ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN ĐOẠT

CHỮ KÝ SỐ TRONG QUẢN LÝ, ĐIỀU HÀNH VĂN BẢN NỘI BỘ CƠ QUAN TỈNH YÊN BÁI

THÁI NGUYÊN 2015

LỜI CẢM ƠN

Trong thời gian hai năm của chương trình đào tạo thạc sỹ, trong đó gần một nửa thời gian dành cho các môn học, thời gian còn lại dành cho việc lựa chọn đề tài, giáo viên hướng dẫn, tập trung vào nghiên cứu, viết, chỉnh sửa và hoàn thiện đề tài. Với quỹ thời gian như vậy và với vị trí công việc đang phải đảm nhận, không riêng bản thân em mà hầu hết các sinh viên cao học muốn hoàn thành tốt luận văn của mình trước hết đều phải có sự sắp xếp thời gian hợp lý, có sự tập trung học tập và nghiên cứu với tinh thần nghiêm túc, nỗ lực hết mình; tiếp đến cần có sự ủng hộ về tinh thần, sự giúp đỡ về chuyên môn một trong những điều kiện không thể thiếu quyết định đến việc thành công của đề tài.

Để hoàn thành được đề tài này trước tiên em xin gửi lời cảm ơn đến thầy giáo hướng dẫn **TS. Nguyễn Văn Tảo**, người đã có những định hướng cho em về nội dung và hướng phát triển của đề tài, người đã có những đóng góp quý báu cho em về những vấn đề chuyên môn của đề tài, giúp em tháo gỡ kịp thời những vướng mắc trong quá trình làm luận văn.

Em cũng xin cám ơn các thầy cô giáo Trường Đại học Công nghệ thông tin và Truyền thông Thái Nguyên cũng như bạn bè cùng lớp đã có những ý kiến đóng góp bổ sung cho đề tài luận văn của em. Xin cảm ơn gia đình, người thân cũng như đồng nghiệp luôn quan tâm, ủng hộ hỗ trợ về mặt tinh thần trong suốt thời gian từ khi nhận đề tài đến khi hoàn thiện đề tài này.

Em xin hứa sẽ cố gắng hơn nữa, tự trau dồi bản thân, tích cực nâng cao năng lực chuyên môn của mình để sau khi hoàn thành đề tài này sẽ có hướng tập trung nghiên cứu sâu hơn, không ngừng hoàn thiện hơn nữa đề tài của mình để có những ứng dụng thực tiễn cao trong thực tế.

Thái Nguyên, tháng 4 năm 2015

Sinh viên

Nguyễn Đoạt

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

Các ký hiệu

gcd(a,b)	Ước số chung lớn nhất của a và b
H(.)	Hàm băm
||	Toán tử nối/trộn 2 xâu
a|b	a là ước số của b
ID_i	Thông tin nhận dạng thực thể cuối U_i

M	Thông điệp dữ liệu
x_i	Khóa bí mật của thực thể ký U_i
y_i	Khóa công khai của thực thể ký U_i

Các chữ viết tắt

CA	Certificate Authority
CRL	Certificate Revocation List
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EE	End Entity
LDAP	Lightweight Directory Access Protocol
ITU	Internet Telecommumications Union
ISO	International Organization for Standardization
PKC	Public Key Certificate
PKC[1]	Public Key Cryptography
PKI	Public Key Infrastructure
RA	Registration Authority
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
CNTT	Công nghệ thông tin

DANH MỤC CÁC HÌNH VẼ

MỞ ĐẦU

1. Tính cấp thiết của đề tài:

Thực hiện ứng dụng công nghệ thông tin vào hoạt động, từ năm 2009, các cơ quan Nhà nước tỉnh Yên Bái đã xây dựng và phát triển phần mềm Quản lý điều hành nhằm thực hiện việc quản lý, điều hành văn bản nội bộ trong cơ quan.

Qua từng năm, phần mềm này đã được nâng cấp giúp cho các cơ quan điều hành công việc và giao dịch văn bản trong nội bộ các đơn vị có hiệu quả thiết thực, giúp cải cách hành chính và tạo phong cách làm việc hiện đại cho cán bộ, công chức. Phần mềm chạy trên nền web, các cán bộ công chức, viên chức của các cơ quan, đơn vị được cấp tài khoản truy nhập để sử dụng. Phần mềm có 2 chức năng cơ bản đó là: Chức năng quản lý văn bản đến và chức năng quản lý văn bản đi.

Chức năng quản lý văn bản đi là việc cán bộ soạn thảo một văn bản, sau đó trình lãnh đạo phòng, lãnh đạo phòng sửa, cho ý kiến và trình lên lãnh đạo cơ quan, lãnh đạo cơ quan xem, sửa, cho ý kiến và chuyển văn thư phát hành văn bản.

Chức năng quản lý văn bản đến là: hàng ngày các công văn, tài liệu gửi đến cơ quan sẽ được văn thư scan và trình lãnh đạo đơn vị, lãnh đạo đơn vị sẽ xử lý văn bản bằng việc cho ý kiến và giao cho các phòng, bộ phận trực thuộc xử lý, lãnh đạo các phòng, bộ phận trực thuộc sẽ tiếp tục cho ý kiến và giao cho cán bộ thuộc phòng, bộ phận mình xử lý.

Ban đầu, mỗi cơ quan có một phần mềm riêng, chỉ tiếp nhận và chuyển văn bản trong nội bộ cơ quan mình. Sau một thời gian hầu hết các cơ quan tại Yên Bái đã sử dụng phần mềm này, lúc này nảy sinh nhu cầu liên thông văn bản từ cơ quan này sang cơ quan khác, liên thông văn bản vừa nhanh lại vừa không phải scan, văn bản đi của cơ quan này là văn bản đến của cơ quan kia và ngược lại. Vì vậy, Yên Bái đã nâng cấp phần mềm và liên thông văn bản giữa các cơ quan lại với nhau.

Tuy nhiên, trong quá trình liên thông văn bản lại phát sinh nhưng khó khăn đó là: các văn bản giao dịch, trao đổi trên phần mềm chưa có tính pháp lý

và tính bảo mật chưa cao, mặc dù đã dùng biện pháp các văn bản đi văn thư lấy chữ ký, con dấu và scan gắn vào phần mềm và gửi đi nhưng độ tin tưởng không cao. Chính vì vậy, đòi hỏi văn bản phải được ký số và lưu chuyển trên phần mềm đáp ứng yêu cầu xác định tính đúng đắn và toàn vẹn của văn bản khi nhận.

Xuất phát từ lý do đó, đề tài đặt vấn đề nghiên cứu về Chữ ký số và ứng dụng chữ ký số trên phần mềm quản lý điều hành văn bản nội bộ của các cơ quan tỉnh Yên Bái để xác thực nguồn gốc, tính toàn vẹn của dữ liệu nhận được trên phần mềm quản lý, điều hành của các cơ quan tỉnh Yên Bái.

Với ý tưởng trên, em cũng đã nghiên cứu mô hình ký số của các tỉnh Quảng Ninh, Thái Bình, Quảng Ngãi và của Hệ thống quản lý Thuế, cụ thể như sau:

* Mô hình ký số của tỉnh Quảng Ninh:

UBND tỉnh đề nghị Ban cơ yếu Chính phủ cấp chữ ký số cho các cán bộ lãnh đạo và các cơ quan nhà nước mỗi cá nhân, tổ chức. Các cán bộ và tổ chức này sẽ ký văn bản tại máy clien sau đó mở thư điện tử mail.quangninh.gov.vn gắn kèm văn bản đã ký và gửi cho người nhận.

Ưu điểm: Văn bản ký này có thể gửi cho bất kỳ ai, trên bất kỳ phương thức nào đều được, giúp cho người nhận biết văn bản đó chính là của cá nhân, tổ chức đã ký số.

Nhược điểm: Người dùng mất nhiều thao tác, phải ký trên máy trạm rồi gắn kèm văn bản đó vào hệ thống thư mới thực hiện gửi nhận được, dẫn đến người dùng ngại sử dụng và trên thực tế ít người sử dụng.

* Mô hình ký số của tỉnh Thái Bình:

UBND tỉnh Thái Bình cũng đề nghị Ban cơ yếu chính phủ cấp chữ ký số cho các cán bộ lãnh đạo và các cơ quan nhà nước trên địa bàn tỉnh. Các cán bộ, công chức và các tổ chức sẽ ký số văn bản tại máy clien sau đó gắn vào phần mềm quản lý văn bản của tỉnh để gửi văn bản đi. Sau một thời gian triển khai, các cá nhân hầu như không sử dụng vì việc ký số riêng không được thực hiện trực tiếp trên phần mềm nên ngại sử dụng mà chỉ chữ ký số của các tổ chức là thường xuyên được sử dụng.

Ưu điểm: Việc Thái Bình sử dụng ký số rồi gửi nhận trên phần mềm quản lý văn bản của tỉnh mang lại hiệu quả khá cao, giúp giảm chi phí và tiết kiệm thời gian.

Nhược điểm: Vẫn chưa xây dựng được modul ký số trên phần mềm vì vậy vẫn phải sử dụng nhiều thao tác tạo cho người dùng ngại sử dụng.

* Mô hình ký số của tỉnh Quảng Ngãi:

Tỉnh đã cấp hơn 1000 chữ ký số cho cán bộ, công chức và các cơ quan nhà nước, các cán bộ, công chức và cơ quan nhà nước chưa sử dụng phổ biến phần mềm quản lý văn bản và thư điện tử nên việc cấp chữ ký số trở thành hình thức không mang lại hiệu quả thiết thực.

* Sử dụng chữ ký số trong kê khai thuế và nộp thuế:

Thông tư 180/2010/TT-BTC của Bộ Tài Chính công nhận tính pháp lý của hình thức giao dịch điện tử sử dụng chữ ký số giữa người nộp thuế và cơ quan Thuế.

Theo hình thức này, các tổ chức, cá nhân đăng ký với các doanh nghiệp được Bộ Thông tin và Truyền thông cho phép cung cấp chữ ký số như Vietel, VNPT, FPT, BKV…để được cấp chữ ký số và thực hiện việc nộp tờ khai, kê khai trực tuyến với các cơ quan thuế qua mạng.

Việc kê khai và ký số được thực hiện trên phần mềm kê khai thuế điện tử của ngành thuế, người kê khai chỉ cần thực hiện công việc kê khai và nhấn nút ký điện tử trên phần mềm tờ khai sẽ được ký và chuyển đến cơ quan thuế.

Việc ký trên phần mềm giúp người sử dụng dễ dàng hơn, tiết kiệm thời gian và kinh phí đi lại, giao dịch, tránh được tiêu cực phát sinh.

Qua nghiên cứu mô hình triển khai của các tỉnh Quảng Ninh, Thái Bình, Quảng Ngãi và của ngành Thuế, em đưa ra mô hình ký số của Yên Bái là:

Đề nghị với Ban Cơ yếu chính phủ cấp chữ ký số cho các cơ quan nhà nước trên địa bàn tỉnh để ký trực tiếp trên phần mềm quản lý văn bản tại tài khoản của văn thư các cơ quan, đơn vị trước khi phát hành công văn đi, văn bản trước khi ký sẽ được conver từ file word sang pdf để tránh việc sửa chữa văn bản đã ký trên phần mềm.