao dich như sau:

- Giao dịch G2C

Các dịch vụ trong G2C bao gồm việc phổ biến thông tin tới công chúng, các dịch vụ công dân cơ bản như gia hạn giấy phép, cấp giấy khai sinh, khai tử, đăng ký kết hôn và kê khai các biểu mẫu nộp thuế thu nhập cũng như hỗ trợ người dân đối với các dịch vụ cơ bản như giáo dục, chăm sóc y tế, thông tin bệnh viện, thư viện và rất nhiều dịch vụ khác. Qua đó người dân có thể truy cập một cửa đến các dịch vụ của Chính phủ. Một số dịch vụ điện tử thông dụng nhất được cung cấp cho công dân là: yêu cầu cấp chứng nhận quyền sở hữu nhà đất, tìm kiếm thông tin về các

trường học, tìm kiếm việc làm. Phát triển nghề nghiệp và đăng ký bầu cử và bỏ phiếu bầu cử…

- Giao dịch G2B

Các dịch vụ trong G2B là những dịch vụ trao đổi giữa Chính phủ và cộng đồng doanh nghiệp bao gồm cả việc phổ biến các chính sách, biên bản ghi nhớ, các qui định và thể chế. Các dịch vụ được cung cấp bao gồm truy xuất các thông tin về kinh tế, tải các mẫu đơn, gia hạn giấy phép, đăng ký kinh doanh, xin cấp phép và nộp thuế… Các dịch vụ được cung cấp thông qua giao dịch G2B cũng hỗ trợ việc phát triển kinh doanh, đăch biệt là phát triển các doanh nghiệp vừa và nhỏ. Việc đơn giản hóa các thủ tục xin cấp phép, hỗ trợ quá trình phê duyệt đối với các yêu cầu của các doanh nghiệp vừa và nhỏ sẽ thúc đẩy kinh doanh phát triển. Ở mức cao hơn, các dịch vụ G2B bao gồm cả việc mua sắm điện tử và trao đổi trực tuyến giữa Chính phủ với các nhà cung cấp để mua sắm hàng hòa và dịch vụ cho Chính phủ.

- Giao dịch G2E

Dịch vụ trong G2E bao gồm các dịch vụ G2C và các dịch vụ chuyên ngành khác dành riêng cho các công chức Chính phủ như việc cung cấp đào tạo và phát triển nguồn nhân lực qua đó cải tiến các chức năng hành chính hàng ngày cũng như cách thức giải quyết công việc với người dân.

- Giao dịch G2G

Các dịch vụ trong G2G được triển khai ở hai cấp độ: ở địa phương hoặc trong nước và ở cấp độ quốc tế. Các dịch vụ G2G là các giao dịch giữa Chính phủ trung ương(quốc gia) và các chính quyền địa phương, giữa các vụ và các công ty, cơ quan có liên quan. Đồng thời, các dịch vụ G2G là các giao dịch giữa các Chính phủ và có thể được sử dụng như một công cụ của các mối quan hệ quốc tế và ngoại giao.

Hiệu quả Chính phủ điện tử

Về mặt kinh tế, Chính phủ điện tử là một ý tưởng nhằm giảm thiểu chi phí giao dịch để tăng hiệu quả của nền hành chính công quyền. Tuy nhiên, ở góc độ xã hội và chính trị, hiệu quả của Chính phủ điện tử còn đi xa hơn trong việc xây dựng lòng tin, thúc đẩy tính minh bạch và tăng cường sự giam gia của cộng đồng đối với quá trình ra quyết định của chính phủ. Điều này còn có ý nghĩa đăch biệt hơn nữa

khi mà tại các nước phương Đông, nơi mà bộ máy hành chính công quyền luôn cồng kềnh và ít hiệu quả. Chính phủ điện tử là một công cụ nhằm giảm thiểu những "va chạm" không muốn và không đáng có giữa những đối tác trong quá trình giao dịch kiểu đối diện (face to face) đầy nhạy cảm con người. Chính phủ điện tử là một trong những sang kiến không những đạt được sự giảm thiểu về chi phí giao dịch để tăng tính hiệu quả như những quan hệ kinh tế mà còn đem lại nhiều tác động hơn thế nữa, đó là thúc đẩy tính công khai minh bạch và xây dựng lòng tin cũng như tăng cường sự tham gia của cộng đồng xã hội đối với hoạt động của chính chỉ. Thành công của E-gov được thể hiện ở các nội dung sau:

Hiệu quả hơn trong các hoạt động quản lý nhà nước của chính phủ. Mô hình E-gov sẽ làm cho các dịch vụ của chính phủ được cung cấp trực tuyến 24 giờ trong 7 ngày thay vì theo lịch làm việc công chức truyền thống. Các ứng dụng phổ biến nhất hiện nay như là hệ thống tài chính, các hoạt động về mua sắm của chính phủ, giao dịch nội bộ giữa các cơ quan hành chính lẫn việc chia sẽ thông tin với cộng đồng.

Chất lượng dịch vụ được cải thiện. Sự thảo luận trao đổi thông tin giữa các đối tác bằng mô hình E-gov ít tốn kém thời gian và chi phí đã là một điều kiện tốt trong việc trao đổi giữa nhà cung cấp dịch vụ (chính phủ) và khách hàng (doanh nghiệp và dân chúng) của mình. Chính sự thảo luận này đã giúp không những bản thân chất lượng dịch vụ được nâng cao và đáp ứng nhu cầu mà còn là một cầu nối ý tưởng trong hoạc định các chính sách vi mô và vĩ mô của chính phủ.

Xây dựng và tăng cường lòng tin giữa chính phủ và dân chúng. Đây là lợi ích chính trị cực kỳ nền tảng mà bất cứ một chính phủ nào cũng hướng đến. Bởi lẽ, một khi thiếu vắng sự tin tưởng thì vai trò của pháp luật, hiệu quả cưỡng chế của các quyết định chính phủ cũng như các chương trình đổi mới của chính phủ thường được người dân đón nhận mờ nhạt. Trong khi đó, sự tương tác giữa chính phủ với dân chúng tăng lên cùng với hiệu quả và chất lượng dịch vụ cung cấp được cải thiện nhờ các dịch vụ trực tuyến từ E-gov sẽ là yếu tố tăng cường lòng tin của nhân dân đối với chính phủ. Lợi ích chính trị này có được khi áp dụng E-gov là động cơ đầu tiên và mạnh nhất cho các nhà làm chính sách khi họ muốn cải cách hệ thống quản lý công của mình.

Mức độ phát triển của các dịch vụ hành chính công

Ứng dụng công nghệ thông tin phục vụ công tác nghiệp vụ, quản lý, điều hành trong các cơ quan nhà nước, bộ, ngành, tỉnh, thành là nhiệm vụ đã được xác định rõ ràng, quán triệt từ nhiều năm nay, thông qua các chỉ thị, nghị định, quyết định quan trọng của Nhà nước và Chính phủ. Nghị định 64 của Chính phủ ban hành năm 2007 là định hướng mới nhất cho con đường ứng dụng công nghệ thông tin trong các cơ quan nhà nước, tiến tời hình thành Chính phủ điện tử ở Việt Nam.

Việc cung cấp thông tin về tổ chức, hoạt động của các cơ quan nhà nước, chính sách và hướng dẫn thủ tục hành chính trên mạng thông qua những trang thông tin điện tử, cổng tác nghiệp điện tử của các bộ, ngành, UBND tỉnh, thành trong cả nước là một trong những bước đi cơ bản, phục vụ trực tiếp cho người dân và doanh nghiệp, tiến tới xây dựng Chính phủ điện tử.

Nằm trong lộ trình đẩy mạnh hoạt động ứng dụng công nghệ thông tin và xây dựng Chính phủ điện tử, bộ TT-TT đã công bố bản đánh giá các trang thông tin điện tử của các bộ, ngành, địa phương theo 2 tiêu chí: số lượng truy cập và mức độ của dịch vụ hành chính công.

Mô hình 4 mức độ phát triển của các dịch vụ hành chính công trực tuyến được áp dụng đối với Việt Nam bao gồm:

Mức độ 1: Cổng thông tin điện tử có đầy đủ thông tin về quy trình thủ tục thực hiện dịch vụ, các giấy tờ cần thiết, các bước tiến hành, thời gian thực hiện, chi phí thực hiện dịch vụ.

Mức độ 2: Ngoài thông tin đầy đủ như mức độ 1, Cổng thông tin điện tử cho phép người sử dụng tải về các mẫu đơn, hồ sơ để người sử dụng có thể in ra giấy, hoặc điền vào các mẫu đơn. Việc nộp lại hồ sơ sau khi hoàn thành được thực hiện qua đường bưu điện hoặc người sử dụng trực tiếp mang đến cơ quan thụ lý hồ sơ.

Mức độ 3: Lúc này cổng thông tin điện tử cho phép người sử dụng điền trực tuyến vào các mẫu đơn, hồ sơ và gửi lại trực tuyến các mẫu đơn, hồ sơ sau khi điền xong tới cơ quan và người thụ lý hồ sơ. Các giao dịch trong quá trình thụ lý hồ sơ và cung cấp dịch vụ được thực hiện qua mạng. Tuy nhiên, việc thanh toán chi phí và

kết quả sẽ được thực hiện khi người sử dụng đến trực tiếp cơ quan cung cấp dịch vụ.

Mức độ 4: Việc thanh toán chi phí sẽ được thực hiện trực tuyến, việc trả kết quả có thể thực hiện trực tuyến hoặc gửi qua đường bưu điện.

2.2.2 Cổng thông tin điện tử

Theo kết quả đánh giá mới nhất về mức độ truy nhập và cung cấp dịch vụ hành chính công của các trang thông tin điện tử của các bộ và địa phương, công bố ngày 2/7/2008 của bộ TT-TT, ở cấp địa phương hiện nay có 54,7% địa phương (tính trên số 64 tỉnh, thành trực thuộc Trung ương) đã triển khai dịch vụ hành chính công trực tuyến ở mức 1; 28,1% đã triển khai ở mức 2; 4,7% triển khai ở mức 3. Trang thông tin điện tử của Thành phố Hồ Chí Minh tính trên tổng thể các tiêu chí được đưa ra trong đánh giá này thuộc nhóm dẫn đầu.

Ở cấp bộ, trang thông tin điện tử của Bộ Nông nghiệp và Phát triển nông thôn và Bộ Tư pháp cung cấp nhiều dịch vụ hành chính công trực tuyến nhất. Dịch vụ hành chính công cấp 3 chỉ có tại trang thông tin điện tử của Bộ Ngoại giao.

Có 16/22 Bộ, Ngành đã có trang thông tin điện tử, trong đó cổng thông tin điện tử Chính phủ cung cấp nhiều thông tin phong phú và có lượng truy cập cao.

- **Cổng thông tin điện tử Chính phủ**

  Cổng thông tin điện tử Chính phủ trên Internet có tên quốc gia là Viet Nam Government Portal thực hiện 3 chức năng chính gồm: cơ quan báo điện tử của Chính phủ, mạng thông tin hành chính của Chính phủ, cổng tích hợp dịch vụ công của Chính phủ và chính quyền các cấp.

  Kể từ khi Thủ tướng Chính phủ bấm nút hòa mạng Internet cách đây 3 năm, website Chính phủ nay là Cổng Thông tin điện tử Chính phủ đã trở thành cầu nối tin cậy giữa người dân, doanh nghiệp và Chính phủ.

  Suốt những năm qua, từ nhịp cầu này, rất nhiều quyết đinh, chính sách chỉ đạo của Chính phủ đã nhanh chóng đến với người dân và ngược lại, những khó khăn, vướng mắc, vấn đề dân sinh bức xúc kịp thời được phản ánh, chuyển tới các cơ quan chức năng giải quyết.

Việc khai trương website Chính phủ 3 năm trước đã mở ra một kênh thông tin quan trọng truyền tải kịp thời chủ trương, chính sách, hoạt động nhiều mặt của Chính phủ, tình hình thời sự nổi bật của đất nước và trở thành diễn đàn giao lưu trực tuyến giữa Chính phủ, các thành viên Chính phủ với nhân dân, doanh nghiệp.

Góp phần đưa Chính phủ đến gần dân hơn

Chỉ sau 3 năm, khối lượng rất lớn thông tin đã được Cổng thông tin điện tử truyền tải đến người dân, doanh nghiệp và bạn bè quốc tế. Riêng năm 2008, Cổng thông tin điện tử Chính phủ đã đăng tải gần 3.000 văn bản quy phạm pháp luật; gần 2.500 văn bản chỉ đạo điều hành của Thủ tướng Chính phủ; cập nhật các bảo cáo tổng hợp về tình hình kinh tế - xã hội của Bộ, ngành, địa phương trong cả nước, cùng hàng chục nghìn dữ liệu thông tin điện tử và dữ liệu điện tử đa phương tiện được lưu trữ, khai thác trong hoạt động chỉ đạo điều hành hàng ngày, các phóng viên của Cổng thông tin điện tử Chính phủ đã bám sát vào hoạt động của Thủ tướng, các Phó Thủ tướng, hoạt động của Bộ, ngành, địa phương kể cả từ những vùng lũ, vùng sâu, vùng xa, ở những nơi điều kiện tác nghiệp khó khăn, để truyền đi kịp thời ý kiến chỉ đạo của lãnh đạo Chính phủ, nhanh chóng giải quyết các vấn đề gắn bó mật thiết với đời sống người dân.

Các chuyên viên kỹ thuật đã xử lý hàng vạn cuộc tấn công của các lực lượng tin tặc, đảm bảo vận hành thông suốt 24/24 giờ hàng ngày trong suốt 3 năm qua của Cổng thông tin điện tử Chính phủ.

Trong năm 2008, Cổng TTĐT Chính phủ truyền đến bạn đọc, người dân, doanh nghiệp hơn 8.000 tin, bài; hơn 2.000 ảnh, phục vụ khoảng 7 triệu lượt người truy cập mỗi ngày.

Có thể nói, các sự kiện trọng đại của đất nước, công điện khẩn, chỉ đạo khẩn… của Thủ tướng Chính phủ được Cổng TTĐT Chính phủ truyền tải kịp thời, có định hướng rất tốt cho người dân, cũng như cung cấp thông tin quan trọng cho chính quyền cơ sở nắm bắt triển khai.

Đến nay, nhiều người vẫn còn nhắc đến sự kiện sau buổi giao ban truyền hình trực tuyến sáng 27/4/2008 tại trụ sở Cổng TTĐT Chính phủ giữa Thủ tướng Nguyễn Tấn Dũng và Thường trực Chính phủ với lãnh đạo các địa phương. Nội

dung chỉ đạo giao ban đã được đăng tải lập tức trên Cổng TTĐT Chính phủ, trong đó có việc yêu cầu xử lý nghiêm các trường hợp đầu cơ, đẩy giá gạo lên cao bất thường. Ngay ngày hôm sau, giá gạo tại Hà Nội, TP HCM cùng nhiều địa phương khác đã chững lại và liên tục giảm trong các ngày tiếp theo.

Cổng TTĐT Chính phủ cũng đã đăng tải kịp thời các ý kiến chỉ đạo khẩn của Ngân hàng Nhà nước, Bộ Công thương... trước tình hình có nhiều thông tin nhiễu, gây bất ổn cho tâm lý nhân dân, đã giúp người dân nắm được thông tin chính thức của cơ quan có thẩm quyền, trách nhiệm; giúp nhân dân, doanh nghiệp hiểu rõ tình hình, từ đó, ổn định tâm lý, góp phần làm tan các cơn sốt ảo.

Nhiều kiều bào đã bày tỏ, Cổng TTĐT Chính phủ là cầu nối cho những người xa xứ luôn hướng về Đất Mẹ.

Thông qua nhịp cầu này, nhiều kiều bào cho biết, qua Cổng TTĐT Chính phủ hầu như tức thời, họ đã nắm bắt rõ hơn về tình hình đất nước, hoạt động của lãnh đạo Đảng, Nhà nước, Chính phủ về những chính sách thân thiết với họ và cảm thấy sự gần gũi hơn của lãnh đạo Đảng, Nhà nước, Chính phủ.

Kết nối người dân với Chính phủ.

Với việc mở rộng 11 cửa giao tiếp điện tử, Cổng TTĐT Chính phủ đã trở thành nơi người dân phản ánh những kiến nghị, cũng như gửi gắm những tâm tư, nguyện vọng tới Chính phủ, Thủ tướng Chính phủ, các cơ quan có trách nhiệm của Nhà nước.

Người dân không chỉ phản ánh qua đường bưu điện, thư điện tử, điện thoại, mà nhiều người còn đến tận trụ sở Cổng TTĐT Chính phủ tại 16 Lê Hồng Phong, Hà Nội, với mong muốn được Cổng TTĐT Chính phủ giúp chuyển nguyện vọng, kiến nghị đến các địa chỉ tin cậy để được hồi đáp nhanh chóng.

Từ khoảng 4.000 thư, kiến nghị năm 2006, 6.000 năm 2007, đến năm 2008, Cổng TTĐT Chính phủ đã nhận được khoảng 7.500 thư, phản ánh, kiến nghị của người dân, doanh nghiệp.

Những con số này cho thấy, người dân đã ngày càng tin tưởng hơn vào Cổng TTĐT Chính phủ, cũng đồng thời cho thấy chủ trương của Đảng, Nhà nước trong việc chủ động lắng nghe và tích cực giải quyết những vấn đề của người

dân, doanh nghiệp qua Cổng TTĐT Chính phủ đã phát huy hiệu ứng tích cực trong cuộc sống.

2.3 Đảm bảo an toàn thông tin trong giao dịch hành chính

2.3.1 Thực trạng

Hiện nay hầu hết các cơ quan nhà nước đã được trang bị cơ sở hạ tầng công nghệ thông tin tương đối đồng bộ (được trang bị máy vi tính, kết nối mạng cục bộ, mạng internet và có cán bộ tin học chuyên trách), đồng thời cán bộ công chức đã được đào tạo qua lớp tin học văn phòng. Đây là yếu tố thúc đẩy nhanh việc ứng dụng CNTT phục vụ quản lý hành chính nhà nước trong thời gian tới.

Bên cạnh việc trang bị hạ tầng CNTT đồng bộ và đào tạo đội ngũ cán bộ sử dụng các ứng dụng tin học văn phòng, một số ứng dụng phần mềm cũng được Chính phủ và các ngành đầu tư xây dựng, bước đầu đem lại hiệu quả, góp phần đổi mới tác phong làm việc của cán bộ, nâng cao chất lượng công tác chỉ đạo, điều hành tại đơn bị triển khai dự án.

Một số đơn vị đã từng bước ứng dụng hiệu quả các hệ thống thông tin hỗ trợ chỉ đạo, điều hành, đặc biệt trong việc giới thiệu, tuyên truyền, công khai hóa các thủ tục hành chính và các văn bản quy phạm pháp luật. Hiện nay có trên 70% các tỉnh thành phố trực thuộc trung ương, các bộ các ngành đều có cổng giao tiếp điện tử góp phần đưa thông tin đầy đủ để với người dân, doanh nghiệp, tạo sự công khai hóa, minh bạch hóa các thủ tục hành chính.

Tuy nhiên việc đưa vào vận hành một số Giao dịch điện tử trong hành chính công vẫn chưa đạt hiệu quả cao, một phần do trình độ chuyên môn của một bộ phận công chức và người dân chưa cao, nhưng lý do chính có tính quyết định là chúng ta có môi trường pháp lý và hạ tầng kỹ thuật đảm bảo ATTT trong Giao dịch điện tử chưa hoàn thiện. Nếu không đảm bảo ATTT trong Giao dịch điện tử, thông tin giao dịch dễ bị đánh cắp, sửa đổi sẽ gây những tổn hại lớn ở múc vĩ mô. Ví dụ, các nhà phân tích của Chính phủ định kỳ đưa ra dữ liệu về nền kinh tế quốc gia, các kết quả được đưa tới công chúng vào ngày giờ xác định trước. Trước thời gian đó, việc truy

nhập vào dữ liệu có thể đem lại lợi nhuận cho ai đó biết trước tác động có thể của dữ liệu tới thị trường chứng khoán.

Do vậy, để xây dựng và triển khai rộng rãi và đạt hiệu quả cao trọng việc áp dụng công nghệ thông tin và truyền thông trong các Giao dịch điện tử nói chung hay giao dịch hành chính nói riêng đòi hỏi phải xây dựng hạ tầng kỹ thuật đảm bảo ATTT trong giao dịch.

Một số giải pháp công nghệ về an toàn và bảo mật thông tin đã được xây dừng và triển khai. Tuy nhiên chúng ta không thể sử dụng lại do tính an toàn và bảo mật của hệ thống được đảm bảo, nhất là trong trường hợp gặp sự cố chúng ta không có cơ sở khoa học để xử lý. Mặt khác đối với các cơ quan quản lý hành chính nhà nước ở Việt Nam có những yêu cầu nghiệp vụ về an toàn và bảo mật thông tin cho riêng mình.

Nghị định, quy định chi tiết về thi hành luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số mới được ban hành. Tuy nhiên, hiện tại chúng ta vẫn chưa có các trung tâm CA chuyên dụng. Các hệ thống Giao dịch điện tử thực thụ mới chỉ được ứng dụng triển khai tại một số đơn vị hành chính, ngân hàng còn các cơ quan nhà nước chưa có những giao dịch thực thụ.

2.3.2 Các yêu cầu đảm bảo An toàn thông tin trong Giao dịch điện tử

Hệ thống Giao dịch điện tử phải đảm bảo sự an toàn, khả năng bảo mật cho người sử dụng cũng như các thông tin cho người sử dụng như thông tin về định danh người dung, thông tin giao dịch… Hệ thống Giao dịch điện tử phải đảm bảo được các mục tiêu chính đó là: tính bí mật, tính toàn vẹn, tính xác thực, tính không thể phủ nhận và tính sẵn sàng.

- **Tính bí mật**

Tính bí mật là việc đảm bảo thông tin không bị lộ hay bày ra đối với những người không được phép. Thông tin có thể được lưu trữ trên máy tính hay có thể được truyền từ máy này sang máy khác qua mạng. Các dịch vụ bảo mật bảo vệ thông tin trước những đe dọa của việc theo dõi giao tiếp. Trong Giao dịch điện tử, tính bí mật rất quan trọng, hệ thống cần đảm bảo ngăn chặn hoặc hạn chế tuyệt đối

sự rò rỉ các thông tin giao dịch (định danh người mua, người bán, thông điệp giao dịch, chữ ký điện tử của các bên tham gia giao dịch, thông tin tài khoản…) đối với người dùng không liên quan.

Kỹ thuật phổ biến để thực thi dịch vụ bí mật là mã hóa. Mã hóa làm thay đổi hình dạng thông tin gốc làm cho người khác "khó" nhận ra để ngăn chặn sự truy cập trái phép.

- **Tính toàn vẹn**

Đảm bảo tính toàn vẹn là việc ngăn chặn hay hạn chế các hành động trái phép như thay đổi, sao chép thông tin, chèn những thông điệp thừa vào chuỗi thông tin, xóa một phần hay toàn bộ chuỗi thông tin, sắp xếp lại các thành hần trong chuỗi thông tin. Tính toàn vẹn dữ liệu cũng là việc chống lại việc tạo trái phép các thông điệp và xem các thông điệp cũ. Tính toàn vẹn chỉ cho những người hoặc nhóm người được phép mới có thể biến đổi theo cách hợp pháp.

Toàn vẹn dữ liệu là hết sức quan trọng. Một số ý nghĩa cho tính toàn vẹn gồm: đúng, chính xác, không bị thay đổi, thay đổi theo những cách có thể chấp nhận được, chỉ người dùng được phép mới có thể thay đổi được, nhất quán, nhất quán nội tại và các kết quả đúng và có ý nghĩa.

Một số kỹ thuật mật mã được sử dụng để thực thi tính toàn vẹn dữ liệu như mã hóa, hàm băm.

- **Tính xác thực**

Tính xác thực hay dịch vụ kiểm soát truy nhập là việc chống lại sự truy cập trái phép tới dữ liệu hay các tài nguyên máy tính tới những người dùng bất hợp pháp. Tính xác thực thiết lập những quyền hạn đối với người dùng. Kiểu truy cập ở đây là kiểu truy cập đọc, viết dữ liệu, thực thi một chương trình hay sử dụng tài nguyên phần cứng như máy in. Một hệ thống an ninh cần phải xác thực một người dùng trước khi định nghĩa những quyền hạn cho người dùng đó. Trong Giao dịch điện tử, hệ thống cần đảm bảo tính xác thực gồm xác thực đúng thực thể cần kết nối, giao dịch và xác thực đúng thực thể có trách nhiệm về nội dung thông tin (xác thực nguồn gốc thông tin). Nói cách khác, khi tiến hành giao dịch, người sử dụng sẽ

không thể an tâm khi mà họ không biết chính xác đối tác tham gia giao dịch với mình hay nguồn gốc của thông tin giao dịch. Vì vậy đảm bảo tính xác thực của hệ thống là cần thiết.

Danh sách kiểm soát truy cập và các phân bổ chính sách là hai kỹ thuật phổ biến dùng để thực thi các dịch vụ xác thực.

- **Tính không thể phủ nhận**

Tính không thể phủ nhận ngăn chặn một bên tham gia giao dịch sáu đó phủ nhận có tham gia một phần hoặc toàn bộ giao dịch, phủ nhận nội dung của giao dịch, thời gian giao dịch hay định danh của các đối tác. Chống chối cãi vệ thực chất là đưa ra moth hay một số chứng cứ quan trọng để phân xử giữa các bên. Chống chối cái về thực chất là đưa ra một hay một số chứng cứ quan trọng để phân xử giữa các bên. Có hai loại dịch vụ chống chối bỏ là chống chối bỏ nguồn gốc và chống chối bỏ phân phát.

- Chống chối bỏ nguồn gốc bảo vệ người nhận thông điệp ngăn chặn người khởi tạo sau đó chối bỏ đã tạo thông điệp, chối bỏ nội dung, thời gian khởi tạo của thông điệp.
- Chống chối bỏ phân phát bảo vệ người khởi tạo thông điệp ngăn chặn người nhận được thông điệp sau đó chối bỏ việc đã nhận thông điệp, chối bỏ nội dung và thời gian thông điệp.

Ví dụ, trong các giao dịch hành chính công trên mạng, chống chối cãi là bảo vệ chống lại sự từ chối của công dân, doanh nghiệp, cơ quan cấp dưới đối với những thông báo, chỉ thị, nghị quyết của cơ quan nhà nước do không thi hành đúng thời hạn hay có hành vi chống đối các quy định trên và sự từ chối của cơ quan nhà nước đối với những quyết định đã cấp cho công dân, doanh nghiệp và người lao động.

Trong các hệ thống thanh toán điện tử, chống chối cãi là bảo vệ chống lại sự từ chối của khách hàng đối với những đơn đặt hàng đã đặt và sừ từ chối của người bán hàng đối với những khoản thanh toán đã được trả.

Mã hóa, chữ ký số, công chứng là những kỹ thuật chính được dùng để thực thi dịch vụ chống chối bỏ.

- **Tính sẵn sàng**

Tính sẵn sàng là thông tin luôn sẵn sàng với những người dùng hợp pháp. Tính sẵn sàng phải đạt được các yêu cầu: sự hiện diện của đối tượng hoặc dịch vụ dưới dạng có thể dùng được; khả năng đáp ứng các yêu cầu về dịch vụ; tiến trình - giới hạn thời gian đợi; thời gian đầy đủ/tuyến thời gian của dịch vụ. Tính sẵn sàng của hệ thống phải đạt được các mục tiêu: đáp ứng về thời gian; cấp phát hợp lý; khả năng chịu lỗi; có lợi hoặc có khả năng sử dụng(có thể dùng được như mong muốn); đồng thời kiểm soát - hỗ trợ truy nhập đồng thời, quản lý tắc nghẽn và truy nhập loại trừ như yêu cầu.

Hai phương thức chính để đạt được tính sẵn sàng đó là thiết jế hệ thống gọn nhẹ và mạnh tránh các điểm xử lý có thể dẫn tới tình trạng quá tải và quản trị hệ thống thận trọng, các giao dịch tiến hành trên các giao dịch nguyên tử tức là giao dịch hoặc được kết thúc hoàn toàn hoặc bị hủy bỏ.

2.3.3 Làm thế nào để đảm bảo an toàn thông tin trong giao dịch điện tử

Vấn đề bảo đảm an toàn thông tin trong GDĐT, nhìn nhận một cách toàn diện, thực sự là một vấn đề phức tạp và bao hàm nhiều khía cạnh, nó không đơn giản như lời khuyên của một số chuyên gia nghiệp dư về CNTT là '*muốn tiếp cận với Internet thì hãy trang bị bức tường lửa, nếu cần sự bảo vệ thì hãy mã hóa và mật khẩu là đủ để xác thực*'. Thực tế việc bảo đảm an toàn thông tin trong GDĐT muốn đạt hiệu qủa thiết thực và tiết kiệm cần phải được hiểu theo khái niệm như là '*biết cách bảo vệ để chống lại sự tấn công tiềm ẩn*'. Bởi vậy, nó phải là tổng hòa các giải pháp của hạ tầng cơ sở bảo mật. Đó là:

- ✓ ***Về mặt Pháp lý và tổ chức***: trước hết phải xây dựng chính sách an toàn thông tin cho GDĐT nhằm tạo sự rõ ràng và có thể tiên liệu được, phản ánh được sự cân bằng quyền lợi của các chủ thể tham gia giao dịch điện tử , quan tâm tính riêng tư và an toàn xã hội, bảo đảm sự thi hành pháp luật và lợi ích an ninh quốc gia; ban hành các văn bản quy phạm pháp luật cần thiết, tiêu chuẩn mật mã và chữ ký điện tử sử dụng trong GDĐT, giải quyết khiếu nại và tố cáo khi có sự tranh chấp liên quan đến sử dụng mật mã; tổ chức các cơ quan chứng nhận, cấp phép, quản lý và

phân phối sản phẩm mật mã, phản ứng giải quyết sự cố, thanh tra và kiểm tra, vấn đề lưu trữ và phục hồi khoá, v.v...;

- Đối với **các kỹ thuật an toàn,** vấn đề đặt ra là kỹ thuật nào được chấp nhận để đảm bảo an toàn thông tin trong giao dịch điện tử, ví dụ: công nghệ mã hóa đối xứng, mã hóa phi đối xứng, công nghệ chữ ký số, công nghệ chữ ký sinh học v.v.; các chuẩn công nghệ đối với các kỹ thuật an toàn; công nhận về mặt pháp lý các kỹ thuật an toàn được chấp nhận, ví dụ: văn bản pháp quy về chữ ký ký điện tử nói chung và về chữ ký số nói riêng. Ở đây có một vấn đề cần quan tâm là: nói chung các văn bản quy phạm pháp luật liên quan cần phải trung lập về mặt công nghệ để đảm bảo sự phát triển bình đẳng của các công nghệ, nhưng trong từng thời kỳ không thể không đề cập đến các công nghệ cụ thể. Trong trường hợp đó việc đề cập đến công nghệ cụ thể sẽ được thực hiện như thế nào? Ví dụ: công nghệ chữ ký số là một công nghệ cụ thể so với các công nghệ khác như công nghệ chữ ký sinh học và các công nghệ khác sẽ xuất hiện trong tương lai. Có nên đưa chữ ký số vào trong luật hay chỉ đưa vào các văn bản dưới luật như nghị định, thông tư ? Các nước trên thế giới cũng có 2 quan điểm về vấn đề này: đưa thẳng vào luật và chỉ đưa vào văn bản dưới luật.

- Đối với **các dịch vụ an toàn**, vấn đề đặt ra là: ai được phép cung cấp dịch vụ, được phép đến mức nào v.v. Ví dụ: Có cho phép các tổ chức tư nhân hoặc nước ngoài cung cấp dịch vụ xác thực (Certificattion Authority - CA) không? Ai được phép cung cấp các dịch vụ mã hóa? v.v.

- Đối với **các cơ chế quản lý an toàn**, vấn đề đặt ra là: ai quản lý, quản lý đến mức nào và quản lý như thế nào các dịch vụ và cơ chế an toàn. Ví dụ: Dịch vụ xác thực CA (có cần quản lý không, ai quản lý và quy trình cấp phép cung cấp dịch vụ), xuất/nhập khẩu kỹ thuật và thiết bị mã hóa (ai quản lý và quản lý đến mức nào) v.v.

✓***Về mặt kỹ thuật***: Kết hợp chặt chẽ với hạ tầng công nghệ, quy định thống nhất tiêu chuẩn cấu trúc thiết lập hệ thống mạng và sử dụng công nghệ, ngôn ngữ giao tiếp và phần mềm ứng dụng, tổ chức hệ thống chứng thực và phân phối khóa

mã, các công cụ nghiệp vụ kỹ thuật kiểm tra và phát hiện xâm nhập; các giải pháp dự phòng, khắc phục sự cố xẩy ra đối với KTMM sử dụng trong GDĐT v.v.

✓ ***Về phía người sử dụng (tổ chức, cá nhân)***: Trước hết họ phải được "giác ngộ" về an toàn thông tin trong GDĐT - họ cần biết phải bảo vệ cái gì trong hệ thống của họ, ước định mức rủi ro và các nguy cơ tiềm tàng khi kết nối mạng của mình với các đối tượng khác, việc mở rộng mạng của mình trong tương lai v.v. - để họ có ý thức đầu tư bảo mật cho hệ thống của họ ngay từ khi bắt đầu xây dựng; chấp nhận và chấp hành chính sách, các quy định pháp luật về sử dụng mật mã, và phải chịu trách nhiệm trước pháp luật về bảo vệ bí mật quốc gia trong quá trình xử lý và truyền tải thông tin trong GDĐT v.v.

Với hệ thống thông tin mở, sử dụng công nghệ đa phương tiện như hiện nay thì về mặt lý thuyết không thể đảm bảo an toàn thông tin 100%, điều cốt yếu là chúng ta phải *tiên liệu được các nguy cơ tấn công tiềm ẩn đối với cái cần phải bảo vệ và biết bảo vệ như thế nào* cho hiệu qủa đối với hệ thống của mình. Cuối cùng, yếu tố con người vẫn là quyết định. Con người không được đào tạo kỹ năng và không có ý thức bảo mật cũng là kẽ hở cho những kẻ bất lương khai thác, và nếu con người trong hệ thống phản bội lại lợi ích của cơ quan, xí nghiệp và rộng hơn là của quốc gia thì không có giải pháp kỹ thuật an toàn nào có hiệu quả. Nói cách khác, an toàn thông tin trong GDĐT cần phải được bổ sung giải pháp an toàn nội bộ đặc biệt chống lại những đe doạ từ bên trong.

2.3.4 Giải pháp

CHỨNG CHỈ ĐIỆN TỬ

Khái niệm

Chứng chỉ điện tử 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

- 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.

- 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.

Một cách hiểu nôm na, nếu chứng chỉ số là một chứng minh thư nhân dân, thì khóa công khai đóng vai trò như danh tính của bạn trên giấy chứng minh thư (gồm tên, địa chỉ, ảnh...), còn khóa cá nhân là gương mặt và dấu vân tay của bạn. Nếu coi một bưu phẩm là thông tin truyền đi, được "mã hóa" bằng địa chỉ và tên người nhận của bạn, thì dù ai đó có dùng chứng minh thư của bạn với mục đích lấy

bưu phẩm này, họ cũng không được nhân viên bưu điện giao bưu kiện vì ảnh mặt và dấu vân tay không giống.

- 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.

Quy trình tạo chứng chỉ

Quá trình tạo ra một chứng chỉ bao gồm các bước sau đây:

1. CA nhận được các thông tin cần thiết cho chứng chỉ.
2. CA kiểm tra sự chính xác các thông tin đó (phù hợp với các chuẩn và các chính sách áp dụng).
3. Chứng chỉ được ký bởi một thiết bị ký sử dụng khóa riêng của CA.
4. Một bản sao của chứng chỉ được chuyển tới thuê bao và nếu được yêu cầu, thuê bao sẽ trả lại một xác nhận cho biết thuê bao đã nhận được chứng chỉ.
5. Như một dịch vụ của CA, một bản sao của chứng chỉ có thể được đưa tới một kho chứa chứng chỉ (ví dụ như một dịch vụ thư mục) để công bố.
6. Như một dịch vụ tùy chọn của CA, một bản sao của chứng chỉ có thể được CA lưu giữ.
7. CA ghi lại các chi tiết của quá trình tạo chứng chỉ vào nhật ký kiểm toán.

Cấu trúc chung của một chứng chỉ điện tử bao gồm:

- *ISSuer:* Tên của CA tạo ra chứng nhận
- *Period of validity:* ngày hết hạn của chứng nhận
- *Subject:* bao gồm những thông tin về thực thể được chứng nhận
- *Public key:* khoá công khai được chứng nhận
- *Signature:* do private key của CA tạo ra và đảm bảo giá trị của chứng nhận.

Sau khi chứng chỉ điện tử được cung cấp bởi CA thì nó có thể được đem ra sử dụng như một giấy thông hành trong trao đổi thương mại điện tử.

Lợi ích của chứng chỉ số

Mã hóa

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 điện

tử, 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.

Chữ ký điện tử

Email đóng một vai trò khá quan trọng trong trao đổi thông tin hàng ngày của chúng ta vì ưu điểm nhanh, rẻ và dễ sử dụng. Những thông điệp có thể gửi đi nhanh chóng, qua Internet, đến những khách hàng, đồng nghiệp, nhà cung cấp và các đối tác. Tuy nhiên, email rất dễ bị tổn thương bởi các hacker. Những thông điệp có thể bị đọc hay bị giả mạo trước khi đến người nhận. Bằng việc sử dụng chứng chỉ số cá nhân, bạn sẽ ngăn ngừa được các nguy cơ này mà vẫn không làm giảm những lợi thế của email. Với chứng chỉ số cá nhân, bạn có thể tạo thêm một chữ ký điện tử vào email như một bằng chứng xác nhận của mình. Chữ ký điện tử cũng có các tính năng xác thực thông tin, toàn vẹn dữ liệu và chống chối cãi nguồn gốc. Ngoài ra, chứng chỉ số cá nhân còn cho phép người dùng có thể chứng thực mình với một web server thông qua giao thức bảo mật SSL. Phương pháp chứng thực dựa trên chứng chỉ số được đánh giá là tốt, an toàn và bảo mật hơn phương pháp chứng thực truyền thống dựa trên mật khẩu

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...).

2.3.5 Lợi ích của việc áp dụng Giao dịch điện tử trong giao dịch hành chính

Giao dịch điện tử có thể được thực hiện giữa các cơ quan nhà nước với nhau hoặc với các tổ chức, cá nhân... Đây là một loại hình giao dịch góp phần đổi mới phương thức hoạt động của các cơ quan nhà nước, tạo cơ sở pháp lý để thúc đẩy cải cách hành chính, tăng cường hiệu lực, hiệu quả, tính công khai minh bạch, cung cấp thông tin, dịch vụ tốt hơn cho người dân, doanh nghiệp và các tổ chức...

- Giảm thiểu thời gian xử lý hồ sơ và các thủ tục hành chính.
- Nâng cao hiệu suất của chính quyền trong việc cung cấp dịch vụ công.
- Chuẩn hóa quy trình tác nghiệp, nâng cao khả năng giám sát, theo dõi quy trình giải quyết thủ tục hành chính.
- Hỗ trợ trao đổi thông tin trực tuyến trong quá trình giải quyết công việc của cán bộ, chuyên viên.

- Phân tích đánh giá hiệu quả công việc của từng cá nhân và phòng ban trong đơn vị.
- Là kho thông tin đầy đủ và phong phú nhất về thủ tục hành chính (quy trình giải quyết, hồ sơ thủ tục, thời gian giải quyết, phí và lệ phí) và các văn bản có liên quan.
- Công khai hóa và minh bạch hóa các thủ tục hành chính, hướng dẫn chi tiết cho tổ chức, công dân về từng loại thủ tục hành chính. Tổ chức, công dân có thể nhanh chóng tìm kiếm được thông tin mình quan tâm.
- Giảm tình trạng tham nhũng, thái độ thiếu tong trọng người dân ở các cơ quan nhà nước.
- Khai thông kênh thông tin hai chiều giữa chính quyền với doanh nghiệp và công dân.
- Công dân có thể khai thác thông tin về thủ tục hành chính và tình trạng hồ sơ của mình qua Website.

Vai trò của ứng dụng Công nghệ thông tin trong cải cách hành chính

Nói đến vai trò của ứng dụng công nghệ thông tin trong cải cách hành chính thực chất là đề cập đến khả năng tạo ra sự thay đổi đối với hành chính, phù hợp với mục tiêu, yêu cầu của cải cách hành chính thông qua ứng dụng công nghệ thông tin. Sơ bộ có thể thấy rõ vấn đề này trên những phương diện sau:

- Một là, thông qua ứng dụng công nghệ thông tin có thể tạo ra sự tiếp cận trên diện rộng của người dân, doanh nghiệp với các cơ quan hành chính nhà nước. Một trong những yêu cầu của cải cách hành chính là giảm thiểu những khó khăn, trở ngại trong giao tiếp giữa cơ quan hành chính với dân và doanh nghiệp. Cách thức truyền thống trong giao tiếp là người dân, doanh nghiệp trực tiếp đến cơ quan hành chính và cách thức thứ hai thông qua ứng dụng công nghệ thông tin người dân, doanh nghiệp có thể ngồi tại nhà, tại nơi làm việc vẫn liên hệ giao tiếp được với cơ quan hành chính. Môi trường giao tiếp điện tử toàn cầu và trong từng quốc gia góp phần đáng kể trong giảm thiểu tốn kém chi phí, thời gian, công sức người dân, doanh nghiệp khi cần liên hệ, giao tiếp với hành chính.

- Hai là, thông qua ứng dụng công nghệ thông tin có thể tạo ra một lượng thông tin lớn thường xuyên được lưu giữ, cập nhật và công bố chung cho cả xã hội. Thay vì trực tiếp đến cơ quan hành chính để tìm hiểu các quy định của pháp luật, các thủ tục hành chính, quy trình giải quyết… đối với từng vấn đề cụ thể như chuyển quyền sử dụng đất, cấp giấy phép xây dựng, đăng ký kinh doanh… người dân ngồi tại nhà vẫn có được những thông tin này một cách dễ dàng và nhanh chóng. Dưới góc độ này mà xem xét mới thấy vai trò lớn của công nghệ thông tin đáp ứng tốt yêu cầu về tính công khai, minh bạch của nền hành chính.
- Ba là, thông qua công nghệ thông tin, cơ quan hành chính có thể cung cấp qua mạng các dịch vụ công cho người dân, doanh nghiệp. Khả năng giải quyết công việc của người dân, doanh nghiệp qua mạng trực tuyến mở ra cơ hội thay đổi về chất trách nhiệm của các cơ quan công quyền cung cấp dục vụ công cho xã hội, đáp ứng yêu cầu và mục tiêu của cải cách hành chính là tạo sự thuận lợi tối đa cho dân, doanh nghiệp. Thực tiễn của nhiều nước và của Việt Nam về hải quan điện tử, chứng minh thư điện tử, cấp giấy phép kinh doanh qua mạng… là những minh chứng rõ ràng và thuyết phục về tác động do ứng dụng công nghệ thông tin mang lại cho nền hành chính và xã hội.

Trên đây là những khả năng tạo ra tác động phục vụ cho những mục tiêu, yêu cầu của cải cách hành chính thông qua ứng dụng công nghệ thông tin. Tuy nhiên sẽ là không đầy đủ nếu không xem xét đến những tác động qua ứng dụng công nghệ thông tin đối với bản thân nền hành chính nói chung và từng cơ quan hành chính nói riêng. Dưới góc độ này mà xem xét có thể rút ra mấy vấn đề sau:

+ Thứ nhất, thông qua ứng dụng công nghệ thông tin có thể tạo ra một sự thay đổi lớn trong cách thức làm việc của cơ quan hành chính: trao đổi thông tin (gửi báo cáo, số liệu thống kê, gửi ý kiếm tham gia, thẩm định, chia sẻ thông tin…) qua thư điện tử thay vì qua bưu điện, qua fax; tổ chức họp, hội thảo qua mạng; giải quyết công việc của dân, doanh nghiệp qua mạng trực tuyến…

+ Thứ hai, ứng dụng công nghệ thông tin dẫn đến thay đổi quy trình làm việc của cơ quan hành chính theo hướng phục vụ dân, doanh nghiệp tốt hơn. Thực tiễn

ứng dụng công nghệ thông tin tại bộ phận một cửa cấp huyện ở Hải Phòng, Bà Rịa - Vũng tàu đã khẳng định vấn đề này.

+ Thứ ba, ứng dụng công nghệ thông tin trong hành chính dẫn đến sắp xếp lại tổ chức, nhân sự phù hợp với yêu cầu của cải cách hành chính là tổ chức gọn nhẹ, rõ chức năng, nhiệm vụ, hoạt động có hiệu quả.

2.4 Đề xuất định hướng phát triển trong giao dịch hành chính

Triển khai hành chính công trực tuyến năm 2009

Kế hoạch ứng dụng Công nghệ thông tin trong hoạt động của cơ quan nhà nước giai đoạn 2009-2010 đã được Chính phủ phê duyệt, theo Cục trưởng cục ứng dụng Công nghệ thông tin, bộ TT&TT – đơn vụ trực tiếp soạn thảo kế hoạch, một số hạng mục dự án có thể lập dự toán và triển khai năm 2009. Các kế hoạch ứng dụng Công nghệ thông tin trong cơ quan nhà nước và xây dựng Chính phủ điện tử do bộ TT&TT chủ trì đã đặt ra những mục tiêu cụ thể, ngắn hạn, từng bước. Kế hoạch thứ nhất đến hết năm 2008 kết thúc với một số kết quả nhất định như hoàn thiện gần 100% các trang thông tin điện tử và Cổng thông tin điện tử các tỉnh, thành, bộ, ngành và hầu hết các cán bộ nhà nước đã có hộp thư điện tử để liên hệ công việc.

Năm 2009-2010: Xây dựng các cơ quan điện tử

Kế hoạch được Chính phủ phê duyệt cũng xác định trong giai đoạn ngắn 2009-2010, với một số mục tiêu nổi bật như: nâng cao năng lực quản lý, điều hành của các cơ quan nhà nước, hướng tới xây dựng các cơ quan điện tử. Đến hết năm 2010, bảo đảm trung bình 60%(năm 2009 là 30%) các thông tin chỉ đạo, điều hành của lãnh đạo các cấp bộ, cấp tỉnh được đưa lên Cổng thông tin điện tử.

Đến năm 2010, đảm bảo 80% các trang thông tin điện tử của các cơ quan cấp bộ, các UBND cấp tỉnh có cung cấp dịch vụ công trực tuyến mức độ 2 cho người dân và doanh nghiệp, đảm bảo 90% (năm 2009 là 80%) các vụ, văn phòng bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, văn phòng UBND thành phố trực thuộc Trung ương triển khai sử dụng phần mềm ứng dụng quản lý văn bản và điều hành trên môi trường mạng.

Bên cạnh đó, các cuộc họp của Chính phủ, Thủ tướng Chính phủ với các bộ, các tỉnh và các cuộc họp của các bộ với các cơ quan trực thuộc cũng phải đảm bảo thực hiện từ xa, như đã tiến hành lần đầu tiên vào phiên họp tháng 3/2009 vừa qua.

Trong giai đoạn 2009-2010, ưu tiên triển khai các nhóm dịch vụ công trực tuyến mức độ 3, gồm: cấp giấy đăng ký kinh doanh; cấp giấy phép đầu tư, giấy phép thành lập chi nhánh, văn phòng đại diện, giấy phép xây dựng; chứng chỉ hành nghề hoạt động xây dựng; chứng nhận quyền sở hữu nhà và quyền sử dụng đất; giấy đăng ký ô tô, xe máy; đăng ký tạm vắng, tạm trú; giải quyết khiếu nại, tố cáo; giấy đăng ký hành nghề y dược và cấp giấy phép hoặc dịch vụ đặc thù.

Kế hoạch cũng đề ra biện pháp từng bước xây dựng nền tảng phục vụ Chính phủ điện tử như: hoàn thành việc xây dựng mạng truyền số liệu chuyên dùng của cơ quan Đảng, Nhà nước; xây dựng và nâng cấp các mạng LAN và mạng diện rộng của các cơ quan nhà nước và tiếp tục nghiên cứu, đánh giá và lựa chọn mô hình ứng dụng Công nghệ thông tin điển hình cấp huyện để phổ biến rộng rãi.

Đối với việc phát triển nguồn nhân lực công nghệ thông tin, kế hoạch đã đề ra phương án tiếp tục xây dựng và phát triển đổi ngũ giám đốc công nghệ thông tin, bồi dưỡng kiến thức công nghệ thông tin cho cán bộ, công chức trong cơ quan nhà nước, nghiên cứu xây dựng chế độ ưu đãi đối với cán bộ, công chức chuyên trách về Công nghệ thông tin và đẩy mạnh ứng dụng đào tạo trực tuyến cho cán bộ, công chức.

Năm 2015 sẽ là dịch vụ công trực tuyến mức độ 3 và 4

Bản kế hoạch cũng đề ra định hướng đến năm 2015, trong đó xác định ứng dụng Công nghệ thông tin để đổi mới phương thức cung cấp thông tin và dịch vụ công cho người dân và doanh nghiệp, phấn đấu đến năm 2015 sẽ có thể cung cấp hầu hết các dịch vụ công cơ quản trực tuyến mức độ 3 hoặc 4, người dân và doanh nghiệp có thể trao đổi thông tin, gửi nhận hồ sơ, thanh toán phí dịch vụ, nhận kết quả dịch vụ qua mạng.

Ngoài ra, Công nghệ thông tin cũng được khai thác triệt để tính tối ưu để đổi mới phương thức quản lý tài nguyên thông tin trong các cơ quan nhà nước, phát triển các cơ sở dữ liệu quốc gia về con người, đất đai, tài chính, kinh tế, công nghiệp và thương mại tạo nền tảng triển khai Chính phủ điện tử, từng bước tích hợp

các hệ thống thông tin, tiếp tục xây dựng và mở rộng hệ thông thông tin và cơ sở dữ liệu phục vụ cho hoạt động quản lý, điều hành chung của cơ quan nhà nước và phục vụ người dân, doanh nghiệp…

CHƯƠNG 3. TÌM HIỂU THỰC TIỄN ỨNG DỤNG CÔNG NGHỆ THÔNG TIN TRONG GIAO DỊCH HÀNH CHÍNH

3.1. Thực tiễn ứng dụng Công nghệ thông tin trong hành chính công ở Hải Phòng

Hơn 20 năm qua, Việt Nam kiên trì thực hiện đường lối đổi mới toàn diện đất nước và đã thu được những thành tựu quan trọng trong phát triển kinh tế - xã hội, ổn định chính trị, từng bước nâng cao đời sống của nhân dân. Công cuộc đổi mới được tiến hành trên hầu hết các lĩnh vực của đời sống xã hội, từ đổi mới từng bước hệ thống chính trị, đến cải cách bộ máy nhà nước, cải cách kinh tế, cải cách giáo dục, y tế v.v… Có thể khẳng định, cải cách hành chính nhà nước luôn là một chủ trương quan trọng trong đường lối đổi mới của Việt Nam. Từ yêu cầu của bước chuyển sang nền kinh tế thị trường định hướng xã hội chủ nghĩa, từ yêu cầu của quá trình hội nhập sâu rộng vào nền kinh tế thế giới và từ chính những yêu cầu của người dân, doanh nghiệp về một nền hành chính phục vụ dẫn đến không có cách nào khác phải cải cách nền hành chính nhà nước. Nhiều nghị quyết của Đảng đã khẳng định và chỉ rõ phải đẩy mạnh cải cách hành chính. Chính phủ đã thông qua Chương trình tổng thể cải cách hành chính nhà nước giai đoạn 2001-2010, Chương trình hành động thực hiện Nghị Quyết TW 5 khóa X về "Đẩy mạnh cải cách hành chính, nâng cao hiệu lực, hiệu quả quản lý của bộ máy nhà nước".

Các nghị quyết của Đảng và Nhà nước Việt Nam đã xác định mục tiêu cải cách hành chính nhằm tiếp tục xây dựng và hoàn thiện nhà nước pháp quyền xã hội chủ nghĩa; xây dựng một nền hành chính dân chủ, trong sạch, vững mạnh, từng bước hiện đại; đội ngũ cán bộ, công chức có đủ phẩm chất và năng lực; hệ thống các cơ quan nhà nước hoạt động có hiệu lực, hiệu quả, phù hợp với thể chế kinh tế thị trường định hướng xã hội chủ nghĩa và hội nhập kinh tế quốc tế; đáp ứng tốt yêu cầu phát triển nhanh và bên vững của đất nước.

Cùng với cả nước trong công cuộc cải cách hành chính, Hải Phòng đang từng bước áp dụng các thành tựu về công nghệ thông tin trong hành chính công, đưa công nghệ thông tin vào hầu hết các hoạt động của các cơ quan nhà nước, xây dựng các cổng thông tin điện tử đối với các Sở, ban, ngành, các quận huyện và các phường. Các cổng thông tin điện tử là nơi cung cấp các thông tin về thành phố cũng như địa phương, cập nhật những chủ trương, chính sách mới, các hướng dẫn về các thủ tục hành chính, ngoài ra đó còn là nơi đối thoại công tư giữa chính quyền thành phố với các doanh nghiệp, tổ chức và người dân của thành phố. Ở các Sở, ban, ngành đều xây dựng hệ thống mạng Lan nội bộ để điều hành các hoạt động công tác chuyên môn, hình thành kho dữ liệu dùng chung của cơ quan. Bên cạnh đó, các sở ngành còn thành lập bộ phận "một cửa" liên thông nội bộ với các phòng nghiệp vụ trong cơ quan để rút ngắn thời gian giải quyết công việc. Hải Phòng cũng đẩy mạnh việc triển khai mô hình "một cửa" mẫu hiện đại, áp dụng quản lý chất lượng theo tiêu chuẩn TCVN 9001:2000 ở các quận, huyện, sở và các ban, ngành… Thành phố ưu tiên và khuyến khích các địa phương đầu tư trang bị các thiết bị hiện đại, sớm hoàn thành công cuộc cải cách hành chính, nhờ đó tạo khâu đột phá trong phát triển kinh tế - xã hội, nhằm thu hút mạnh mẽ đầu tư, khơi dậy các nguồn lực, tận dụng tối đa những cơ hội thuận lợi đang đến với thành phố.

3.1.1. Ứng dụng CNTT trong cải cách hành chính ở quận Ngô Quyền

Quận Ngô Quyền là một trong những quận đi đầu ở Hải Phòng ứng dụng công nghệ thông tin cải cách hành chính và quản lý nhà nước. Được bắt đầu từ năm 2004 và triển khai mạnh từ năm 2006, đến nay mục tiêu xây dựng "cổng thông tin điện tử" của quận Ngô Quyền đang dần phát huy hiệu quả. Giữa tháng 12-2008, Ngô Quyền trở thành quận đầu tiên của Hải Phòng hoàn tất việc liên thông các cổng thông tin điện tử từ các phường, phòng, ban với UBND quận. Việc điều hành từ quận xuống các phường hay việc phục vụ nhân dân đều được giải quyết thông qua mạng điện tử công nghệ thông tin.

Quận Ngô Quyền đang áp dụng các quy trình quản lý chất lượng theo tiêu chuẩn Việt Nam ISO 9001:2000 và ứng dụng công nghệ thông tin (CNTT) trong dịch

vụ hành chính công theo hướng liên thông hiện đại. Hệ thống 40 trang thông tin điện tử thành phần của các phường và phòng, ban chức năng trong quận luôn bảo đảm phục vụ kịp thời, nhanh chóng, chính xác thông tin tới người dân. Mọi quy trình thủ tục đều được hướng dẫn chi tiết trong các quyển sổ bàn hay bảng tra cứu điện tử…

Theo Chủ tịch UBND quận Nguyễn Xuân Phi cho biết: Quận đã triển khai hai ứng dụng cơ bản. Một là, xây dựng website của quận để chia sẻ thông tin; hai là, hệ điều hành tác nghiệp, sử dụng nhiều phần mềm quy trình xử lý công việc có kết nối với tất cả các đơn vị phòng ban trong toàn quận. Quy trình này được thiết lập theo tiêu chuẩn chất lượng ISO 9001:2000. Phần mềm "một cửa liên thông" cũng nằm trong hệ thống này.

Trước đây, mỗi lần đi làm hồ sơ cấp phép đất đai - xây dựng, thường thì người dân thấy rất mệt mỏi vì phải tự cầm hồ sơ đến từng bộ phận, từ Phòng Địa chính sang Phòng Tài nguyên, đến Phòng Quản lý đô thị rồi Phòng Thu thuế, lệ phí... Vất vả như thế nhưng vẫn không biết lúc nào mới nhận được hồ sơ. Đôi khi hồ sơ được giải quyết xong nhưng cũng không biết tìm ai để nhận. Chưa kể cách giao tiếp của cán bộ, công chức cũng thường gây khó chịu. Nay thì người dân chỉ cần đem hồ sơ đến bộ phận "một cửa", nhận giấy hẹn và chờ ngày trả kết quả. Loại hồ sơ nào giải quyết bao nhiêu ngày đã có quy định rõ ràng, không lo chuyện nhậm nhèm. Hơn nữa, thái độ của cán bộ phòng "một cửa" rất nhã nhặn, mọi quy trình thủ tục đều được hướng dẫn trong cuốn sổ để trên bàn, bảng tra cứu điện tử, loa công cộng… Trong ngày chờ kết quả, người dân có thể vào website của quận, vào "mục tra cứu hồ sơ", gõ mã số trên giấy hẹn vào mục tra cứu để biết hồ sơ của mình đang ở bộ phận nào, do ai giải quyết, giải quyết đến đâu, còn thiếu những gì… Ngoài ra, người dân cũng có thể đến UBND quận, đưa giấy hẹn vào máy đọc mã vạch để kiểm tra tình trạng hồ sơ.

Từ khi triển khai "một cửa" điện tử, thời gian giải quyết hồ sơ rút ngắn đáng kể, do đó số lượng hồ sơ được giải quyết tăng lên rất nhiều. Chẳng hạn, trước đây xác nhận một hồ sơ đi học/đi làm mất ít nhất ba ngày, nay chỉ còn khoảng 15 phút.

"Một cửa"chỉ là một trong những thay đổi nằm trong toàn bộ những thay đổi lớn xuất phát từ nỗ lực cải cách hành chính kết hợp với ứng dụng CNTT ở quận Ngô Quyền.

Hiện nay quận Ngô Quyền đã cung cấp nhiều dịch vụ trực tuyến cho người dân và doanh nghiệp như đăng ký kinh doanh, tra cứu hồ sơ, tra cứu thủ tục và trao đổi thông tin trực tuyến, cung cấp thông tin hai chiều… tiết kiệm được chi phí hành chính, giảm hồ sơ thủ tục giấy tờ. Quận đã tiến hành giảm hội họp bằng cách giao ban và điều hành trên mạng. Với đầu tư ban đầu không lớn (năm 2006 là 1 tỷ, mỗi năm sau là 300 triệu đồng), nhưng hiệu quả mà quận đạt được là rất to lớn. Việc ứng dụng Công nghệ thông tin của quận Ngô Quyền giúp khắc phục được tình trạng một cửa nhiều dấu, hình thức. Cán bộ kho bạc sang bên quận có thể in hóa đơn tại chỗ vì có phần mềm kết nối với kho bạc. Người dân đến đóng thuế, không cần phải đến kho bạc mà có thể nộp ngay ở phòng "một cửa" của Ủy ban quận. Bằng việc chuẩn hóa và mã hóa các thủ tục hành chính bằng phần mềm điều hành tác nghiệp, đây là công cụ hữu hiệu trong cải cách hành chính, hỗ trợ tích cực cho lãnh đạo quản lý, kiểm tra điều hành, dễ dàng truy xuất khai thác hồ sơ tài liệu, công khai minh bạch đối với công việc, với tổ chức và người dân.

Quận có văn phòng chuyên giải quyết tất cả những vướng mắc của người dân. Không nhất thiết phải đến tận UBND quận, mà chỉ cần vào website của quận là có thể tra cứu được mọi hồ sơ, thủ tục. Để tránh tình trạng hồ sơ có sai sót, quận đã bố trí cán bộ nghiệp vụ thật giỏi ở ngay khâu "một cửa" để nhận hồ sơ, kiểm tra hồ sơ và ghi giấy biên nhận, người dân chỉ việc nộp tiền và sau vài ngày thì đến nhận hồ sơ. Nếu hồ sơ nào không đạt yêu cầu thì phải hướng dẫn luôn cho người dân.

Vấn đề an ninh bảo mật được đặc biệt chú trọng. Quận có 2 hệ thống lưu trữ. Một là bản cứng bằng giấy, thứ hai là bản mềm. Hai hệ thống này có chung mã vạch. Bản mềm để tra cứu cho nhanh, còn bản gốc vẫn để lưu trữ. Để đảm bảo, quận tiến hành không lưu trã ở một nơi mà ở nhiều chỗ khác nhau. Máy chủ có nhiều ổ cứng và cùng một lúc dữ liệu được lưu ở hai ổ. Hiện nay quận có 2 máy chủ, và dự định sẽ làm việc với công ty viễn thông gửi một máy chủ lên Hà Nội để tốc độ đường truyền cao.

Nhờ có phần mềm hữu ích, thông minh, việc chỉ đạo từ quận xuống các phường, hay việc báo cáo ngược lại, từ phường lên quận đều được kết nối trên cùng một hệ thống, nên công việc được thực hiện đồng bộ, nhanh chóng, không mất công và thời gian. Quận giao việc là phường biết ngay, tự xử lý và nhập kết quả vào máy. Kết quả hằng ngày được tự động tổng hợp và hiển thị trong phần mềm, khi cần là lãnh đạo có thông tin về tình hình hoạt động trong tuần, chi tiết đến từng cán bộ, công chức, từng phòng, ban. Những việc chậm so với thời gian giải quyết thì báo đỏ. Việc lưu giữ, tổ chức thông tin cũng được thực hiện tự động: hồ sơ nào xử lý đến đâu, cái nào chuyển đi, cái nào lưu trữ đều được cập nhật. Thông tin từ các cơ sở liên tục được chuyển lên, phân loại và nhập vào cơ sở dữ liệu dùng chung. Với các công chức, từ khi có quy trình mới, áp lực công việc lớn hơn vì trước kia không ai theo dõi, nay có máy giám sát khoa học và chính xác, không làm hoặc làm sai là lãnh đạo quận biết ngay. Mặt khác, họ buộc phải thao tác công việc trên máy mới có kết quả.

Thật ra, sự tiện lợi đó mới chỉ là những thay đổi nhìn thấy được. Đằng sau đó là một sự đổi mới mạnh mẽ về quy trình hành chính, trong đó CNTT đóng vai trò quan trọng. Theo Chủ tịch UBND quận: Có được thành công nêu trên là nhờ quận Ngô Quyền đã đẩy mạnh việc ứng dụng CNTT, lấy con người làm nhân tố trung tâm. Quận đã tổ chức tập huấn rất nhiều về cải cách hành chính và một trong những nội dung là chuyển biến mạnh về nhận thức cho đội ngũ cán bộ lãnh đạo và công chức. Đồng thời, quận có chính sách động viên khen thưởng đối với công chức, đặc biệt là đào tạo, đề bạt đối với những cán bộ trẻ có năng lực. Một trong những tiêu chuẩn để được đề bạt trưởng, phó phòng là phải biết ứng dụng CNTT.

Theo Chủ tịch Nguyễn Xuân Phi, cần đầu tư đạt ngưỡng: ít nhất mỗi đơn vị phải có máy trạm, đường truyền, phần mềm để kết nối với nhau và chia sẻ thông tin. Vì vậy, từ tháng 9-2006, quận đã đầu tư ban đầu hơn một tỷ đồng đầu tư hệ thống máy tính cho 10 quầy giao dịch, màn hình cảm ứng, phần mềm tra cứu điện tử, xếp hàng điện tử... Đặt trong điều kiện hiện nay, việc cải cách hành chính nếu không đi đôi với ứng dụng CNTT thì đó cũng chỉ là hô khẩu hiệu "suông". Việc đầu tư về công nghệ với máy tính, phần mềm mới chỉ là bước đi ban đầu, vấn đề mấu chốt

quyết định hiệu quả của sự đầu tư phụ thuộc ở trình độ, năng lực chuyên môn của đội ngũ cán bộ, công chức.

Trong thời gian qua, Quận đã xây dựng và đưa vào áp dụng cổng thông tin điện tử phục vụ cho điều hành tác nghiệp chung, triển khai website riêng của quận và các website thành phần đơn vị trực thuộc quận để chia sẻ tài nguyên. Dự định trong thời gian tới, quận sẽ nâng cấp cổng thông tin điện tử và ứng dụng triệt để phần mềm điều hành tác nghiệp trong toàn quận, dự kiến tìm hiểu và sử dụng chữ ký điện tử đối với các giấy tờ thủ tục nếu thủ tục pháp lý cho phép. Ngoài ra quận cũng đang lên kế hoạch đào tạo nguồn nhân lực, tập trung phát triển Công nghệ thông tin.

3.1.2. Quận Hồng Bàng

Ngoài quận Ngô Quyền, Quận Hồng Bàng cũng là một trong hai địa phương của thành phố được chọn để thực hiện xây dựng điểm bộ phận tiếp nhận và trả hồ sơ "một cửa" theo hướng hiện đại, chuyên trách, độc lập và liên thông. Việc ứng dụng Công nghệ thông tin trong cải cách hành chính ở đây là một bước đột phá, không chỉ góp phần giảm thiểu đáng kể thời gian, nâng cao tính chính xác của quá trình giải quyết thủ tục mà còn giảm số cấn bộ công nhân viên tại bộ phận "một cửa". Nếu ứng dụng công nghệ thông tin một cách hiệu quả sẽ từng bước hiện đại hóa công tác giải quyết thủ tục hành chính, quá trình cải cách hành chính đã đạt kết quả cao hơn, rút ngắn hơn nữa thời gian giải quyết hồ sơ. Điều này tạo tiền đề để hướng đến Chính phủ điện tử.

3.2. Ứng dụng giao dịch điện tử trong giao dịch hành chính ở TP Hồ Chí Minh

Cùng với Hải Phòng, TPHCM là một trong những địa phương đầu tiên triển khai rộng rãi ứng dụng Công nghệ thông tin trong giao dịch hành chính. Tuy nhiên so với Hải Phòng, TPHCM đã ứng dụng rộng rãi hơn rất nhiều mà mức độ ứng dụng cũng đã nhanh hơn và cao hơn. Các ứng dụng chủ yếu là triển khai cổng thông tin điện tử và mô hình một cửa điện tử để cung cấp thông tin đến người dân, doanh nghiệp. TPHCM đã thành công trong việc xây dựng hệ thống tương tác hai chiều phục vụ các nhu cầu của nhân dân trong các thủ tục hành chính, đăng ký kinh doanh, chứng nhận quyền sở hữu…

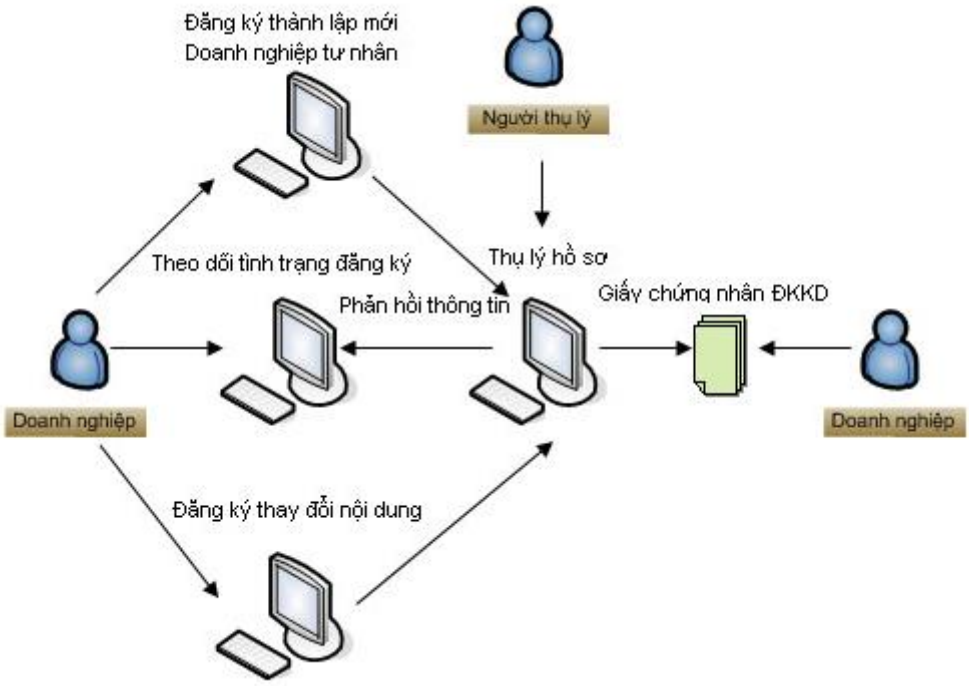
Việc ứng dụng công nghệ thông tin và truyền thông trong các cơ quannhà nước ngày càng được coi trọng và đẩy nhanh quá trình triển khai. Một số hoạt động

giao dịch hành chính đã được áp dụng rộng rãi trong các cơ quan nhà nước. Chúng góp phần đẩy nhanh quá trình cải cách hành chính. Sau đây ta sẽ tìm hiểu vấn đề ứng dụng Giao dịch điện tử trong hoạt động hành chính công, đó là đăng ký kinh doanh trực tuyến. Đây là một dịch vụ rất quan trọng trong việc cải cách hành chính, dịch vụ này đã được triển khai ở nước ta và đã nhanh chóng được triển khai rộng khắp.

Đăng ký kinh doanh trực tuyến

Đăng ký kinh doanh trực tuyến là chương trình cho phép các doanh nghiệp, các nhà đầu tư xin cấp giấy chứng nhận đăng ký kinh doanh bằng cách gửi các thông tin đăng ký tới sở kế hoạch và đầu tư thông qua mạng. Thực hiện đăng ký kinh doanh trực tuyến thúc đẩy cải cách hành chính trong lĩnh vực kinh doanh của hành chính công. Chương trình này sẽ hỗ trợ các nhà đầu tư soạn thảo hồ sơ đăng ký kinh doanh cho từng loại doanh nghiệp và hướng dẫn thủ tục gia nhập thị trường, đăng ký mã số thuế và khắc dấu qua mạng. Các loại hình doanh nghiệp được phép đăng ký kinh doanh qua mạng gồm: Đăng ký thành lập doanh nghiệp tư nhân; Đăng ký thành lập chi nhánh; Đăng ký thành lập công ty cổ phần; Đăng ký thành lập công ty trách nhiệm hữu hạn; Thay đổi nội dung đăng ký kinh doanh.

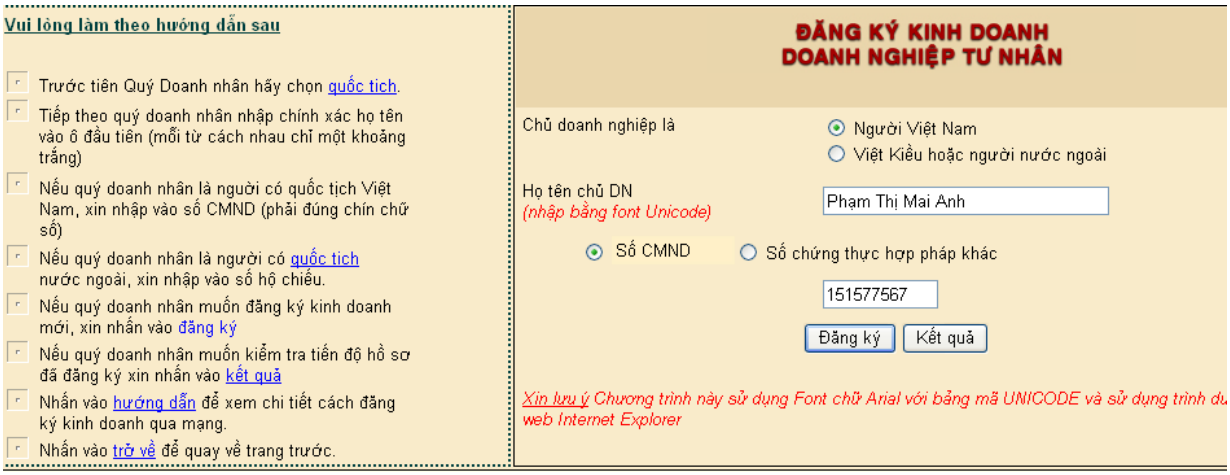
Quy trình thực hiện đăng ký kinh doanh trực tuyến



Bao gồm các bước sau:

Bước 1: Vào website của sở kế hoạch và đầu tư, chọn mục Đăng ký kinh doanh để chọn loại hình doanh nghiệp đăng ký.

Nhập các thông tin kiểm tra ban đầu bao gồm: Họ tên chủ Doanh nghiệp; Số Chứng minh nhân dân hoặc số chứng thực hợp pháp khác. Sau đó nhấn "Đăng ký".



Form nhập dữ liệu ban đầu

Người đăng ký nhận tiếp các thông tin chi tiết về doanh nghiệp, về ngành nghề kinh doanh theo mẫu. Đối với phần đăng ký ngành nghề kinh doanh, hệ thống có một danh sách các ngành nghề. Người đăng ký chỉ cần chọn ngành nghề trong danh sách. Doanh nghiệp chỉ được đăng ký trực tuyến đối với những ngành nghề được phép, do một số ngành nghề vẫn bị hạn chế, chưa được phép đăng ký kinh doanh trực tuyến.

Doanh nghiệp cần gửi kèm theo giấy phép đăng ký kinh doanh các tài liệu đính kèm liên quan như xác nhận hoặc chứng chỉ hành nghề, điều lệ công ty mẫu.

Sau khi nhập đầy đủ các thông tin và hoàn tất các thủ tục trên, doanh nghiệp bấm nút "Đăng ký" để chuyển các thông tin đăng ký kinh doanh về Sở kế hoạch và đầu tư.

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

ĐĂNG KÝ KINH DOANH
DOANH NGHIỆP TƯ NHÂN

Kính gởi: Phòng đăng ký kinh doanh Sở Kế hoạch và Đầu tư TpHCM.

(Lưu ý: vui lòng nhập thông tin bằng font Unicode)

Tôi là * Ph?m Th?Mai Anh Giới tính: * Nam ○ Nữ ●

Sinh ngày(ng/th/nnnn) * Dân tộc *

Số chứng thực * 151577566

Ngày cấp (ng/th/nnnn)* Nơi cấp *

Nơi đăng ký hộ khẩu thường trú * (Số nhà, đường, phường, quận)

Chỗ ở hiện tại * (Số nhà, đường, phường, quận)

Điện thoại

Fax

Đăng ký kinh doanh doanh nghiệp tư nhân do tôi làm chủ với nội dung sau:

1. Tên doanh nghiệp * Doanh nghi?p tu nh

Tên giao dịch

Tên viết tắt

2. Địa chỉ trụ sở chính * (Số nhà, đường, phường, quận)

Điện thoại

Fax

Email

3. Ngành nghề kinh doanh *

4. Vốn đầu tư ban đầu

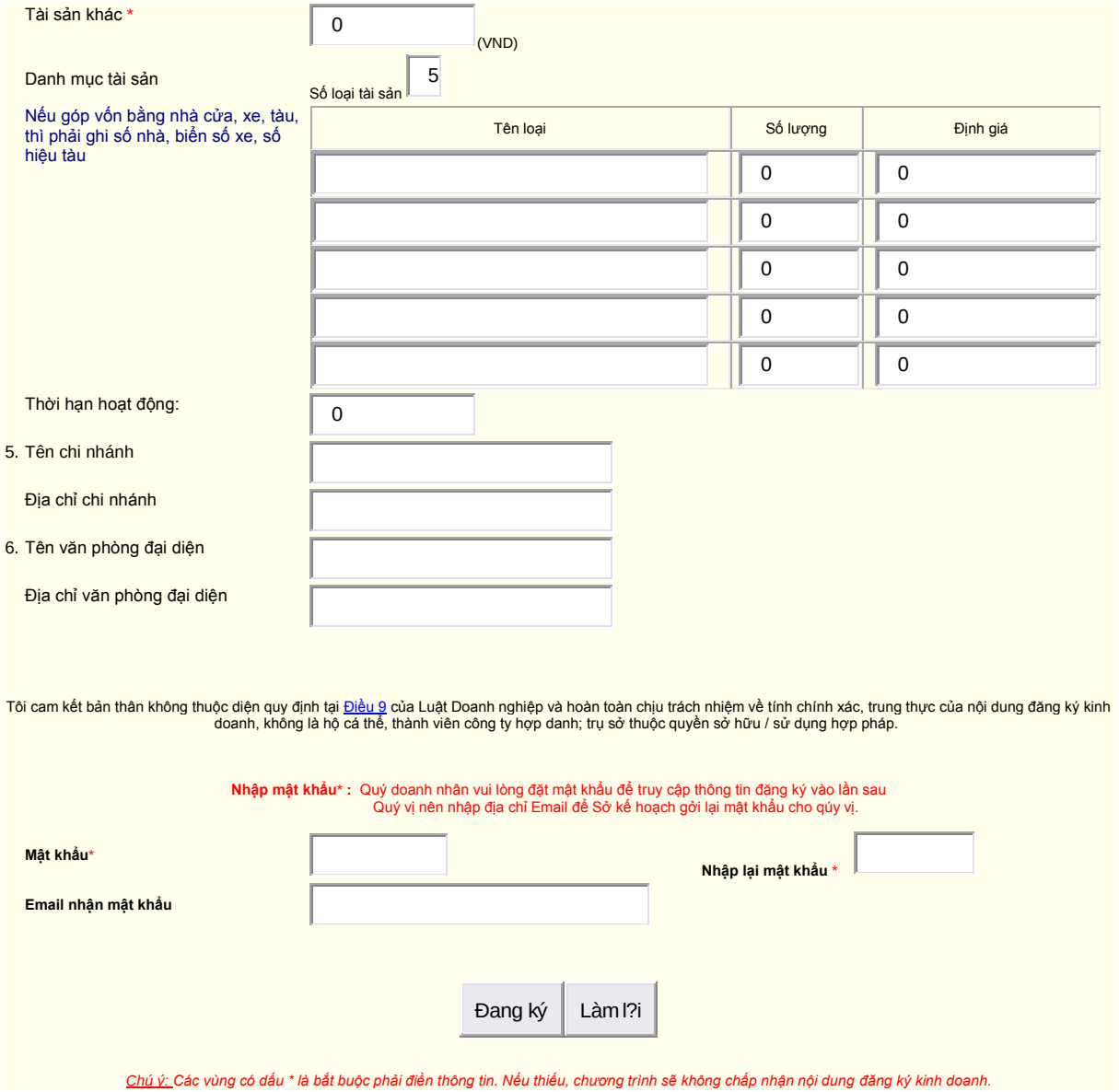
Tổng số * 0 (VND) Vốn Pháp định: 0

Trong đó

Tiền Việt Nam * 0 (VND)

Ngoại tệ tự do chuyển đổi * 0 (VND)

Vàng * 0 (VND)



Form đăng ký thông tin chi tiết doanh nghiệp

Bước 2: Thẩm định hồ sơ, cấp và nhận giấy Chứng nhận đăng ký kinh doanh

Sau khi nhấn nút "Đăng ký", chương trình sẽ thông báo kết quả chuyển hồ sơ về Sở. Nếu tên doanh nghiệp người đăng ký chọn đã có người đăng ký rồi thì chương trình sẽ thông báo để chọn lại tên doanh nghiệp khác. Nếu được chấp nhận thì chương trình hiện lại toàn bộ thông tin đã đăng ký để người đăng ký kiểm tra lại lần cuối, nếu cần có thể nhấn nút "Thay đổi" để điều chỉnh thông tin. Ngoài ra còn có thể in thông tin này để lưu trữ nếu thấy cần thiết.

Trước khi đến nhận hồ sơ chính thức tại Phòng Đăng ký kinh doanh – Sở kế hoạch và đầu tư, người đăng ký còn có thể thay đổi hoặc hủy thông tin bằng cách vào lại họ tên và số Chứng minh nhân dân hay hộ chiếu và nhấn nút "Kết quả", nếu muốn thay đổi thông tin thì nhấn nút "Thay đổi", muốn hủy thông tin thì nhấn nút "Hủy". Sau khi người đăng ký thay đổi thông tin thì sự chấp nhận của Phòng Đăng ký kinh doanh Sở kế hoạch và đầu tư trước đó sẽ không còn giá trị nữa.

Sau khi gửi thông tin đăng ký qua mạng tới Sở, Sở kế hoạch và Đầu tư sẽ tiến hành thẩm định hồ sơ xem có hợp lệ không: thông tin đăng ký có đầy đủ và chính xác không, có đầy đủ các giấy tớ cần thiết không… Sau không quá 2 ngày làm việc, người đăng ký sẽ nhận được kết quả xử lý hồ sơ qua phần "Kết quả" và email nếu có. Nếu hồ sơ được chấp nhận, thông tin trả lời sẽ hẹn ngày để người đăng ký đến Phòng Đăng ký kinh doanh Sở kế hoạch đầu tư để hoàn tất thủ tục đăng ký kinh doanh tại chỗ và nhận giấy chứng nhận đăng ký kinh doanh chỉ trong 1 giờ. Trong trường hợp hồ sơ của bạn chưa được chấp nhận, thông tin trả lời sẽ nêu rõ lý do và hướng dẫn cho bạn thực hiện lại. Ngoài ra còn có thể in thông báo đó ra giấy để lưu trữ.

Khi doanh nghiệp đến Sở để nhận giấy chứng nhận đăng ký kinh doanh cần chú ý xem thông tin về những hồ sơ mang theo và ngày hẹn trong phần "Thông tin trả lời".

Sau khi nhận được giấy chứng nhận đăng ký kinh doanh, doanh nghiệp phải tiến hành đăng ký mã số thuế và đăng ký khắc dấu. Trong thời hạn 10 ngày kể từ ngày nhận được chứng nhận đăng ký kinh doanh, doanh nghiệp phải thực hiện đăng ký thuế với cơ quan thuế. Doanh nghiệp có thể nộp hồ sơ trực tiếp tại cục thuế tỉnh/ thành phố hoặc chi cục thuế Quận/ Huyện/ Thị xã và nhận phiếu hẹn ngày nhận mã số thuế. Thời gian để nhận được mã số thuế là không quá 15 ngày.

Thuận lợi và hạn chế của đăng ký kinh doanh trực tuyến ở nước ta

- Thuận lợi: việc triển khai đăng ký kinh doanh trực tuyến đã mang lại những thuận lợi
  - Cho phép doanh nghiệp thực hiện việc đăng ký một cách dễ dàng và thuận tiện, ở bất kỳ nơi nào, bất kỳ thời điểm nào.
  - Minh bạch và công khai hóa các thủ tục hành chính.

- Thời gian xử lý hồ sơ và đăng ký nhanh hơn.
- Hiện nay, nhà nước ta đang rất chú trọng việc triển khai áp dụng Giao dịch điện tử trong giao dịch hành chính.

➢ Hạn chế

- Các thủ tục đăng ký còn chưa hoàn toàn được thực hiện qua mạng.
- Thời gian xử lý còn dài
- Tính hiệu quả chưa cao, tỉ lệ các doanh nghiệp thực hiện đăng ký qua mạng chưa cao do các doanh nghiệp chưa hoàn toàn tin tưởng vào việc đăng ký kinh doanh qua mạng và nhiều người còn chưa biết đến dịch vụ này.

3.3 Ứng dụng Công nghệ thông tin trong giao dịch hành chính ở Hà Nội

Cũng như TPHCM và Hải Phòng, Hà Nội cũng đã triển khai rộng rãi ứng dụng Công nghệ thông tin trong giao dịch hành chính và trong việc tương tác thông tin hai chiều giữa lãnh đạo thành phố với người dân và doanh nghiệp. Từ ngày 1/6/2009, UBND TP Hà Nội sẽ chuyển công văn, văn bản quy phạm pháp luật mới ban hành tới các sở, ban, ngành, quận, huyện bằng thư điện tử.

Đối với các văn bản cần có bản gốc (đóng dấu đỏ), trong vòng 1 tuần, UBND TP sẽ gửi tới các đơn vị theo đường bưu điện. Văn phòng UBND TP vừa có thông báo yêu cầu các đơn vị bố trí bộ phận trực mở hộp thư điện tử hàng ngày. Trước đó, UBND TP đã triển khai gửi giấy mới họp bằng thư điện tử và tin nhắn điện thoại di động. Trong vòng 1 tháng từ 16/4 đến 16/5, UBND TP đã gửi 200 loại giấy mời theo cách này. Việc làm này đã làm giảm đáng kể thời gian và chi phí vận chuyển cho các công văn và văn bản. Ứng dụng này nên được phát triển rộng rãi nhằm tạo sự chuyên môn hóa đối với các ứng dụng Công nghệ thông tin.

Tuy nhiên, cần phải có các phương pháp cũng như các công cụ bảo mật tin cậy để đảm bảo an toàn cho các bức thư điện tử được gửi đi. Điều này là đặc biệt quan trọng đối với các tài liệu bí mật và quan trọng. Với vấn đề này, khóa luận xin đưa ra một số phương pháp mã hóa e-mail nhằm đảm bảo an toàn cho thông tin được gửi đi trên đường truyền.

1. PGP - Pretty Good Privacy

Mật mã hóa PGP (**Pretty Good Privacy**) làm một phần mềm máy tính dùng để mật mã hóa dữ liệu và xác thực. Mục tiêu ban đầu của PGP nhằm vào mật mã hóa nội dung các thông điệp thư điện tử và các tệp đính kèm cho người dùng phổ thông, PGP hiện nay đã trở thành một giải pháp mã hóa cho các công ty lớn, chính phủ cũng như các cá nhân. Các phần mềm dựa trên PGP được dùng để mã hóa và bảo vệ thông tin lưu trữ trên máy tính xách tay, máy tính để bàn, máy chủ và trong quá trình trao đổi thông qua email, IM hoặc chuyển file. Giao thức hoạt động của hệ thống này có ảnh hưởng lớn và trở thành một trong hai tiêu chuẩn mã hóa.

Phiên bản PGP Desktop 9.x dành cho máy để bàn bao gồm các tính năng: thư điện tử, chữ ký số, bảo mật IM, mật mã hóa ổ đĩa cứng máy tính xách tay, bảo mật tệp và thư mục, tệp nén tự giải mã, xóa file an toàn. Các tính năng riêng biệt được cấp phép theo các cách khác nhau tùy theo yêu cầu… Ngoài ra còn rất nhiều phiên bản khác.

Hoạt động của PGP

PGP sử dụng kết hợp mật mã hóa khóa công khai và thuật toán khóa đối xứng cộng thêm với hệ thống xác lập mối quan hệ giữa khóa công khai và chỉ danh người dùng (ID). Phiên bản đầu tiên của hệ thống này thường được biết dưới tên mạng lưới tín nhiệm dựa trên các mối quan hệ ngang hàng (khác với hệ thống X.509 với cấu trúc cây dựa vào các nhà cung cấp chứng thực số). Các phiên bản PGP về sau dựa trên các kiến trúc tương tự như hạ tầng khóa công khai.

PGP sử dụng thuật toán mật mã hóa khóa bất đối xứng. Trong các hệ thống này, người sử dụng đầu tiên phải có một cặp khóa: khóa công khai và khóa bí mật. Người gửi sử dụng khóa công khai của người nhận để mã hóa một khóa chung (còn gọi là khóa phiên) dùng trong các thuật toán mật mã hóa khóa đối xứng. Khóa phiên này chính là khóa để mật mã hóa các thông tin được gửi qua lại trong phiên giao dịch. Rất nhiều khóa công khai của những người sử dụng PGP được lưu trữ trên các máy chủ khóa PGP trên khắp thế giới.

Người nhận trong hệ thống PGP sử dụng khóa phiên để giải mã các gói tin. Khóa phiên này cũng được gửi kèm với thông điệp nhưng được mật mã hóa bằng hệ thống mật mã bất đối xứng và có thể tự giải mã với khóa bí mật của người nhận. Hệ thống phải sử dụng cả 2 dạng thuật toán để tận dụng ưu thế của cả hai: thuật toán bất đối xứng đơn giản việc phân phối khóa còn thuật toán đối xứng có ưu thế về tốc độ (nhanh hơn cỡ 1000 lần).

2. **Flexcrypt**

Với mỗi 1 địa chỉ, ta cần phải nhập 1 mật khẩu. Mật khẩu này sẽ được dùng để giải mã thông điệp, có nghĩa là ta phải xác nhận rằng mình đã nhận được đúng email. Việc này chỉ cần làm 1 lần đầu tiên, sau đó chương trình sẽ tự động mã hoá/ có giới hạn: chỉ được phép gửi/nhận email đối với 3 người. **Flexcrypt** tương thích với Windows Vista/XP.

Secure Message giải mã trong những lần sau.

Lưu ý: Bạn cần phải dùng 1 chương trình gửi/nhận email như Thunderbird, Outlook Express, … để hoạt động với **Flexcrypt**. Chương trình không chạy với các webmail.

3. Chương trình hoàn toàn miễn phí, nhưng

Với phương pháp này, chỉ có người nhận với mật khẩu do bạn cung cấp mới có thể dùng chương trình Secure Message để giải mã e-mail đã mã hóa thành e-mail ban đầu được thôi. Còn người khác nhìn vào chỉ thêm hoa mắt bởi trong e-mail là một "rừng" các chữ cái xếp lộn xộn nhau. Chương trình tương thích với Windows, được cung cấp miễn phí tại địa chỉ: http://www.blaizgraphics.net/SMESSAGE.ZIP.

Trong chương trình Secure Message có năm mức độ mã hóa cho người sử dụng lựa chọn, đó là: Nominal, Low, Medium, High và Extreme, được xếp theo thứ tự từ thấp đến cao. Phiên bản miễn phí của chương trình chỉ cho phép bạn mã hóa văn bản ở mức Nominal, dù là mức thấp nhất nhưng cũng đủ để bạn có thể yên tâm về tính bảo mật. Nếu bạn muốn sử dụng các mức độ mã hóa cao hơn thì phải trả phí cho nhà sản xuất chương trình Secure Message.

…

KẾT LUẬN

Việc ứng dụng các Giao dịch điện tử trong các giao dịch hành chính công ở các cơ quan nhà nước góp phần đẩy nhanh quá trình cải cách thủ tục hành chính. Tuy nhiên hiện nay đó vẫn còn hạn chế và đạt hiệu quả chưa cao. Tuy nhiên, 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. Chúng ta có thể hi vọng rằng trong tương lai không xa, chúng ta có thể áp dụng thành công giao dịch điện tử trong các cơ quan hành chính, góp phần xây dựng hệ thống hành chính trong sạch, minh bạch, và hiệu quả. Để đạt được điều này, chúng ta phải chú trọng xây dựng hệ thống hạ tầng đảm bảo ATTT trong giao dịch.

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

- Tìm hiểu và nghiên cứu về chứng chỉ số, mật mã hóa khóa công khai và hạ tầng khóa công khai.
- Các loại giao dịch trong các cơ quan nhà nước và các yếu tố đảm bảo an toàn trong giao dịch.
- Tìm hiểu và đưa ra các ứng dụng điển hình tại một số địa phương đi đầu trong việc ứng dụng Công nghệ thông tin trong giao dịch hành chính công.

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

Tài liệu tham khảo

1. Phan Đình Diệu, *Lý thuyết mật mã và an toàn thông tin*, NXB Đại Học Quốc gia Hà Nội, 2002

2. CHARLES P. PFLEEGER, *An toàn tính toán*, Học viện mật mã

3. http://www.blaizgraphics.net/SMESSAGE.ZIP.

4. www.haiphongcity.gov.vn