ỦY BAN NHÂN DÂN TỈNH LÂM ĐỒNG

**TRƯỜNG CAO ĐẲNG ĐÀ LẠT**

**GIÁO TRÌNH**

**MÔN HỌC/MÔ ĐUN: AN NINH MẠNG**

**NGÀNH/NGHỀ: THƯƠNG MẠI ĐIỆN TỬ**

**TRÌNH ĐỘ: CAO ĐẲNG**

**(LƯU HÀNH NỘI BỘ)**

**Đà Lạt – Tháng 11/2019**

# TUYÊN BỐ BẢN QUYỀN

Tài liệu này thuộc loại sách giáo trình nên các nguồn thông tin có thể được phép dùng nguyên bản hoặc trích dùng cho các mục đích về đào tạo và tham khảo.

Mọi mục đích khác mang tính lệch lạc hoặc sử dụng với mục đích kinh doanh thiếu lành mạnh sẽ bị nghiêm cấm.

# LỜI GIỚI THIỆU

**Vài nét về xuất xứ giáo trình:**

Giáo trình này được viết theo Kế hoạch số 06/KH-CĐNĐL ngày 5 tháng 1 năm 2019 của Trường Cao đẳng nghề Đà Lạt về việc triển khai xây dựng chương trình đào tạo theo Luật Giáo dục nghề nghiệp để làm tài liệu dạy nghề trình độ cao đẳng.

**Quá trình biên soạn:**

Trên cơ sở tham khảo các giáo trình, tài liệu về môn học An ninh mạng và chữ ký số, kết hợp với thực tế nghề nghiệp của nghề Thương mại điện tử, giáo trình này được biên soạn có sự tham gia tích cực của các giáo viên có kinh nghiệm cùng với những ý kiến đóng góp quý báu của các chuyên gia về lĩnh An ninh mạng và chữ ký số.

**Mối quan hệ của tài liệu với chương trình, mô đun/môn học:**

Căn cứ vào chương trình đào tạo nghề Thương mại điện tử cung cấp cho người học những kiến thức cơ bản về An ninh mạng và chữ ký số trong xu thế hội nhập toàn cầu, giúp người học có cái nhìn mới, hiểu an ninh mạng như một nghề chuyên môn và có vai trò rất quan trọng để nâng cao lợi thế cạnh tranh của doanh nghiệp trong giai đoạn phát triển kinh tế hiện nay. Môn học giới thiệu các khái niệm, định nghĩa, quan điểm, giá trị, mục đích, phương pháp, và các kỹ thuật, xây dựng hệ thống An ninh mạng và chữ ký số để người học có được cái nhìn tổng quát trước khi đi vào chuyên sâu.

Giáo trình được biên soạn trên cơ sở các văn bản quy định của Nhà nước và tham khảo nhiều tài liệu liên quan có giá trị. Song chắc hẳn quá trình biên soạn không tránh khỏi những thiếu sót nhất định. Ban biên soạn mong muốn và thực sự cảm ơn những ý kiến nhận xét, đánh giá của các chuyên gia, các thầy cô đóng góp cho việc chỉnh sửa để giáo trình ngày một hoàn thiện hơn.

*Lâm Đồng, ngày……tháng……năm………*

**Chủ biên**

Mục lục

[TUYÊN BỐ BẢN QUYỀN 2](#_Toc54008242)

[LỜI GIỚI THIỆU 3](#_Toc54008243)

[CHƯƠNG 1: AN NINH MẠNG VÀ AN TOÀN DỮ LIỆU TRONG THƯƠNG MẠI ĐIỆN TỬ 7](#_Toc54008244)

[1. Các nguy cơ ảnh hưởng tới an ninh mạng và dữ liệu trong TMĐT 7](#_Toc54008245)

[1.1. Vấn đề an ninh trong thương mại điện tử 7](#_Toc54008246)

[1.2. Các khía cạnh của an ninh thương mại điện tử 9](#_Toc54008247)

[1.2.1. Những quan tâm về vấn đề an ninh trong Thương mại điện tử 9](#_Toc54008248)

[1.2.2. Các khía cạnh của an ninh trong Thương mại điện tử 9](#_Toc54008249)

[1.2.3. Những nguy cơ đe dọa an ninh mạng và dữ liệu trong Thương mại điện tử 11](#_Toc54008250)

[2. Các phương pháp tấn công an ninh mạng và dữ liệu trong TMĐT 11](#_Toc54008251)

[3. An toàn dữ liệu trong thanh toán điện tử 3.1. Đặt vấn đề 13](#_Toc54008252)

[3.2. Yêu cầu an toàn dữ liệu cho các chủ thể tham gia thương mại điện tử 14](#_Toc54008253)

[3.3. Các giải pháp an toàn dữ liệu trong thương mại điện tử 14](#_Toc54008254)

[3.4. Một số khuyến nghị về an toàn dữ liệu trong thanh toán điện tử 15](#_Toc54008255)

[4. Các phương pháp đảm bảo an ninh mạng và dữ liệu trong TMĐT 17](#_Toc54008256)

[4.1. Xây dựng kế hoạch đảm bảo an ninh mạng và dữ liệu 17](#_Toc54008257)

[4.2. Các biện pháp đảm bảo an ninh mạng và dữ liệu 18](#_Toc54008258)

[CHƯƠNG 2: CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI VÀ CHỨNG CHỈ ĐIỆN TỬ 21](#_Toc54008259)

[2.Mật mã đối xứng 21](#_Toc54008260)

[1.1. Mật mã học là gì 21](#_Toc54008261)

[1.2. Mật mã đối xứng 21](#_Toc54008262)

[1.2.1. Mật mã đối xứng là gì 21](#_Toc54008263)

[1.2.2. Thuật toán mật mã 22](#_Toc54008264)

[1.3. Ưu/ Nhược điểm và phạm vi sử dụng của mật mã đối xứng. 24](#_Toc54008265)

[2. Mật mã khóa công khai 25](#_Toc54008266)

[2.1 Khái niệm chung 25](#_Toc54008267)

[2.2 Hạ tầng mật mã khóa công khai 26](#_Toc54008268)

[2.3.1. Hệ mật mã ElGamal 28](#_Toc54008269)

[2.3.2. Hệ mật mã “xếp ba lô” Merkle-Hellman 29](#_Toc54008270)

[2.3.3. Hệ mật mã đường cong Elliptic 30](#_Toc54008271)

[2.4 Các ứng dụng hệ thống mã công khai 30](#_Toc54008272)

[2.4.1.Công cụ mã hoá 30](#_Toc54008273)

[2.4.2. Hàm băm mật mã học 30](#_Toc54008274)

[2.4.2.Cấp phát chứng thực số. 31](#_Toc54008275)

[3. Chữ ký số 33](#_Toc54008276)

[3.1 Yêu cầu chữ ký số 33](#_Toc54008277)

[3.2 Chứng thực điện tử 34](#_Toc54008278)

[CHƯƠNG 3: HỆ THỐNG CẤP PHÁT VÀ QUẢN LÝ CHỨNG CHỈ SỐ 36](#_Toc54008279)

[1. Mô hình hoạt động của hệ thống chứng chỉ số 36](#_Toc54008280)

[2. Chu trình cấp phát chứng chỉ số 2.1. Chuẩn bị hồ sơ 40](#_Toc54008281)

[2.2. Xác thực hồ sơ đăng ký 40](#_Toc54008282)

[2.3. Phát hành chứng thư số 41](#_Toc54008283)

[2.4. Chấp nhận, công bố và thông báo chứng thư số 41](#_Toc54008284)

[3. Các thao tác với chứng chỉ: 41](#_Toc54008285)

[3.1. Phần mềm SmartSign 41](#_Toc54008286)

[3.2. Môi trường thực hiện 41](#_Toc54008287)

[3.3 Hướng dẫn cài chương trình SmartSign 41](#_Toc54008288)

[3.4 Hướng dẫn cài đặt java (Nếu máy có Java thích hợp vui lòng bỏ qua bước này) 45](#_Toc54008289)

[3.5 Hướng dẫn gửi yêu cầu cập nhật chữ ký số 47](#_Toc54008290)

[3.7 Hướng dẫn cập nhật chữ ký số cách 2 sử dụng Java 54](#_Toc54008291)

[3.8 Hướng dẫn cập nhật chữ ký số cách 2 sử dụng Java 59](#_Toc54008292)

[3.9 Hướng dẫn bật ActiceX cho trình duyệt IE 64](#_Toc54008293)

# CHƯƠNG 1: AN NINH MẠNG VÀ AN TOÀN DỮ LIỆU TRONG THƯƠNG MẠI ĐIỆN TỬ

Mục tiêu:

Học xong bài này người học sẽ có khả năng:

- Đoán biết được những nguy cơ mất an toàn dữ liệu;

- Đoán biết các hình thức tấn công làm mất an toàn dữ liệu;

- Đưa ra được các phương pháp hữu hiệu nhất để phòng tránh mất an toàn dữ liệu trong TMĐT.

# 

## 1. Các nguy cơ ảnh hưởng tới an ninh mạng và dữ liệu trong TMĐT

## 1.1. Vấn đề an ninh trong thương mại điện tử

Ngày nay, vấn đề an ninh cho thương mại điện tử đã không còn là vấn đề mới mẻ. Các bằng chứng thu thập được từ hàng loạt các cuộc điều tra tiếp tục cho thấy những vụ tấn công qua mạng hoặc tội phạm mạng trong thế giới thương mại điện tử đang gia tăng mạnh. Theo báo cáo của Viện An ninh Máy tính (CSI) và FBI (Mỹ) về thực trạng các vụ tấn công vào hoạt động thương mại điện tử năm 2002:

- Các tổ chức tiếp tục phải chịu những cuộc tấn công qua mạng từ cả bên trong lẫn bên ngoài tổ chức đó. Trong những tổ chức được điều tra, khoảng 90% cho rằng họ đã thấy có sự xâm phạm an ninh trong vòng 12 tháng gần nhất.

- Các hình thức tấn công qua mạng mà các tổ chức phải chịu rất khác nhau. Ví dụ, 85% bị virus tấn công, 78% bị sử dụng trái phép mạng internet, 40% là nạn nhân của tấn công từ chối dịch vụ (DoS)

- Thiệt hại về tài chính qua các vụ tấn công qua mạng là rất lớn: 80% các tổ chức được điều tra trả lời rằng họ đã phải chịu thiệt hại về tài chính do hàng loạt các kiểu tấn công khác nhau qua mạng. Tổng thiệt hại của những tổ chức này khoảng 455 triệu đôla Mỹ.

- Cần phải sử dụng nhiều biện pháp đồng thời để nâng cao khả năng phòng chống các vụ tấn công qua mạng. Hầu hết các tổ chức được điều tra đều trả lời rằng họ đã sử dụng các thiết bị bảo vệ an ninh, tường lửa, quản lý việc truy cập hệ thống. Tuy nhiên, không có tổ chức nào tin rằng hệ thống thương mại điện tử của mình tuyệt đối an toàn.  
Ngoài ra, theo báo cáo của Trung tâm ứng cứu khẩn cấp máy tính (CERT) của đại học Carnegie Mellon (Mỹ), số lượng nạn nhân của những vụ tấn công qua mạng tăng từ 22.000 vụ năm 2000 lên đến 82.000 vụ năm 2002, và con số này cao gấp 20 lần so với con số nạn nhân năm 1998. Để đối phó với tình trạng mất an ninh qua mạng, ở hầu hết các nước đã thành lập những trung tâm an ninh mạng mang tính quốc gia, như Trung tâm bảo về Cơ sở hạ tầng quốc gia (NIPC) trực thuộc FBI (Mỹ), có chức năng ngăn chặn và bảo vệ hạ tầng quốc gia về viễn thông, năng lượng, giao thông vận tải, ngân hàng và tài chính, các hoạt động cấp cứu và các hoạt động khác của chính phủ. Tại Việt Nam cũng đã thành lập Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VnCERT) vào tháng 12/2005.Những trang web thương mại điện tử nào dễ bị tấn công?

Giả sử doanh nghiệp bạn quyết định xây dựng một trang web B2B để phục vụ khách hàng và các nhà cung cấp. Vì trang web này không phải là trang web công cộng, những người sẽ biết về trang web này chỉ là chính doanh nghiệp bạn, các nhà cung cấp và các đối tác kinh doanh. Do đó, bạn cho rằng không cần thiết phải xây dựng những giải pháp mạnh cho vấn đề bảo đảm an ninh. Như vậy là sai lầm! Với những ưu thế của các công cụ rà soát tự động, chỉ cần sau một thời gian tính bằng ngày, các hacker đã tìm ra trang web của doanh nghiệp bạn. Sau khi đã tìm ra, nếu trang web của bạn được đánh giá là dễ bị tấn công, sau thời gian vài giờ hoặc thậm chí vài phút, các hacker đã có thể xâm nhập và chiếm quyền điều khiển website của bạn. Một trang web dù không được quảng cáo, hình thức không hấp dẫn hay không được ai biết tới, bất kể trang web thương mại điện tử nào cũng cần phải tính tới giải pháp an ninh. Các trang web này cần được xem xét kỹ càng những yêu cầu về an ninh và áp dụng các biện pháp hữu hiệu để bảo vệ trang web chống lại những hiểm họa tấn công từ trên mạng.  
Những website càng hoạt động tốt, càng nổi tiếng thì càng có khả năng bị tấn công. Có nhiều khả năng, một phần có thể do cạnh tranh, một phần do các hacker muốn chứng tỏ khả năng của mình bằng cách tấn công vào những website thành công vốn có hệ thống bảo mật kiên cố. Đặc biệt, những website có giao dịch điện tử trực tuyến, có liên quan đến các thông tin nhạy cảm như thẻ tín dụng, thông tin khách hàng, các cơ sở dữ liệu phục vụ kinh doanh...

Những nhóm rủi ro chính doanh nghiệp có thể gặp phải trong thương mại điện tử?  
Rủi ro trong thương mại điện tử với những hình thái muôn màu muôn vẻ, tuy nhiên tựuchung lại có thể chia thành bốn nhóm cơ bản sau:

- Nhóm rủi ro dữ liệu

- Nhóm rủi ro về công nghệ

- Nhóm rủi ro về thủ tục quy trình giao dịch của tổ chức

- Nhóm rủi ro về luật pháp và các tiêu chuẩn công nghiệp

Các nhóm rủi ro này không hoàn toàn độc lập với nhau mà đôi khi chúng đồng thời cùng xảy đến và không xác định tách bạch rõ ràng được. Nếu các rủi ro này đồng thời xảy ra, thiệt hại đối với tổ chức có thể rất lớn cả về uy tín, thời gian và chi phí đầu tư để khôi phục hoạt động trở lại bình thường.

Các loại tội phạm trong thương mại điện tử rất tinh vi trong khi việc giảm các rủi ro thương mại điện tử là một quá trình phức tạp liên quan đến những đạo luật mới, công nghệ mới, nhiều thủ tục và các chính sách tổ chức.

Thương mại điện tử đã hấp dẫn các tin tặc khi khách hàng sử dụng thẻ để mua hàng hoặc dịch vụ trực tuyến, dùng email để thực hiện các giao dịch kinh tế.

Các yếu tố làm số lượng các tấn công trên mạng phát triển:

+ Các hệ thống an ninh luôn tồn tại các điểm yếu.

+ Vấn đề an ninh và dễ dàng sử dụng.

+ Vấn đề an ninh thường xuất hiện sau khi có sức ép thị trường.

+ Vấn đề an ninh của thương mại điện tử còn phụ thuộc vào an ninh của internet, số lượng các trang web của các trường, thư viện, cá nhân…

## 1.2. Các khía cạnh của an ninh thương mại điện tử

## 1.2.1. Những quan tâm về vấn đề an ninh trong Thương mại điện tử

- Phía người mua: Bằng cách nào biết chắc Website do một công ty hợp pháp quản lý và sở hữu; Biết chắc trang web không chứa các đoạn mã nguy hiểm hoặc các nội dung không lành mạnh; Biết chắc rằng web server sẽ không cung cấp các thông tin của người sử dụng cho một người khác.

- Phía công ty: Bằng cách nào biết chắc rằng người sử dụng sẽ không xâm nhập vào trang web để thay đổi các trang và nội dung trên đó; Người sử dụng sẽ không phá hoại website để những người khác không thể sử dụng được.

- Từ phía cả công ty và ngƣời sử dụng: Bằng cách nào họ có thể biết chắc rằng: Đường truyền sẽ không bị người thứ ba theo dõi; Các thông tin được lưu chuyển giữa hai bên sẽ không bị thay đổi.

## 1.2.2. Các khía cạnh của an ninh trong Thương mại điện tử

Các giao dịch điện tử nói chung là giao dịch trong môi trường mở, giao dịch trên Internet, giao dịch xuyên quốc gia. Trong các quá trình trao đổi thông tin đó các đối tác thường là không “mặt đối mặt” để có thể nhận diện ra nhau. Vì thế rất khó để có thể thực hiện các yêu cầu để trao đổi thông tin được xem là những nguyên lí cơ bản của bảo mật thông tin.

- Tính toàn vẹn: trong quá trình truyền tin, có thể vì lý do khách quan của môi trường, nhất là do sự xâm nhập phá hoại của ké thứ ba, nội dung của thông tin ban đầu chứa trong vật mang tin có thể bị mất mát hay bị thay đổi. Nguyên nhân này không yêu cầu đến mức phải đảm bảo rằng thông tin không bị thay đổi trong quá trình truyền tin, nhưng phải đảm bảo mỗi khi thông tin bị thay đổi là người nhận (và cả người gửi) đều phát hiện được.

- Chống phủ định: Đòi hỏi rằng khi quá trình truyền tin kết thúc, A đã gửi cho B một thông tin và B đã nhận thông tin thì A không thể chối bỏ rằng thông tin đó không do mình gửi (hoặc mình không gửi tin), mặt khác B cũng không chối bỏ rằng mình chưa nhận được.

- Tính xác thực: Trong quá trình truyền tin, người nhận tin và có khi cả người gửi tin có biện pháp thể chứng minh với đối tác rằng “họ chính là họ” chứ không phải là người thứ ba nào khác. Chẳng hạn khi bạn nhận được một lá thư bảo đảm tại Bưu điện thì bạn phải có cách nào chứng minh được rằng bạn có quyền nhận lá thư đó, bằng cách xuất trình chứng minh nhân dân hoặc giấy giới thiệu có giá trị nào đó. Sự xác thực này là xác thực một chiều (one-way authenication): người nhận được xác thực mình với người gửi, nhưng cũng có những trường hợp đòi hỏi xác thực hai chiều (mutual authenication): người nhận với người gửi và ngược lại.

- Tính đáng tin cậy: Khi chia sẻ một bí mật cho một người, bạn phải tin tưởng vào khả năng bảo vệ bí mật của người đó. Nhưng điều khó khăn ở đây là: tin tưởng là một phạm trù có tính tâm lý, xã hội không có đặc trưng của một loại quan hệ toán học nào với tính không phản xạ (Một người có luôn luôn tin tưởng vào chính mình không?), tính không đối xứng (A tin vào B nhưng liệu B có tin tưởng vào A không?), tính không bắc cầu (A tin B, B tin C, nhưng không đảm bảo là A tin C). Chính vì vậy trong các vấn đề bảo mật nhiều khi chúng ta không thể hoàn toàn dùng các phương pháp suy luận logic thông thường mà phải chú ý đến việc tuân thủ các nguyên lý bảo mật thông tin.

- Tính riêng tư: Giả sử A gửi một “vật mang tin” đến cho B. Nguyên lý đầu tiên của bảo vật thông tin là phải đảm bảo tính bí mật và tính riêng tư cho quá trình truyền tin. Điều này nghĩa là việc truyền tin phải đảm bảo rằng chỉ có hai đối tác A và B khi tiếp cận vật mang tin mới nắm bắt được nội dung thông tind được truyền. Trong quá trình truyền tin, nếu có kẻ thứ ba C có thể tiếp cận được vật mang tin thì phải đảm bảo rằng kẻ đó vẫn không thể nắm bắt được, không thể hiểu được nội dung “thực sự” của thông tin chứa trong vật mang tin đó

## 1.2.3. Những nguy cơ đe dọa an ninh mạng và dữ liệu trong Thương mại điện tử

Các đoạn mã nguy hiểm (malicious code): gồm nhiều mối đe dọa khác nhau như các loại virus, worm.

Tin tặc (hacker) và các chương trình phá hoại (cybervandalism)

Gian lận thẻ tín dụng

Sự lừa đảo: Tin tặc sử dụng các địa chỉ thư điện tử giả hoặc mạo danh một người nào đó nhằm thực hiện những hành động phi pháp.

Sự khước từ dịch vụ: là việc các hacker sử dụng những giao thông vô ích làm tràn ngập hoặc tắc nghẽn mạng truyền thông, hoặc sử dụng số lượng lớn máy tính tấn công vào một mạng. Nghe trộm, giám sát sự di chuyển của thông tin trên mạng. Xem lén thư điện tử là sử dụng các đoạn mã ẩn bí mật gắn vào một thông điệp thư điện tử, cho phép người xem lén có thể giám sát toàn bộ các thông điệp chuyển tiếp được gửi đi với thông điệp ban đầu.

## 2. Các phương pháp tấn công an ninh mạng và dữ liệu trong TMĐT

- Virus tấn công vào thương mại điện tử thường gồm 3 loại chính: virus ảnh hưởng tới các tệp (file) chương trình (gắn liền với những file chương trình, thường là.COM hoặc.EXE), virus ảnh hưởng tới hệ thống (đĩa cứng hoặc đĩa khởi động), và virus macro. Virus macro là loại virus phổ biến nhất, chiếm từ 75% đến 80% trong tổng số các virus được phát hiện.

Đây là loại virus đặc biệt chỉ nhiễm vào các tệp ứng dụng soạn thảo, chẳng hạn như các tệp ứng dụng của MS Word, Excel và Power Point. Khi người sử dụng mở các tài liệu bị nhiễm virus trong các chương trình ứng dụng, virus này sẽ tự tạo ra các bản sao và nhiễm vào các tệp chứa đựng các khuôn mẫu của ứng dụng, để từ đó lây sang các tài liệu khác. Các loại virus có thể gây ra những tác hại nghiêm trọng, đe doạ tính toàn vẹn và khả năng hoạt động liên tục, thay đổi các chức năng, thay đổi các nội dung dữ liệu hoặc đôi khi làm ngưng trệ toàn bộ hoạt động của nhiều hệ thống trong đó có các website thương mại điện tử. Nó được đánh giá là mối đe doạ lớn nhất đối với an toàn của các giao dịch thương mại điện tử hiện nay.

- Tin tặc (hacker) và các chương trình phá hoại (cybervandalism): Tin tặc hay tội phạm máy tính là thuật ngữ dùng để chỉ những người truy cập trái phép vào một website, một cơ sở dữ liệu hay hệ thống thông tin. Thực chất mục tiêu của các hacker rất đa dạng. Có thể là hệ thống dữ liệu của các website thương mại điện tử, hoặc với ý đồ nguy hiểm hơn chúng có thể sử dụng các chương trình phá hoại (cybervandalism) nhằm gây ra các sự cố, làm mất uy tín hoặc phá huỷ website trên phạm vi toàn cầu. Thí dụ như ngày 1-4-2001, tin tặc đã sử dụng chương trình phá hoại tấn công vào các máy chủ có sử dụng phần mềm Internet Information Server (IIS) của Microsoft nhằm làm giảm uy tín của phần mềm này và rất nhiều nạn nhân như hãng hoạt hình Walt Disney, Nhật báo phố Wall …đã phải gánh chịu hậu quả cả về tài chính và uy tín.

- Rủi ro về gian lận thẻ tín dụng: Trong thương mại điện tử, các hành vi gian lận thẻ tín dụng xảy ra đa dạng và phức tạp hơn nhiều so với thương mại truyền thống. Nếu như trong thương mại truyền thống, việc mất thẻ hoặc thẻ bị đánh cắp là mối đe doạ lớn nhất đối với khách hàng thì trong thương mại điện tử mối đe doạ lớn nhất là bị “mất” (hay bị lộ) các thông tin liên quan đến thẻ tín dụng hoặc các thông tin giao dịch sử dụng thẻ tín dụng trong quá trình thực hiện các giao dịch mua sắm qua mạng và các thiết bị điện tử. Các tệp chứa dữ liệu thẻ tín dụng của khách hàng thường là những mục tiêu hấp dẫn đối với tin tặc khi tấn công vào website thương mại điện tử. Hơn thế, những tên tội phạm có thể đột nhập vào các cơ sở dữ liệu của website thương mại điện tử để lấy cắp các thông tin của khách hàng như tên, địa chỉ, điện thoại… với những thông tin này chúng có thể mạo danh khách hàng thiết lập các khoản tín dụng mới nhằm phục vụ những mục đích phi pháp.

- Tấn công từ chối dịch vụ: Tấn công từ chối dịch vụ (DOS - Denial Of Service attack, DDOS – Distributed DOS hay DR DOS) là kiểu tấn công khiến một hệ thống máy tính hoặc một mạng bị quá tải, dẫn tới không thể cung cấp dịch vụ hoặc phải dừng hoạt động. Sơ khai nhất là hình thức DoS (Denial of Service), lợi dụng sự yếu kém của giao thức TCP, tiếp đến là DdoS (Distributed Denial of Service) - tấn công từ chối dịch vụ phân tán, và gần đây là DRDoS

- Tấn công theo phương pháp phản xạ phân tán (Distributed Reflection Denial of Service). Những cuộc tấn công DoS có thể là nguyên nhân khiến cho mạng máy tính ngừng hoạt động và trong thời gian đó, người sử dụng sẽ không thể truy cập vào các website thương mại điện tử. Những tấn công này cũng đồng nghĩa với những khoản chi phí rất lớn vì trong thời gian website ngừng hoạt động, khách hàng không thể thực hiện các giao dịch mua bán. Đồng thời, sự gián đoạn hoạt động này sẽ ảnh hưởng đến uy tín và tiếng tăm của doanh nghiệp, những điều không dễ dàng gì lấy lại được. Mặc dù những cuộc tấn công này không phá huỷ thông tin hay truy cập vào những vùng cấm của máy chủ nhưng tạo ra phiền toái, gây trở ngại cho hoạt động của nhiều doanh nghiệp. Vụ tấn công DOS điển hình đầu tiên xảy ra vào tháng 2-2000, các hoạt động tấn công liên tục khiến hàng loạt website trên thế giới ngừng hoạt động trong nhiều giờ, trong đó có những website hàng đầu như: eBay ngừng hoạt động trong 5 giờ, Amazon gần 4 giờ, CNN gần 3.5 giờ, Etrade gần 3 giờ, Yahoo và Buy.com và ZDNet cũng ngừng hoạt động từ 3 đến 4 giờ.Ngay cả người khổng lồ Microsoft cũng đã từng phải gánh chịu hậu quả của những cuộc tấn công này. Ở Việt Nam, cũng đã có rất nhiều doanh nghiệp bị tấn công dưới hình thức này.

- Kẻ trộm trên mạng (sniffer): Kẻ trộm trên mạng (sniffer) là một dạng của chương trình theo dõi, nghe trộm, giám sát sự di chuyển của thông tin trên mạng. Khi sử dụng vào những mục đích hợp pháp, nó có thể giúp phát hiện ra những yếu điểm của mạng, nhưng ngược lại, nếu sử dụng vào các mục đích phi pháp, các phần mềm ứng dụng này sẽ trở thành các mối hiểm hoạ lớn và rất khó có thể phát hiện. Kẻ trộm sử dụng các phần mềm này nhằm lấy cắp các thông tin có giá trị như thư điện tử, dữ liệu kinh doanh của các doanh nghiệp, các báo cáo mật…từ bất cử nơi nào trên mạng.Xem lén thư điện tử là một dạng mới của hành vi trộm cắp trên mạng. Kỹ thuật xem lén thư điện tử sử dụng một đoạn mã (ẩn) bí mật gắn vào thông điệp thư điện tử, cho phép người nào đó có thể giám sát toàn bộ các thông điệp chuyển tiếp được gửi đi cùng với thông điệp ban đầu. Chẳng hạn một nhân viên phát hiện thấy lỗi kỹ thuật trong khâu sản xuất, anh ta lập tức gửi một báo cáo thông báo cho cấp trên thông báo phát hiện của mình.  
Người này sau đó sẽ tiếp tục gửi thông báo đến tất cả các bộ phận có liên quan trong doanh nghiệp. Một kẻ nào đó sử dụng kỹ thuật xem lén thư điện tử có thể theo dõi và biết được toàn bộ thông tin trong bức thư điện tử gửi tiếp sau đó bàn về vấn đề này..

## 3. An toàn dữ liệu trong thanh toán điện tử 3.1. Đặt vấn đề

Mối de doạ và hậu quả tiềm ẩn với thông tin trong hệ thống mạng phục vụ hoạt động thương mại điện tử là rất lớn, và được đánh giá trên nhiều khía cạnh khác, như: kiến trúc hệ thống công nghệ thông tin, từ chính sách bảo mật thông tin, các công cụ quản lý và kiểm tra, quy trình phản ứng…

Nguy cơ tiềm ẩn trong kiến trúc hệ thống công nghệ thông tin là tổ chức hệ thống kỹ thuật không có cấu trúc bảo vệ an toàn thông tin, tổ chức và khai thác CSDL, quản lý và lưu trữ và sắp đặt thông tin đã phân loại, cơ cấu tiếp cận từ xa, sử dụng phần mềm ứng dụng; chương trình kiểm tra, kiểm soát người sử dụng, phát hiện và xử lý sự cố

Nguy cơ mất an toàn thông tin tiềm ẩn trong chính sách bảo mật an toàn. Thông tin trong hệ thống thương mại điện tử cũng dễ bị tổn thất nếu công cụ quản lý và kiểm tra của các tổ chức quản lý điều khiển hệ thống không được thiết lập. Nguy cơ còn tiềm ẩn trong cấu trúc cứng của các thiết bị tin học và trong phần mềm hệ thống và ứng dụng.

## 3.2. Yêu cầu an toàn dữ liệu cho các chủ thể tham gia thương mại điện tử

Việc phân tích các nguy cơ tiềm ẩn cho thấy rằng vấn đề bảo mật thông tin của các chủ thể tham gia thương mại điện tử là rất quan trọng trong việc hoạch định các phương án bảo mật thông tin trong hệ thống thương mại điện tử. Các chủ thể tham gia thương mại điện tử là người tiêu dùng, doanh nghiệp và chính phủ, nhưng mối quan tâm bảo mật thông tin của các chủ thể tuy có mục đích giống nhau song yêu cầu thì hoàn toàn khác nhau và sự khác nhau về yêu cầu bảo mật thông tin có thể còn có ngay trong cùng một chủ thể do bởi thông tin giao dịch với chủ thể khác nhau có nguy cơ de doạ về an toàn dữ liệu là khác nhau.

Một khía cạnh rất quan trọng là cần phải tiên liệu quá trình xây dựng phương án bảo mật thông tin trong hệ thống thương mại điện tử, đó là phân luồng các thông tin và các dạng thức thông tin giao tiếp trong hệ thống thương mại điện tử để xác định phương thức tổ chức hệ thống kỹ thuật mật mã phù hợp nhằm bảo mật thông tin có hiệu quả.

## 3.3. Các giải pháp an toàn dữ liệu trong thương mại điện tử

Vấn đề bảo mật thông tin trong hệ thống thương mại điện tử được nhìn nhận một cách toàn diện như trên 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 công nghệ thông tin là “muốn tiếp cận Internet thì hãy trang bị tường lửa, nếu cần sự bảo vệ thì hãy mã hoá và mật khẩu là đủ để xác thực”. thực tế quy trình bảo mật thông tin trong hệ thống thương mại điện tử muốn đạt hiệu quả thiết thực và tiết kiệm cần phải được hiểu theo khái niệm như là “biết các bảo vệ để chống lại sự tấn công tiềm ẩn”. Bởi vậy, nó phải là tổng hoà các giải pháp của hạ tầng cơ sở bảo mật. Đó là:

- Pháp lý và tổ chức: xây dựng chính sách mật mã cho thương mại điện tử rõ ràng và có thể tiên liệu được, phản ánh sự cân bằng quyền lợi của các chủ thể tham gia thương mại 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 luật chứng cứ đối với “hồ sơ điện tử”, tiêu chuẩn mật mã và chữ ký điện tử sử dụng trong thương mại điện tử, 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 và quản lý và phân phối sản phẩm mật mã, phản ứng và giải quyết sự cố, thanh tra và kiểm tra, vấnd dề lưu trữ và phục hồi khoá.

- Về 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 khoá mã, các công cụ nghiệp vụ kỹ thuật kiểm tra và phát hiện xâm nhập, dự phòng, khắc phục sự cố xảy ra đối với kỹ thuật mật mã sử dụng trong hệ thống thương mại điện tử.

- Về phía người sử dụng: trước hết phải được giác ngộ về bảo mật thông tin trong hệ thống thương mại điện tử, họ cần phải biết bảo vệ cái gì trong hệ thống của họ, ước định mức độ rủi ro và các nguy cơ tiềm tàng khi kết nối mạng của mình với các đối tợng khác, việc mở rộng mạng của mình trong tương lai… để họ có ý thức đầu tư bảo mật của 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 hệ thống thương mại điện tử.

## 3.4. Một số khuyến nghị về an toàn dữ liệu trong thanh toán điện tử

Lựa chọn hình thức thanh toán

Đầu tiên, người dùng cần quan tâm đến việc chọn hình thức và loại thẻ thanh toán trực tuyến. Có rất nhiều dịch vụ thanh toán trực tuyến và loại thẻ khác nhau được các công ty tài chính, ngân hàng cung cấp. Khi mua hàng ở nước ngoài, đa phần hình thức thanh toán là sử dụng PayPal, thẻ tín dụng hay thẻ ghi nợ. Còn trong nước, các cổng thanh toán điện tử hoặc các dịch vụ ngân hàng trực tuyến (Internet Banking) được người dùng sử dụng phổ biến hơn cả.

Thường xuyên kiểm tra và theo dõi tình trạng tài khoản

Việc đánh cắp tiền từ tài khoản không phải lúc nào cũng diễn ra ngay lập tức. Sau khi đã đánh cắp được thông tin của người dùng, kẻ tấn công cần một khoảng thời gian để sử dụng được tài khoản đó. Đặc biệt, trong những trường hợp tài khoản có hạn mức thanh toán theo ngày hoặc tháng. Do đó, các chuyên gia bảo mật khuyến nghị rằng, nên dành thời gian để kiểm tra tài khoản vài tuần một lần để xem xét chi tiết từng giao dịch trong tài khoản nhằm phát hiện các giao dịch bất thường. Nếu phát hiện ra bất cứ điều gì khác thường cần báo cho ngân hàng chủ quản ngay lập tức.

Người dùng cũng có thể đăng ký các dịch vụ thông báo biến động tài khoản qua email hoặc tin nhắn văn bản. Hiện nay, đa số ngân hàng cho phép người dùng giám sát tài khoản của mình theo thời gian thực thông qua các dịch vụ cảnh báo kích hoạt giao dịch. Các thông tin mà người dùng nhận được như: yêu cầu chuyển khoản, yêu cầu thanh toán hóa đơn mới được thiết lập cho tài khoản.

Kích hoạt xác thực 2 yếu tố cho tất cả các giao dịch trực tuyến

Hầu hết, các ngân hàng đã cung cấp tính năng xác thực 2 yếu tố để bổ sung một lớp bảo vệ cho các giao dịch nhạy cảm. Khi người dùng thực hiện việc chuyển khoản, ngân hàng sẽ gửi đến người dùng một mã đặc biệt thông qua một tin nhắn văn bản hoặc email mà người dùng sẽ phải trả lời để hoàn thành giao dịch. Vì vậy, ngay cả khi kẻ tấn công có được thông tin tài khoản của người dùng thì cũng khó có thể thực hiện giao dịch gian lận. Khi nhận được các mã xác thực không xuất phát từ yêu cầu bản thân, người dùng có thể loại bỏ giao dịch bằng cách không đồng ý xác nhận. Gần đây, bên cạnh tính năng OTP, các ngân hàng đã bổ sung biện pháp xác thực bằng vân tay. Điều này giúp bảo vệ tài khoản của người dùng tốt hơn.

Không lưu trữ thông tin thẻ tín dụng trực tuyến

Một số nhà bán lẻ trực tuyến cung cấp tùy chọn lưu trữ thông tin thẻ tín dụng sau khi người dùng thực hiện giao dịch. Mặc dù điều này mang lại sự thuận tiện hơn cho các giao dịch trong tương lai, nhưng có thể gây ra những rủi ro rò rỉ thông tin thẻ tín dụng cho khách hàng. Do đó, người dùng không nên lưu trữ thông tin thẻ tín dụng trực tuyến, cũng như không nên cung cấp các chi tiết về thẻ tín dụng của mình qua email hoặc điện thoại.

Vô hiệu hóa tính năng tự động điền thông tin (Autofill) trên trình duyệt

Tương tự với việc lưu trữ thông tin thẻ tín dụng trực tuyến, người dùng cũng nên tránh để thông tin thẻ tín dụng lưu trữ trên trình duyệt bằng cách vô hiệu hóa tính năng Autofill của trình duyệt.

Không thực hiện các giao dịch tài chính qua mạng wifi công cộng

Kẻ tấn công có thể dễ dàng kiểm soát mạng wifi công cộng và chặn bắt thông tin cá nhân của người dùng. Nếu bắt buộc phải thực hiện các giao dịch tài chính khi đang di chuyển, người dùng cần sử dụng dữ liệu di động và tránh kết nối đến bất cứ mạng wifi không tin cậy.

Cảnh giác với các trang web lừa đảo

Kẻ tấn công có thể tạo ra các trang web giả mạo các trang web phổ biến để lừa người dùng tiết lộ các thông tin cá nhân thông qua các phương pháp khác nhau. Một cách tiếp cận phổ biến mà kẻ tấn công sử dụng là thay thế các ký tự tương tự trong địa chỉ web, ví dụ: *www.amaz0n.com* thay vì *www.amazon.com*. Vì vậy, người dùng cần xem xét địa chỉ web một cách cẩn thận, hoặc cân nhắc sử dụng các công cụ như Google Safe Browsing của Google để kiểm tra trạng thái an toàn hiện tại của trang web. Một số đặc điểm nhận biết trang web an toàn:

- Sử dụng giao thức HTTPS cho các giao dịch trực tuyến.

- Hiển thị logo của VeriSign. Người dùng có thể nhấp vào biểu tượng để xác minh danh tính trang web trước khi bắt đầu mua sắm hoặc hoàn thành giao dịch ngân hàng.

Cảnh giác với những lời đề nghị khó tin

Trong các sự kiện quảng cáo, các trang web mua sắm trực tuyến thường cung cấp các ưu đãi hấp dẫn. Tội phạm mạng thường lợi dụng những giai đoạn ưu đãi này để thực hiện lừa đảo. Mặc dù có nhiều giao dịch và tin khuyến mãi là chính xác, tuy nhiên cần luôn cảnh giác với những lời đề nghị lạ, khó tin.

Sử dụng mật khẩu an toàn

Mật khẩu là một yếu tố xác thực không thể bỏ qua đối với mọi giao dịch. Khi sử dụng mật khẩu, người dùng cần lưu ý:

- Sử dụng mật khẩu khó đoán có chứa chữ in hoa và chữ thường, số và ký hiệu.

- Không sử dụng cùng tên người dùng và mật khẩu cho tất cả các tài khoản trực tuyến.

- Thay đổi mật khẩu thường xuyên nhất có thể (ít nhất ba tháng một lần).

- Không chia sẻ mật khẩu hoặc thông tin nhận dạng người dùng. Gần đây, đã xuất hiện các vụ lừa đảo liên quan đến email giả mạo nhà cung cấp Internet của người dùng để yêu cầu các thông tin này. Cần lưu ý, các nhà cung cấp Internet, ngân hàng, thẻ tín dụng và các doanh nghiệp có uy tín không bao giờ liên hệ với khách hàng để yêu cầu mật khẩu hoặc tên người dùng của họ.

- Không nhấp vào bất kỳ liên kết nào trong email yêu cầu thông tin nhận dạng. Liên lạc trực tiếp với tổ chức chủ quản nếu cảm thấy dấu hiệu nghi ngờ.

## 4. Các phương pháp đảm bảo an ninh mạng và dữ liệu trong TMĐT

## 4.1. Xây dựng kế hoạch đảm bảo an ninh mạng và dữ liệu

Các bước xây dựng kế hoạch an ninh thương mại điện tử như thế nào?  
Việc xây dựng kế hoạch an ninh thương mại điện tử cho doanh nghiệp bao gồm 4 giai đoạn sau:

- Giai đoạn đánh giá: Giai đoạn này xác định những tài sản doanh nghiệp có, bao gồm cả tài sản hữu hình và vô hình. Giá trị tài sản phải được định rõ, cả về mặt tài chính và phi tài chính và định rõ tầm quan trọng của từng tài sản đối với doanh nghiệp và từ đó đánh giá khả năng bị tấn công của từng tài sản. Việc đánh giá gồm các nội dung sau:

+ Xác định các mối đe dọa: đa số những vụ xâm phạm an ninh trái phép là do sự can thiệp trực tiếp hay gián tíếp của con người các hệ thống và những người có quyền truy cập tới tài sản phải được định rõ như giám đốc IT, nhân viên, các nhà tư vấn,… Khả năng mối đe dọa trở thành hiện thực cũng cần được đánh giá.

+ Xác định hình thức thiệt hại: ví dụ các thông tin quan trọng có thể bị sửa đổi hoặc đánh cắp bởi các cá nhân, hoặc có thể bị phá hủy do bị tấn công.

- Giai đoạn lên kế hoạch: Xác định rõ ràng đe dọa nào cần phải chống đỡ và giải pháp tương ứng cần được tiến hành, thời gian cụ thể và người chịu trách nhiệm triển khai. Đánh giá và lựa chọn các giải pháp phù hợp.

- Giai đoạn thực thi: Các công nghệ đặc thù có thể được chọn để chống đỡ với các nguy cơ dễ xảy ra nhất. Việc lựa chọn công nghệ dựa vào những định hướng đã được nêu ra ở giai đoạn Lập kế hoạch. Ngoài những công nghệ đặc thù, các phần mềm an ninh từ những nhà cung cấp khác cũng có thể được lựa chọn.

- Giai đoạn giám sát: Xác định những biện pháp nào mang lại thành công, những biện pháp nào không hiệu quả cần thay đổi, liệu có những mối đe dọa mới xuất hiện hay có những cải tiến hoặc thay đổi gì trong công nghệ, hoặc có những tài sản nào khác của doanh nghiệp cần bảo đảm an ninh.

## 4.2. Các biện pháp đảm bảo an ninh mạng và dữ liệu

Kỹ thuật mã hóa thông tin: là quá trình chuyển các văn bản hay các tài liệu gốc thành các văn bản dưới dạng mật mã để bất cứ ai, ngoài người gửi và người nhận đều không thể đọc được. - Hệ thống mã hóa hiện đại thường được số hóa – thuật toán dựa trên các bit đơn của thông điệp chứ không dựa trên ký hiệu chữ cái. Máy tính lưu trữ dữ liệu dưới dạng một chuỗi nhị phân, trình tự của các số 1 và 0. Mỗi ký tự gọi là một bit. Các mã khóa và mã mở là các chuỗi nhị phân với độ dài khóa được xác định sẵn.

Ngày nay, hai kỹ thuật cơ bản thường được sử dụng để mã hóa thông tin trên internet là mã hóa “khóa riêng” hay mã hóa “khóa bí mật” và mã hóa “khóa công cộng”. + Mã hóa “khóa bí mật” còn gọi là mã hóa đối xứng, người gửi mã khóa một thông điệp sử dụng khóa bí mật đối xứng, sau đó gửi thông điệp đã mã hóa và bí mật đối xứng cho người nhận bằng một cách nào đó mà họ cảm thấy là an toàn.

Mã hóa công cộng: là phương pháp sử dụng hai mã khóa cho quá trình mã hóa, một mã dùng để mã hóa thông điệp, một mã để giải mã thông điệp. Mỗi người sử dụng có hai loại mã khóa: mã khóa bí mật chỉ riêng người đó biết, còn mã khóa công cộng được thông báo rộng rãi cho những người sử dụng khác trong hệ thống. Người gửi sử dụng mã khóa công cộng của người nhận để mã hóa thông điệp. Người nhận khi nhận được thông điệp sẽ sử dụng mã khóa cá nhân của mình để giải mã thông điệp.

- Giao thức thỏa thuận mã khóa: Một trong những giao thức thỏa thuận mã khóa là phong bì số hóa. Thông điệp được mã hóa bằng mã khóa bí mật và sau đó mã khóa bí mật được mã hóa bằng mã khóa công cộng. Người gửi sẽ gửi kèm thông điệp đã được mã hóa (bằng khóa bí mật) và khóa bí mật được mã hóa (bằng khóa công cộng) và gửi toàn bộ cho người nhận.

- Chữ ký điện tử: Về mặt công nghệ, chữ ký điện số là một thông điệp dữ liệu đã được mã hóa gắn kèm theo một thông điệp dữ liệu khác nhằm xác thực người gửi thông điệp đó. Quá trình ký và xác nhận chữ ký điện như sau: Người gửi muốn gửi thông điệp cho bên khác thì sẽ dùng một phần mềm rút gọn thông điệp dữ liệu điện tử, xử lý chuyển thông điệp dữ liệu điện tử thành một “thông điệp tóm tắt” (Message Digest), thuật toán này được gọi là thuật toán rút gọn (hash function). Người gửi mã hoá bản tóm tắt thông điệp bằng khóa bí mật của mình (sử dụng phần mềm bí mật được cơ quan chứng thực cấp) để tạo thành một chữ ký điện tử.Sau đó, người gửi tiếp tục gắn kèm chữ ký điện tử này với thông điệp dữ liệu ban đầu. Sau đó gửi thông điệp đã kèm với chữ ký điện tử một cách an toàn qua mạng cho người nhận.Sau khi nhận được, người nhận sẽ dùng khoá công khai của người gửi để giải mã chữ ký điện tử thành bản tóm tắt thông điệp. Người nhận cũng dùng rút gọn thông điệp dữ liệu giống hệt như người gửi đã làm đối với thông điệp nhận được để biến đổi thông điệp nhận được thành một bản tóm tắt thông điệp. Người nhận so sánh hai bản tóm tắt thông điệp này. Nếu chúng giống nhau tức là chữ ký điện tử đó là xác thực và thông điệp đã không bị thay đổi trên đường truyền đi.  
Ngoài ra, chữ ký điện tử có thể được gắn thêm một “nhãn” thời gian: sau một thời gian nhất định quy định bởi nhãn đó, chữ ký điện tử gốc sẽ không còn hiệu lực, đồng thời nhãn thời gian cũng là công cụ để xác định thời điểm ký.Là một biện pháp mã khóa công cộng được sử dụng phổ biến trong e.commerce, đó là bất cứ âm thanh điện tử, ký hiệu hay quá trình điện tử gắn với hoặc liên quan một cách logic với một văn bản điện tử khác theo một nguyên tắc nhất định và được người ký (hay có ý định ký) văn bản đó thực thi hoặc áp dụng. Chứng thực điện tử: là trung tâm an ninh trong TMĐT, thông qua bên thứ 3, là công cụ dễ dàng và thuận tiện để các bên tham gia giao dịch tmđt tin tưởng lẫn nhau.

- An ninh mạng và bức tường lửa: Tường lửa là một thành phần của mạng, gồm phần mềm hoặc phần cứng hoặc kết hợp cả phần mềm và phần cứng, cho phép những người sử dụng mạng máy tính của một tổ chức có thể truy cập tài nguyên của các mạng khác (ví dụ, mạng Internet), nhưng đồng thời ngăn cấm những người sử dụng khác, không được phép từ bên ngoài truy cập vào mạng máy tính của tổ chức.

+Về cơ bản, tường lửa cho phép những người sử dụng mạng máy tính bên trong tường lửa được bảo vệ nhưng vẫn có khả năng truy cập toàn bộ các dịch vụ bên ngoài mạng; đồng thời ngăn chặn và chỉ cho phép một số các truy cập từ bên ngoài vào mạng trên cơ sở đã kiểm tra tên và mật khẩu của người sử dụng, địa chỉ IP hoặc tên miền (domain name) …Tường lửa bảo vệ mạng máy tính của tổ chức tránh khỏi những tổn thương do những tin tặc, những người tò mò từ bên ngoài tấn công. Tất cả mọi thông điệp được gửi đến và gửi đi đều được tường lửa kiểm tra đối chiếu với những quy định về an toàn do tổ chức xác lập. Các tường lửa phổ biến hiện nay gồm: Windows XP Personal firewall, Microsoft ISA server (đa chức năng), Checkpoint.

+ Các loại tường lửa: + Tường lửa lọc gói + Cổng ứng dụng + Cổng mức mạch - Lựa chọn tường lửa: + Cấu hình tường lửa là sự áp dụng chính sách an ninh thông tin cho mạng máy tính. + Triển khai tường lửa tùy thuộc vào yêu cầu an ninh của tổ chức hay DN và khả năng tài chính của DN đó

- Sử dụng password đủ mạnh: Để đảm bảo bí mật cho mật khẩu, khi thiết lập nên xem xét các tiêu chí như:

+ Mật khẩu có số ký tự đủ lớn, tối thiểu 8 ký tự và có sự kết hợp giữa chữ hoa, chữ thường, chữ số và biểu tượng. Như vậy sẽ mất rất nhiều thời gian mới có thể tìm ra và phá mật khẩu, mà tới thời gian đó mật khẩu đã có thể đã được thay đổi. Mật khẩu cũng nên thường xuyên thay đổi (thường từ 30-60 ngày) và không nên sử dụng lại mật khẩu cũ.

+ Kích hoạt tự động việc khóa không cho truy cập hệ thống nếu sau từ 3-5 lần nhập mật khẩu vẫn không đúng.

+ Không sử dụng chức năng tự động điền (auto complete) của một số phần mềm ứng dụng như Microsoft Explorer để lưu mật khẩu và số tài khoản

# CHƯƠNG 2: CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI VÀ CHỨNG CHỈ ĐIỆN TỬ

Mục tiêu:

Học xong chương này người học sẽ có khả năng: Sử dụng cơ sở hạ tầng khoá công khai và chứng chỉ điện tử để đảm bảo an toàn dữ liệu trong TMĐT

## 2.Mật mã đối xứng

## 1.1. Mật mã học là gì

Người ta gọi mật mã học là một khoa học nghiên cứu nghệ thuật nhằm che giấu thông tin, bằng cách mã hóa (encryption) tức là biến đổi “thông tin gốc” dạng tường minh (plaintext) thành “thông tin mã hóa” dạng ẩn tàng (cipher text) bằng cách sử dụng một khóa mã (thuật toán mã hóa) nào đó. Chỉ có những người giữ chìa khóa (key) bí mật mới có thể giải mã (decryption) thông tin dạng ẩn tàng trở lại thành dạng thông tin có dạng tường minh.

Thông tin ẩn tàng đôi khi vẫn bị khám phá mà không cần biết khóa bí mật: việc đó gọi là bẻ khóa. Ngành học nghiên cứu về việc bẻ khóa (attack/crack/hack) này còn gọi là cryptanalysis. Như đã nói ở ví dụ trên, trong các phương pháp tấn công thám mã ta gọi tấn công bạo lực - brute-force attack (exhaustive key search): là phương pháp tấn công bằng cách thử tất cả những khả năng chìa khóa có thể có. Đây là phương pháp tấn công thô sơ nhất và cũng khó khăn nhất. Theo lý thuyết, tất cả các thuật toán hiện đại đều có thể bị đánh bại bởi tấn công bạo lực nhưng trong thực tiễn việc này chỉ có thể thực hiện được trong thời gian rất dài nên thực tế là không khả thi. Vì thế có thể coi một thuật toán là an toàn nếu như không còn cách nào khác để tấn công nó ngoài cách sử dụng brute-force attack. Để chống lại tấn công này, chìa khóa bí mật được thay đổi một cách thường xuyên hơn.

## 1.2. Mật mã đối xứng

## 1.2.1. Mật mã đối xứng là gì

Có 2 loại thuật toán mật mã chính là mật mã đối xứng (symmetric cryptography) và mật mã bất đối xứng (asymmetric cryptography). Mật mã đối xứng đã được sử dụng từ rất lâu đời. Căn cứ các dữ liệu khảo cổ, người ta tin rằng người Ai Cập cổ đã biết dùng loại mật mã này.

Mã khóa (cryptographic key) là thành phần quan trọng trong thuật toán mật mã. Mã khóa có thể ví như chìa của một ổ khóa. Ta có thể lắp được rất nhiều chìa (có cùng chiều dài, chiều rộng, kích thước rãnh…) vào một ổ khóa nhưng chỉ chìa nào có các răng cưa thích hợp mới có thể mở được ổ khóa. Tương tự, mỗi thuật toán mật mã cần một mã khóa có chiều dài (dung lượng tính bằng bit) chính xác. Ta có thể thực thi một thuật toán mật mã với một mã khóa bất kỳ có chiều dài như yêu cầu nhưng chỉ duy nhất mã khóa có cách sắp xếp các bit phù hợp mới có thể mã hóa hoặc giải mã văn bản.  
Mã khóa dùng trong mật mã đối xứng thực chất là một chuỗi (chiều dài xác định) các bit được sắp xếp ngẫu nhiên. Nếu thuật toán đối xứng dùng mã hóa đối xứng 40 bit thì dung lượng mã khóa là 40 bit. Mã khóa dung lượng 128 bit được dùng cho mã hóa đối xứng 128 bit…

Một chuỗi 40 bit sẽ có thể cho ta 2 lũy thừa 40 mã khóa hay 1.1E12 mã khóa, tức là có hơn 1.000 tỷ mã khóa.

Một chuỗi 60 bit sẽ có thể cho ta 2 lũy thừa 60 mã khóa hay 1.8E19 mã khóa, tức là có gần 20 tỷ tỷ mã khóa.

Hiện nay, mã khóa đối xứng chuẩn có chiều dài 128 bit. Vậy ta có thể có 3.4E38 mã khóa, tức là có hơn 340 tỷ tỷ tỷ tỷ mã khóa.

## 1.2.2. Thuật toán mật mã

Thuật toán mật mã đối xứng dùng một mã khóa cho 2 quá trình mã hóa và giải mã. Mật mã đối xứng lại có thể được chia thành 2 hình thức: block cipher và stream cipher.

**Block cipher**: Block cipher chia thông tin thành những đoạn ngắn có chiều dài cố định (thường là 64 bit) và mã hóa từng đoạn này. Một số thuật toán block cipher: DES, 3-DES, RC2, RC5, RC6 và Rijndaen (còn được gọi là AES).

Thuật toán DES (Data Encryption Standard) phổ biến nhất và là thuật toán tiêu biểu cho mật mã đối xứng, được IBM phát triển vào cuối thập niên 1970. DES chia thông tin thành chuỗi 64 bit và mã hóa bằng mã khóa 56 bit. Do sự gia tăng mạnh mẽ năng lực của máy tính, mã khóa 56 bit hiện nay trở nên thiếu an toàn nếu bị tấn công brute-force. 3-DES (viết tắt của Triple DES) được phát triển để lấp yếu điểm này bằng cách mã hóa 3 lần hoặc phối hợp 3 phép toán.

Các thuật toán họ RC được phát triển bởi Ron Rivest (chữ R trong RSA). RC là từ viết tắt của Ron’s Code hoặc Rivest Cipher. RC2 được phát triển để thay thế cho DES và có tốc độ nhanh gấp đôi DES. RC5 mã hóa chuỗi dữ liệu 64 hoặc 128 bit và có thể sử dụng nhiều chiều dài mã khóa, tối đa đến 2.048 bit. RC6 được phát triển trên cơ sở RC5, mã hóa chuỗi 128 bit với mã khóa 128 bit. RC6 cũng nhằm thay thế cho DES và có thể được xem là thuật toán cuối cùng trong thế hệ đầu của các chuẩn thuật toán mật mã đối xứng.

Thế hệ kế tiếp của các chuẩn mã đối xứng được gọi chung là AES – Advanced Encryption Standard – dùng mã khóa 128 bit có ưu thế vượt trội so với RC6. Thuật toán AES mạnh nhất là Rijindael do 2 người Bỉ đề xướng: Daemen và Rijmen. Một số thuật toán AES mới nhất gồm MARS (IBM), Serpent (Anderson, Riham và Knudsen), Twofish (Scheier, Kelsey, Whiting, Wagner, Hall và Ferguson)

**Stream cipher**: Stream cipher mã hóa từng bit của thông tin. Stream cipher thông dụng nhất là RC4 có thể dùng nhiều chiều dài mã khóa và có tốc độ nhanh hơn rất nhiều so với block cipher

Một khi đã có thuật toán mật mã đối xứng và một số ngẫu nhiên dùng làm mã khóa, quá trình mã hóa có thể tóm lược như sau: M + K = C

Trong đó:

– M: Công thức nấu bún mắm viết bằng ngôn ngữ thông thường, ai cũng đọc được (bạch văn – văn bản thuần – plain text)

– K: Mã khóa và thuật toán mật mã đối xứng.

– C: Bản mật mã, nhìn vào chẳng ai biết là cái chi (cipher text)

Ất (thật ra là máy tính của Ất) sẽ phát sinh một mã khóa ngẫu nhiên và dùng mã khóa đó để mã hóa công thức. Ất có thể an tâm gửi bản mật mã cho Bính. Khi nhận được, Bính sẽ tiến hành giải mã cũng bằng chính mã khóa đã dùng để mã hóa:  
C – K = M

Ất và Bính đã dùng chung 1 mã khóa để mã hóa và giải mã, đó chính là quá trình triển khai mật mã đối xứng.

Trải qua thử thách của thời gian và biết bao lần “vạch lá tìm sâu” của các chuyên gia phân tích mật mã (cryptanalyst), các thuật toán mật mã đối xứng đã chứng minh được mức độ bảo mật rất cao của chúng. Mật mã đối xứng còn có tốc độ hoạt động nhanh. Điều này đồng nghĩa với hiệu suất hoạt động của máy tính không hề bị ảnh hưởng nhiều cho dù phải triển khai mã hóa một lượng thông tin lớn. Bên cạnh đó, mã hóa đối xứng còn có thêm một ưu điểm là dung lượng của bản mã gần như tương đương với dung lượng của văn bản thuần.

Mọi chuyên xem ra có vẻ xuôi chèo mát mái, thế nhưng vẫn có một vấn đề rất lớn mà ta đã vô tình không xét đến. Để Bính có thể giải mã Ất phải gửi mã khóa kèm theo bản mã… Nếu làm thế thì chẳng khác nào bỏ vàng vào tủ sắt, khóa tủ lại rồi … treo chìa khóa ngay bên cạnh!…

Vẫn có một cách để giải quyết, đó là Ất, sau khi đã gửi bản mã đi, sẽ đáp máy bay qua Mỹ để giao mã khóa tận tay Bính. Nếu thế thì Ất cũng có thể giao công thức tận tay Bính cho rồi cần chi phải mã hóa.

Tình hình thật ra còn tệ hơn nữa vì người ta không hề khuyên dùng một mã khóa nhiều lần. Nói một cách khác, mỗi lần muốn mã hóa thì phải dùng một mã khóa khác nhau. Điều này tất yếu dẫn đến việc phải giải quyết vấn đề gửi mã khóa mỗi khi gửi một bản mã.

Ta hãy giả định Bính nhận được công thức nấu bún mắm và làm ăn phát đạt, mở 20 chi nhánh bún mắm Bà Sáu trên toàn nước Mỹ. Các chi nhánh tìm cách hoàn thiện món ăn thơm tho này và trao đổi các “bí kiếp” cho nhau (dĩ nhiên là mã hóa trước khi gửi đi). Mỗi lần gửi, một chi nhánh sẽ phải phát sinh 19 mã khóa khác nhau để gửi cho 19 chi nhánh còn lại. 20 chi nhánh sẽ phải phát sinh 20 x 19 = 380 mã khóa (xấp xỉ bằng bình phương số chi nhánh).

Nếu muốn lưu lại các bản mã, Bính tất nhiên sẽ phải lưu cả các mã khóa. Để bảo đảm an toàn, bản mã và mã khóa phải được lưu riêng biệt. Thêm một vấn đề phát sinh là phải có một hệ thống quản lý mã khóa để có thể xác định được mã khóa nào dùng giải bản mã nào.

## 1.3. Ưu/ Nhược điểm và phạm vi sử dụng của mật mã đối xứng.

Ưu điểm nổi bật của mã hóa đối xứng là tốc độ lập mã, giải mã khá nhanh chóng. Hiện nay có nhiều phần mềm thương mại hỗ trợ thuật toán mã hóa đối xứng hữu hiệu và rất phổ dụng.

Ưu điểm thứ hai là tuy có nhiều nghiên cứu thám mã đã thực hiện nhưng với các thuật toán được cải tiến gần đây như 3-DES và nhất là AES thì độ bảo mật khá cao, trong thực tế việc phá mã cũng không dễ dàng.

Tuy vậy nhược điểm lớn nhất của thuật toán mã hóa đối xứng là vấn đề chuyển giao chìa khóa giữa các đối tác, đặc biệt là trong môi trường mở.

Giả sử A và B “hoàn toàn tin tưởng vào nhau” và trao cho nhau mã khóa đối xứng bằng một phương pháp đáng tin cậy nào đó (trao tay trực tiếp hoặc có một phương pháp nào có thể thay thế cho trao tay trực tiếp mà cũng có giá trị tương đương như thế) và sau đó hai người sử dụng mã khóa truyền các thông điệp mã hóa cho nhau, ta thấy rằng:

- Sử dụng mã đối xứng (trong các điều kiện nói trên) đảm bảo được nguyên lý bí mật/riêng tư vì thông tin không thể bị lộ.

- Đảm bảo tính xác thực, tính không chối bỏ và tính nhận dạng, những điều này chủ yếu được thực hiện khi chuyển giao khóa mã cho nhau chứ không phải trong quá trình trao đổi thông điệp mã hóa về sau. Vì giả sử A và B trực tiếp trao khóa mã K cho nhau và “tin tưởng nhau” là không làm lộ khóa mã cho người thứ ba, như vậy khi nhận được thông điệp được mã hóa bởi K, hai đối tác có thể nhận dạng ra thông điệp đó chính là do đối tác của mình gửi. Mặt khác nếu B nhận được thông điệp của A mã hóa bởi K thì A không thể chối bỏ rằng không phải do mình phát hành thông điệp đó (vì ngoài B chỉ có A biết khóa K). Tuy nhiên khi B nhận được mà chối là không nhận được thì phải do “tính tin tưởng” giữa hai đối tác chứ không phải do khóa K đảm bảo.

- Mã hóa đối xứng không đảm bảo tính toàn vẹn dữ liệu. Giả sử thư của A gửi cho B đã lọt vào tay C. C không hiểu gì về nội dung thông điệp nhưng vẫn có thể thêm bớt dữ liệu làm thay đổi, sai lệch nội dung thông điệp rồi vẫn gửi tiếp cho B: B không thể biết là thông điệp đã bị thay đổi nội dung (Có thể do không biết khóa mã nên dữ liệu thêm bớt của C có thể làm cho thông điệp không giải mã được hay là vô nghĩa nhưng B vẫn không thể chắc chắn là có người can thiệp mà vẫn nghĩ là chính do A tạo ra như vậy!)

Vì những lý do trên các thuật toán mã hóa đối xứng loại này là những phương pháp mã hóa lý tưởng cho một người sử dụng (single user) với mục đích mã hóa dữ liệu của cá nhân hay tổ chức đơn lẻ để chống xâm nhập của kẻ xấu. Không phải chỉ có những bí mật về an ninh quốc phòng mà ngay những thông tin bí mật trong công nghệ,trong thương mại v.v. đều có thể là mục tiêu xâm nhập của những gián điệp công nghệ, kinh tế, hoặc xâm nhập trực tiếp hoặc sử dụng các biện pháp như gửi và cài Spyware, Trojan hay các phần mềm độc.

Vì vậy cá nhân hay tổ chức, trước khi lưu giữ các dữ liệu thông tin quan trọng có thể và nên mã hóa bằng những khóa mã tự tạo và giữ bí mật khóa cho riêng mình biết.

Mã đối xứng bộc lộ hạn chế khi thông tin mật cần được chia sẻ với một bên thứ hai vì khi đó cần phải chuyển giao chìa khóa cho đối tác mà việc chuyển giao chìa khóa trong môi trường mở có nhiều nguy cơ bị lộ và như vậy việc mã hóa về sau trở thành vô nghĩa!

Mã đối xứng chỉ có thể sử dụng cho nhiều đối tác (multiple users) với điều kiện là có thể “mặt đối mặt” để trực tiếp chuyển giao khóa mã trong môi trường tin cậy hoặc có một biện pháp tin cậy nào đó để chuyển giao khóa mã một cách an toàn. Nếu không có biện pháp chuyển giao khóa mã an toàn, tương đương với việc trao tay trực tiếp thì hầu như mã đối xứng không đảm bảo được yêu cầu nào trong 5 nguyên lý bảo mật thông tin đã nêu ở chương trước cả.

## 2. Mật mã khóa công khai

## 2.1 Khái niệm chung

Mã hóa khóa công khai (mã hoá khoá công khai) là một dạng mã hóa cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa 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 (Public key) và khóa riêng (Private key) hay khóa bí mật (secret key).

Thuật ngữ mã hóa bất đối xứng thường được dùng đồng nghĩa với mã hóa khóa công khai mặc dù hai khái niệm không hoàn toàn tương đương. Có những thuật toán mã bất đối xứng không có tính chất khóa công khai và bí mật như đề cập ở trên mà cả hai khóa (cho việc mã hóa và giải mã) đều cần phải giữ bí mật. Trong mật mã khóa công khai, khóa riêng cần 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 (hoặc rất khó) 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 xem nó có phải đã được tạo với một khóa bí mật nào đó hay không.

- Thỏa thuận khóa: cho phép thiết lập khóa để trao đổi thông tin mật giữa hai bên.

Thông thường, các kỹ thuật mật mã hóa khóa công khai đòi hỏi khối lượng tính toán nhiều hơn các kỹ thuật mã hóa khóa đối xứng nhưng do những ưu điểm nổi bật nên chúng được sử dụng nhiều.

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

## 2.2 Hạ tầng mật mã khóa công khai

Trong mật mã học, hạ tầng cơ sở khóa công khai PKI (Public Key Infrastructure) là một cơ chế để cho một bên thứ 3 (thường là cơ quan cấp chứng thực số) cung cấp và xác thực định danh các bên tham gia vào quá trình trao đổi thông tin. Cơ chế này cũng cho phép gán cho mỗi người sử dụng trong hệ thống một cặp khóa công khai/khóa bí mật. Các quá trình này thường được thực hiện bởi một phần mềm đặt tại trung tâm và các phần mềm phối hợp khác tại các địa điểm của người dùng.

Khóa công khai thường được phân phối trong chứng thực điện tử. Khái niệm hạ tầng khóa công khai thường được dùng để chỉ toàn bộ hệ thống bao gồm cơ quan cấp chứng thực số (CA) cùng các cơ chế liên quan đồng thời với toàn bộ việc sử dụng các thuật toán mật mã hóa khóa công khai trong trao đổi thông tin. Tuy nhiên phần sau được bao gồm không hoàn toàn chính xác bởi vì các cơ chế trong PKI không nhất thiết sử dụng các thuật toán mã hóa khóa công khai. PKI cho phép những người tham gia xác thực lẫn nhau và sử dụng thông tin từ các chứng thực khóa công khai để mã hóa và giải mã thông tin trong quá trình trao đổi. Thông thường, PKI bao gồm phần mềm máy khách (client), phần mềm máy chủ (server), phần cứng (như thẻ thông minh) và các quy trình hoạt động liên quan. Người sử dụng cũng có thể ký các văn bản điện tử với khóa bí mật của mình và mọi người đều có thể kiểm tra với khóa công khai của họ. PKI cho phép các giao dịch điện tử được diễn ra đảm bảo tính bí mật, toàn vẹn và xác thực lẫn nhau mà không cần phải trao đổi các thông tin mật từ trước. Hầu hết các hệ thống PKI quy mô doanh nghiệp đều dựa trên các chuỗi chứng thực để xác thực các thực thể. Chứng thực của người dùng sẽ được một cơ quan cấp chứng thực số cấp, đến lượt nhà cung cấp này lại có chứng thực được một nhà cung cấp khác ở cấp cao hơn tạo ra... (hình cây). Hệ thống sẽ bao gồm nhiều máy tính thuộc nhiều tổ chức khác nhau với các gói phần mềm tương thích từ nhiều nguồn khác nhau. Vì vậy, các tiêu chuẩn là yếu tố rất quan trọng đối với hoạt động của các PKI. Hầu hết các tiêu chuẩn về PKI hiện tại được soạn thảo bởi nhóm làm việc PKIX của IETF.

Các hệ thống PKI doanh nghiệp thường được tổ chức theo mô hình danh bạ trong đó khóa công khai của mỗi người dùng được lưu trữ (bên trong các chứng thực số) kèm với các thông tin cá nhân (số điện thoại, E-mail, địa chỉ, nơi làm việc...). Hiện nay, công nghệ danh bạ tiên tiến nhất là LDAP và định dạng chứng thực phổ biến nhất X.509 cũng được phát triển từ mô hình trước đó của LDAP là X.500.

Mục tiêu chính của PKI là cung cấp khóa công khai và xác định mối liên hệ giữa khóa và định dạng người dùng. Nhờ vậy người dùng có thể sử dụng trong một số ứng dụng như:

• Mã hóa E-mail hoặc xác thực người gửi E-mail (OpenPGP hay S/MIME).

• Mã hóa hoặc nhận thực văn bản (Các tiêu chuẩn chữ ký XML hoặc mã hóa XML khi văn bản được thể hiện dưới dạng XML).

• Xác thực người dùng ứng dụng (Đăng nhập bằng thẻ thông minh nhận thực người dùng trong SSL).

• Các giao thức truyền thông an toàn dùng kỹ thuật Bootstrapping (IKE, SSL): trao đổi khóa bằng khóa bất đối xứng, còn mã hóa bằng khóa đối xứng.

Các hệ thống mật mã công khai

Các hệ thống mã hóa khóa công khai thông thường được thực hiện với 3 bước cơ bản. Bước thứ nhất là công đoạn sinh khóa, một cặp khóa public key và private key có quan hệ về toán học được tạo ra dựa vào các bài toán cửa lật một chiều. Bước hai là bước mã hóa sử dụng khóa công khai (public key), khóa này có thể được chuyển giao trên môi trường mở. Quá trình giải mã là bước cuối cùng sử dụng khóa riêng bí mật (private key).

Các bước thực hiện như sau:

- A chọn một số ngẫu nhiên lớn để sinh cặp khóa, khóa công khai E và khóa bí mật riêng D.

- A gửi E-khóa công khai (public key) cho B, giữ D-khóa riêng (private key) cho mình.

- Dùng khóa công khai để mã hóa, nhưng dùng khóa bí mật để giải mã.

- B nhận được khóa công khai E. B có thông điệp gốc P, dùng E mã hóa E(P) = C, C là thông điệp mã hóa gửi cho A.

- A nhận được C, dùng D giải mã D(C) = P: được lại thông điệp gốc.

+ Chỉ riêng có A (có D) mới giải mã được

+ Ai có E đều mã hóa được

+ D dùng để giải E, nhưng nếu chỉ biết E thì hầu như chắc chắn là không thể tìm được D.

## 2.3.1. Hệ mật mã ElGamal

Hệ mật mã ElGamal là một thuật toán tương tự như hệ thốngDiffie-Hellman trình bày ở mục sau, được xây dựng trên bài toánlogarit rời rạc.

Dù rằng tác giả của hệ mật mã này (Taher Elgamal) không đăngký xin cấp bản quyền cho sáng tạo của mình nhưng những người sởhữu bản quyền của hệ mật mã Diffie-Hellman vì lý do nào đó vẫn xemhệ này cũng thuộc phạm vi bảo vệ của giấy phép bản quyền củamình. Cũng không ai rõ lý do thực sự của việc đăng ký tên thuậttoán là ElGamal (chữ G viết hoa) trong khi họ của tác giả là Elgamal(chữ g không viết hoa).Có thể thấy ngay nhược điểm rõ ràng của hệ ElGamal là thôngđiệp sau khi mã hóa có kích thước rất lớn, xấp xỉ gấp hai lần thôngđiệp gốc! Chính vì vậy hệ mật mã này thường không dùng để mã hóacác khối dữ liệu thông tin lớn mà chủ yếu dùng cho các thông điệpngắn chẳng hạn như để tạo các khóa chung.

Tạo khóa công khai ElGamal

Cũng như trong trường hợp của mã Diffie-Hellman, hai đối tác A và B có chung (công khai) một số nguyên tố p và một số sinhg (generator). A chọn một số ngẫu nhiên a và tính A = ga, B cũng chọn một số ngẫu nhiên b và tính B = gb. Khóa công khai của A và khóa riêng là a; tương tự như vậy, khóa công khai củaB còn khóa riêng là b.

## 2.3.2. Hệ mật mã “xếp ba lô” Merkle-Hellman

Merkle-Hellman là một hệ mật mã bất đối xứng, có nghĩa là khi giao dịch cần có hai khóa: một khóa công khai và một khóa riêng. Hai khóa đó đều là một chiều với nghĩa là khóa công khai chỉ dùng để mã hóa còn khóa riêng chỉ dùng để giải mã. Cũng vì vậy nó không thể sử dụng để nhận dạng qua việc ký tên bằng mật mã.

Về mặt toán học, hệ Merkle-Hellman dựa trên bài toán tổng tập hợp con subset sum problem (một trường hợp riêng trong bài toán “cái ba lô” (knapsack) quen thuộc trong Toán rời rạc). Bài toán có thể phát biểu như sau: Cho một tập hợp các con số A và một con số b, hãy tìm một tập hợp con của A cộng lại bằng b. Trong trường hợp tổng quát, bài toán đó được biết là có tính NP- đủ (NP complete) (khó giải bậc NP). Tuy nhiên trong trường hợp riêng khi tập hợp các con số (được gọi là cái ba lô) là “siêu tăng” (superincreasing) với nghĩa là có thể sắp xếp thành một dãy để cho mỗi phần tử của tập hợp đều lớn hơn tổng các phần tử đi trước nó, thì bài toán có thể giải được “dễ dàng” trong thời gian đa thức bằng một thuật toán “tham lam” đơn giản.

Tạo khóa

Trong hệ mật mã Merkle-Hellman, các khóa là các “ba lô”. Khóa công khai là một “ba lô đầy” còn khóa riêng là môt “ba lô vơi” (hard and easy knapsacks) kết hợp với hai số phần tử của phép cộng, một số nhân và một modulo, các số này được dùng để biến đổi các ba lô siêu tăng thành ba lô đầy. Những con số đó cũng được dùng để biến đổi tổng của các tập con của ba lô đầy thành tổng các tập con của ba lô vơi, tính toán thực hiện được trong thời gian đa thức.

Mã hóa

Để mã hóa một thông điệp, một tập con cả ba lô đầy được chọn ra bằng cách so sánh nó với một tập hợp các bit (plaintext) có độ dài bằng độ dài chìa khóa và làm cho mỗi thành phần ứng với số 1 trong plaintext một phần tử trong tập con mà bỏ qua những thành phần ứng với số 0 trong plaintext. Các phần tử của tập con đó cộng lại với nhau, tổng số thu được cho ta ciphertext.

Giải mã

Việc giải mã thực hiện được bởi vì số nhân và modulo đã dùng để biến đổi ba lô vơi siêu tăng thành khóa công khai, cũng có thể dùng để biến đổi con số đại diện cho ciphertext thành tổng các phần tử tương ứng của balô siêu tăng. Như vậy, dùng một thuật toán tham lam đơn giản, balô vơi giải ra được bằng cách dùng O(n) phép toán số học để giải mã.

## 2.3.3. Hệ mật mã đường cong Elliptic

Mật mã đường cong elliptic ECC (Elliptic Curve Cryptography) là một dạng mã hóa khóa công khai dựa trên cấu trúc đại số của các đường cong elliptic trên những trường hữu hạn. Việc sử dụng các đường cong elliptic trong mật mã học do Neal Koblitz và Victor S, Miller đề xuất vào năm 1985. Trong giao dịch xã hội nói chung ít sử dụng hệ mật mã đường cong elliptic. Vì vậy trong phạm vi cuốn sách này chúng ta không đi sâu mô tả hệ thống mật mã này mà chỉ giới thiệu qua một số tính chất và đặc điểm của nó.

Mật mã khóa công khai dựa trên tính chất khó giải của một số bài toán tìm thuật toán ngược. Đối với các thủ tục lập - giải mã dựa trên cơ sở đường cong elliptic thì có thể khẳng định rằng việc tìm được logarit rời rạc của một phần tử của đường cong elliptic ngẫu nhiên dựa trên một điểm cơ sở đã biết là không thể làm được. Kích thước của đường cong elliptic xác định độ khó của bài toán. Người ta tin rằng độ bảo mật của một hệ thống mã hóa RSA với modulo lớn có thể đạt được với một nhóm đường cong elliptic bé hơn rất nhiều. Mà nếu ta sử dụng một nhóm bé thì có thể giảm bớt bộ lưu trữ cũng như giảm bớt các yêu cầu về truyền tin.

## 2.4 Các ứng dụng hệ thống mã công khai

## ****2.4.1.Công cụ mã hoá****

Mật mã khóa công khai giải quyết một trong những vấn đề tồn tại lâu của thuật toán đối xứng - vấn đề giao tiếp của chìa khóa được sử dụng cho cả mã hóa và giải mã. Việc gửi chìa khóa qua một kết nối không an toàn sẽ có nguy cơ để lộ cho bên thứ ba đọc được bất kỳ thông điệp nào được mã hóa bằng chìa khóa dùng chung. Mặc dù có các kỹ thuật mật mã (như giao thức trao đổi chìa khóa Diffie-Hellman-Merkle) để giải quyết vấn đề này, nguy cơ bị tấn công vẫn dễ xảy ra. Ngược lại, với mật mã khóa công khai, khóa được sử dụng để mã hóa có thể được chia sẻ an toàn trên bất kỳ kết nối nào. Kết quả là, các thuật toán bất đối xứng cung cấp mức độ bảo vệ cao hơn so với các thuật toán đối xứng.

## ****2.4.2. Hàm băm mật mã học****

Trong ngành mật mã học, một hàm băm mật mã học(Cryptographic hash function) là một hàm băm với một số tính chất bảo mật nhất định để phù hợp việc sử dụng trong nhiều ứng dụng bảo mật thông tin đa dạng, chẳng hạn như chứng thực(authentication) và kiểm tra tính nguyên vẹn của thông điệp(message integrity). Một hàm băm nhận đầu vào là một xâu kí tự dài có độ dài tùy ý và tạo ra kết quả là một xâu kí tự có độ dài cố định, đôi khi được gọi là bản tóm tắt thông điệp(message digest) hoặc chữ kí số (digital fingerprint).

Hàm băm mật mã học là hàm băm có tính chất một chiều. Từ khối dữ liệu ban đầu chỉ có thể đưa ra 1 giá trị băm duy nhất. Một người nào đó bắt được giá trị băm cũng không thể suy ngược ra giá trị, đoạn tin nhắn khởi điểm.

Giá trị đầu vào bị thay đổi thì giá trị băm tương ứng cũng thay đổi. Do vậy nếu 1 kẻ tấn công phá hoại, chỉnh sửa dữ liệu thì server biết ngay lập tức.

Một vài hàm băm thường dùng hiện nay là MD4, MD5, SHA – 0, SHA -1, trong đồ án này sử dụng hàm băm SHA -1, được đánh giá là an toàn hơn MD5 và tạo ra thông điệp tóm tắt 160bit.

## ****2.4.2.Cấp phát chứng thực số.****

Tại Client hệ thống PKI sẽ sử dụng thuật toán sinh khóa hợp lí (ở đây là RSA) để cấp phát cặp khóa riêng và khóa công khai.

Sau khi tạo khóa ngẫu nhiên, hệ thống PKI Client sẽ tạo ra chữ kí số tương ứng với cặp khóa ngẫu nhiên của từng Client và kí theo từng văn bản ngẫu nhiên.

Sau khi Client tạo cặp khóa ngẫu nhiên, kí lên văn bản bất kì. Các thông tin bảo gồm khóa công khai, văn bản rõ, văn bản đã kí được gửi đến Server.

Tại server, server sẽ xác thực những thông tin mà client gửi đến có chính xác và đúng đắn. Nếu thông tin chứng thực là đúng, server sẽ cấp cho client 1 chứng thực số bao gồm thông tin cá nhân, khóa công khai, ngày tạo, ngày hết hạn và ID của chứng thực số có tính duy nhất với mỗi client.

Xác thực: Một người thứ 3 bất kì đều có thể kiểm tra tính đúng đắn của 1 chứng thực số bởi vì PKI Client sẽ cung cấp 1 dịch vụ xác thực. Người dùng nhập vào ID của 1 chứng thực số bất kì và gửi lên Server. Nếu chứng thực số đó tồn tại Server sẽ gửi trả về cho Client vừa kiểm tra.

Một chứng thực số có thể bị thu hồi khi hết hạn hoặc client phát hiện kháo bí mật của mình bị lộ,... Sau đó client có thể xin cấp 1 chứng thực số mới nếu cần.

**Ứng dụng**

Trong thực tế, với những lợi thế về mặt bảo mật, an toàn, dễ triển khai trên hệ thống mạng không an toàn, chứng thực số được ứng dụng rất nhiều, cụ thể là trong việc mã hóa, chống giả mạo, xác thực, chống chối bỏ nguồn gốc, bảo mật phần mềm, bảo mật website,...

Loại mật mã này được sử dụng bởi nhiều hệ thống máy tính hiện đại nhằm cung cấp bảo mật cho thông tin nhạy cảm. Email, ví dụ, có thể được mã hóa bằng các kỹ thuật mã hóa khóa công khai để giữ bí mật nội dung. Giao thức Lớp cổng bảo mật (SSL) giúp kết nối an toàn đến các trang web có thể cũng sử dụng mật mã bất đối xứng. Các hệ thống PKC thậm chí đã được sử dụng như một phương tiện cung cấp một môi trường bỏ phiếu điện tử an toàn có khả năng cho phép cử tri tham gia các cuộc bầu cử từ máy tính tại nhà của họ.

PKC cũng góp mặt nổi bật trong công nghệ blockchain và tiền điện tử. Khi một ví tiền điện tử mới được thiết lập, một cặp chìa khóa sẽ được tạo (chìa khoá công khai và chìa khoá cá nhân). Địa chỉ công khai được tạo bằng cách sử dụng chìa khoá công khai và có thể được chia sẻ an toàn với người khác. Mặt khác, chìa khóa cá nhân được sử dụng để tạo ra các chữ ký kỹ thuật số và xác minh các giao dịch, và do đó, phải được giữ bí mật. Khi một giao dịch đã được xác minh bằng cách xác nhận hash có trong chữ ký kỹ thuật số, giao dịch đó có thể được thêm vào sổ cái blockchain. Hệ thống xác minh chữ ký kỹ thuật số đảm bảo rằng chỉ người có chìa khóa cá nhân được liên kết với ví tiền điện tử tương ứng mới có thể rút tiền. Cần lưu ý rằng các mật mã bất đối xứng được sử dụng trong các ứng dụng tiền điện tử là khác với các mật mã được sử dụng cho mục đích bảo mật máy tính. Ví dụ, [Bitcoin](https://academy.binance.com/vi/articles/what-is-bitcoin) và [Ethereum](https://academy.binance.com/vi/articles/what-is-ethereum) sử dụng một mật mã chuyên dụng được gọi là Thuật toán Chữ ký số Elliptic Curve (ECDSA) để xác minh các giao dịch.

Từ bảo mật máy tính đến xác minh các giao dịch tiền điện tử, mật mã khóa công khai đóng một vai trò quan trọng trong việc bảo mật các hệ thống kỹ thuật số hiện đại. Bằng cách sử dụng các chìa khóa công khai và chìa khoá cá nhân theo cặp, các thuật toán mã hóa bất đối xứng giải quyết các vấn đề bảo mật cơ bản được đưa ra bởi các mã hoá đối xứng. Mặc dù PKC đã được sử dụng trong nhiều năm, các cách sử dụng và các ứng dụng mới vẫn thường xuyên được phát triển cho nó, đặc biệt là trong lĩnh vực blockchain và tiền điện tử.

Các vấn đề quản lý khóa

Cũng giống như các thuật toán mã hóa khác, cách thức phân phối khóa công khai là một trong những yếu tố quyết định đối với độ an toàn của mã bất đối xứng. Quá trình phân phối khóa cần chống lại được tấn công của người đứng giữa.

Giả sử người thứ ba C có thể gửi cho B một khóa bất kỳ và khiến B tin rằng đó là khóa (công khai) của A. Như vậy đồng thời C có khả năng đọc được thông tin trao đổi giữa Bvà A. Muốn vậy, C sẽ gửi cho B khóa công khai của chính mình (và làm cho B nghĩ rằng đó là khóa của A). Sau đó, C đọc tất cả văn bản mã hóa do B gửi, giải mã với khóa bí mật của mình, giữ lại một bản copy đồng thời mã hóa bằng khóa công khai của A và gửi cho A. Về nguyên tắc, cả B và A đều không phát hiện ra sự can thiệp của người thứ ba. Các phương pháp chống lại dạng tấn công này dựa trên các chứng thực số (digital certificate) hoặc các thành phần của hạ tầng khóa công khai PKI (Public Key Infrastructure)

## 3. Chữ ký số

## 3.1 Yêu cầu chữ ký số

Chữ ký số có thể xem là một lớp con của chữ ký điện tử. Sau khi hai đối tác đã trao đổi khóa mã K, A dùng khóa K để mã hóa một nội dung dữ liệu cố định S nào đó: K(S) = S’ và sẽ gắn S’ vào mọi thông điệp của mình phát hành. Khi A nhận được một thông điệp có gắn S’, dùng K để giải mã được lại S thì nhận ra thông điệp là do A phát hành. S’ là chữ ký số của An. Nội dung chữ ký số rấtphong phú: có thể là một đoạn văn bản (họ và tên, chữ ký thật scan lên máy tính, chữ ký vẽ lên máy tính và lưu trữ lại...), một hình ảnh, một câu nói, hoặc một đoạn video và cũng có thể sử dụng hàm bămđể lấy giá trị băm trước khi mã hóa.

Hiện nay có những nhà cung cấp dịch vụ tạo khóa mã và tạo chữký số cho những người cần sử dụng, họ chỉ cần trả phí. Tất nhiênchữ ký số có tính bảo mật thấp hơn vì nội dung cố định nên sau mộtthời gian có thể dùng phương pháp thống kê để thám mã. Để tăngđộ bảo mật, người sử dụng có thể thường xuyên thay đổi nội dungchữ ký số. Chữ ký điện tử hay chữ ký số thường thuộc quyền sử dụngriêng của một người, giống như chữ ký thông thường.

Một tổ chức, một cơ quan hay doanh nghiệp cũng có thể tạomột chữ ký số sử dụng chung để xác nhận cho những thông điệp màcơ quan mình phát hành. Nội dung chữ ký số dùng chung đó là logobiểu tượng của doanh nghiệp, một câu khẩu hiệu của tổ chức hoặcchính là con dấu của tổ chức đó. Vì vậy chữ ký số sử dụng chung chotổ chức cũng được gọi là con dấu số của tổ chức.

Tuy nhiên phần nhiều trong các quy định pháp lý của giao dịch điện tử người ta không nói đến giá trị của con dấu số, nói khác đi, trong giao dịch điện tử không dùng con dấu số đi kèm với chữ ký số/chữ ký điện tử của người có trách nhiệm phát hành thông điệp của cơ quan tổ chức vì hai lý do sau đây:

- Chữ ký số/điện tử chỉ có một người biết và được quyền sử dụng trong khi con dấu số của một tổ chức (nếu có) thì rất nhiều người được quyền sử dụng, do vậy độ bảo mật của con dấu số thấp hơn chữ ký số.

- Trong một cơ quan, tổ chức, người giữ con dấu số thường có mức độ trách nhiệm thấp hơn nhiều so với những người dùng chữ ký số.

Vì vậy, nếu một tổ chức có tạo con dấu số sử dụng trong các thông điệp do cơ quan mình phát hành (kèm với chữ ký số của người có trách nhiệm trong tổ chức) thì cũng chỉ được xem như một sự xác nhận bổ sung không có giá trị tin cậy cao, giống như trong các văn bản thông thường của một tổ chức người ta dùng các giấy tờ, phong bì có in logo, tiêu đề của tổ chức vậy thôi!

## 3.2 Chứng thực điện tử

Trong mật mã học, chứng thực khóa công khai (còn gọi là chứng thực số /chứng thực điện tử) là một chứng thực sử dụng chữ kí số để gắn khóa công khai với một thực thể(cá nhân, máy chủ hoặc công ti...).

Một chứng thực khóa công khai tiêu biểu thường gồm khóa công khai và các thông tin(tên, địa chỉ,...) về thực thể sở hữu khóa đó. Chứng thực số có thể được sử dụng để xác định một khóa công khai thuộc về ai

Nhà cung cấp chứng thực số (Certificate Authoirity – CA) phát hành các chứng thực khóa công khai trong đó CA đó chứng nhận khóa công khai nằm trong mỗi chứng thực thuộc về cá nhân, tổ chức, máy chủ hay bất kì thực thể nào ghi cùng trong chứng thực đó. Nhiệm vụ của CA là kiểm tra tính chính xác của thông tin liên quan đến thực thể được cấp chứng thực. Khi người sử dụng tin tưởng vào một CA và họ có thể kiểm tra chữ kí số của CA thì họ cũng có thể tin vào khóa công khai và thực thể ghi trong chứng thực

Một chứng thực khóa công khai có thể bị thu hồi nếu như khóa riêng tương ứng của nó đã bị lộ hoặc mối liên hệ giữa khóa công khai và chủ thể sở hữu đã thay đổi. Điều này có thể xảy ra ở mức độ không thường xuyên nhưng người sử dụng phải luôn kiểm tra tính pháp lý của chứng thực mỗi khi sử dụng.

Việc kiểm tra này có thể thực hiện bằng cách so sánh chứng thực cụ thể cần xem xét với danh sách các chứng thực bị thu hồi CRL (Certificate Revocation List). Việc đảm bảo danh sách này chính xác và cập nhật là chức năng cơ bản của hạ tầng khóa công cộng tập trung. Tuy nhiên công việc này đòi hỏi tốn kém lớn về nhân công cũng như ngân sách nên thường không được thực hiện đầy đủ. Đểthực sự đạt hiệu quả, danh sách này phải luôn sẵn sàng cho bất kỳ ai cần đến vào bất kỳ thời điểm nào tại mọi nơi.

Một cách kiểm tra khác là truy vấn vào nơi đã cung cấp chứng thực với giao thức kiểm tra chứng thực trực tuyến OCSP (Online Certificate Status Protocol).

Cả hai phương pháp trên đều có thể bị thay thế bằng một chuẩn mới là chuẩn XKMS. Tuy nhiên tiêu chuẩn XKMS này hiện nay còn chưa được sử dụng rộng rãi. Một chứng thực số tiêu biểu gồm các thành phần sau:

- Khóa công khai;

- Tên: có thể là tên người, máy chủ hoặc tổ chức;

- Thời hạn sử dụng;

- Địa chỉ URL của trung tâm thu hồi chứng thực (để kiểm tra).

Cơ quan cấp chứng thực số tự động: Các rô bốt CA (Robot CA) là các chương trình máy tính tự động có khả năng kiểm tra và xác nhận một số khía cạnh của khóa công cộng. Các rô bốt này có thể làm giảm đáng kể những tấn công vào hệ thống, đặc biệt là các tấn công nhằm vào việc làm chệch hướng các luồng thông tin trên mạng. Các khía cạnh của khóa công cộng thường được kiểm tra là:

- Khóa được công bố dưới nhận thức của người sở hữu địa chỉ E-mail gắn với khóa,

- Người sở hữu địa chỉ E-mail đang có khóa bí mật,

- Tình trạng sử dụng khóa.

Phân loại chứng thực số

Công ty Verisign đưa ra mô hình gồm 3 loại chứng thực điện tử sau đây:

- Loại 1 dành cho cá nhân, dự kiến dùng gắn vào cho E-mail.

- Loại 2 dành cho tổ chức với yêu cầu chứng minh nguồn gốc và tư cách pháp nhân.

- Loại 3 dành cho máy chủ và phần mềm với khả năng kiểm trađộc lập bằng cách truy vấn tới CA nơi cung cấp.

# CHƯƠNG 3: HỆ THỐNG CẤP PHÁT VÀ QUẢN LÝ CHỨNG CHỈ SỐ

Mục tiêu:

- Nhằm trang bị cho người học những kĩ năng, thao tác cấp phát và quản lí chứng chỉ số.

1. Mô hình hoạt động của hệ thống chứng chỉ số Thông tin qua Internet sử dụng giao thức **TCP/IP**. Đây là giao thức cho phép các thông tin được gửi từ máy tính này tới máy tính khác thông qua một loạt các máy trung gian hoặc các mạng riêng biệt. Chính điều này đã tạo cơ hội cho những ''kẻ trộm''công nghệ cao có thể thực hiện các hành động phi pháp. Các thông tin truyền trên mạng đều có thể bị nghe trộm (Eavesdropping), giả mạo (Tampering), mạo danh (Impersonation) .v.v.

Các biện pháp bảo mật hiện nay, như dùng mật khẩu, đều không đảm bảo vì có thể bị nghe trộm hoặc bị dò ra nhanh chóng.

Để bảo mật, dữ liệu truyền trên Internet ngày nay đều có xu hướng được mã hoá. Trước khi truyền qua mạng Internet, người gửi thực hiện mã hoá dữ liệu, trong quá trình truyền, dù có ''chặn'' được các dữ liệu này, kẻ trộm cũng không thể đọc được vì bị mã hoá. Khi tới đích, người nhận sẽ sử dụng một công cụ để giải mã.

Phương pháp mã hoá và bảo mật phổ biến nhất đang được thế giới áp dụng là chứng chỉ số (Digital Certificate). Với chứng chỉ số, người sử dụng có thể mã hoá thông tin một cách hiệu quả, chống giả mạo (cho phép người nhận kiểm tra thông tin có bị thay đổi không), xác thực danh tính của người gửi. Ngoài ra chứng chỉ số còn là bằng chứng giúp chống chối cãi nguồn gốc, ngăn chặn người gửi chối cãi nguồn gốc tài liệu mình đã gửi.

**Chứng chỉ số là gì?**

Chứng chỉ số là một tệp tin điện tử dùng để xác minh danh tính một cá nhân, một máy chủ, một công ty... trên Internet. Nó giống như bằng lái xe, hộ chiếu, chứng minh thư hay những giấy tờ xác minh cá nhân. Để có chứng minh thư, bạn phải được cơ quan Công An sở tại cấp.

Chứng chỉ số cũng vậy, phải do một tổ chức đứng ra chứng nhận những thông tin của bạn là chính xác, được gọi là Nhà cung cấp chứng thực số (CA - Certificate Authority). 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:**

     + Dữ liệu cá nhân của người được cấp

     + Khoá công khai (Public key) của người được cấp

    + Chữ ký số của CA cấp chứng chỉ  
**Dữ liệu cá nhân:**

Bao 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**:

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, 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.

Một cách hiểu nôm na, nếu chứng chỉ số là một chứng minh thư nhân dân, thì khoá công khai đóng vai trò như danh tính của bạn trên giấy chứng minh thư (gồm tên địa chỉ, ảnh...), còn khoá cá nhân là gương mặt và dấu vân tay của bạn.

Nếu coi một bưu phẩm là thông tin truyền đi, được "mã hoá" bằng địa chỉ và tên người nhận của bạn, thì dù ai đó có dùng chứng minh thư của bạn với mục đich lấy bưu phẩm này, họ  cũng không được nhân viên bưu điện giao bưu kiện vì ảnh mặt và dấu vân tay không giống.

**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 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.

Lợi ích của chứng chỉ số

**Mã hoá - Bảo mật:**

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 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 dữ liệu 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. 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 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 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. 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.

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 trên 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 và nhân viên.

**Công nghệ SSL có các tính năng nổi bật như:**

+ 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

**Xác thực 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. Chu trình cấp phát chứng chỉ số 2.1. Chuẩn bị hồ sơ

Đối tượng có nhu cầu đăng ký chữ ký số cần phải chuẩn bị hồ sơ cấp chứng thư số bao gồm:

Đối với cá nhân: Chứng minh nhân dân/Căn cước công dân hoặc hộ chiếu của cá nhân đăng ký chữ ký số

Đối với doanh nghiệp, tổ chức, cơ quan: Quyết định thành lập hoặc quyết định quy định về chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức, hoặc giấy chứng nhận đăng ký doanh nghiệp hoặc giấy chứng nhận đầu tư. Kèm theo đó là chứng minh nhân dân/căn cước công dân hoặc hộ chiếu của người đại diện theo pháp luật của tổ chức.

Cá nhân, tổ chức có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc nộp bản sao xuất trình kèm bản chính để đối chiếu. Ngoài ra, cá nhân hoặc tổ chức có nhu cầu đăng ký chữ ký số cần nộp đơn cấp chứng thư số theo mẫu của đơn vị cung cấp dịch vụ chứng thực cho đơn vị đó để được xác thực hồ sơ.

## 2.2. Xác thực hồ sơ đăng ký

Đơn vị cung cấp dịch vụ chứng thực chữ ký số sẽ thực hiện nhận dạng và xác thực hồ sơ của người đăng ký trong quá trình cấp Chứng thư số và thay đổi thông tin.

Sau khi xác thực, đơn vị cung cấp sẽ chấp nhận yêu cầu đăng ký trong trường hợp nhận dạng và xác thực thành công mọi thông tin trong yêu cầu đăng ký, đồng thời nhận được các khoản phí cần thiết để phát hành chứng thư số và tạo lập chữ ký số. Nếu không đáp ứng đủ các điều kiện trên, đơn vị cung cấp có quyền từ chối yêu cầu đăng ký.

## 2.3. Phát hành chứng thư số

Khi yêu cầu cấp Chứng thư số được đơn vị cung cấp chấp nhận, lúc này chứng thư số sẽ được tạo và phát hành dựa theo các thông tin trong bản yêu cầu cấp chứng thư số đã được xác thực định danh.

Đơn vị cung cấp sẽ thông báo cho thuê bao về việc đã tạo xong chứng thư số và cho phép thuê bao truy xuất chứng thư số ngay khi chứng thư số có hiệu lực.

## 2.4. Chấp nhận, công bố và thông báo chứng thư số

Sau khi nhận được thông báo từ đơn vị cung cấp, thuê bao thực hiện xác nhận các thông tin trong Chứng thư số được cấp là chính xác.

Sau đó, đơn vị cung cấp sẽ công bố chứng thư số đã cấp cho thuê bao trên cơ sở dữ liệu về chứng thư số của mình sau khi có xác nhận của thuê bao về tính chính xác của thông tin trên cCTS đó.

Việc thông báo việc cấp phát chứng thư số thuê bao đến các tổ chức, cá nhân khác được thực hiện bằng cách công bố chứng thư số thuê bao trên hệ thống trực tuyến về chứng thư số của đơn vị cung cấp.

## 3. Các thao tác với chứng chỉ:

## 3.1. Phần mềm SmartSign

## 3.2. Môi trường thực hiện

- Trình duyệt Internet Explorer(32 bit) 7 trở lên. IE 32 bit ở máy 64bit nằm ở **C:\Program**

**Files (x86)\Internet Explorer\iexplore.exe**

- Hệ điều hành Windows 7 trở lên

- Cài đặt chương trình SmartSignSetup do SmartSign cung cấp.

- Java plug-in có thể hoạt động trên trình duyệt IE 7 trở lên.

- Token của SmartSign và có chứa chữ ký số do SmartSign cung cấp đang hoạt động.

## 3.3 Hướng dẫn cài chương trình SmartSign

3.1 Tải chương trình SmartSignSetup

- Download tại <https://www.smartsign.com.vn/downloads/SmartSign.rar>

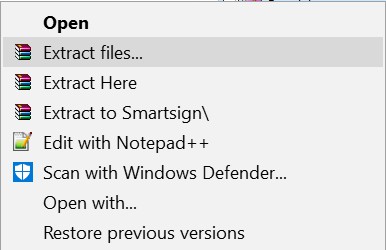
3.2 Hướng dẫn cài đặt

- Bước 1: Mở thư mục chứa tập tin SmartSign vừa mới tải về



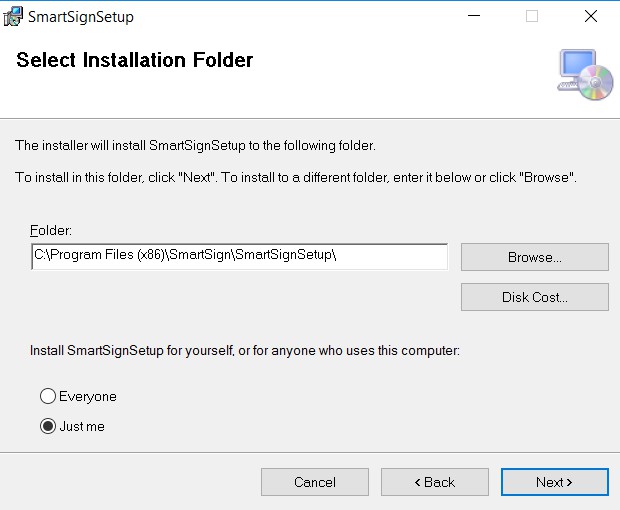
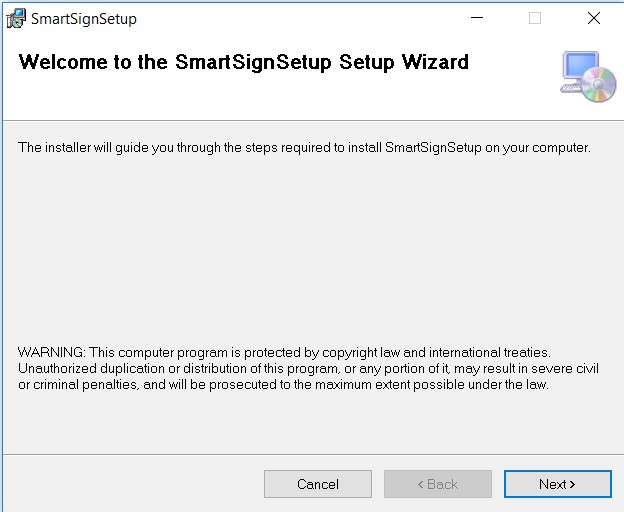
- Bước 2: Giải nén tập tin bằng cách click chuột phải vào tập tin SmartSignSetup.rar sau đó

chọn Extract file giống hình.



- Bước 3: Sau khi giải nén xong vào thư mục SmartSignSetup, Double Click chuột trái vào tập tin SmartSignSetup.msi để cài đặt.

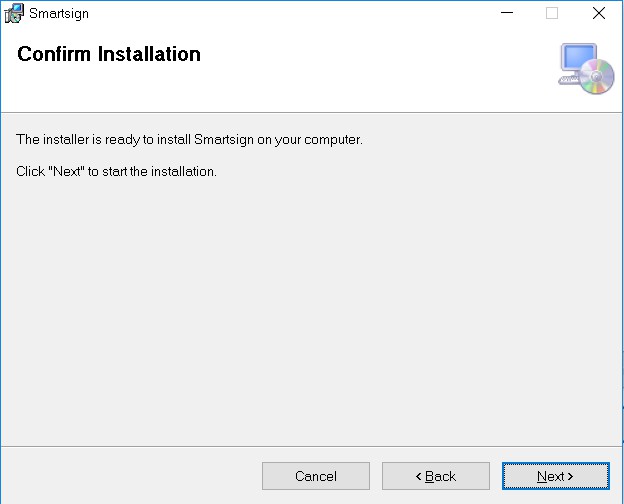
- Bước 4: Click Next để tiếp tục



- Bước 5: Để thay đổi đường dẫn chứa tập tin cài đặt click vào sau đó chọn



vào thư mục cần chứa file. Sau đó Click Next để tiếp tục.

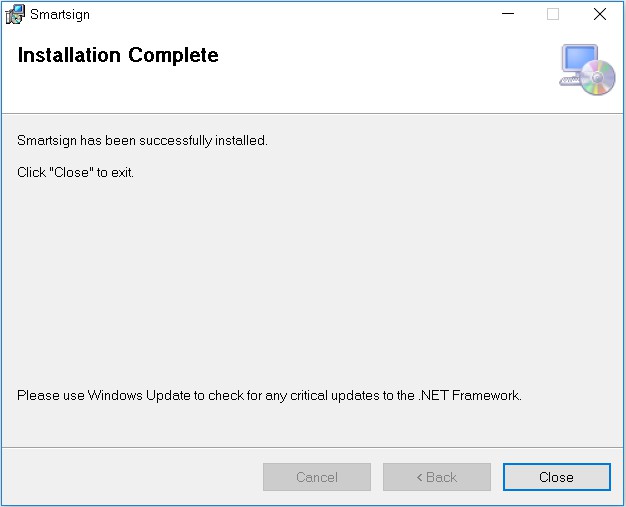


- Bước 6: Click Next để tiếp tục

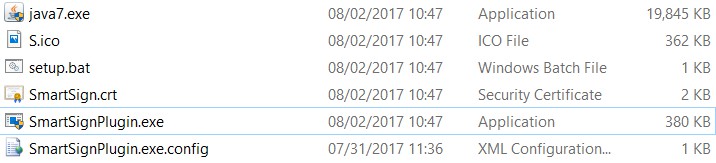


- Bước 7: Click Yes để tiếp tục

- Bước 8 : Click Close để hoàn tất.



- Bước 9: Sau khi cài đặt hoàn tất vào thư mục chứa chương trình SmartSign vừa cài đặt double click chuột vào SmartSignPlugin.exe



- Hoặc ra ngoài Desktop double click chuột trái vào biểu tượng chương trình

SmartSignPlugin

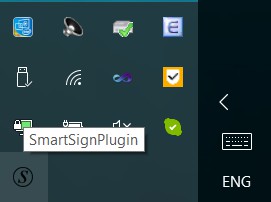


- Bước 10: click Yes để tiếp tục

o Sau khi bấm Yes nếu máy tính sẽ hiện lên màn hình cài đặt java nếu máy tính đã có

java thích hợp để cập nhật chữ ký số thì chương trình sẽ bỏ qua bước cài đặt java.

o Sau khi chạy hoàn tất SmartSignPlugin sẽ hiện thị ở thanh taskbar



## 3.4 Hướng dẫn cài đặt java (Nếu máy có Java thích hợp vui lòng bỏ qua bước này)

4.1 Tải tập tin cài đặt java

- Cách 1: Download tại <https://www.smartsign.com.vn/downloads/java.rar>

- Cách 2: Cài lại chương trình SmartSign như trên

4.2 Hướng dẫn cài đặt

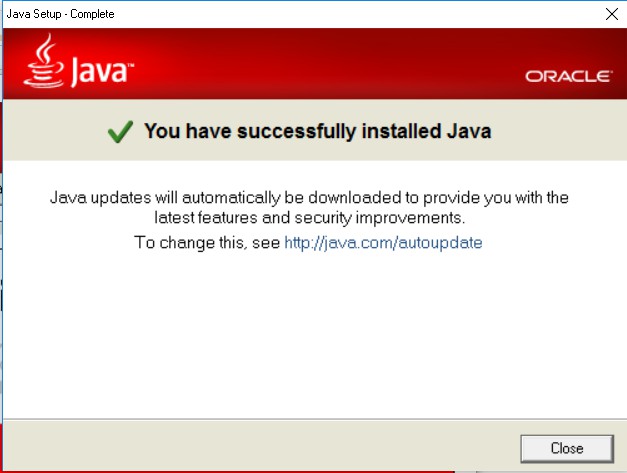
- Bước 1: Khi click vào chương trình cài đặt màn hình hiển thị như sau:



- Bước 2: Click vào Install để tiếp tục



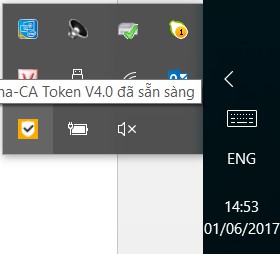
- Bước 3: Click và close để kết thúc quá trình cài đặt



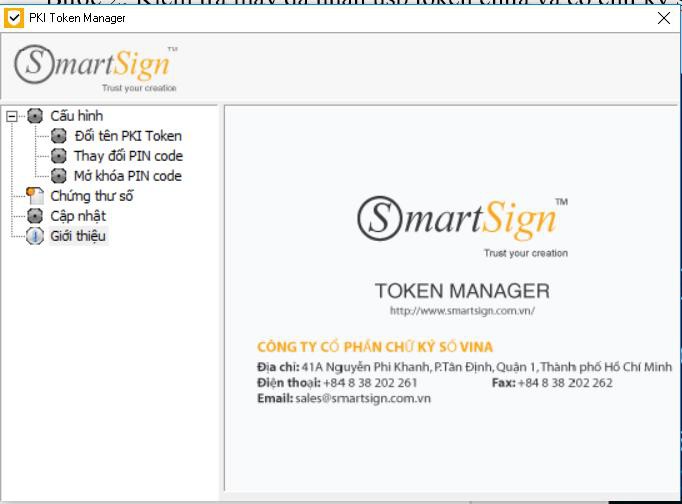
## 3.5 Hướng dẫn gửi yêu cầu cập nhật chữ ký số

- Bước 1: Cắm Token có chứa chữ ký số của SmartSign đang cần cập nhật vào máy.

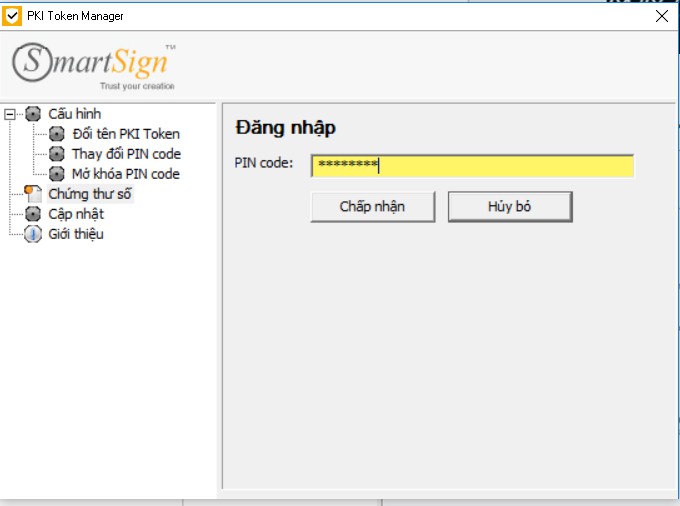
- Bước 2: Kiểm tra máy đã nhận token chưa và có chữ ký số mà cần cập nhật hay không bằng cách click vào biểu tượng ở trên thanh taskbar



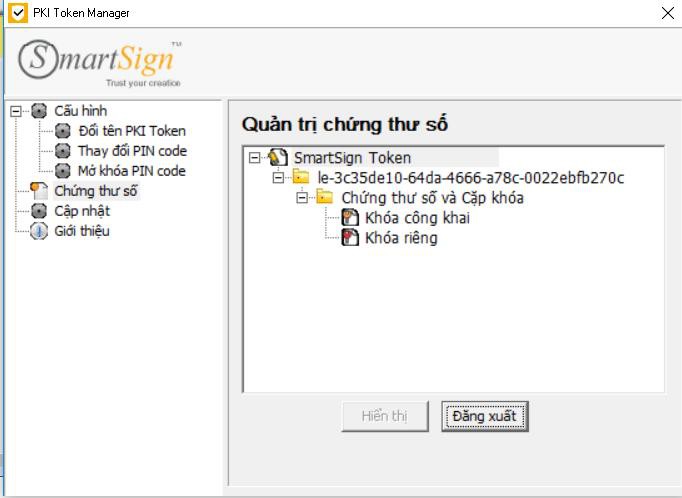
- Sau khi click vào màn hình hiển thị như sau:



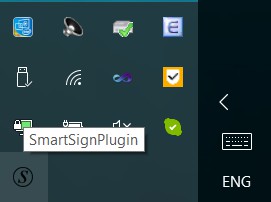
- Bước 3: click vào chứng thư số và sau đó nhập đúng mã pin của token



- Bước 4: Bấm vào nút chấp nhận để xem chữ ký số có trong token



- Bước 5: Kiểm tra chương trình SmartSignPlugin có chạy không bằng cách kiểm tra xem có biểu tượng chữ S ở dưới thanh taskbar



- Bước 6 : Mở trình duyệt lên chọn chứng thư số cần cập nhật thời hạn



- Bước 7: Chọn chứng thư số sau đó chọn ok để tiếp tục



- Bước 8 : Click vào bắt đầu hoặc thử lại để tiếp tục.



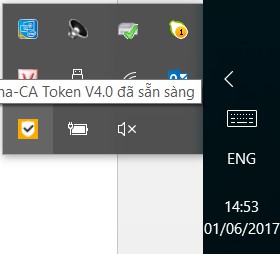
- Bước 9: Kiểm tra lại thông giao dịch và mã số thuế có đúng hay không. Sau đó điền đầy đủ các thông tin người liên hệ, Email và số điện thoại liên lạc vào các text box tương ứng (Vui lòng điền đúng và đủ các thông tin số điện thoại và Email để nhận mã kích hoạt và thông tin hồ sơ). Bấm vào đồng ý để hoàn tất gửi yêu cầu.



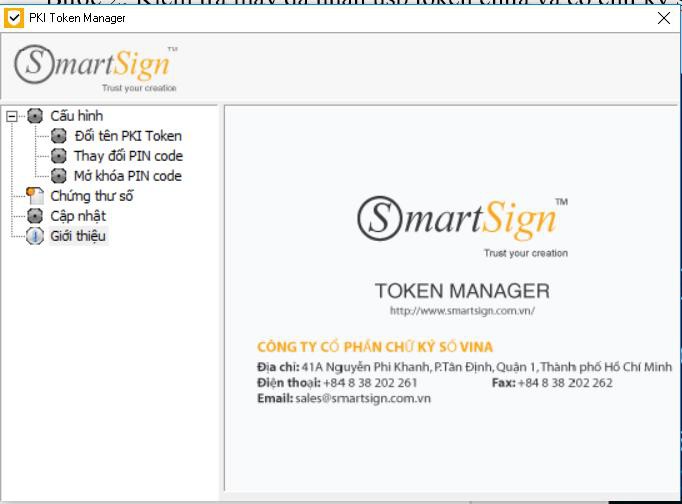
**3.6 Hướng dẫn gửi yêu cầu cập nhật chữ ký số java**

- Bước 1: Cắm Token có chứa chữ ký số của SmartSign đang cần cập nhật vào máy.

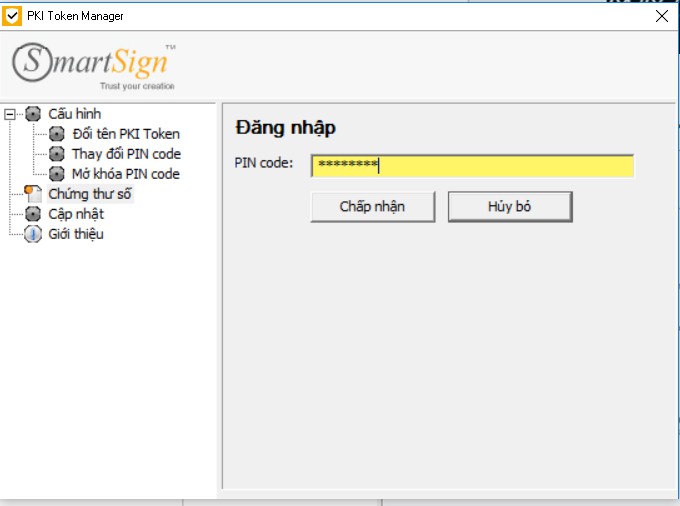
- Bước 2: Kiểm tra máy đã nhận token chưa và có chữ ký số mà cần cập nhật hay không bằng cách click vào biểu tượng ở trên thanh taskbar



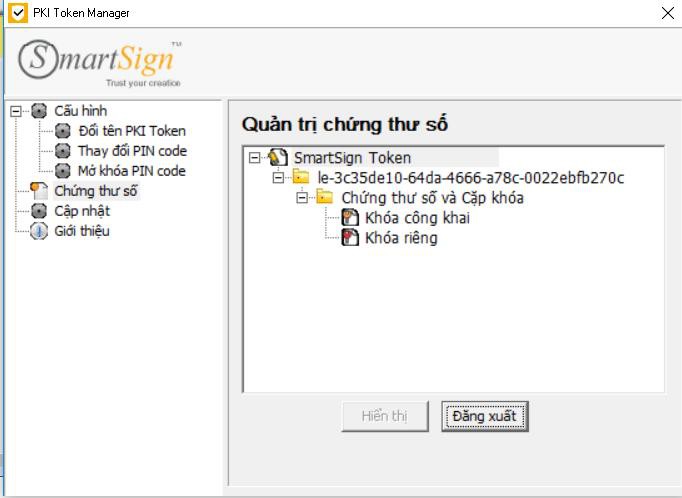
- Sau khi click vào màn hình hiển thị như sau:



- Bước 3: click vào chứng thư số và sau đó nhập đúng mã pin của token



- Bước 4: Bấm vào nút chấp nhận để xem chữ ký số có trong token



- Bước 5: Mở trình duyệt IE 32 bit lên(IE 32 bit ở máy 64bit nằm ở **C:\Program Files**

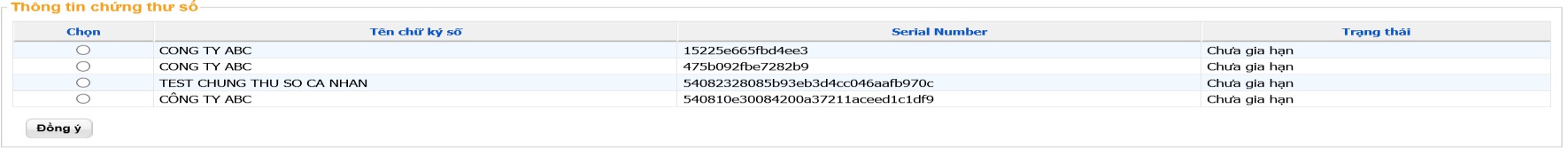
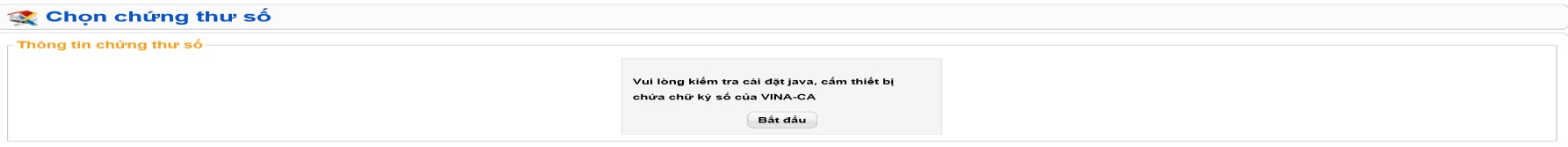
**(x86)\Internet Explorer\iexplore.exe**) và vào đường dẫn <http://dl.smartsign.com.vn/giahan>



- Bước 6: Click vào Run để tiếp tục



- Bước 7: Click vào bắt đầu màn hình hiển thị như sau



- Bước 8: Màn hình trên sẽ hiển thị toàn bộ những chứng thư số có trong token của smartsign.

Chọn đúng chữ ký số cần cập nhật bằng cách click vào sau đó click vào Đồng ý để tiếp tục



- Bước 9: Kiểm tra lại thông giao dịch và mã số thuế có đúng hay không. Sau đó điền đầy đủ

các thông tin người liên hệ, Email và số điện thoại liên lạc vào các text box tương ứng (Vui lòng điền đúng và đủ các thông tin số điện thoại và Email để nhận mã kích hoạt và thông tin hồ sơ). Bấm vào đồng ý để hoàn tất gửi yêu cầu.

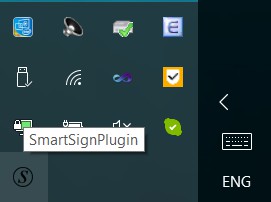


## 3.7 Hướng dẫn cập nhật chữ ký số cách 2 sử dụng Java

- Bước 1: Cắm thiết bị token có chứa chữ ký số mà đã gửi yêu cầu cập nhật vào máy.

- Bước 2: kiểm tra máy tính đã nhận được thiết bị hay chưa giống như ở trên.

- Bước 3: Kiểm tra chương trình SmartSignPlugin có chạy không bằng cách kiểm tra xem có biểu tượng chữ S ở dưới thanh taskbar



- Bước 4: Mở trình duyệt IE 32 bit lên(IE 32 bit ở máy 64bit nằm ở **C:\Program Files (x86)\Internet Explorer\iexplore.exe**) và vào đường dẫn [http://dl.smartsign.com.vn/capnhat và](http://dl.smartsign.com.vn/capnhat) chọn chọn chứng thư số cần cập nhật thời hạn.

- Bước 7: Chọn chứng thư số sau đó chọn ok để tiếp tục

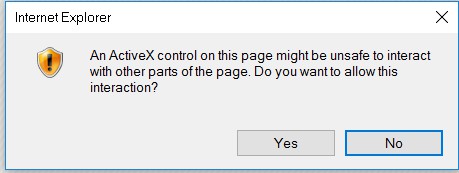


- Bước 8: Click vào bắt đầu màn hình hiển thị như sau:

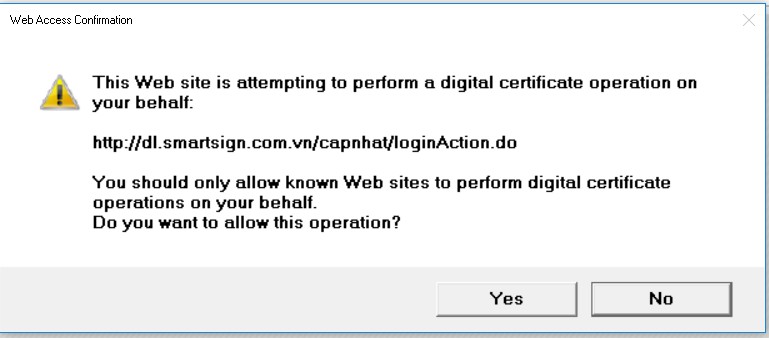


- Bước 9: Nhập mã kích hoạt vào ô mã kích hoạt sau đó click vào đồng ý để tiếp tục

 Lưu ý: Mã kích hoạt là mã mà Quý khách nhận được ở trong email và tin nhấn sau khi yêu cầu Quý khách được duyệt.



- Click Yes để tiếp tục, màn hình hiển thị như sau:



 Lưu ý: Nếu trình duyệt không hiển thị như trên làm thì hướng dẫn mục 7 hướng dẫn bật ActiveX cho trình duyệt.

- Bước 10: click vào Yes để tiếp tục.

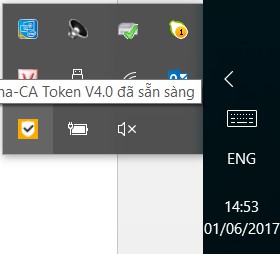
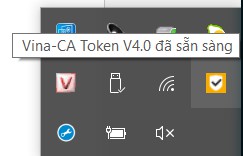


- Bước 11: kiểm tra lại thông tin tên giao dịch và mã số thuế có đúng hay không sau đó chọn

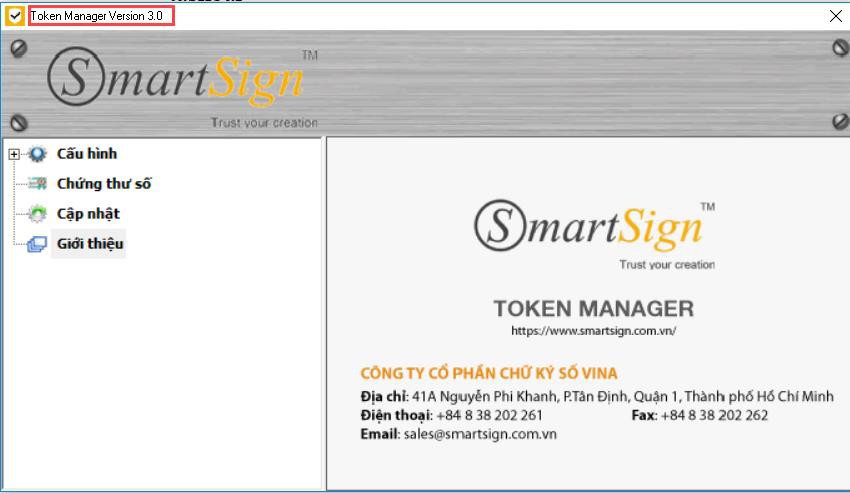
đúng phiên bản token bằng cách click vào



- Lưu ý: Để kiểm tra phiên bản token vui lòng đưa chuột vào biểu tượng ở trên thanh taskbar hoặc click vào biểu tượng ở trên thanh taskbar

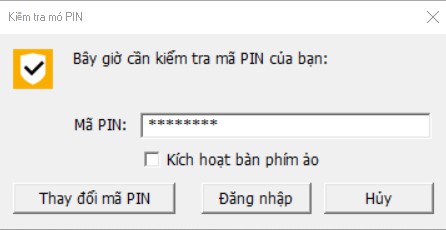


- Màn hình hiển thị như sau:



- Nhìn lên góc trên cùng bên trái sẽ thấy được phiên bản của token

- Bước 12: Sau khi chọn đúng phiên bản chứng thư số click vào tạo chứng thư số để tiếp tục



- Bước 13: Click vào tạo chứng thư số màn hệ thống sẽ bắt nhập mã pin của token. Nhập

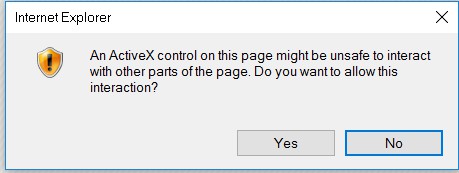
đúng mã pin sau đó nhấn đăng nhập để tiếp tục.



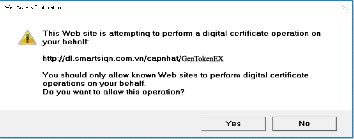
o Lưu ý: Hệ thống có thể sẽ hỏi đi hỏi lại mã pin nhiều lần Quý khách vui lòng nhập đến khi hệ thống không còn hỏi nữa. Trong quá trình tạo chứng thư số vui lòng không tắt trình duyệt và rút thiết bị token cho đến khi quá trình hoàn tất.

- Bước 12: Sau khi hệ thống đã tạo các cặp khóa công khai và bí mật mà hình hiển thị như

sau:



- Click Yes để tiếp tục



- click Yes để tiếp tục.



- Bước 14: Click vào ok để hoàn tất quá trình cập nhật



## 3.8 Hướng dẫn cập nhật chữ ký số cách 2 sử dụng Java

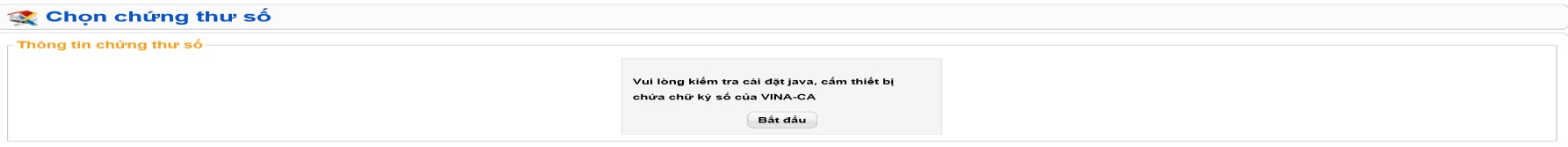
- Bước 1: Cắm thiết bị token có chứa chữ ký số mà đã gửi yêu cầu cập nhật vào máy.

- Bước 2: kiểm tra máy tính đã nhận được thiết bị hay chưa giống như ở trên.

- Bước 3: Mở trình duyệt IE 32 bit lên(IE 32 bit ở máy 64bit nằm ở **C:\Program Files (x86)\Internet Explorer\iexplore.exe**) và vào đường dẫn<http://dl.smartsign.com.vn/capnhat>



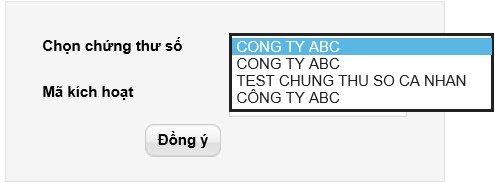
- Bước 4: Click vào Run để tiếp tục



- Bước 5: Click vào bắt đầu màn hình hiển thị như sau:

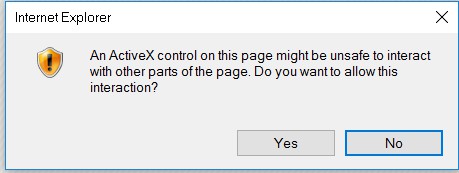


- Bước 6: Chọn đúng chữ ký số cần cập nhật bằng cách click chuột vào khung

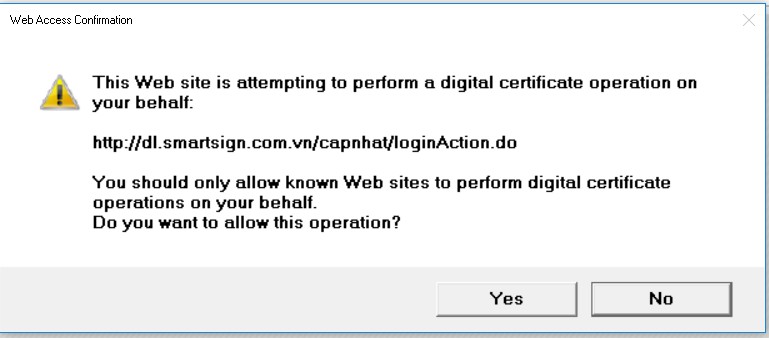


- Bước 7: Nhập mã kích hoạt vào ô mã kích hoạt sau đó click vào đồng ý để tiếp tục

 Lưu ý: Mã kích hoạt là mã mà Quý khách nhận được ở trong email và tin nhấn sau khi yêu cầu Quý khách được duyệt.



- Click Yes để tiếp tục, màn hình hiển thị như sau:



 Lưu ý: Nếu trình duyệt không hiển thị như trên làm thì hướng dẫn mục 7 hướng dẫn bật ActiveX cho trình duyệt.

- Bước 8: click vào Yes để tiếp tục.

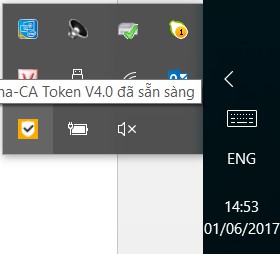
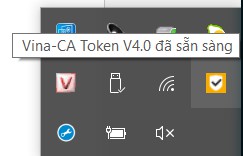


- Bước 9: kiểm tra lại thông tin tên giao dịch và mã số thuế có đúng hay không sau đó chọn

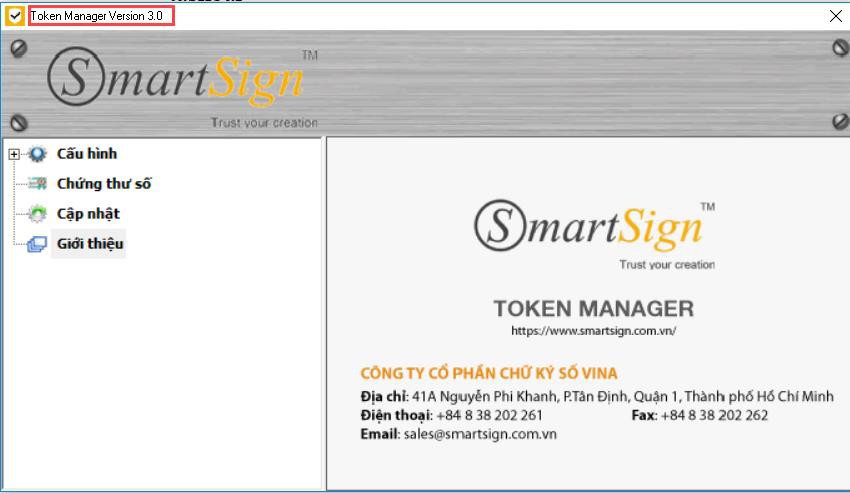
đúng phiên bản token bằng cách click vào



- Lưu ý: Để kiểm tra phiên bản token vui lòng đưa chuột vào biểu tượng ở trên thanh taskbar hoặc click vào biểu tượng ở trên thanh taskbar

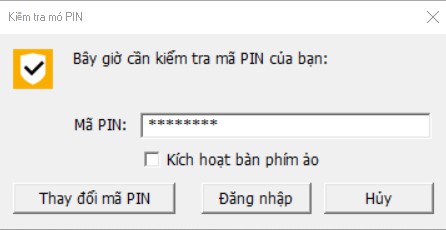


- Màn hình hiển thị như sau:



- Nhìn lên góc trên cùng bên trái sẽ thấy được phiên bản của token

- Bước 10: Sau khi chọn đúng phiên bản chứng thư số click vào tạo chứng thư số để tiếp tục



- Bước 11: Click vào tạo chứng thư số màn hệ thống sẽ bắt nhập mã pin của token. Nhập

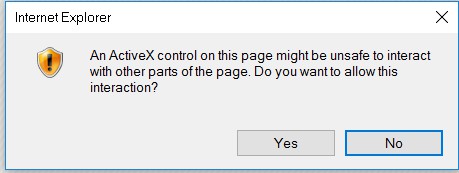
đúng mã pin sau đó nhấn đăng nhập để tiếp tục.



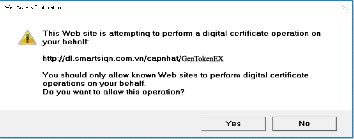
o Lưu ý: Hệ thống có thể sẽ hỏi đi hỏi lại mã pin nhiều lần Quý khách vui lòng nhập đến khi hệ thống không còn hỏi nữa. Trong quá trình tạo chứng thư số vui lòng không tắt trình duyệt và rút thiết bị token cho đến khi quá trình hoàn tất.

- Bước 12: Sau khi hệ thống đã tạo các cặp khóa công khai và bí mật mà hình hiển thị như

sau:



- Click Yes để tiếp tục



- click Yes để tiếp tục.

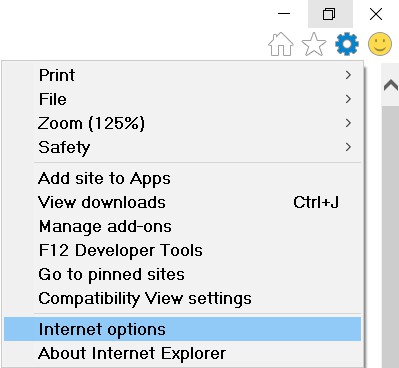


- Bước 13: Click vào ok để hoàn tất quá trình cập nhật

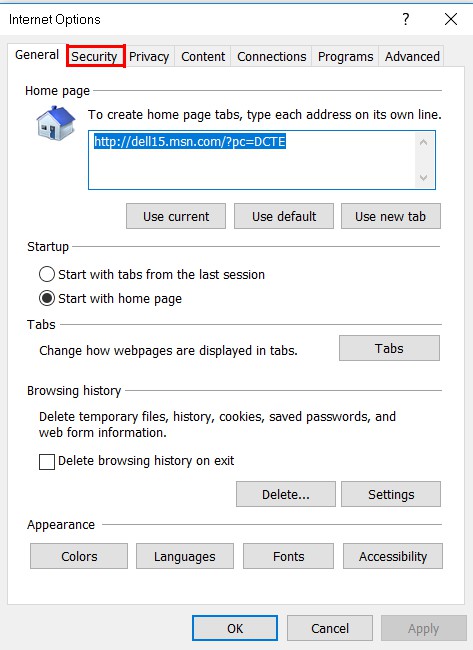


## 3.9 Hướng dẫn bật ActiceX cho trình duyệt IE

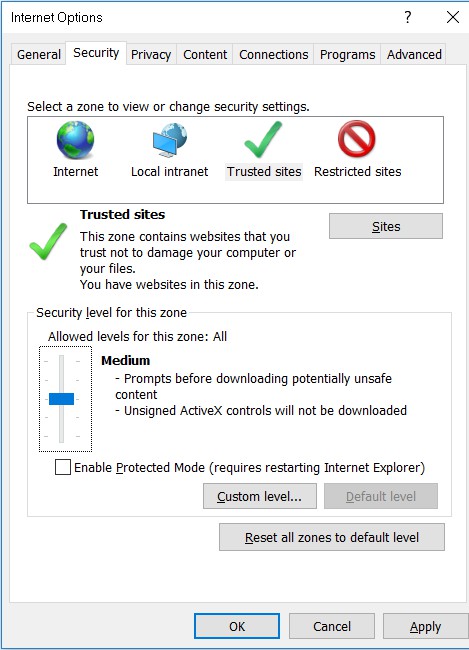
- Bước 1: Mở trình duyệt IE lên click vào biểu tượng ở góc trên bên phải của màn hình hoặc bấm tổ hợp phím ALT+X



- Bước 2: Click vào internet options



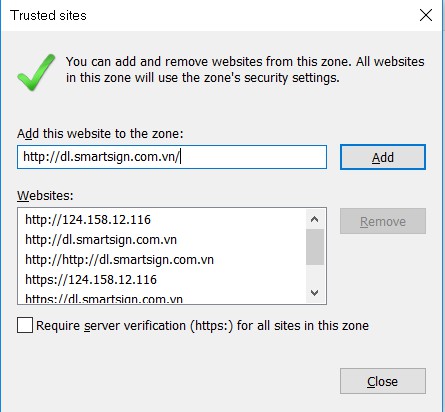
- Bước 3: Chọn tab Security



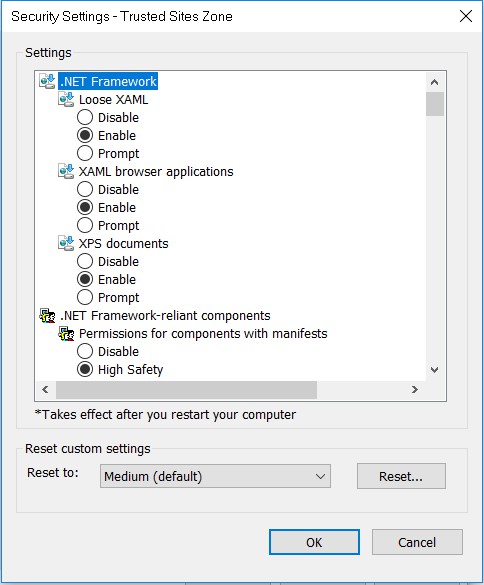
- Bước 4: Chọn Trusted sites ,sau đó chọn



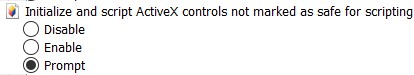
o Kiểm tra xem website [http://dl.smartsign.com.vn c](http://dl.smartsign.com.vn/)ó tồn tại trong danh sách website hay không, Nếu không có thì thêm [http://dl.smartsign.com.vn v](http://dl.smartsign.com.vn/)ào Add this website



- Bước 5: Chọn Trusted sites ,sau đó chọn custom lever



- Bước 6: Kéo xuống phía bên dưới bằng cách lăn chuột hoặc kéo thanh scroll bar trong danh mục ActiveX controls and plug-in tìm Initialize and script ActiceX controls not marked as safe for scripting chọn Enable hoặc Prompt bằng cách click vào .



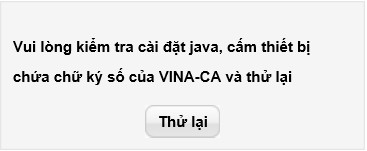
- Bước 7: Click vào Ok để hoàn tất.



**10 Hướng dẫn sửa các lỗi thường gặp**

10.1 Không nhận chữ ký số, không đúng trình duyệt, có nhiều phiên bản java hoặc chưa cài java

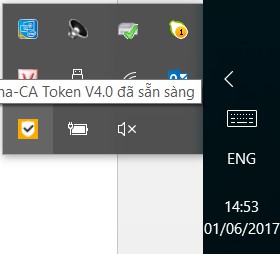
- Khi click vào nút thử lại nhiều lần như vẫn không hiện ra danh sách chữ ký số.



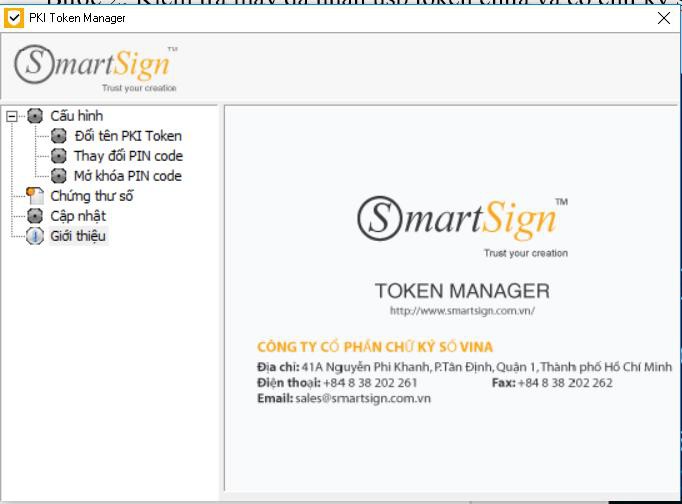
- Kiểm tra lại trình có đúng là IE 7 trở lên hay không.

- Kiểm tra đã cắm Token vào máy và máy đã nhận token hay chưa bằng cách click vào biểu

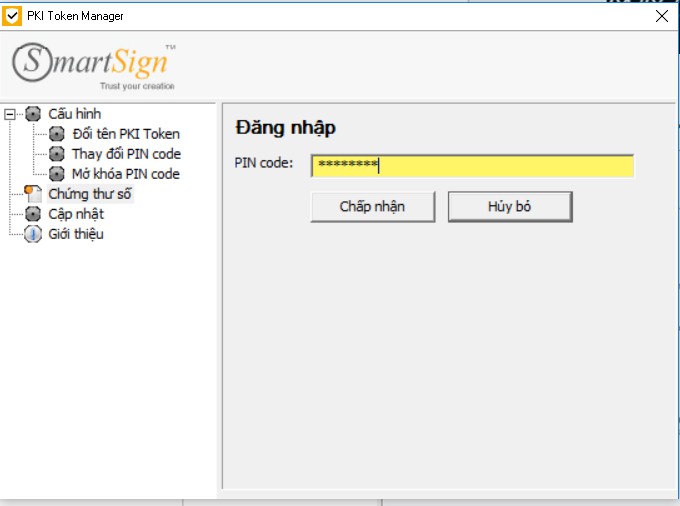
tượng ở trên thanh taskbar



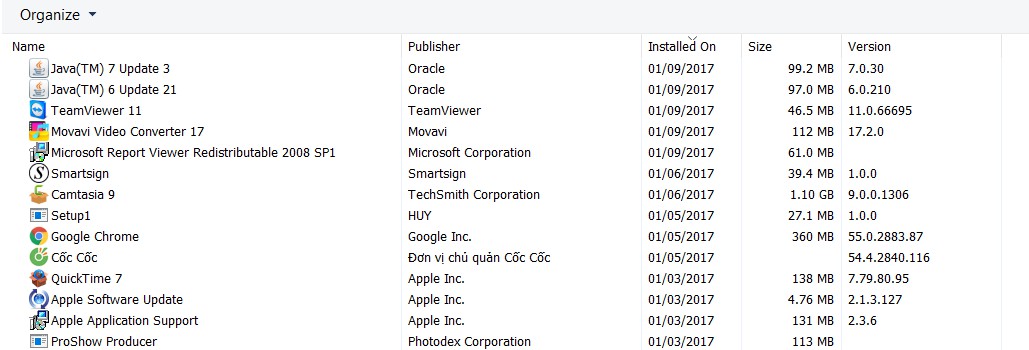
- Sau khi click vào màn hình hiển thị như sau:



- Bước 3: click vào chứng thư số và sau đó nhập đúng mã pin của token



- Kiểm tra phiên bản java bằng cách vào control panel Program and features tìm kiếm những phiên bản java đã cài đặt



- Gởi toàn bộ những phiên bản java đã cài chỉ giữ lại java(TM) 7 update 3.

10.2 Không hiển thị các phiên bản chứng thư số khi vào trang cập nhật

- Bật ActiveX controls and plug-in tìm Initialize and script ActiceX controls not marked as

safe for scripting xem hướng dẫn chi tiết ở mục 7.

IV. ĐIỀU KIỆN THỰC HIỆN MÔN HỌC

+ Giáo trình môn học;

+ Mạng máy tính;

+ Máy chiếu Projector;

- Phần mềm: Các phần mềm liên quan: diệt virus, bảo mật dữ liệu, mã hóa,…

V. PHƯƠNG PHÁP VÀ NỘI DUNG ĐÁNH GIÁ

*\* Đánh giá:*

- Kiến thức: Được đánh giá bằng hình thức kiểm tra viết, trắc nghiệm

- Kỹ năng: Đánh giá kỹ năng thực hành theo hình thức: từng người học, thảo luận nhóm

*\* Hình thức thi:* Tự luận - trắc nghiệm, 60 phút

VI. HƯỚNG DẪN THỰC HIỆN MÔN HỌC

*1. Phạm vi áp dụng chương trình*

Chương trình môn học được sử dụng giảng dạy cho người học năm thứ 3 cao đẳng nghề TMĐT.

*2. Hướng dẫn một số điểm chính về phương pháp giảng dạy môn học:* Nội dung được biên soạn theo phương pháp tích hợp do đó cần lưu ý một số điểm sau:

- Phần mềm, thiết bị giảng dạy, máy tính phải được chuẩn bị trước khi giảng dạy;

- Thực hiện giảng dạy tốt nhất ở nơi thực hành và lí thuyết;

- Người học được chia thành các nhóm nhỏ để thực hành hoặc thảo luận.

*3. Những trong tâm chương trình cần chú ý:*

- Các nguy cơ mất an toàn dữ liệu trong TMĐT;

- Phòng chống và khắc phục mất an toàn dữ liệu.

*4. Tài liệu tham khảo*

- TS. Trần Văn Hoè, Giáo trình Thương mại điện tử căn bản, NXB Đại học Kinh tế Quốc Dân,2007

- Bộ môn CNTT, Giáo trình An toàn dữ liệu, Đại học Thương Mại, 2007.

- Phan Đình Diệu, Lý thuyết mật mã và an toàn thông tin, Đại học Quốc gia Hà Nội, 1999.

- Man Young Rhee. Internet Security: Cryptographic principles, algorithms and protocols. John Wiley & Sons, 2003.