MỤC LỤC

LỜI CẢM ƠN

Em xin chân thành cảm ơn Thầy giáo, Tiến sĩ Phùng Văn Ổn - Trung tâm công nghệ thông tin Bộ Giao thông vận tải, người đã trực tiếp hướng dẫn tận tình chỉ bảo em trong suốt quá trình làm tốt nghiệp.

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

Em cũng xin chân thành cảm ơn tất cả các cô chú, các anh chị tại Trung tâm công nghệ thông tin Bộ Giao thông vận tải, đã giúp đỡ và tạo mọi điều kiện tốt cho em trong thời gian làm việc tại Trung tâm.

Tuy có nhiều cố gắng trong quá trình học tập cũng như trong thời gian làm việc này nhưng không thể tránh khỏi những thiếu sót, em rất mong được sự góp ý quý báu của tất cả các thầy cô giáo cũng như tất cả các bạn để kết quả của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

Hải Phòng, ngày 01 tháng 07 năm 2009

Sinh viên

Bùi Thị Kim Duyên

PHẦN I. GIỚI THIỆU

Tên đề tài:

Tìm hiểu các giải pháp xác thực, bảo mật văn bản trong giao dịch điện tử và đề xuất giải pháp để xác thực, bảo mật tài liệu trong giao dịch qua thư điện tử cho Bộ Giao thông vận tải .

Giáo viên hướng dẫn: **TS. Phùng Văn Ổn**.

Sinh viên: Bùi Thị Kim Duyên – Mã SV: 090014 - Lớp CT901 – Khóa 9

1. Mục đích của đề tài:

Tìm hiểu các giải pháp xác thực, bảo mật văn bản trong giao dịch điện tử, từ đó đề xuất giải pháp để xác thực, bảo mật tài liệu trong giao dịch qua thư điện tử cho Bộ Giao thông vận tải.

2. Giới thiệu về Bộ Giao thông vận tải

Bộ Giao thông vận tải đặt tại số 80 Trần Hưng Đạo, Quận Hoàn Kiếm, Hà Nội, ngày 22 tháng 4 năm 2008 Chính phủ đã ban hành Nghị định số 51/2008/NĐ-CP (thay thế Nghị định số 34/2004/NĐ-CP) quy định chức năng, nhiệm vụ, quyền hạn của Bộ Giao thông vận tải.

2.1 Chức năng

Bộ Giao thông vận tải là cơ quan của Chính phủ, thực hiện chức năng quản lý Nhà nước về giao thông vận tải đường bộ, đường sắt, đường sông, hàng hải và hàng không trong phạm vi cả nước; quản lý nhà nước các dịch vụ công và thực hiện đại diện chủ sở hữu phần vốn của nhà nước tại doanh nghiệp có vốn nhà nước thuộc Bộ quản lý theo quy định của pháp luật.

2.2 Nhiệm vụ và quyền hạn

Bộ Giao thông vận tải có trách nhiệm thực hiện nhiệm vụ, quyền hạn quy định tại Nghị định số 178/2007/NĐ-CP ngày 03 tháng 12 năm 2007 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ, cơ quan ngang Bộ và những nhiệm vụ, quyền hạn cụ thể sau đây :

1. Trình Chính phủ dự án luật, dự thảo nghị quyết của Quốc hội, dự án pháp lệnh, dự thảo nghị quyết của Ủy ban Thường vụ Quốc hội; dự thảo nghị quyết, nghị định của Chính phủ theo chương trình, kế hoạch xây dựng pháp luật hàng năm của Bộ đã được phê duyệt và các dự án, đề án theo phân công của Chính phủ, Thủ tướng Chính phủ.

2. Trình Thủ tướng Chính phủ chiến lược, quy hoạch phát triển, kế hoạch dài hạn, năm năm và hàng năm; các chương trình, dự án quốc gia thuộc các lĩnh vực quản lý nhà nước của Bộ; các dự thảo quyết định, chỉ thị của Thủ tướng Chính phủ.

3. Ban hành các quyết định, chỉ thị, thông tư thuộc phạm vi quản lý nhà nước của Bộ; xây dựng để trình cấp có thẩm quyền ban hành hoặc ban hành theo thẩm quyền các tiêu chuẩn, quy chuẩn kỹ thuật quốc gia trong các lĩnh vực quản lý nhà nước của Bộ.

4. Chỉ đạo, hướng dẫn, thanh tra, kiểm tra và chịu trách nhiệm tổ chức thực hiện các văn bản quy phạm pháp luật, chiến lược, quy hoạch, kế hoạch đã được phê duyệt thuộc phạm vi quản lý nhà nước của Bộ; tuyên truyền, phổ biến, giáo dục pháp luật và thông tin về các lĩnh vực quản lý nhà nước của Bộ.

5. Về kết cấu hạ tầng giao thông đường bộ, đường sắt, đường thủy nội địa, hàng hải và hàng không:

a) Chỉ đạo việc tổ chức thực hiện quy hoạch, kế hoạch phát triển hệ thống kết cấu hạ tầng giao thông đã được Thủ tướng Chính phủ phê duyệt;

b) Ban hành quy chuẩn xây dựng và quy định việc quản lý kết cấu hạ tầng giao thông theo thẩm quyền; quy định việc bảo trì, quản lý sử dụng, khai thác kết cấu hạ tầng giao thông (trừ kết cấu hạ tầng giao thông đô thị) trong phạm vi cả nước; chỉ đạo, kiểm tra việc tổ chức bảo trì, bảo đảm tiêu chuẩn, quy chuẩn kỹ thuật mạng lưới công trình giao thông đang khai thác do Bộ chịu trách nhiệm quản lý;

c) Tổ chức thực hiện nhiệm vụ, quyền hạn của cơ quan quyết định đầu tư, chủ đầu tư đối với các dự án đầu tư xây dựng kết cấu hạ tầng giao thông; công bố danh mục dự án gọi vốn đầu tư và hình thức đầu tư kết cấu hạ tầng giao thông theo quy định của pháp luật;

d) Trình Chính phủ quy định phạm vi hành lang bảo vệ luồng đường thủy nội địa, hành lang an toàn giao thông đường bộ, hành lang an toàn giao thông đường sắt theo quy định của pháp luật; chỉ đạo, kiểm tra Ủy ban nhân dân các cấp trong việc thực hiện các biện pháp bảo vệ hành lang an toàn giao thông;

đ) Công bố và chỉ đạo tổ chức thực hiện việc đóng, mở cảng hàng không, sân bay và thiết lập đường hàng không sau khi được Thủ tướng Chính phủ cho phép; quyết định việc đóng tạm thời và mở lại cảng hàng không, sân bay; công bố đóng, mở cảng biển, vùng nước cảng biển, luồng hàng hải, cảng, bến thủy nội địa có phương tiện thủy nước ngoài ra vào, tuyến đường thủy nội địa, ga đường sắt, tuyến đường sắt theo quy định của pháp luật;

e) Tổ chức thực hiện việc đăng ký và cấp Giấy chứng nhận đăng ký cảng hàng không, sân bay theo quy định của pháp luật;

g) Trình Chính phủ quy định việc phân loại, đặt tên hoặc số hiệu đường và tiêu chuẩn kỹ thuật của các cấp đường bộ; quyết định phân loại, điều chỉnh hệ thống quốc lộ; hướng dẫn cụ thể việc đặt tên, số hiệu đường bộ.

6. Về phương tiện giao thông, phương tiện, thiết bị xếp dỡ, thi công chuyên dùng trong giao thông vận tải (trừ phương tiện phục vụ vào mục đích quốc phòng, an ninh và tàu cá) và trang bị, thiết bị kỹ thuật chuyên ngành giao thông vận tải:

a) Tổ chức thực hiện việc đăng ký tàu biển, tàu bay theo quy định của Chính phủ; quy định việc đăng ký, cấp biển số phương tiện giao thông đường sắt, đường thủy nội địa và xe máy chuyên dùng tham gia giao thông;

b) Quy định chất lượng an toàn kỹ thuật, bảo vệ môi trường đối với phương tiện giao thông cơ giới;

c) Quy định và hướng dẫn thực hiện tiêu chuẩn, quy chuẩn kỹ thuật, việc kiểm tra chất lượng an toàn kỹ thuật của phương tiện giao thông cơ giới đường bộ, phương tiện giao thông đường sắt, đường thủy nội địa, hàng không, hàng hải, các phương tiện, thiết bị xếp dỡ, thi công chuyên dùng, các công trình, phương tiện, thiết bị chuyên dùng sử dụng trong giao thông vận tải và các mục đích khác theo quy định của pháp luật;

d) Tổ chức cấp Giấy chứng nhận đủ điều kiện bay của tàu bay; cấp Giấy chứng nhận đủ điều kiện bay xuất khẩu đối với tàu bay, động cơ tàu bay, cánh quạt tàu bay khi xuất khẩu; cấp hoặc công nhận Giấy chứng nhận loại đối với tàu bay, động cơ tàu bay, cánh quạt tàu bay khi sản xuất tại Việt Nam hoặc nhập khẩu;

đ) Quy định việc thẩm định thiết kế kỹ thuật trong sản xuất, lắp ráp, sửa chữa, hoán cải phương tiện giao thông, phương tiện, thiết bị xếp dỡ, thi công chuyên dùng và trang bị, thiết bị kỹ thuật chuyên ngành giao thông vận tải;

e) Quy định tiêu chuẩn, quy chuẩn kỹ thuật, điều kiện hoạt động của cơ sở thiết kế, sản xuất, bảo dưỡng hoặc thử nghiệm tàu bay, động cơ tàu bay, cánh quạt tàu bay và trang thiết bị tàu bay tại Việt Nam; cơ sở cung cấp dịch vụ bảo đảm hoạt động bay và cơ sở kiểm định chất lượng an toàn kỹ thuật, bảo vệ môi trường đối với phương tiện giao thông cơ giới đường bộ, đường sắt, đường thủy nội địa, hàng hải, hàng không và các phương tiện, thiết bị, công trình khác theo quy định của pháp luật.

7. Quy định việc đào tạo, huấn luyện, sát hạch, cấp, công nhận, thu hồi giấy phép, bằng, chứng chỉ chuyên môn cho người điều khiển phương tiện giao thông, người vận hành phương tiện, thiết bị chuyên dùng trong giao thông vận tải (trừ người điều khiển phương tiện, thiết bị chuyên dùng phục vụ vào mục đích quốc phòng, an ninh và tàu cá) và cho đối tượng làm việc đặc thù trong lĩnh vực giao thông vận tải.

8. Về vận tải đường bộ, đường sắt, đường thủy nội địa, hàng hải, hàng không dân dụng và vận tải đa phương thức:

a) Hướng dẫn, kiểm tra việc thực hiện điều kiện kinh doanh vận tải, cơ chế, chính sách phát triển vận tải, các dịch vụ hỗ trợ vận tải theo quy định của Chính phủ;

b) Quy định tiêu chuẩn, quy chuẩn kỹ thuật, công nghệ vận hành, khai thác vận tải;

c) Công bố đường bay dân dụng sau khi được Thủ tướng Chính phủ cho phép; công bố các tuyến vận tải đường bộ, đường sắt, đường thủy nội địa và mạng vận tải công cộng theo quy định của pháp luật;

d) Hướng dẫn thực hiện vận tải đa phương thức theo quy định của Chính phủ;

đ) Tổ chức cấp phép hoạt động bay dân dụng; chỉ đạo, kiểm tra việc thực hiện quy chế phối hợp quản lý hoạt động bay dân dụng;

e) Quy định chi tiết việc quản lý hoạt động tại cảng hàng không, sân bay, cảng biển, cảng, bến thủy nội địa, ga đường sắt và tuyến luồng giao thông đường sắt, đường thủy nội địa, hàng hải.

9. Về an toàn giao thông:

a) Chủ trì, phối hợp tổ chức thực hiện các đề án tổng thể về bảo đảm an toàn giao thông trên phạm vi cả nước sau khi được Thủ tướng Chính phủ phê duyệt; hướng dẫn, kiểm tra việc thực hiện các biện pháp bảo đảm an toàn giao thông

đường bộ, đường sắt, đường thủy nội địa, hàng hải, hàng không dân dụng thuộc phạm vi chức năng, nhiệm vụ của Bộ;

b) Phê duyệt chương trình an ninh hàng không dân dụng, phương án điều hành tàu bay bị can thiệp bất hợp pháp, chấp thuận chương trình an ninh hàng không dân dụng của các hãng hàng không nước ngoài; chủ trì thực hiện kiểm tra và cung cấp thông tin an ninh, an toàn hàng không, hàng hải theo quy định của pháp luật;

c) Hướng dẫn các thủ tục điều tra sự cố tai nạn tàu bay theo quy định của Chính phủ; tổ chức thực hiện việc điều tra, xử lý tai nạn hàng hải, hàng không dân dụng theo quy định của pháp luật;

d) Tổ chức thực hiện tìm kiếm - cứu nạn trong giao thông đường bộ, đường sắt, đường thủy nội địa, hàng hải và hàng không.

10. Về bảo vệ môi trường trong hoạt động giao thông vận tải:

a) Tổ chức thẩm định và phê duyệt báo cáo đánh giá môi trường chiến lược và báo cáo đánh giá tác động môi trường đối với các dự án đầu tư xây dựng kết cấu hạ tầng giao thông và cơ sở sản xuất công nghiệp thuộc thẩm quyền của Bộ theo quy định của pháp luật;

b) Phối hợp với Bộ Tài nguyên và Môi trường, các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ có liên quan và Ủy ban nhân dân cấp tỉnh để chỉ đạo, hướng dẫn, kiểm tra việc thực hiện pháp luật về bảo vệ môi trường và các quy định khác của pháp luật có liên quan đối với xây dựng kết cấu hạ tầng giao thông và hoạt động giao thông vận tải; theo dõi, kiểm tra việc thực hiện các quy định của pháp luật về bảo vệ môi trường trong các lĩnh vực quản lý nhà nước của Bộ;

c) Quy định việc cấp Giấy chứng nhận đạt tiêu chuẩn môi trường đối với phương tiện giao thông cơ giới đường bộ, phương tiện giao thông đường sắt, đường thủy nội địa, hàng hải và hàng không (trừ phương tiện giao thông của quân đội, công an sử dụng vào mục đích quốc phòng, an ninh); chủ trì hướng dẫn kiểm tra, xác nhận tiêu chuẩn môi trường đối với xe ô tô và xe cơ giới khác.

11. Thực hiện hợp tác quốc tế, các Điều ước quốc tế mà Việt Nam đã ký kết hoặc tham gia trong lĩnh vực giao thông vận tải đường bộ, đường sắt, đường thủy nội địa, hàng hải và hàng không.

12. Chỉ đạo tổ chức thực hiện kế hoạch nghiên cứu khoa học, phát triển và chuyển giao công nghệ trong lĩnh vực giao thông vận tải đường bộ, đường sắt,

đường thủy nội địa, hàng hải và hàng không; chỉ đạo việc xây dựng, triển khai các chương trình, dự án ứng dụng công nghệ thông tin, xây dựng cơ sở dữ liệu, bảo đảm dịch vụ thông tin phục vụ quản lý nhà nước và đáp ứng nhu cầu của tổ chức, cá nhân tham gia hoạt động giao thông vận tải.

13. Về dịch vụ công:

a) Tổ chức thực hiện quy hoạch mạng lưới tổ chức sự nghiệp dịch vụ công trong các ngành, lĩnh vực thuộc phạm vi quản lý nhà nước của Bộ sau khi được cấp có thẩm quyền phê duyệt;

b) Ban hành tiêu chuẩn, quy chuẩn kỹ thuật đối với các hoạt động cung ứng dịch vụ công thuộc ngành giao thông vận tải;

c) Hướng dẫn, hỗ trợ cho các tổ chức thực hiện dịch vụ công theo quy định của pháp luật.

14. Về thực hiện đại diện chủ sở hữu phần vốn của Nhà nước tại doanh nghiệp có vốn nhà nước:

a) Xây dựng đề án sắp xếp, tổ chức lại, chuyển đổi sở hữu doanh nghiệp nhà nước để trình Thủ tướng Chính phủ phê duyệt và chỉ đạo tổ chức thực hiện đề án sau khi được phê duyệt;

b) Trình Thủ tướng Chính phủ bổ nhiệm, bổ nhiệm lại, miễn nhiệm hoặc bổ nhiệm, bổ nhiệm lại, miễn nhiệm theo thẩm quyền các chức danh cán bộ lãnh đạo quản lý, kế toán trưởng của doanh nghiệp nhà nước chưa cổ phần hoá;

c) Trình Thủ tướng Chính phủ phê duyệt hoặc phê duyệt theo thẩm quyền điều lệ tổ chức và hoạt động của doanh nghiệp nhà nước chưa cổ phần hoá.

15. Hướng dẫn, tạo điều kiện cho hội, tổ chức phi Chính phủ tham gia vào hoạt động trong lĩnh vực giao thông vận tải; kiểm tra việc thực hiện các quy định của nhà nước về giao thông vận tải đối với hội, tổ chức phi chính phủ; xử lý hoặc kiến nghị cơ quan nhà nước có thẩm quyền xử lý các vi phạm pháp luật của hội, tổ chức phi Chính phủ theo quy định của pháp luật.

16. Thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo, phòng, chống tham nhũng, tiêu cực và xử lý các vi phạm pháp luật về giao thông vận tải đường bộ, đường sắt, đường thủy nội địa, hàng hải và hàng không thuộc thẩm quyền của Bộ.

17. Quyết định và chỉ đạo thực hiện chương trình cải cách hành chính của Bộ theo mục tiêu và nội dung chương trình cải cách hành chính nhà nước đã được

Thủ tướng Chính phủ phê duyệt; đề xuất hoặc quyết định theo thẩm quyền việc thực hiện phân cấp quản lý nhà nước về ngành, lĩnh vực.

18. Quản lý về tổ chức bộ máy, biên chế; chỉ đạo thực hiện chế độ tiền lương và các chế độ chính sách đối với cán bộ, công chức, viên chức nhà nước và người lao động thuộc phạm vi quản lý của Bộ; đào tạo, bồi dưỡng, xây dựng đội ngũ cán bộ, công chức, viên chức nhà nước thuộc thẩm quyền; quy định chức danh, tiêu chuẩn cấp bậc kỹ thuật, nghiệp vụ trong các ngành thuộc phạm vi quản lý của Bộ.

19. Quản lý tài chính, tài sản được giao và tổ chức thực hiện quản lý ngân sách được phân bổ theo quy định của pháp luật.

20. Thực hiện các nhiệm vụ khác theo quy định của pháp luật và phân công của Chính phủ, Thủ tướng Chính phủ.

Cơ cấu tổ chức:

1. Vụ Kế hoạch - Đầu tư;

2. Vụ Tài chính;

3. Vụ Kết cấu hạ tầng giao thông;

4. Vụ An toàn giao thông;

5. Vụ Pháp chế;

6. Vụ Vận tải;

7. Vụ Khoa học - Công nghệ;

8. Vụ Môi trường;

9. Vụ Hợp tác quốc tế;

10. Vụ Tổ chức cán bộ;

11. Thanh tra;

12. Văn phòng;

13. Tổng cục Đường bộ Việt Nam;

14. Cục Đường sắt Việt Nam;

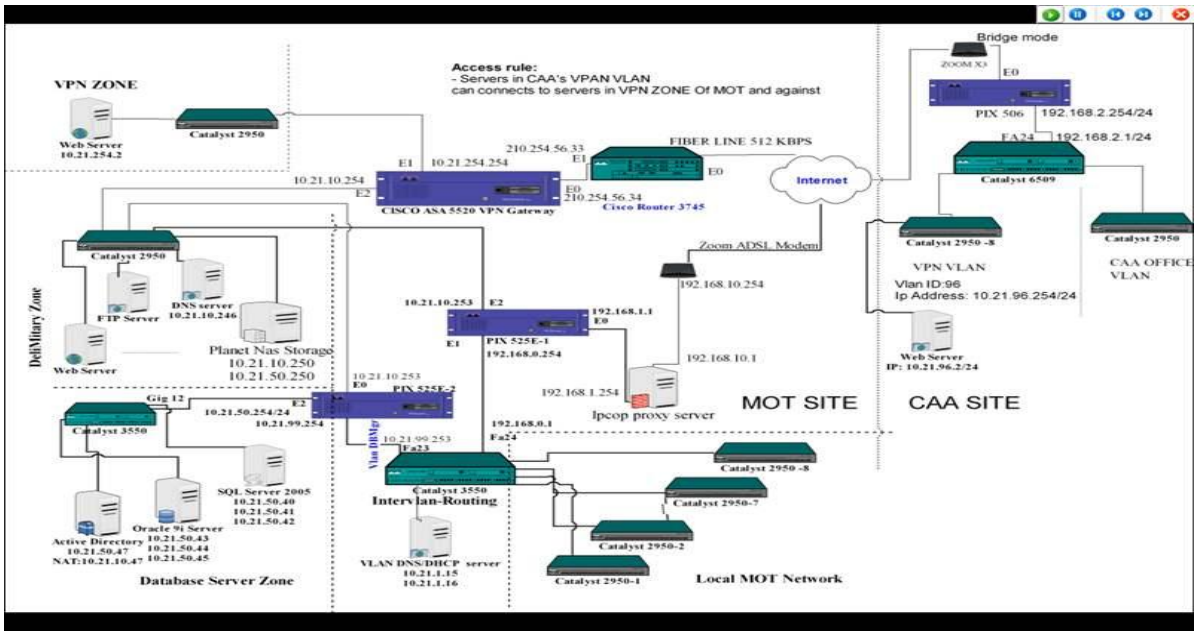
15. Cục Đường thủy nội địa Việt Nam;

16. Cục Hàng hải Việt Nam;

17. Cục Hàng không Việt Nam;

18. Cục Đăng kiểm Việt Nam;
19. Cục Quản lý xây dựng và Chất lượng công trình giao thông;
20. Cục Y tế giao thông vận tải;
21. Viện Chiến lược và Phát triển giao thông vận tải;
22. Trường Cán bộ quản lý giao thông vận tải;
23. Trung tâm Công nghệ thông tin;
24. Báo Giao thông vận tải;
25. Tạp chí Giao thông vận tải

2.3 . Giới thiệu về hệ thống mạng VPN của Bộ



Sơ đồ hệ thống mạng của Bộ GTVT

PHẦN II. TÌM HIỂU CÁC GIẢI PHÁP

A. TỔNG QUAN VỀ ỨNG DỤNG CHỮ KÝ SỐ VÀ CHỨNG THỰC SỐ

1. Chữ ký số, chứng chỉ số và cung cấp chứng thực số

- Chữ ký số

Chữ ký điện tử là thuật ngữ chỉ tất cả các phương pháp khác nhau để một người có thể "ký tên" vào một dữ liệu điện tử, thể hiện sự chấp thuận và xác nhận tính nguyên bản của nội dung dữ liệu đó.

Chữ ký điện tử rất đa dạng, có thể là một cái tên đặt cuối dữ liệu điện tử, một ảnh chụp chữ ký viết tay gắn với dữ liệu điện tử, một mã số bí mật có khả năng xác định người gửi dữ liệu điện tử, một biện pháp sinh học có khả năng xác định nhân thân người gửi dữ liệu điện tử,...

Chữ ký số (Digital Signature) là một dạng chữ ký điện tử, an toàn nhất và cũng được sử dụng rộng rãi nhất trong các giao dịch điện tử hiện nay trên thế giới. Chữ ký số hình thành dựa trên nền tảng hạ tầng khoá công khai (Public Key Infrastruture - PKI), kỹ thuật này bao gồm một cặp khoá: khoá bí mật và khoá công khai. Trong đó, khoá bí mật được người gửi sử dụng để ký (hay mã hoá) một dữ liệu điện tử, còn khoá công khai được người nhận sử dụng để mở dữ liệu điện tử đó (giải mã) và xác thực danh tính người gửi.

- Chứng chỉ số

Chứng chỉ số (Digital Certificate) là một tệp tin điện tử dùng để xác minh danh tính một cá nhân, một tổ chức, một máy chủ... trên Internet. Nó giống như bằng lái xe, hộ chiếu, chứng minh thư hay những giấy tờ xác minh cá nhân.

- Nhà cung cấp chứng thực số

Cũng giống như việc cơ quan công an làm nhiệm vụ cấp giấy chứng minh nhân dân, để có một Chứng chỉ số thì phải có một tổ chức làm nhiệm vụ cấp phát Chứng chỉ số, tổ chức này được gọi là nhà cung cấp chứng thực số (Certificate Authority-CA).

Nhiệm vụ của CA là chứng thực danh tính của những người tham gia vào việc gửi và nhận thông tin qua mạng; cung cấp cho họ những công cụ, những dịch vụ cần thiết để thực hiện việc bảo mật thông tin, chứng thực nguồn gốc và nội dung thông tin, đồng thời CA phải đảm bảo về độ tin cậy, chịu trách nhiệm về độ chính xác của Chứng chỉ số mà mình cấp.

Các hoạt động của CA được dựa trên nền tảng là hạ tầng khoá công khai PKI, hay nói cách khác PKI thường được dùng để chỉ toàn bộ hệ thống bao gồm nhà cung cấp chứng thực số (CA) cùng các cơ chế liên quan đồng thời với toàn bộ việc sử dụng các thuật toán mã khoá công khai trong trao đổi thông tin.

2. Tính cấp thiết

Ngày nay, việc giao tiếp qua mạng Internet đang trở thành một nhu cầu cấp thiết. Thông tin trong các giao dịch điện tử thường là những thông tin quan trọng, có tính chất cơ mật (như là thông điệp giữa các cơ quan chính phủ, hợp đồng kinh tế giữa các doanh nghiệp), nội bộ (ví dụ thông tin giữa các cơ quan trong một tổ chức và các chi nhánh của công ty), hoặc là riêng tư (ví dụ lương, hồ sơ bệnh án). Vì vậy, cần phải có các phương pháp bảo đảm sự chính xác và toàn vẹn của thông tin, và sự tin cậy của những người tham gia vào các giao dịch điện tử. Tuy nhiên, với các thủ đoạn tinh vi, nguy cơ bị ăn cắp thông tin qua mạng cũng ngày càng gia tăng. Hiện giao tiếp qua Internet chủ yếu sử dụng giao thức TCP/IP. Đây là giao thức cho phép các thông tin được gửi từ máy tính này tới máy tính khác thông qua một loạt các máy trung gian hoặc các mạng riêng biệt. Chính điều này dẫn đến nguy cơ mất an toàn thông tin trong giao dịch như bị nghe trộm, bị mạo danh, bị giả mạo, bị chối cãi nguồn gốc.

Do vậy, để bảo mật, các thông tin truyền trên Internet ngày nay đều có xu hướng được mã hoá. Trước khi truyền qua mạng Internet, người gửi mã hoá thông tin, trong quá trình truyền, dù có "chặn" được các thông tin này, kẻ trộm cũng không thể đọc được vì bị mã hoá. Khi tới đích, người nhận sẽ sử dụng một công cụ đặc biệt để giải mã. Phương pháp mã hoá và bảo mật phổ biến nhất đang được thế giới áp dụng là Chứng chỉ số (Digital Certificate) và chữ ký số (Digital Signature).

Với Chứng chỉ số, người sử dụng có thể mã hoá thông tin để giải quyết vấn đề nghe trộm, và sử dụng chữ ký số để giải quyết vấn đề mạo danh, giả mạo và chối cãi nguồn gốc.

3. Ứng dụng trong thực tế

Dựa trên các tính năng cơ bản của Chứng chỉ số và chữ ký số là: Tính xác thực, tính bảo mật, tính toàn vẹn dữ liệu, tính không chối bỏ trong việc thực hiện các giao dịch điện tử qua mạng, cũng như các thủ tục hành chính với cơ quan pháp quyền, nên Chứng chỉ số, chữ ký số được sử dụng trong các công việc như: ký vào văn bản, tài liệu điện tử; bảo mật thư điện tử; bảo đảm an toàn cho Web Server (thiết lập kênh trao đổi bảo mật giữa Web client và Web server trên

Internet), mạng riêng ảo VPN (các điểm kết cuối sẽ nhận thực lẫn nhau thông qua Chứng chỉ số).

Đây chính là nền tảng của 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.

B. HẠ TẦNG KHOÁ CÔNG KHAI (PUBLIC KEY INFRASTRUCTURE)

1. Khái niệm hạ tầng khóa công khai (PKI)

Public Key Infrastructure, viết tắt (PKI) là một cơ chế để cho một tổ chức trung gian cung cấp và xác thực định danh các bên tham gia vào quá trình trao đổi thông tin. Cơ chế này cũng cho phép cấp cho mỗi đối tượng sử dụng trong hệ thống một cặp khóa công khai/cá nhân (public/private key).

PKI thường được dùng để chỉ toàn bộ hệ thống bao gồm nhà cung cấp chứng thực số (CA) cùng các cơ chế liên quan đồng thời với toàn bộ việc sử dụng các thuật toán mã khoá công khai trong trao đổi thông tin.

PKI bản chất là một hệ thống công nghệ vừa mang tính tiêu chuẩn, vừa mang tính ứng dụng được sử dụng để khởi tạo, lưu trữ và quản lý các Chứng chỉ số (Digital Certificate) cũng như các mã khoá công khai và cá nhân.

2. Thành phần cơ bản của một PKI

- Máy trạm PKI (PKI Client): Là thiết bị cuối trong một hệ thống PKI.

- Nhà cung cấp chứng thực số (Certification Authority -CA): Là một tổ chức chuyên cung cấp và xác thực các Chứng chỉ số. Một Chứng chỉ số có 3 thành phần chính:

+ Thông tin về đối tượng được cấp: gồm tên, địa chỉ, điện thoại, email…

+ Khoá công khai (Public key) của đối tượng được cấp: là một giá trị được nhà cung cấp chứng thực đưa ra như một khoá 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.

+ Chữ ký số của CA cấp chứng thực: 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).

- Nhà quản lý đăng ký (Registration Authority - RA): đóng vai trò như người thẩm tra cho CA trước khi một Chứng chỉ số được cấp phát tới đối tượng yêu cầu.

- Hệ thống quản lý, phân phối Chứng chỉ số (Certificate Distribution System - CDS): Danh mục nơi các Chứng chỉ số (với khoá công khai của nó) được lưu giữ, phục vụ cho các nhu cầu tra cứu, lấy khoá công khai của đối tác cần thực hiện giao dịch chứng thực số.

3. Các chuẩn mã hóa khóa công khai(PKCS)

PKCS (Public Key Cryptography Standards) là chuẩn do phòng thí nghiệm RSA Data Security Inc phát triển. Nó dựa vào các cấu trúc ASN.1 (Abstract Syntax Notation - 1). Giao thức chuẩn ISO được sử dụng bởi SNMP để thể hiện các thông điệp (SNMP- Simple Network Management Protocol) là một tập hợp các giao thức không chỉ cho phép kiểm tra nhằm đảm bảo các thiết bị mạng như router, switch hay server đang vận hành mà còn vận hành một cách tối ưu, ngoài ra SNMP còn cho phép quản lý các thiết bị mạng từ xa và thiết kế cho phù hợp với chứng nhận X.09, các tiêu chuẩn này do ANSI thiết kế, theo đó dữ liệu được chia thành từng khối nhỏ nhất là 8 bit (octet). PKCS hiện tại bao gồm các chuẩn PKCS#1, PKCS#3, PKCS#5,PKCS#7, PKCS#8, PKCS#9, PKCS#11, PKCS#12, PKCS#13, PKCS#15.

4. Một số hệ thống PKI

- Microsoft : Với những cải tiến lớn về PKI trong Windows XP Professional (dành cho máy trạm) và Windows Server (dành cho máy chủ), Microsoft đã cung cấp một giải pháp PKI khá hoàn chỉnh cho phép các tổ chức, doanh nghiệp có thể xây dựng một PKI riêng trên hệ thống của mình.

- VeriSign (www.Verisign.com) nhà cung cấp các sản phẩm xác thực và giải pháp hạ tầng mã hoá công khai (CA/PKI) chuyên nghiệp cho lĩnh vực tài chính, ngân hàng, chứng khoán. Ở Việt Nam, Ngân hàng Vietcombank, Ngân hàng Đông Á đã sử dụng dịch vụ chứng thực số của Verisign trong các giao dịch trực tuyến.

- Thawte (www.Thawte.com) là nhà cung cấp Chứng chỉ số hàng đầu hiện nay.

C. ỨNG DỤNG TRÊN NỀN TẢNG HẠ TẦNG KHOÁ CÔNG KHAI: CHỮ KÝ SỐ DÙNG CHO BM, XÁC THỰC VB VÀ THƯ ĐIỆN TỬ

1. Khái niệm

Từ xưa đến nay, chữ ký tay là một phương thức để xác định nguồn gốc của một văn bản, tài liệu. Chữ ký số (Digital Signature) không phải là hình thức số hoá

chữ ký tay rồi gửi kèm theo một thông điệp mà là một phương thức để chứng thực nguồn gốc và nội dung của một thông điệp thông qua kỹ thuật mã hóa.

Chữ ký số là đoạn dữ liệu, đính kèm với thông điệp gốc để chứng minh danh tính của người gửi thông điệp và giúp người nhận kiểm tra tính toàn vẹn của nội dung thông điệp gốc. Một trong những cách phổ biến nhất hiện nay để tạo ra một chữ ký số là sử dụng mật mã khoá công khai.

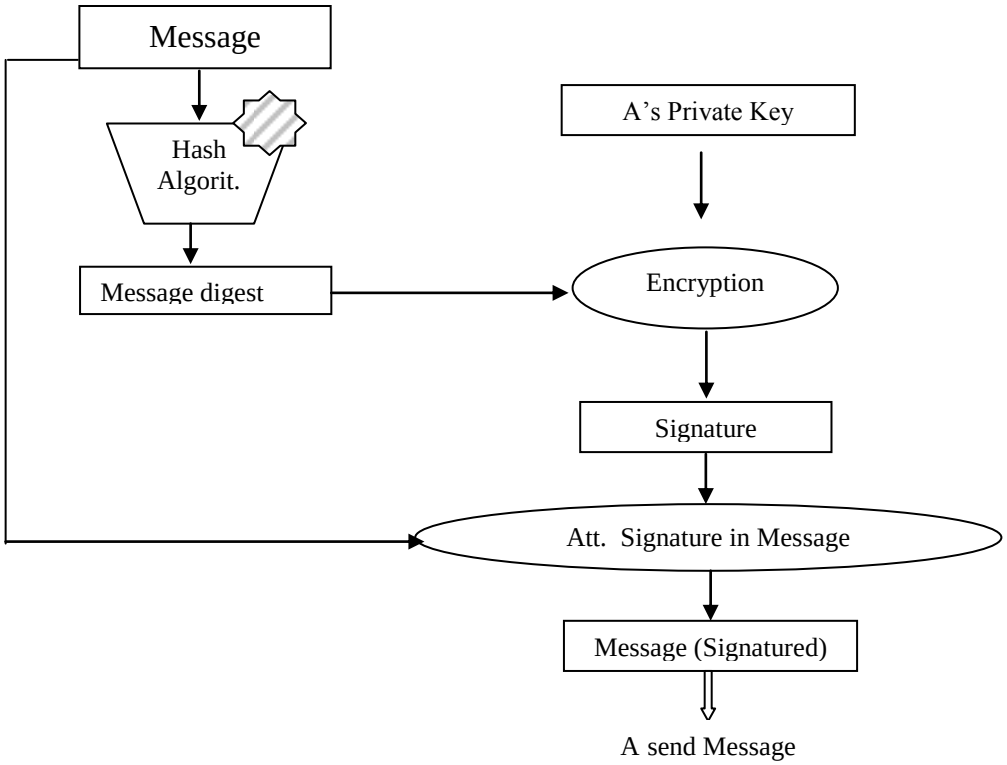
2. Quá trình tạo chữ ký số và xác thực chữ ký

2.1. Quá trình tạo chữ ký số và ký:

- Giả sử A muốn gửi một thông điệp đến B, trước tiên A sử dụng một thuật toán băm (thuật toán SHA hoặc MD5) để tạo ra một bản tóm lược (message digest) cho thông điệp. Bản tóm lược này có độ dài như nhau đối với mọi thông điệp, là duy nhất với một thông điệp, và hai thông điệp khác nhau thì không thể có hai bản tóm lược như nhau.

- Tiếp theo, A mã hoá bản tóm lược sử dụng khoá riêng của mình. Kết quả mã hoá chính là chữ ký số của A.

- Cuối cùng, chữ ký số được gắn với thông điệp rồi gửi cho B. Như vậy là A đã ký xong thông điệp của mình.



Quá trình tạo chữ ký số và ký một thông điệp

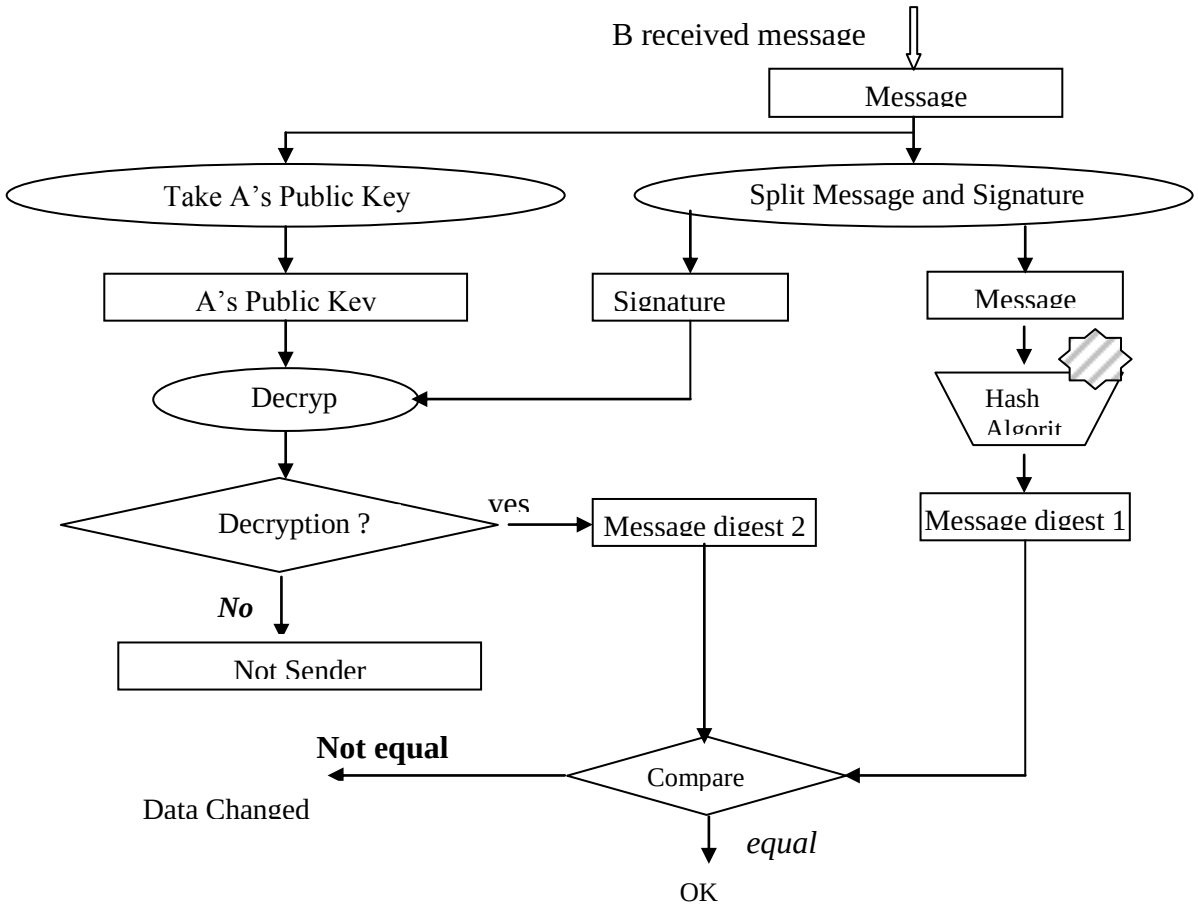
2.2. Quá trình xác thực chữ ký số

Việc chứng thực người gửi, tính toàn vẹn dữ liệu và chống chối bỏ được thực hiện sử dụng chữ ký số. Nói cách khác, người ta tạo ra một chữ ký số và ký vào một thông điệp để người nhận có thể thực hiện việc chứng thực cho nội dung và danh tính người gửi thông điệp đó. Quá trình xác thực được minh hoạ dưới đây, và có thể được mô tả như sau:

- B nhận được thông điệp, biết người gửi là A. B tách chữ ký số của A ra khỏi thông điệp.

- B lấy khoá công khai của A để giải mã chữ ký số của A, và có được bản tóm lược thông điệp. Việc giải mã được chữ ký số của A bằng khoá công khai của A (được lấy từ cơ sở dữ liệu tin cậy) chứng tỏ A đúng là người gửi (chứng thực người gửi và chống chối bỏ).

- B sử dụng thuật toán băm để tạo ra bản tóm lược cho thông điệp đã nhận được từ A, rồi đem so sánh với bản tóm lược đã được giải mã ở trên. Nếu kết quả so sánh cho thấy hai bản tóm lược là như nhau thì chứng tỏ rằng nội dung của thông điệp đúng là nguyên bản từ A mà không bị thay thế hoặc sửa đổi (xác thực tính toàn vẹn dữ liệu).



Quá trình xác thực chữ ký số

3. Quá trình mã hóa và giải mã thư điện tử

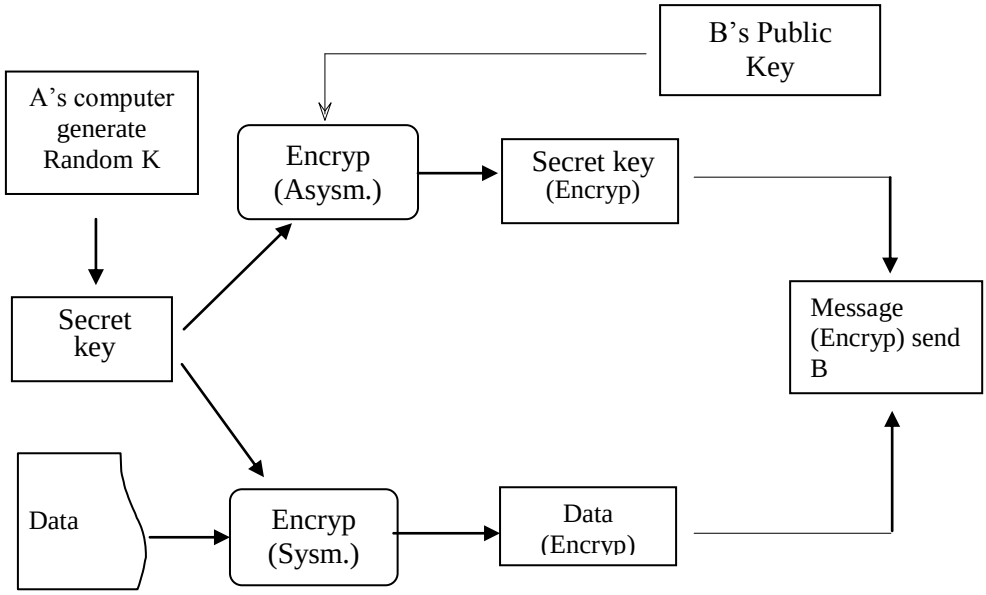
3.1.Quá trình mã hóa thư điện tử

Giả sử A muốn gửi một thông điệp đến B và giả sử A đã có được khóa công khai của B.

Giai đoạn 1 – Mã hóa thông điệp bằng một phương pháp mã hóa đối xứng: Máy tính của A sẽ phát sinh ngẫu nhiên khóa bí mật *K* được sử dụng để mã hóa toàn bộ thông điệp cần gửi đến cho B bằng phương pháp mã hóa đối xứng được chọn.

Giai đoạn 2 – Mã hóa khóa bí mật *K* bằng một phương pháp mã hóa bất đối xứng sử dụng khóa công khai của B.

Nội dung thông điệp sau khi mã hóa ở giai đoạn 1 cùng với khóa bí mật *K* được mã hóa ở giai đoạn 2 sẽ được gửi cho B dưới dạng một bức thư điện tử.



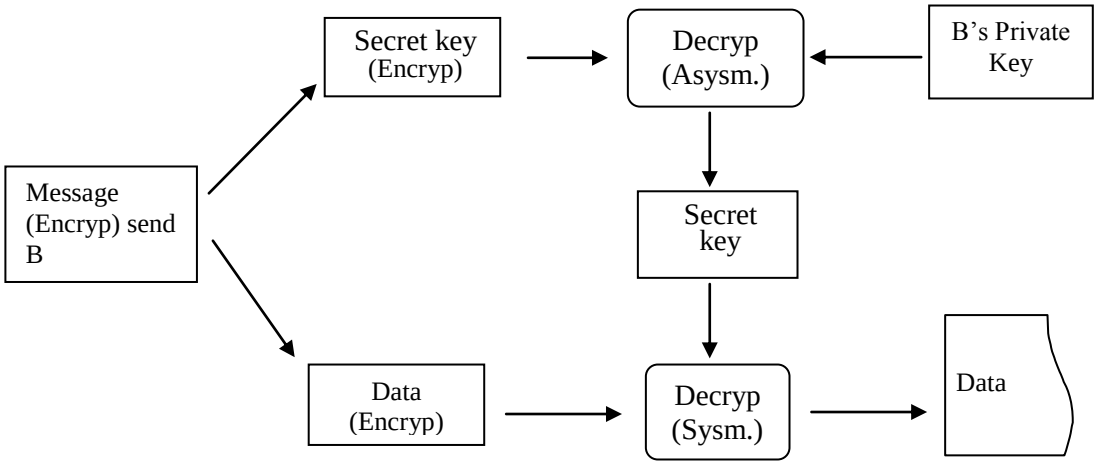
Qúa trình mã hóa thư điện tử

3.2.Quá trình giải mã thư điện tử

Giai đoạn 1 – Giải mã khóa bí mật *K*: B sử dụng khóa riêng của mình để giải mã khóa bí mật *K* bằng phương pháp mã hóa bất đối xứng mà A đã dùng để mã hóa khóa *K*.

Giai đoạn 2 – Giải mã thông điệp của A: B sử dụng khóa bí mật *K* để giải mã toàn bộ thông điệp của A bằng phương pháp mã hóa đối xứng mà A đã dùng.

Sử dụng kỹ thuật trên đây, người gửi thư có thể yên tâm rằng bức thư của mình chỉ có thể được giải mã bởi người nhận hợp lệ, bởi vì chỉ có người này mới có được mã khóa riêng để giải mã được khóa bí mật *K* và từ đó giải mã được nội dung của thông điệp.



Quá trình giải mã thư điện tử

4. Bảo mật, xác thực văn bản và thư điện tử

Thư tín điện tử đang ngày càng được sử dụng rộng rãi trong các lĩnh vực đời sống xã hội. Hệ thống thư điện tử cho phép thực hiện các giao dịch một cách nhanh chóng, hiệu quả. Tuy nhiên, trong môi trường Internet thiếu an toàn, thư điện tử dễ dàng bị đọc trộm, giả mạo, mạo danh trước khi đến người nhận.

Trong môi trường truyền thống chúng ta bảo vệ nội dung thư bằng phong bì và chữ ký. Còn trong môi trường truyền thông điện tử trực tuyến, thư điện tử được bảo vệ bằng việc sử dụng chứng chỉ số, chữ ký số. Với chứng chỉ số và chữ ký số, người sư dụng có thể:

- Ký vào thư điện tử và các tệp đính kèm để đảm bảo tính thừa nhận và không bị từ chối. Giúp người nhận kiểm tra tính nguyên vẹn.

- Mã hoá nội dung thư và các tệp đính kèm, để đảm bảo chỉ người nhận hợp lệ mới xem được thư.

Hầu hết các chương trình thư điện tử đều hỗ trợ hai loại định dạng thông điệp HTML và văn bản thô (plain text). Phiên bản cải tiến Mutipurpose Internet Mail Extensions (MIME) đang được sử dụng phổ biến.

MIME là chuẩn Internet cơ bản để gửi thư điện tử đa phương tiện (multimedia e-mail), cung cấp định dạng HTML cho phép kèm hình ảnh, màu sắc, các siêu liên kết (hyperlink) vào trong email. Hiện nay, MIME đang sử dụng phiên bản bảo mật S-MIME (Secure-MIME).

S-MIME là một tập hợp các mô tả về bảo mật thư điện tử, S-MIME đưa vào hai phương pháp an ninh cho thư điện tử là mã hóa thư điện tử và xác thực. Cả hai phương pháp này đều dựa trên hạ tầng khoá công khai PKI.

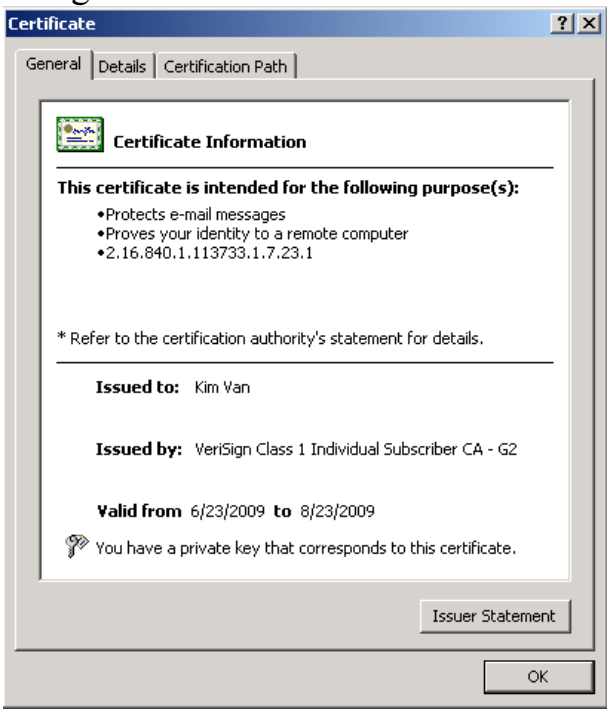
Microsoft Outlook và Microsoft Outlook Express đều hỗ trợ S-MIME phiên bản 3 sử dụng PKI để có thể cài đặt được nhiều phương pháp mã hóa và xác thực bằng sự kết hợp giữa chữ ký số và mã hóa theo yêu cầu của người gửi. Các chứng chỉ sẽ được trao đổi dễ dàng giữa những người dùng sử dụng chữ ký số để thiết lập các giao tiếp bảo mật, hỗ trợ tính năng gửi kèm chứng chỉ vào sổ địa chỉ (address book) và kèm cả định danh số (digital ID) người gửi.

Trong lần giao tiếp đầu tiên, bên gửi và bên nhận cần trao đổi chứng chỉ của nhau. Sau khi bên gửi và bên nhận xác thực đúng các chứng chỉ nhận được thì dùng khóa công khai trên chứng chỉ để mã hóa thông điệp cần gửi đi.

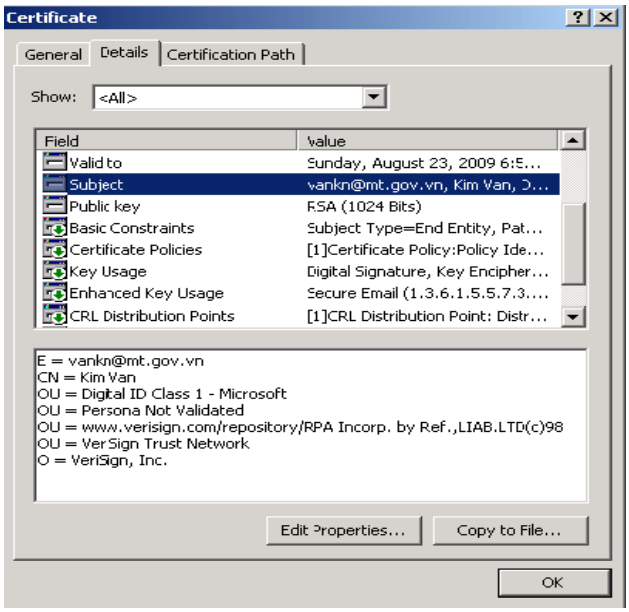
Outlook Express sử dụng giải thuật băm SHA1 cho chữ ký số và những giải thuật mã hóa 3DES (168- bit), DES (56-bit), RC2 (40-bit; 64-bit hoặc 128-bit).

Microsoft Outlook sử dụng giải thuật băm SHA1 và MD5 cho chữ ký số và giải thuật mã hóa 3DES.

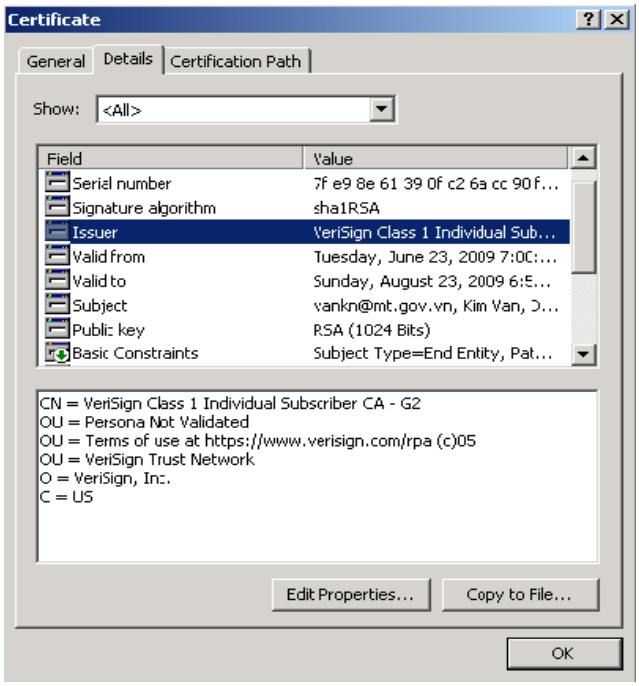
- Thông tin về chứng chỉ



Thông tin về chứng chỉ



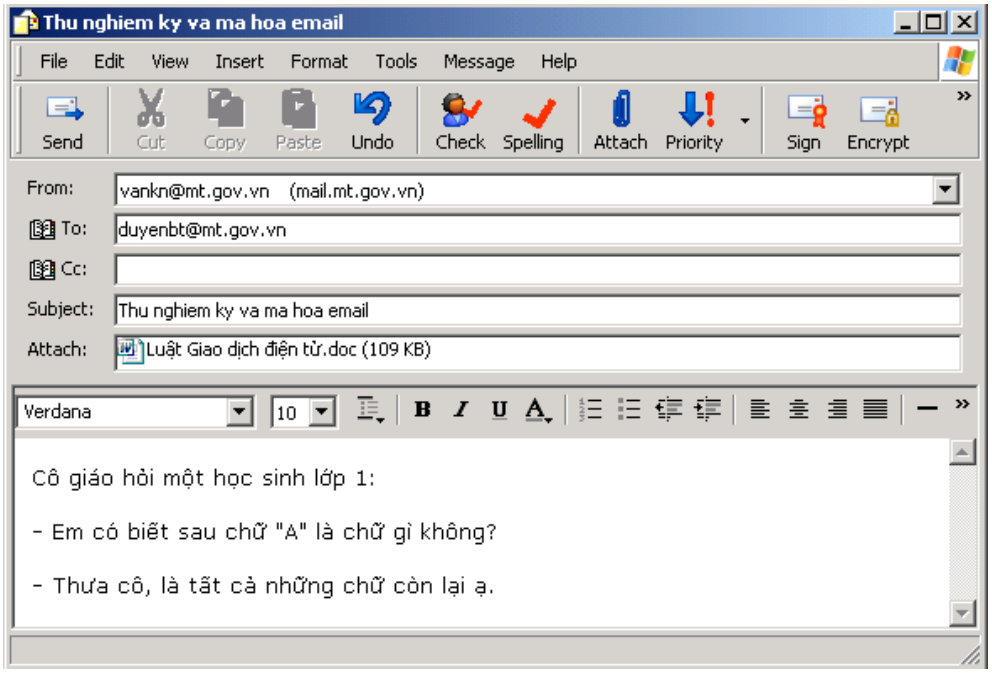
Chứng thực số được gắn cho tài khoản thư



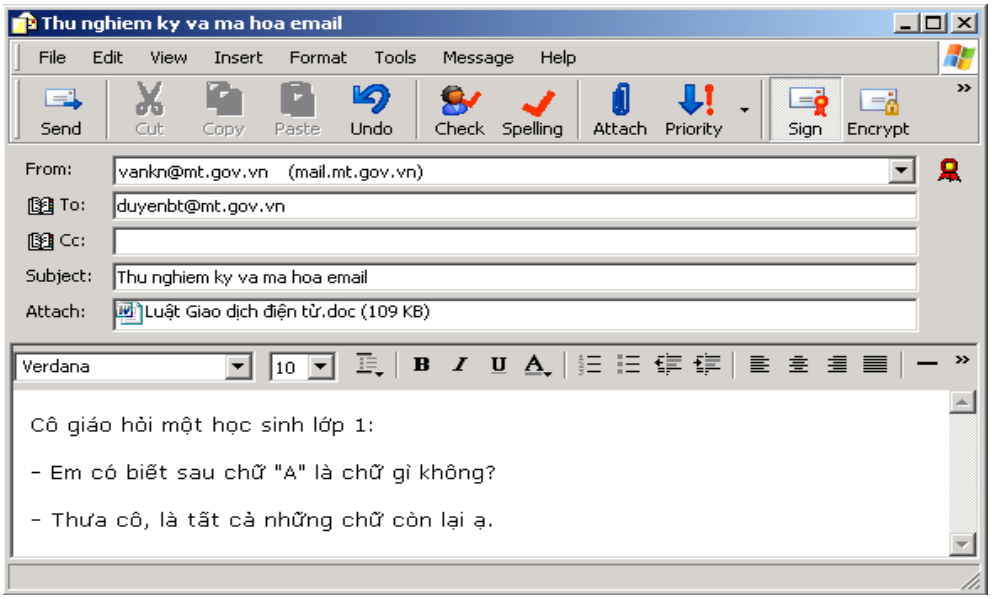
Thông tin về tổ chức cung cấp chứng thực số

4.1. Ký và mã hoá Email

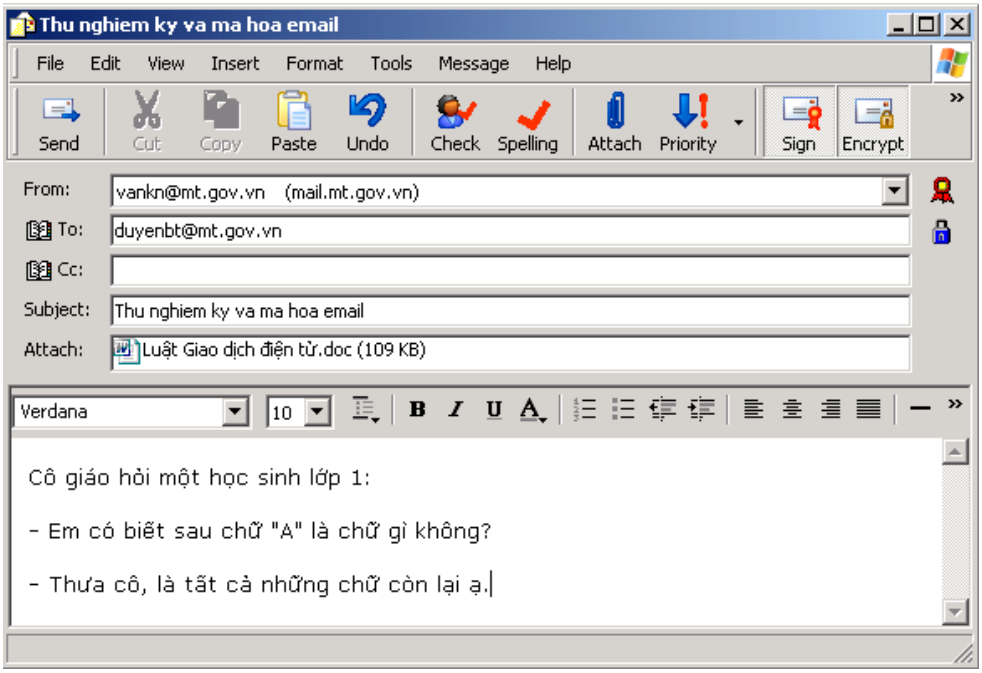
Khi chứng thực số đã được gắn cho tài khoản thư, người sử dụng có thể ký và mã hoá nội dung thư và các tệp đính kèm.



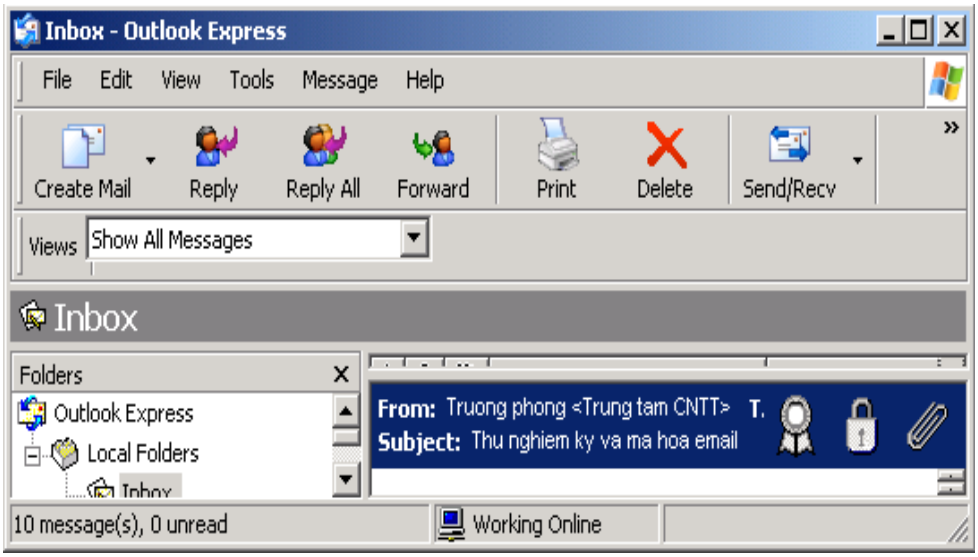
Công cụ ký (Sign) và mã hoá (Encrypt)



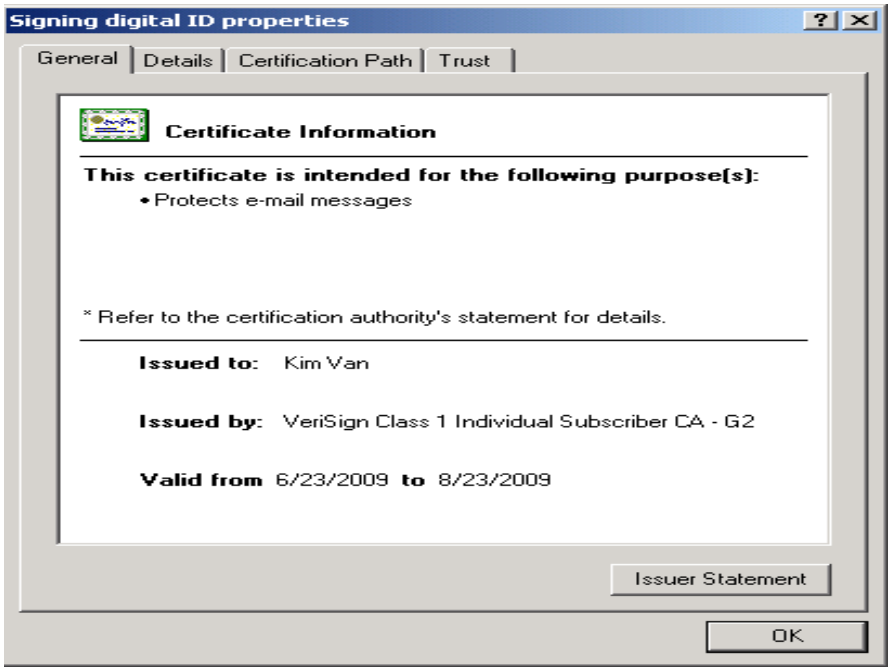
Bên gửi ký vào Email



Bên gửi ký và mã hoá Email

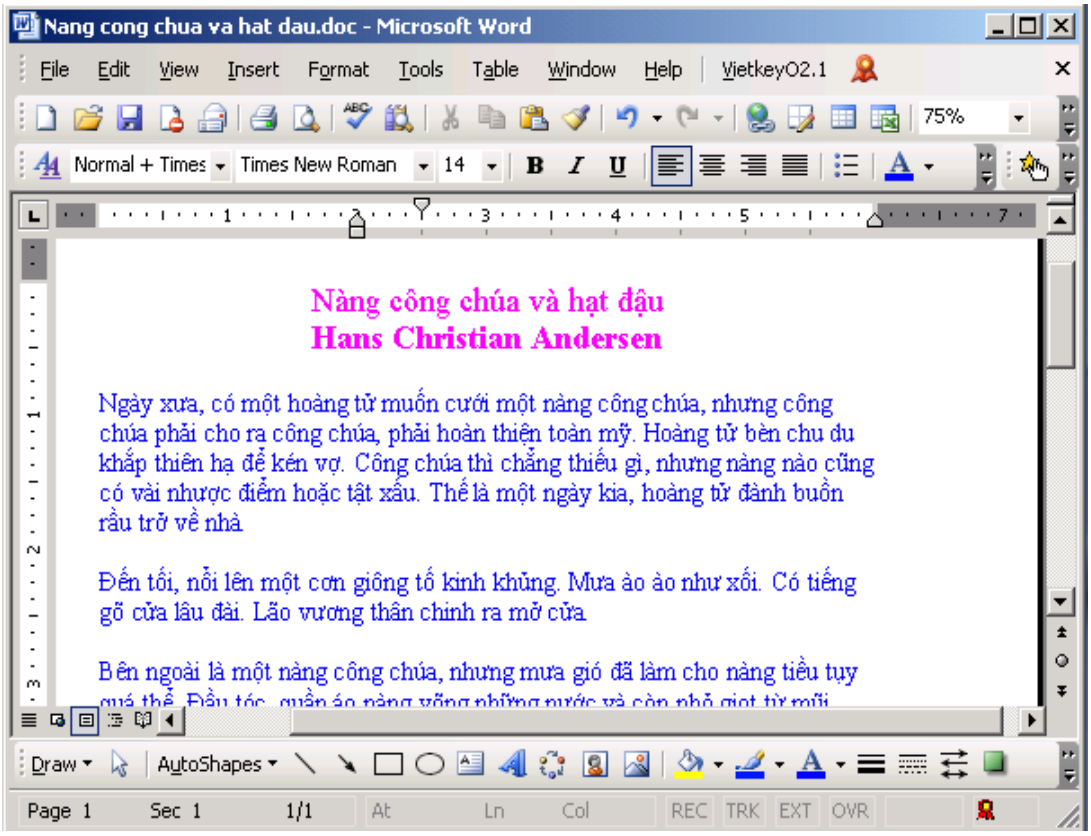


Bên nhận Email có chữ ký số và mã hoá



Chứng chỉ của bên gửi

4.2 Ký trực tiếp vào văn bản



Ký trực tiếp vào văn bản

PHẦN III. ĐỀ XUẤT GIẢI PHÁP

I. KHẢ NĂNG ĐÁP ỨNG VIỆC SỬ DỤNG CHỮ KÝ SỐ TẠI BỘ GTVT

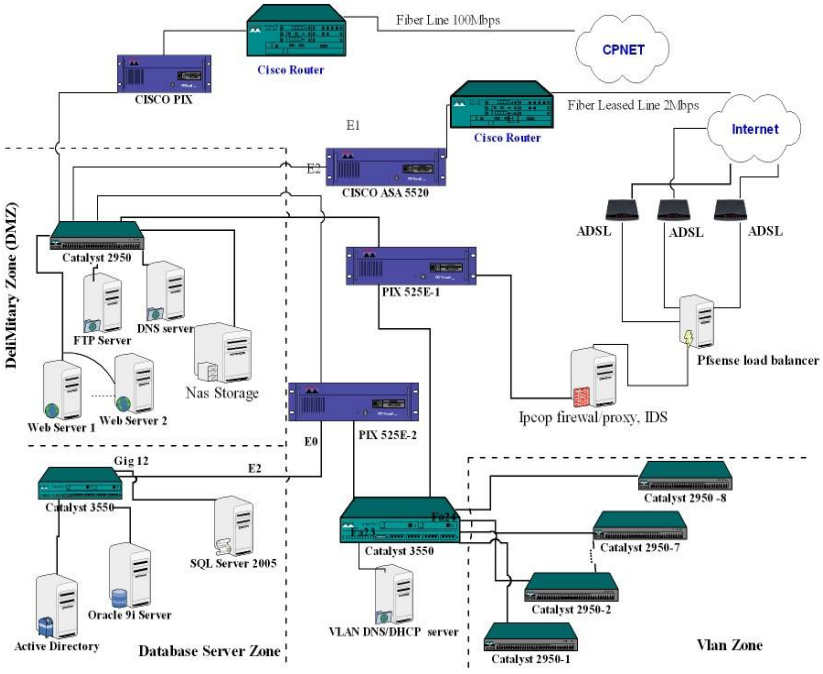
1. Tổng quan về hiện trạng hệ thống CNTT tại Bộ GTVT

1.1. Hệ thống mạng, máy tính và đường truyền

Hiện tại, Hệ thống mạng máy tính của Bộ GTVT được xây dựng trên nền tảng công nghệ mạng LAN 100Mbps với số lượng 250 máy tính nối mạng.Trong đó 98% các máy tính có cấu hình: CPU Pentium 4 hoặc Celeron có tốc độ >1.5 GHz, RAM 512 Mbps, ổ cứng HDD 80 GB, màn hình CRT 17 inches. Mạng LAN được chia nhỏ thành 17 VLAN theo các đơn vị chức năng. Hệ thống mạng chia làm 4 vùng bao gồm: VLAN zone, DMZ zone, Database Zone, Internet Zone. Trung tâm tích hợp dữ liệu có 12 máy chủ, 02 Firewall, 01 router, được kết nối với Trung tâm dữ liệu của các Cục quản lý GTVT chuyên ngành qua mạng VPN.

Đường truyền: 02 đường ADSL; 01 đường cáp quang 2 Mbps, 01 đường cáp quang 10 Mbps của Cục Bưu điện trung ương.

Các Cục quản lý chuyên ngành: đều có mạng LAN từ 50 máy tính như Cục Đường thủy nội địa đến 250 máy tính như Cục Đăng kiểm. Tất cả các mạng máy tính đều được kết nối Internet với đường truyền tốc độ cao. Đặc biệt Cục Hàng hải có các đường truyền: 01 đường trục backbone nối 2 trung tâm (HN-HCM), 2 đường Internet trực tiếp 512 kbps, và một số đường ADSL.



1.2. Hệ điều hành và các phần mềm ứng dụng

- Hệ điều hành: 100% máy tính sử dụng HĐH Microsoft Windows SP2, trình duyệt Internet Explorer 6.0 trở lên.

- Bộ Phần mềm ứng dụng văn phòng: 100% máy tính sử dụng bộ phần mềm Microsoft Office XP trở lên. Trong đó:

+ Hai phần mềm gửi/nhận thư điện tử Microsoft Outlook và Microsoft Outlook Express đều hỗ trợ S-MIME phiên bản 3 sử dụng PKI để có thể cài đặt được nhiều phương pháp mã hóa và xác thực kết hợp giữa chữ ký số và mã hóa .

* Outlook Express sử dụng giải thuật băm SHA1 cho chữ ký số và những giải thuật mã hóa 3DES (168- bit), DES (56-bit), RC2 (40-bit; 64-bit hoặc 128-bit).

* Microsoft Outlook sử dụng giải thuật băm SHA1 và MD5 cho chữ ký số và giải thuật mã hóa 3DES.

+ Phần mềm xử lý văn bản Microsoft Word, và phần mềm xử lý bảng tính Microsoft Excel hỗ trợ chuẩn chữ ký số DSS

Hệ thống thư điện tử của Bộ hiện tại có gần 500 tài khoản, địa chỉ truy cập: http://mail.mt.gov.vn/; hỗ trợ các chuẩn SMTP, POP3, IMAP, HTTP; có hệ thống chống thư rác, virus; hệ thống chạy ổn định; tần suất backup 2 tuần/lần.

1.3. Các ứng dụng và CSDL đã xây dựng

- Hệ thống phần mềm quản lý văn bản đi đến, điều hành công việc, có địa chỉ cục bộ http://congvanbo.mt.gov.vn/.

- Các CSDL: CSDL tiêu chuẩn ngành, CSDL văn bản quy phạm pháp, CSDL văn bản chỉ đạo & điều hành, CSDL chương trình, đề tài KHCN...

1.4. Giải pháp bảo mật hiện tại của Bộ Giao thông vận tải

- Các máy chủ cài đặt hệ quản trị CSDL được chạy trên nền hệ điều hành Windows 2003 SP2. Các máy chủ đều được cài chương trình diệt virus F-Secure.

- Các máy trạm trong mạng LAN của Bộ hiện tại có khoảng 98% máy tính được bảo vệ bằng chương trình diệt virus Bkav Enterprise.

Hiện trạng hệ thống CNTT tại Bộ GTVT là hoàn toàn phù hợp và tương thích về kỹ thuật, công nghệ để triển khai ứng dụng chữ ký số trên nền tảng hạ tầng khóa công khai.

2. Năng lực ứng dụng CNTT của cán bộ công chức Bộ GTVT

Hiện tại, 100% cán bộ công chức cơ quan Bộ và các Cục quản lý chuyên ngành đều sử dụng tốt bộ phần mềm văn phòng Microsoft Office (xử lý văn bản, xử lý bảng tính…), sử dụng Internet và hệ thống thư điện tử trong công tác chuyên môn nghiệp vụ.

II. NHU CẦU TRIỂN KHAI CHỮ KÝ SỐ TẠI BỘ GTVT

1. Sử dụng chữ ký số cho xác thực, bảo mật VB và thư điện tử

Nghị đinh 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng CNTT trong hoạt động của cơ quan nhà nước; Quyết định số 43/2008/QĐ-TTg ngày 24/3/2008 của Thủ tướng Chính phủ, phê duyệt kế hoạch ứng dụng CNTT trong hoạt động của cơ quan nhà nước và Chị thị 15/CT-BGTVT ngày 30/8/2008 của Bộ trưởng Bộ GTVT về việc đẩy mạnh ứng dụng CNTT trong hoạt động của các cơ quan, đơn vị trực thuộc Bộ GTVT yêu cầu tăng cường sử dụng và trao đổi văn bản điện tử qua mạng. Vì vậy, việc ứng dụng chứng chỉ số, chữ ký số cho xác thực, bảo mật văn bản và thư điện tử là nhu cầu cấp thiết hiện nay.

III. GIẢI PHÁP VỀ TỔ CHỨC CUNG CẤP CHỨNG THỰC SỐ (CA)

1. Các quy định về CA và hiện trạng một số CA

1.1. Quy định đối với các tổ chức CA

Các tổ chức cung cấp dịch vụ chứng thực chữ ký số bao gồm tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng và tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia (Root Certification Authority) là tổ chức cung cấp dịch vụ chứng thực chữ ký số cho các tổ chức cung cấp dịch vụ chữ ký số công cộng. Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia là duy nhất.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng là tổ chức cung cấp dịch vụ chứng thực chữ ký số cho cơ quan, tổ chức, cá nhân sử dụng trong các hoạt động công cộng. Hoạt động của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng là hoạt động nhằm mục đích kinh doanh. Có giấy phép cung cấp dịch vụ chứng thực chữ ký số công cộng do Bộ Thông tin và Truyền thông cấp. Có chứng thư số do tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia cấp.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng là tổ chức cung cấp dịch vụ chứng thực chữ ký số cho các cơ quan, tổ chức, cá nhân có cùng tính chất hoạt động hoặc mục đích công việc và được liên kết với nhau thông qua điều lệ hoạt động hoặc văn bản quy phạm pháp luật quy định cơ cấu tổ chức chung hoặc hình thức liên kết, hoạt động chung. Hoạt động của tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng là hoạt động nhằm phục vụ nhu cầu giao dịch nội bộ và không nhằm mục đích kinh doanh.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng phải đáp ứng các điều kiện : 1) Có đủ nhân viên kỹ thuật chuyên nghiệp và nhân viên quản lý phù hợp với việc cung cấp dịch vụ chứng thực chữ ký số; 2) Hệ thống thiết bị cung cấp dịch vụ phù hợp với tiêu chuẩn an ninh, an toàn quốc gia.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng bao gồm:

Chuyên dùng cho hệ thống chính trị, Chuyên dùng nội bộ và chuyên dùng khác.

Ban Cơ yếu Chính phủ thành lập và duy trì hoạt động của tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng phục vụ các cơ quan thuộc hệ thống chính trị. Trung tâm chứng thực điện tử chuyên dùng Chính phủ thuộc Cục Quản lý kỹ thuật nghiệp vụ mật mã -Ban cơ yếu Chính phủ đã đi vào hoạt động và đang triển khai thử nghiệm ở một số bộ/ngành.

1.2. Một số CA nhà nước và doanh nghiệp

+ CA - Ban cơ yếu Chính phủ

Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng phục vụ các cơ quan thuộc hệ thống chính trị do Trung tâm chứng thực điện tử chuyên dùng Chính phủ thuộc Cục Quản lý kỹ thuật nghiệp vụ mật mã -Ban cơ yếu Chính phủ đảm nhận đã đi vào hoạt động và đang triển khai thử nghiệm ở một số bộ/ngành.

+ CA - Sở Bưu chính Viễn thông TP Hồ Chí Minh.

Đã đưa vào hoạt động.

Phạm vi đối tượng cung cấp dịch vụ: cung cấp dịch vụ chứng thực chữ ký số cho các cán bộ công chức thuộc các sở/ngành, quận/huyện trên địa bàn thành phố HCM và các sở BCVT trên cả nước.

Các dịch vụ triển khai chữ ký số bao gồm: Hỗ trợ đăng nhập hệ thống sử dụng thẻ thông minh làm công cụ xác thực quyền quản trị hệ thống và sử dụng các tiện ích; ứng dụng chữ ký số trên các hệ thống văn bản, báo cáo…

+ CA - Ngân hàng Nhà nước

Đã đưa vào hoạt động.

Phạm vi đối tượng cung cấp dịch vụ: tất cả các ngân hàng thương mại, các tổ chức tín dụng đang hoạt động tại Việt Nam.

Các dịch vụ đã ứng dụng chữ ký số: các ứng dụng nghiệp vụ của NHNN và các hoạt động nghiệp vụ liện ngân hàng do NHNN chủ trì.

+ CA - VDC (doanh nghiệp)

Đã triển khai xong các hạ tầng cơ bản và có thể cung cấp các dịch vụ về chứng thư số phục vụ nhu cầu của các tổ chức, cá nhân sử dụng chữ ký số.

2. Các giải pháp triển khai

2.1. Xây dựng một hệ thống CA riêng tại Bộ GTVT

Giải pháp này đòi hỏi việc đầu tư kinh phí tương đối lớn và mất thời gian cho việc thiết lập Trung tâm CA; Trung tâm CA dự phòng; Hệ thống Directory (cho phép người sử dụng đầu cuối tại các địa điểm khác nhau truy cập).

Ngoài ra giải pháp còn cần đội ngũ vận hành có kinh nghiệm, quy chế hoạt động CA chặt chẽ để đảm bảo an toàn cho hệ thống.

2.2. Đăng ký sử dụng với một tổ chức cung cấp dịch vụ chứng thực số

Giải pháp này yêu cầu đầu tư nhỏ hơn nhiều cả về kinh phí và nhân lực so với giải pháp 1. Mặt khác, đối với các giao dịch G2G, G2B và G2C chỉ cần đăng ký sử dụng với một tổ chức cung cấp dịch vụ chứng thực số để xin cấp chứng chỉ số cho các giao dịch cần triển khai.

IV. GIẢI PHÁP VỀ BẢO MẬT KHÓA RIÊNG

Trong suốt quá trình sử dụng chứng chỉ số người dùng có trách nhiệm lưu giữ và đảm bảo sự an toàn và bí mật cho khoá riêng của mình. Khoá riêng của người sử dụng thường được lưu trữ trong đĩa mềm, thẻ thông minh (SmartCard), USBToken,… của người đó. Thẻ thông minh và USB token là thiết bị có tích hợp chip trên nó nhằm đáp ứng các nhu cầu về lưu trữ dữ liệu, bảo vệ dữ liệu và xử lý dữ liệu (nhờ vào bộ vi xử lý trên chip), bộ vi xử lý 32 bit trên chip thông

thường có EEPROM (Electrically Erasable Programmable Read-only Memory) khoảng 32KB hoặc 64K (EPPROM có thể cùng lúc ở mode đọc hoặc ghi).

Thẻ thông minh giao tiếp với máy tính qua một thiết bị đọc thẻ (*smart card reader*), còn USB token không cần thiết bị đọc thẻ mà sử dụng cổng USB trên máy tính. Thiết bị đọc thẻ và USB token đều cần một trình điều khiển (driver). Khi người dùng sử dụng thẻ thông minh hoặc USB Token trong các ứng dụng PKI (chữ ký số, mã hóa) thì phải nhập vào số PIN (Personal Indentification Number) để xác thực.

Hiện nay, USB Token là thiết bị được dùng phổ biến trong các ứng dụng PKI và có nhiều loại khác nhau. Việc lựa chọn USB Token được dựa trên các tiêu chí chính sau đây:

- Khả năng hỗ trợ các ứng dụng PKI
- Khả năng hỗ trợ hệ điều hành và ngôn ngữ lập trình
- Tiêu chuẩn bảo mật
- Giá thành.

1. Giới thiệu eToken Pro USB

eToken Pro USB là một sản phẩm thuộc dòng sản phẩm eToken™ của Aladdin Knowledge Systems Ltd., Israel.

eToken Pro 32K

eToken Pro USB là một thiết bị bảo mật cao, giao tiếp với máy tính qua cổng USB, sử dụng tiện lợi, an toàn, dễ mở rộng. eToken Pro USB hỗ trợ tất cả hạ tầng khóa công khai eToken PKI như xác thực người dùng, quản lý mật khẩu, bảo mật chữ ký số và bảo mật dữ liệu…

Ngoài ra, do eToken Pro USB hỗ trợ các giao diện và hệ thống bảo mật theo tiêu chuẩn công nghiệp, nên eToken Pro USB còn đảm bảo việc tích hợp dễ dàng với hạ tầng và các chính sách bảo mật.

* Đặc tính kỹ thuật của eToken Pro USB

Operating systems	Windows 2000/XP/2003/Vista Mac OS X; Linux
API & standards support	PKCS#11 v2.01, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE
Models	32K: Siemens CardOS / 32K memory 64K: Siemens CardOS / 64K memory Java: Java Virtual Machine / 72K memory
On board security algo.	RSA 1024-bit / 2048-bit, DES, 3DES, SHA1, SHA256
Security certifications	FIPS 140-1 L2&3; Common Criteria EAL4+/EAL5+ (smart card chip and OS) Pending: FIPS 140-2 and CC EAL4+ PP-SSCD (Certifications differ per model; please inquire)
Dimensions	52 x 16 x 8 mm (2.05 x 0.63 x 0.31 inches)
ISO specification support	Support for ISO 7816-1 to 4 specifications
Operating temperature	0 C to 70 C (32 F to 158 F)
Storage temperature	-40 C to 85 C (-40 F to 185 F)
Humidity rating	0-100% without condensation
Water resistance cert.	IP X8 – IEC 529
Connector	USB type A (Universal Serial Bus)
Casing	Hard molded plastic, tamper evident
Memory data retention	At least 10 years
Memory cell rewrites	At least 500,000

* Giá thành: Khoảng 50USD

Dựa trên các tiêu chí đánh giá, eToken Pro USB có tính năng nổi trội về khả năng hỗ trợ hệ điều hành, hỗ trợ các ứng dụng PKI, hỗ trợ các chuẩn bảo mật và khả năng tích hợp. Vì vậy, eToken Pro USB là sản phẩm được Ban cơ yếu Chính phủ lựa chọn và khuyến cáo các bộ/ngành sử dụng sản phẩm này.

V. LỰA CHỌN GIẢI PHÁP THỬ NGHIỆM TẠI BỘ GTVT

1. Phạm vi thử nghiệm

Trung tâm công nghệ thông tin.

2. Nội dung thử nghiệm

Sử dụng chứng chỉ số để tạo chữ ký số và mã hóa văn bản, thư điện tử phục vụ trao đổi văn bản, thư điện tử trên Internet.

3. Tổ chức cung cấp chứng thực số

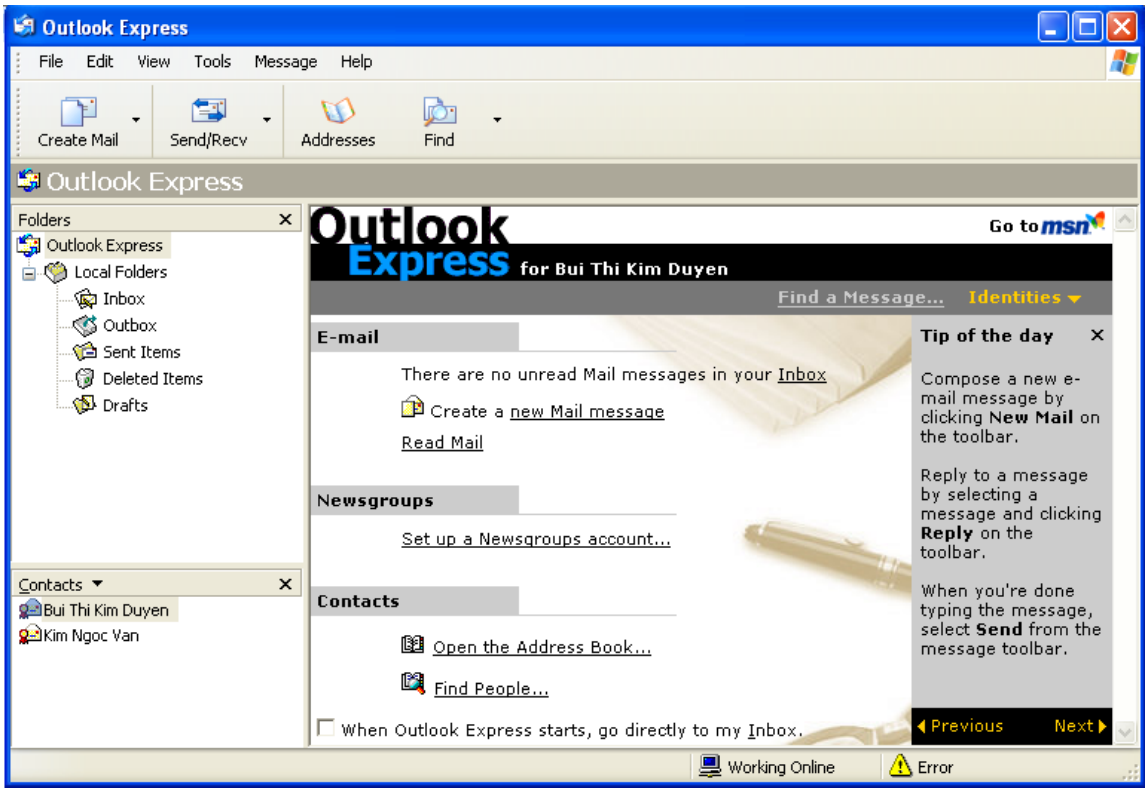
Sử dụng chứng chỉ số do VeriSign cấp dùng thử nghiệm trong 60 ngày.

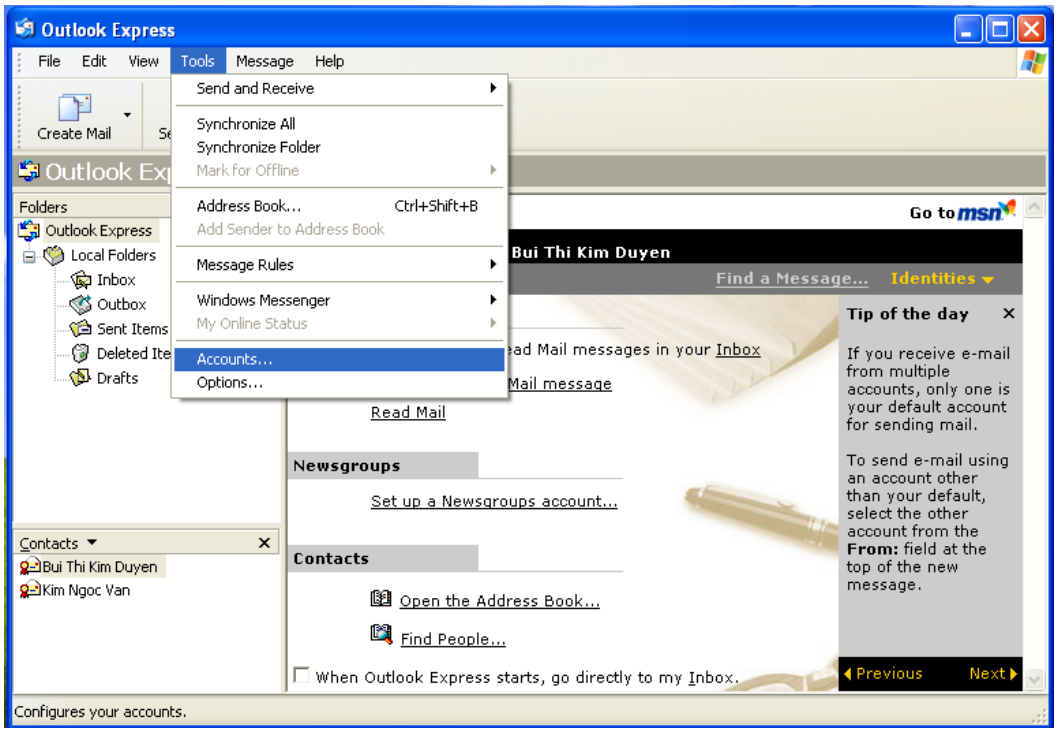
4. Thiết bị bảo mật khóa riêng

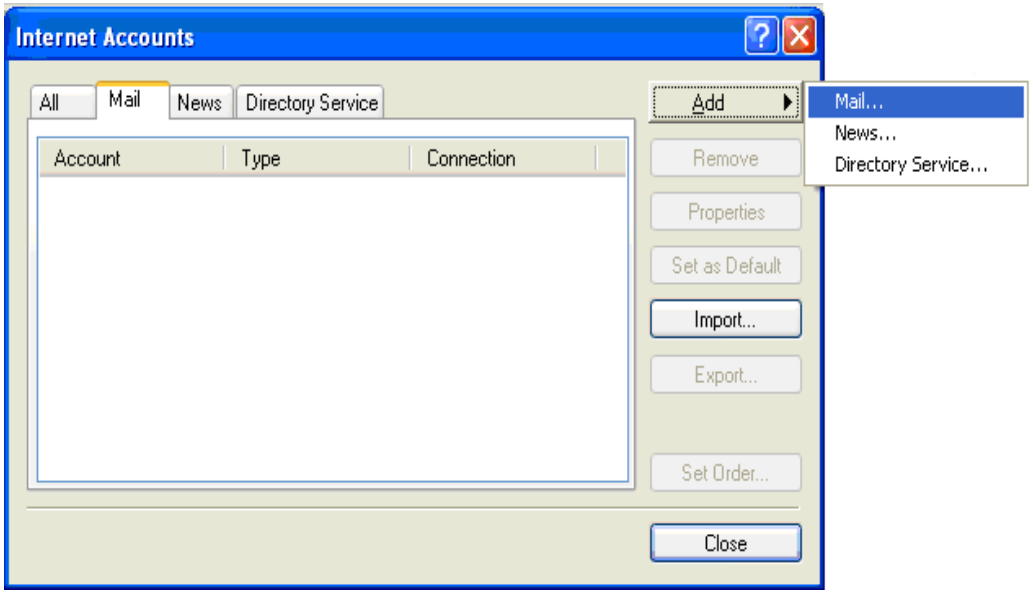
Sử dụng eToken Pro 32 K USB.

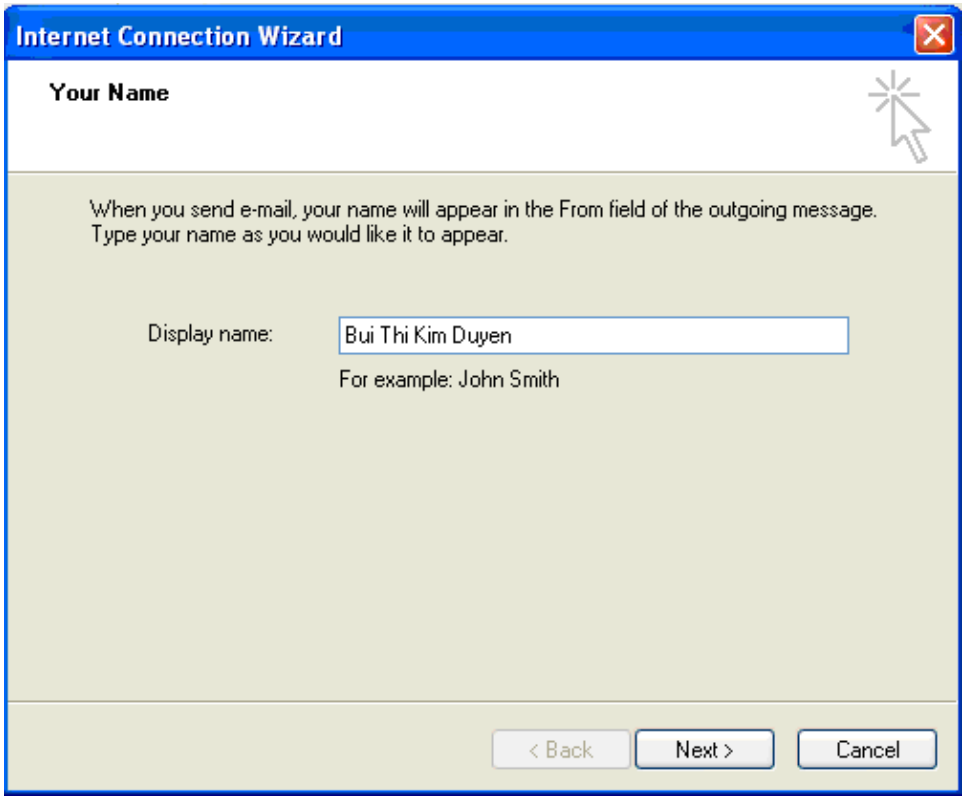
VI. TRIỂN KHAI THỬ NGHIỆM SỬ DỤNG CHỮ KÝ SỐ

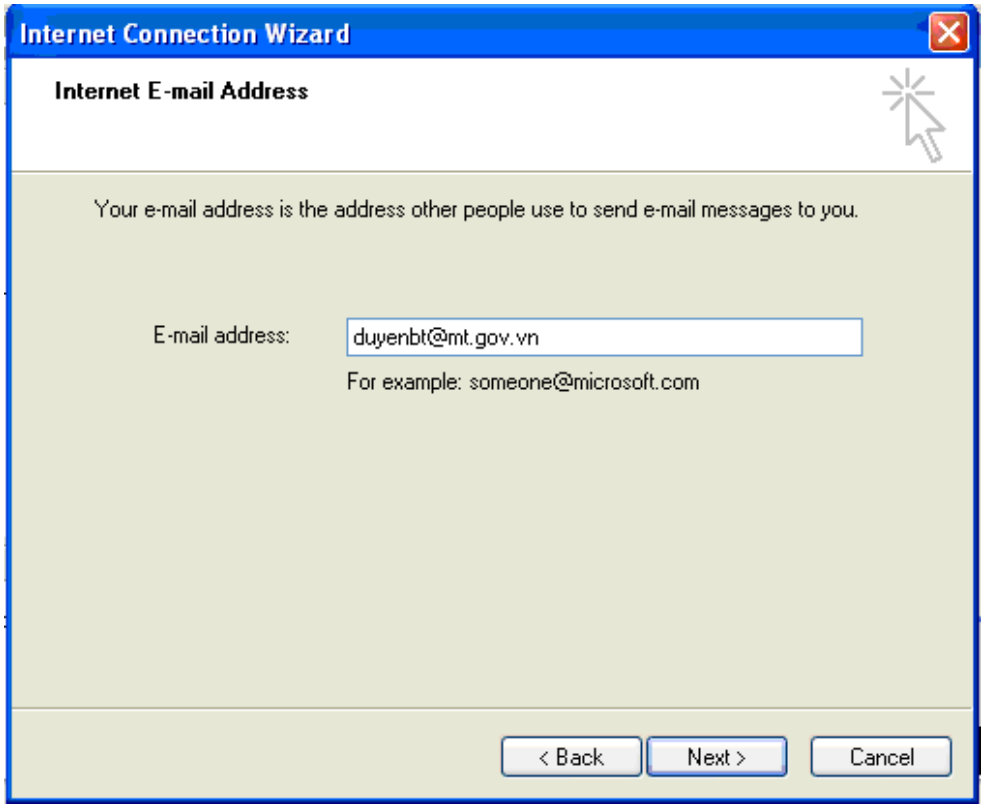
1. Thiết lập một tài khoản Email (Pop3)

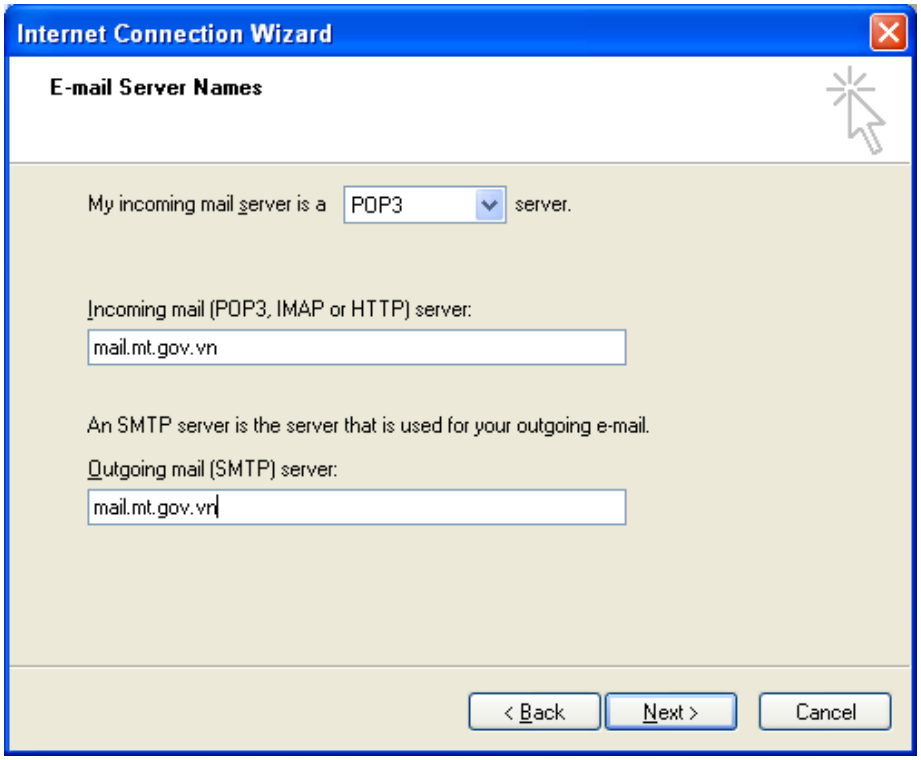


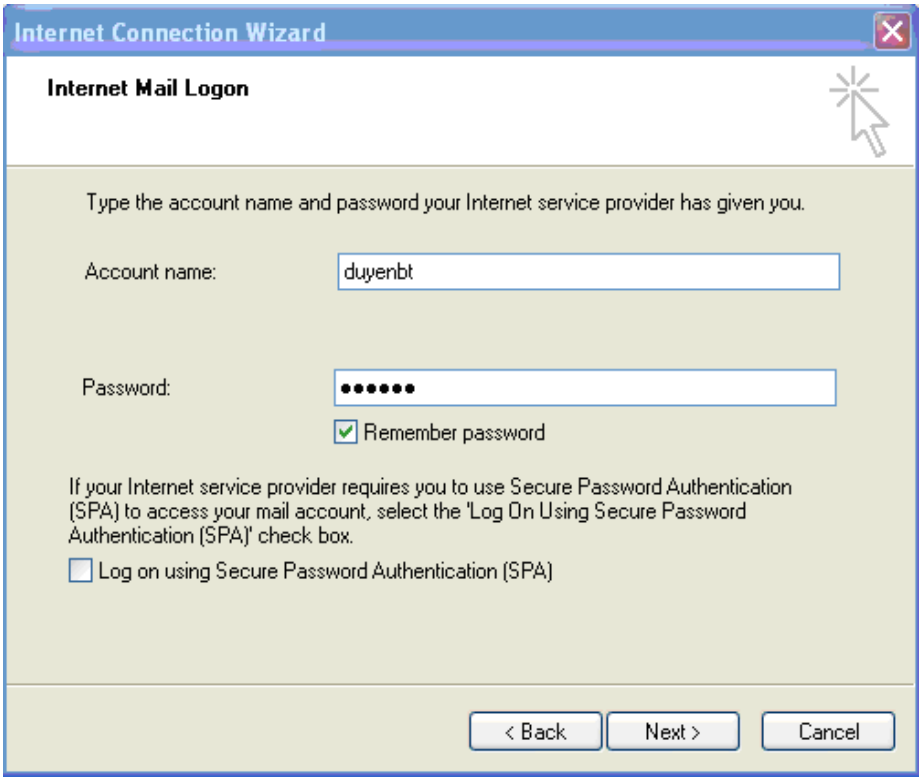

Outlook Express
File Edit View Tools Message Help
Create Mail
Send and Receive
Synchronize All
Synchronize Folder
Mark for Offline
Address Book... Ctrl+Shift+B
Add Sender to Address Book
Message Rules
Windows Messenger
My Online Status
Accounts...
Options...
Folders
Outlook Express
Local Folders
Inbox
Outbox
Sent Items
Deleted Ite
Drafts
Contacts
Bui Thi Kim Duyen
Kim Ngoc Van
Go to msn
Bui Thi Kim Duyen
Find a Message... Identities
Tip of the day
If you receive e-mail from multiple accounts, only one is your default account for sending mail.
To send e-mail using an account other than your default, select the other account from the From: field at the top of the new message.
ad Mail messages in your Inbox
Mail message
Read Mail
Newsgroups
Set up a Newsgroups account...
Contacts
Open the Address Book...
Find People...
When Outlook Express starts, go directly to my Inbox.
Previous Next
Configures your accounts.


Internet Accounts
All Mail News Directory Service
Account Type Connection
Add
Remove
Properties
Set as Default
Import...
Export...
Set Order...
Close
Mail...
News...
Directory Service...


Internet Connection Wizard
Your Name
When you send e-mail, your name will appear in the From field of the outgoing message.
Type your name as you would like it to appear.
Display name:
Bui Thi Kim Duyen
For example: John Smith
< Back
Next >
Cancel

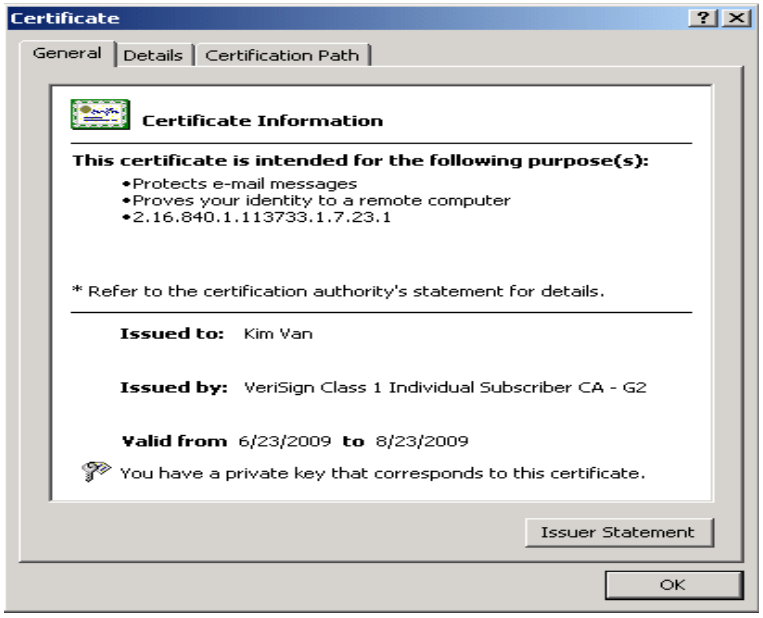

Internet Connection Wizard
Internet E-mail Address
Your e-mail address is the address other people use to send e-mail messages to you.
E-mail address:
duyenbt@mt.gov.vn
For example: someone@microsoft.com
< Back
Next >
Cancel


Internet Connection Wizard
E-mail Server Names
My incoming mail server is a
POP3
server.
Incoming mail (POP3, IMAP or HTTP) server:
mail.mt.gov.vn
An SMTP server is the server that is used for your outgoing e-mail.
Outgoing mail (SMTP) server:
mail.mt.gov.vn
< Back
Next >
Cancel


Internet Connection Wizard
Internet Mail Logon
Type the account name and password your Internet service provider has given you.
Account name:
duyenbt
Password:
Remember password
If your Internet service provider requires you to use Secure Password Authentication (SPA) to access your mail account, select the 'Log On Using Secure Password Authentication (SPA)' check box.
Log on using Secure Password Authentication (SPA)
< Back
Next >
Cancel

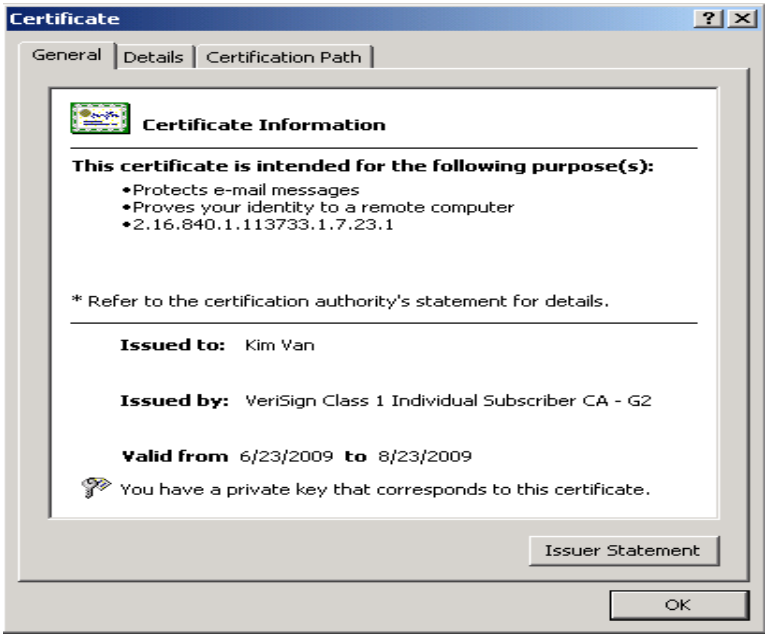
2. Cài đặt chứng chỉ số

2.1. Cài đặt chứng chỉ gốc



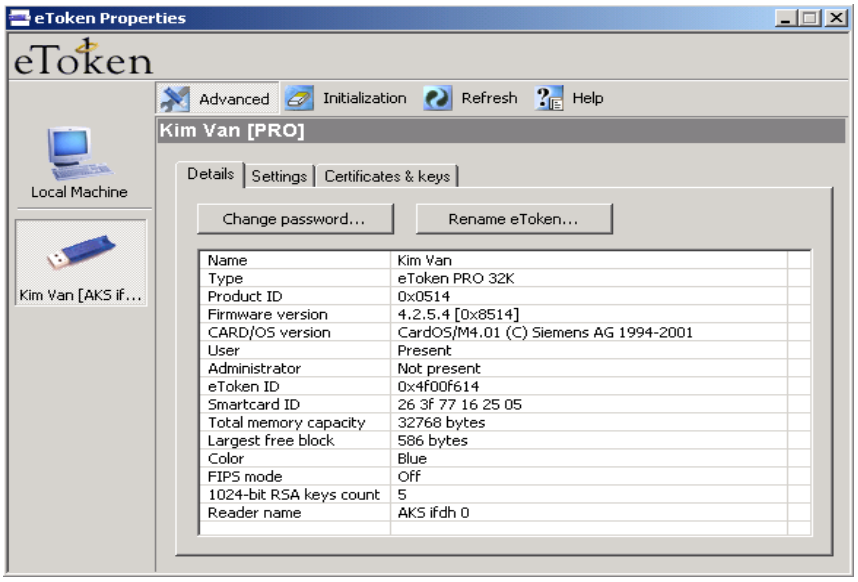
Chứng chỉ gốc

2.2. Cài đặt chứng chỉ được cấp

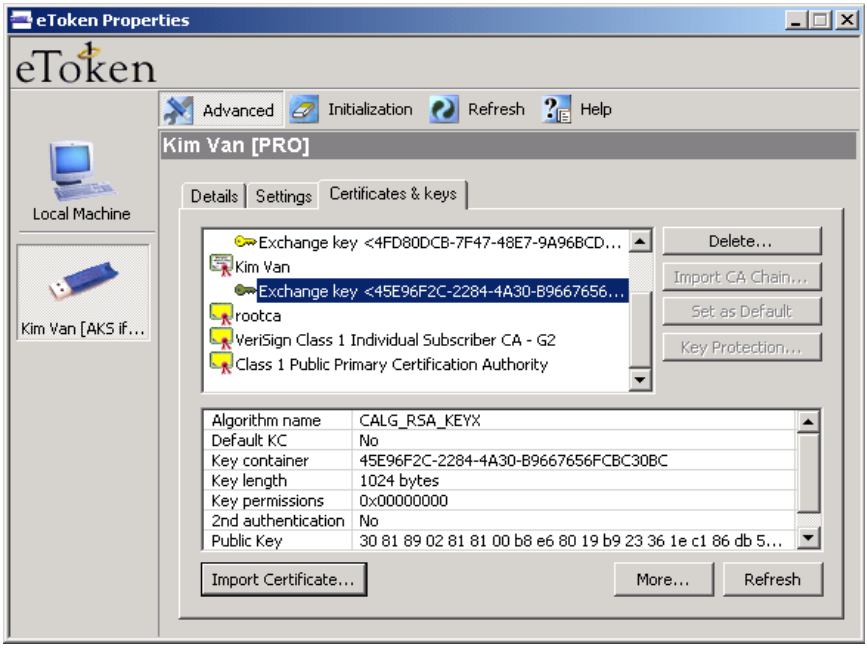


Chứng chỉ được cài trên máy tính

2.3. Cài đặt eToken



Giao diện chính của eToken Pro

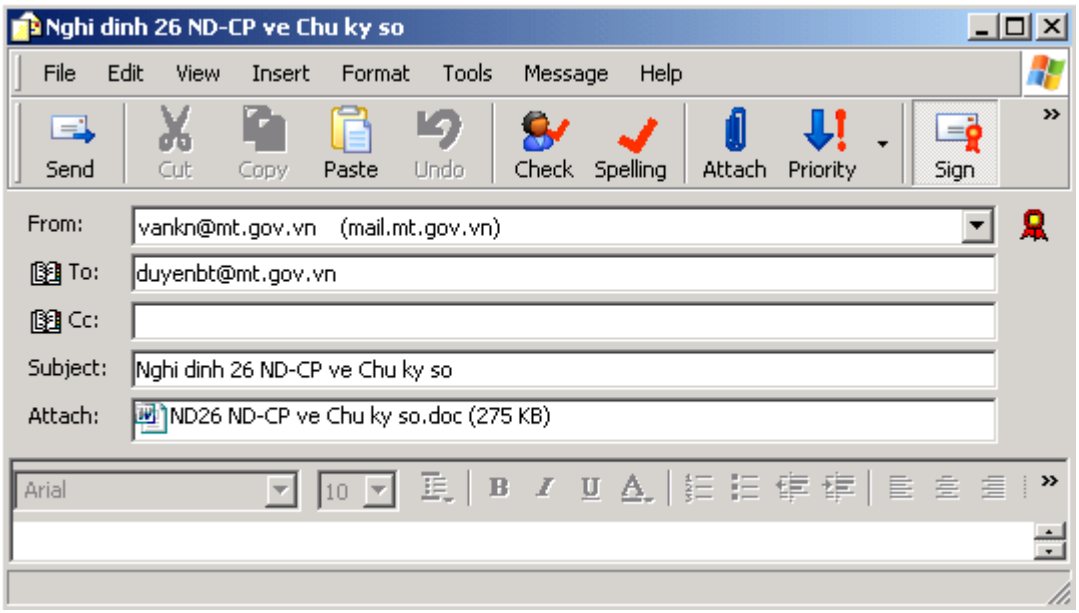


Chứng chỉ của Trung tâm CNTT được lưu trong eToken Pro

3. Thử nghiệm

3.1. Dùng chữ ký số cho Email

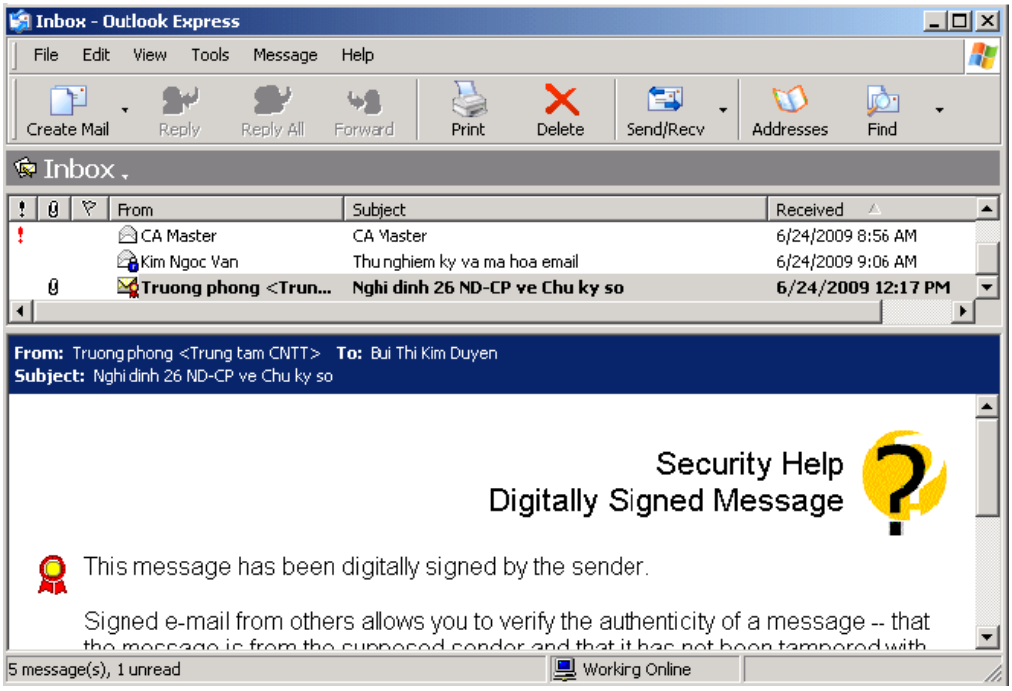
- Trưởng phòng của Trung tâm CNTT ký vào Email (đính kèm công văn Nghị định 26 ND-CP ve Chu ky so) để gửi cho nhân viên.



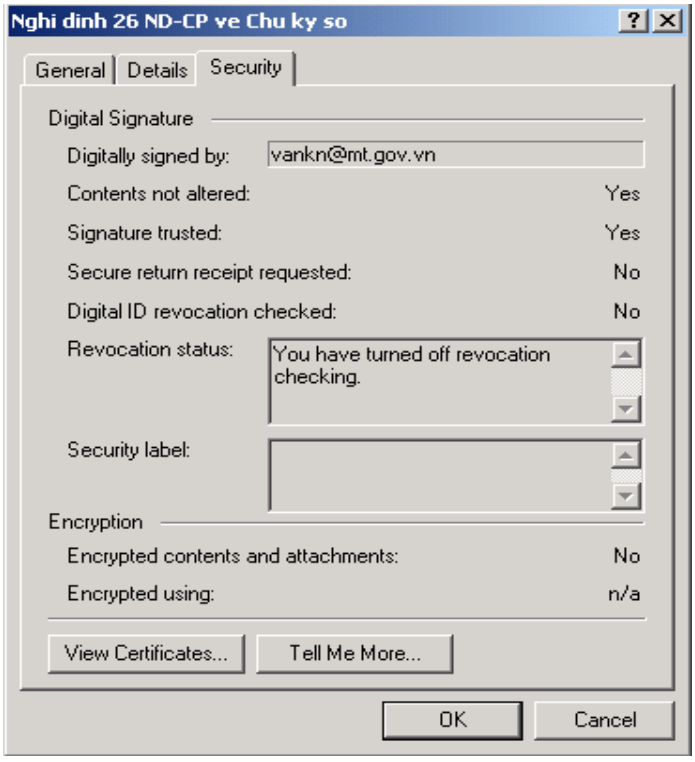
Ký vào Email ( )

Nhập vào mật khẩu để gửi đi

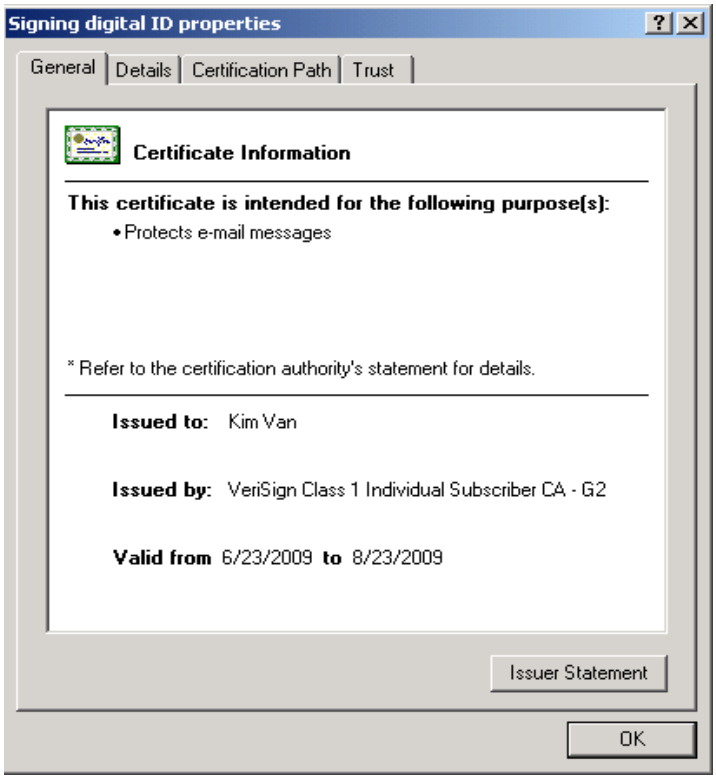
- Nhân viên phòng Trung tâm CNTT nhận Email



Email đã được ký



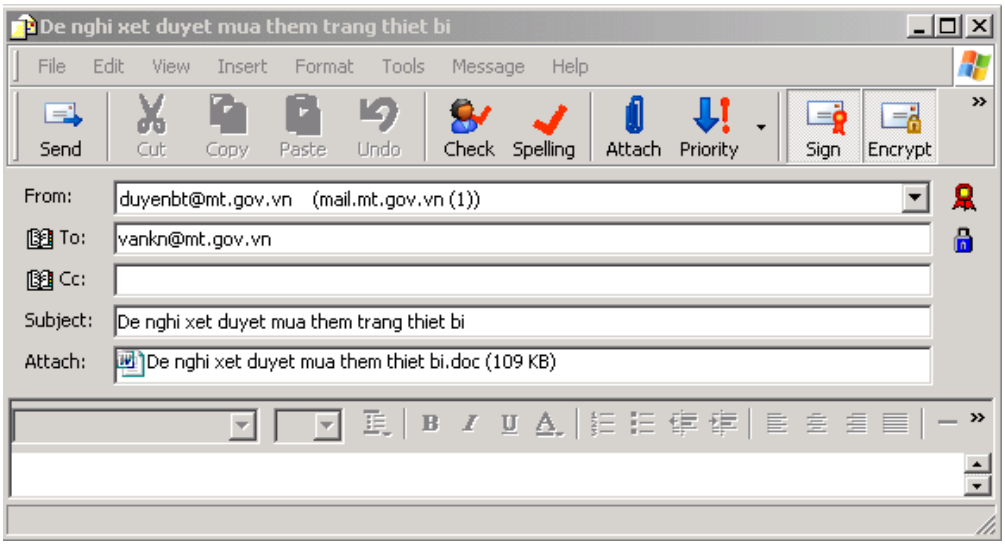
Kiểm tra thông tin bảo mật



Kiểm tra chứng chỉ của bên gửi

3.2. Mã hóa Email

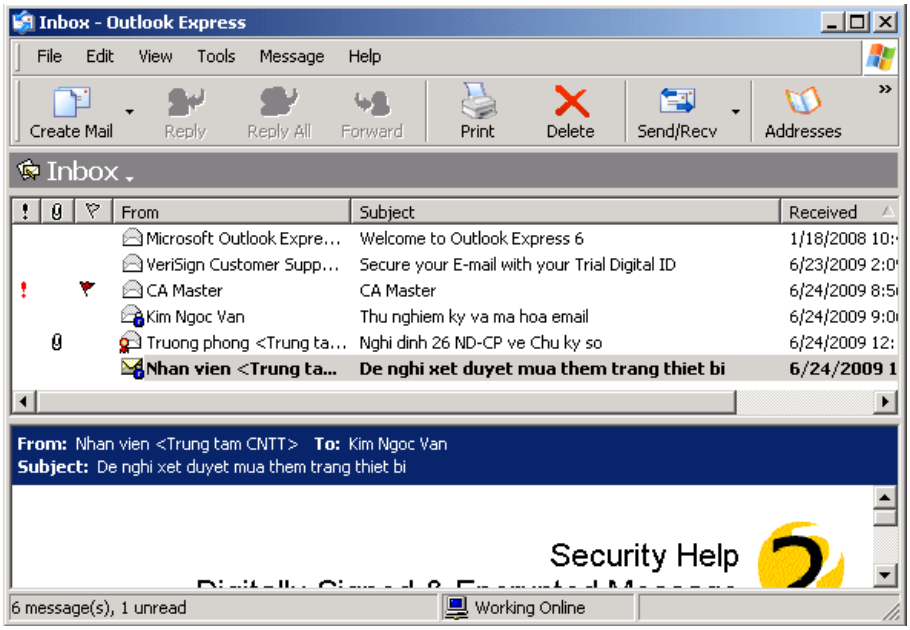
- Nhân viên phòng Trung tâm CNTT ký và mã hoá Email gửi Trưởng phòng Trung tâm Tin học (đính kèm công văn đề nghị mua thêm thiết bị cho phòng)



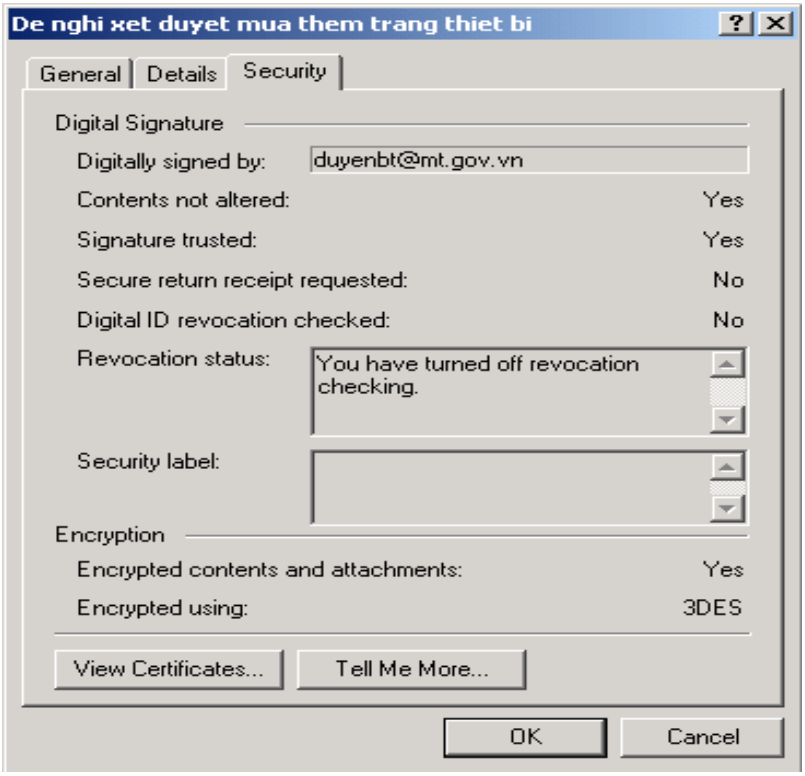
Ký ( ) và mã hoá ( ) Email

Nhập vào mật khẩu để gửi đi

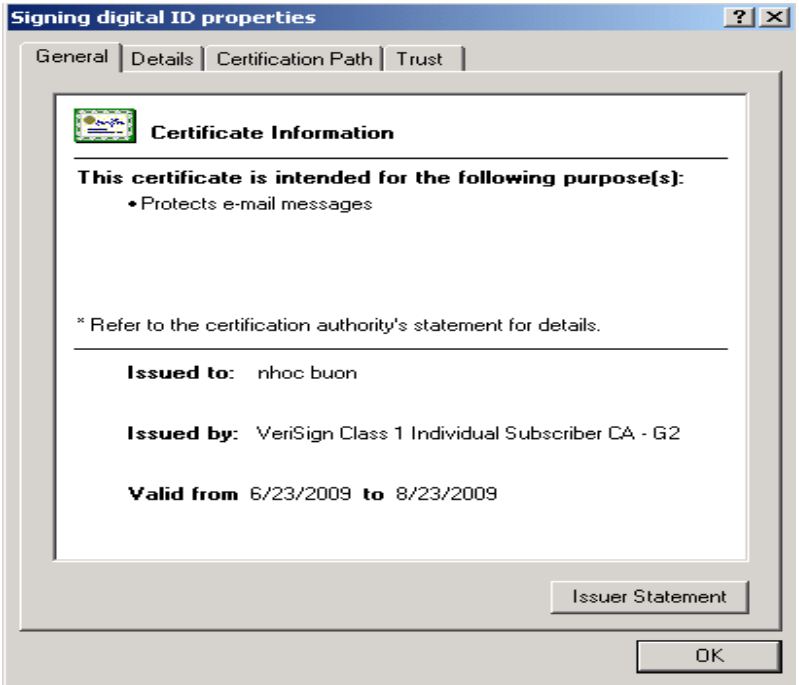
- Trưởng phòng Trung tâm CNTT nhận Email



Email đã được ký và mã hoá

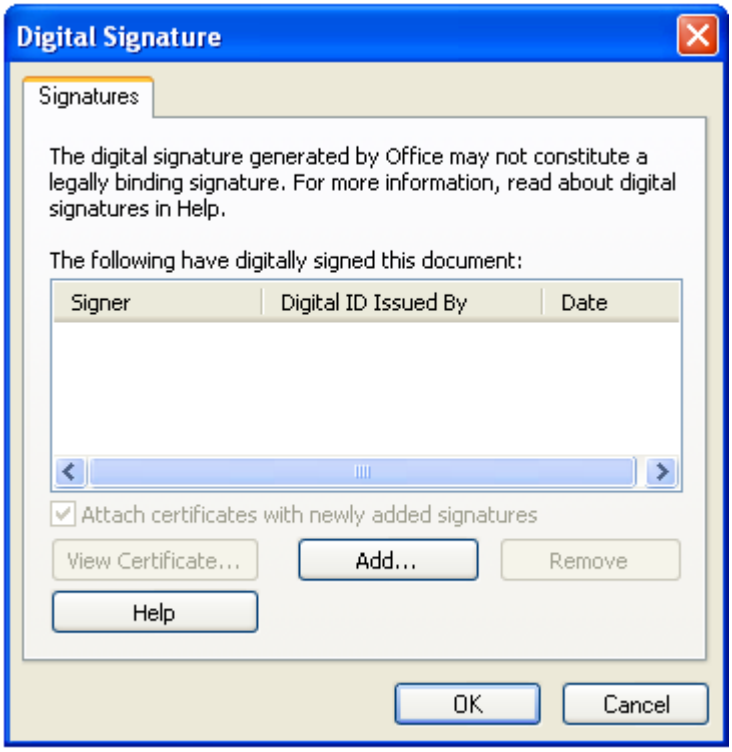


Kiểm tra thông tin bảo mật

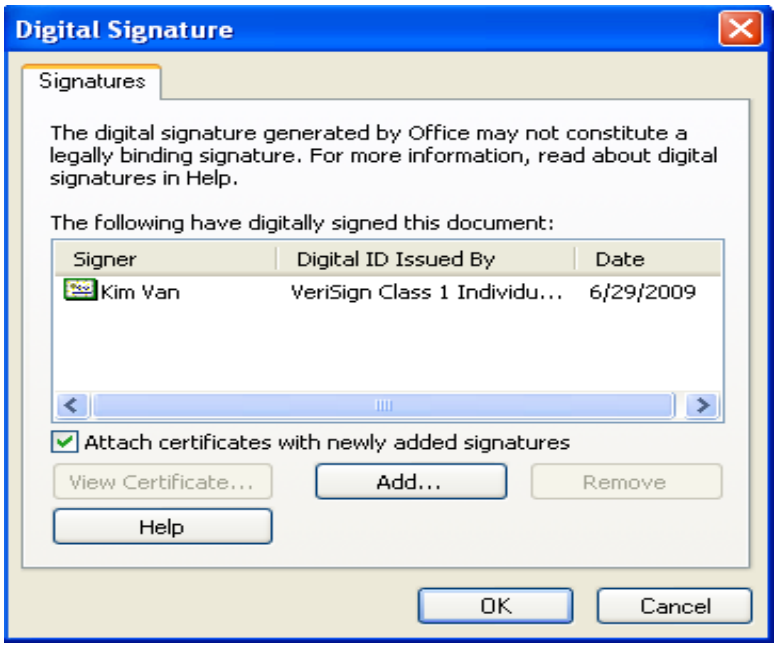


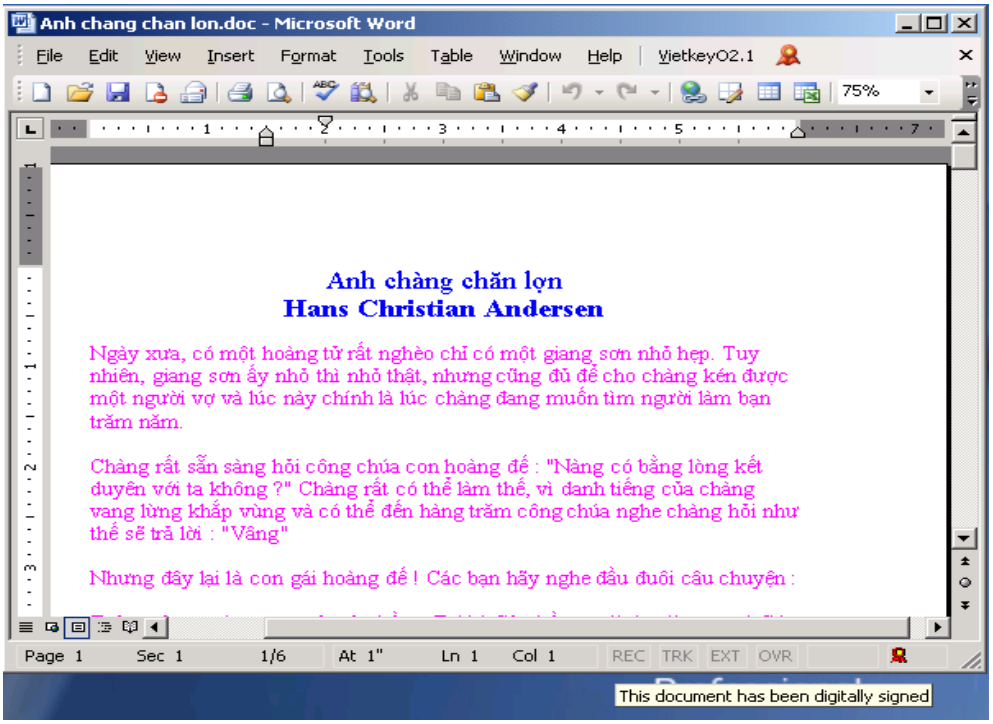
Kiểm tra chứng chỉ của bên gửi

3.3. Ký trực tiếp vào văn bản



Nhập mật khẩu để ký





Văn bản đã được ký ( )

4. Đánh giá kết quả thử nghiệm

4.1. Kết quả thử nghiệm

Như vậy đã hoàn thành việc cài đặt và thử nghiệm sử dụng chữ ký số cho xác thực, bảo mật văn bản và thư điện tử tại Trung tâm CNTT. Nội dung thử nghiệm, gồm:

- Cài đặt chứng chỉ số và hướng dẫn sử dụng chữ ký số cho xác thực, bảo mật văn bản và thư điện tử.

- Trao đổi văn bản sử dụng chữ ký số.

- Gửi/nhận thư điện tử sử dụng chữ ký số, mã hóa.

4.2. Nhận xét, đánh giá

Như đã trình bày ở trên, cùng với quá trình khảo sát và triển khai thử nghiệm tại cơ quan Bộ GTVT, từ đó em đã rút ra một số nhận xét, đánh giá sau đây:

Hiện nay, nhu cầu sử dụng chữ ký số lớn nhất là việc xác thực, bảo mật văn bản khi trao đổi qua mạng (ký vào các văn bản điện tử và mã hóa chúng), bảo đảm thư điện tử trên mạng (ký vào thư điện tử).

Việc lựa chọn nhà cung cấp dịch vụ chứng thực số (CA-Ban cơ yếu Chính phủ) vừa đảm bảo tiết kiệm đầu tư kinh phí, đầu tư nhân lực vừa đáp ứng được các tiêu chuẩn về an toàn bảo mật thông tin.

Việc lựa chọn thiết bị bảo mật khóa riêng eToken Pro USB là phù hợp bởi vì thiết bị này đáp ứng đầy đủ các yêu cầu về bảo mật thông tin, giá thành hợp lý, đã được Ban cơ yếu Chính phủ thử nghiệm tại một số bộ/ngành, tỉnh/thành phố và được khuyến cáo sử dụng.

Cơ sở hạ tầng kỹ thuật CNTT (Hệ thống mạng, máy tính, đường truyền...) của Bộ GTVT hoàn toàn tương thích về công nghệ kỹ thuật và đáp ứng tốt các yêu cầu khi triển khai chữ ký số và các ứng dụng trên nền PKI.

Hệ điều hành, các phần mềm ứng dụng đang được cài đặt và sử dụng tại Bộ đều hỗ trợ cho việc triển khai chữ ký số.

Kỹ năng sử dụng phần mềm ứng dụng văn phòng, sử dụng Internet và hệ thống thư điện tử của cán bộ công chức là tương đối tốt nên việc triển khai sẽ nhanh chóng, thuận lợi.

KẾT LUẬN VÀ ĐỀ XUẤT

Sử dụng chữ ký số, chứng thực số là một giải pháp toàn diện về bảo mật, xác thực và toàn vẹn dữ liệu trong các giao dịch điện tử. Việc ứng dụng chữ ký số, chứng thực số vào thực tiễn sẽ tăng cường hiệu lực, hiệu quả của công tác quản lý điều hành, thúc đẩy cải cách hành chính và quá trình xây dựng Chính phủ điện tử.

Hiện nay, ở nước ta môi trường pháp lý và chính sách cho hoạt động chứng thực số đã được xác lập. Công tác tổ chức, quản lý và cung cấp dịch vụ chứng thực số đang được khẩn trương hoàn thiện. Nhiều bộ/ngành, tỉnh/thành đã và đang triển khai sử dụng chữ ký số phục vụ công tác quản lý và chuyên môn nghiệp vụ.

ĐỀ XUẤT

Từ kết quả thử nghiệm trong phạm vi đề tài, em xin đề xuất với Bộ GTVT việc ứng dụng chữ ký số tại Bộ GTVT như sau:

1. Nội dung: Sử dụng chữ ký số cho xác thực, bảo mật văn bản và thư điện tử trong giao dịch điện tử.

2. Quy mô: - Giai đoạn 1: Triển khai cho khối cơ quan Bộ và các Cục quản lý chuyên ngành.

- Giai đoạn 2: Mở rộng đến các cơ quan, đơn vị thuộc Bộ.

3. Giải pháp:

- Sử dụng chứng chỉ số của CA -Ban cơ yếu Chính phủ**.**
- Sử dụng eToken Pro 32K USB để bảo mật khóa riêng.
- Xây dựng và ban hành Quy chế sử dụng chữ ký số của Bộ GTVT.

TÀI LIỆU THAM KHẢO

1. Duong Anh Duc, Tran Minh Triet, Luong Han Co (2001), Applying the Advanced Encryption Standard and its variants in Secured Electronic-Mail System In Vietnam, Workshop on Applied Cryptology: Coding Theory and Data Integrity, Singapore.

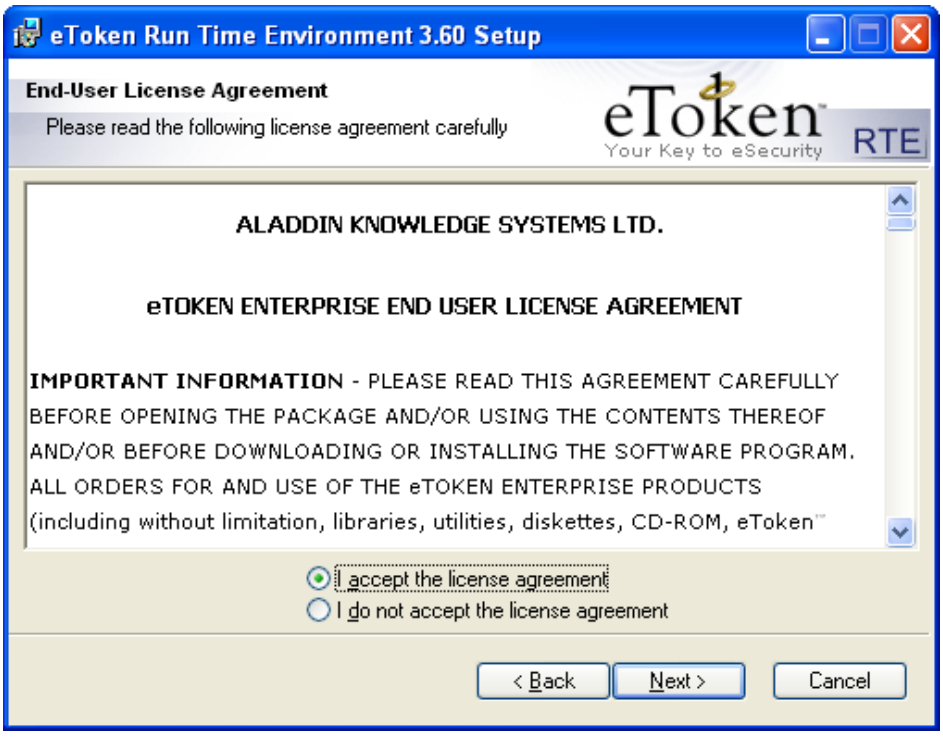
2. Cryptography and computer privacy, H. Feistel (1973), Scientific, American, Vol. 228, No. 5, pp. 15-23.

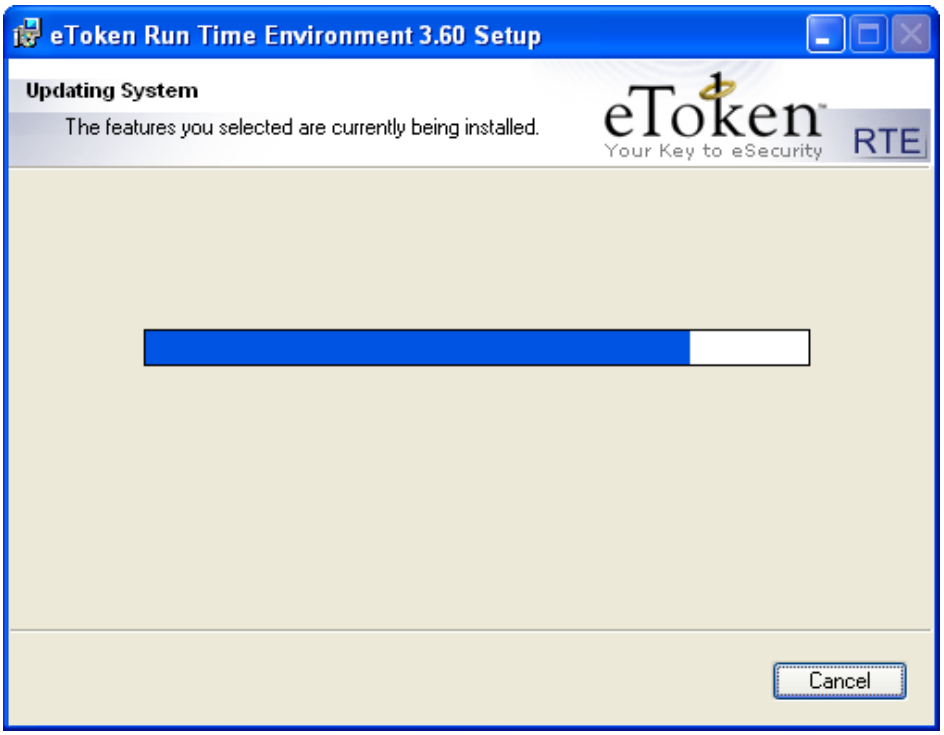
3. PKI Security Soloution for the Enterprice, Kapil Raina, Wiley Publishing, Inc.

PHỤ LỤC

Cài đặt eToken

Run "E:\Chu ky so\Driver_USB_token\RTE_3.60.msi"




eToken Run Time Environment 3.60 Setup
Updating System
The features you selected are currently being installed.
eToken
Your Key to eSecurity
RTE
Cancel


eToken Run Time Environment 3.60 Setup
eToken
Your Key to eSecurity
RTE
eToken Run Time Environment 3.60 has been successfully installed.
Click the Finish button to exit this installation.
< Back
Finish
Cancel