ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

Phan Trọng Khanh

AN TOÀN THÔNG TIN TRONG THUẾ ĐIỆN TỬ

KHOÁ LUẬN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

Ngành: Công nghệ thông tin

HÀ NỘI - 2010

Lời cảm ơn

Lời đầu tiên, tôi xin gửi lời cảm ơn chân thành tới thầy giáo, Tiến sĩ Lê Phê Đô, người đã hướng dẫn và chỉ bảo tận tình cho tôi trong suốt quá trình học tập cũng như thực hiện khóa luận tốt nghiệp này.

Tôi cũng xin cảm ơn các thầy, cô giáo đã chỉ bảo trong suốt quá trình học tập tại trường Đại học Công Nghệ - Đại học Quốc Gia Hà Nội. Cảm ơn bạn Đỗ Đức Bảo đã giúp đỡ, hợp tác với tôi nghiên cứu các vấn đề an toàn và các phần đề liên quan đến thuế được trình bày trong khóa luận này.

Cuối cùng, tôi muốn gửi lời cám ơn tới bố mẹ tôi, tới gia đình và bạn bè - những người đã hết sức ủng hộ, giúp đỡ và động viên tôi trong suốt quá trình học tập đã qua.

Tóm tắt khóa luận

Khóa luận tốt nghiệp này trình bày một số hiểu biết cơ bản về thuế và thuế điện tử như các loại thuế, tình hình triển khai thuế điện tử ở Việt Nam. Qua đó giúp người đọc hiểu thêm về một lĩnh vực khá lạ với công nghệ thông tin đó là thuế, đồng thời cũng giúp hình dung được viễn cảnh thuế điện tử ở Việt Nam.

Khóa luận cũng trình bày những kiến thức tổng quát về phương pháp mã hóa khóa công khai, một phương pháp được sử dụng rộng rãi trong việc mã hóa văn bản và chữ ký số. Cùng với chữ ký số, hệ thống PKI (Cơ sở hạ tầng khóa công khai) cũng được giới thiệu giúp người đọc hiểu được phần nào cốt lõi của hệ thống thuế điện tử.

Phần chính của khóa luận là đưa ra những giải pháp triển khai thuế điện tử. Phần này cũng phân tích kĩ các giải pháp và đưa và những phương án có thể sử dụng để triển khai trong thực tế. Phần ứng dụng sẽ trình bày mẫu một hệ thống PKI qua đó người đọc có thể hiểu về chữ ký số, chứng nhận số,... một cách trực quan hơn.

Mục lục

Danh mục hình ảnh

Mở đầu

Thủ tục hành chính đang là một trong những vấn đề nhức nhối ở Việt Nam hiện nay. Theo Tổng cục Thuế, thủ tục hành chính thuế hiện nay "bao gồm 330 thủ tục hành chính thuế, trong đó, 5 thủ tục hành chính do cấp Tổng cục Thuế thực hiện, 172 thủ tục hành chính do cấp Cục Thuế thực hiện và 153 thủ tục hành chính cấp Chi cục Thuế thực hiện"*. Cải cách thủ tục hành chính nói chung và trong lĩnh vực Thuế nói riêng là điều thực sự cần thiết. Biện pháp đang được tiến hành hiện nay là triển khai Thuế điện tử và chính phủ điện tử. Việc này sẽ tiết kiệm được rất nhiều chi phí và thời gian làm việc của các doanh nghiệp cũng như cơ quan thuế.

Thuế điện tử sẽ tạo ra những điều kiện thuận lợi nhất cho người nộp thuế, thực hiện nghĩa vụ thuế sẽ không cần phải đi lại, xếp hàng chờ đợi như hiện nay mà có thể làm mọi lúc, mọi nơi, trong thời gian rất ngắn.

Khóa luận này tập trung vào việc nghiên cứu những giải pháp an toàn trong triển khai Thuế điện tử. Từ đó cũng đề xuất những phương án thực hiện cũng như lựa chọn công nghệ sử dụng trong quá trình xây dựng hệ thống Thuế điện tử ở Việt Nam.

* Công văn của Tổng cục Thuế số 3343/TCT-CC

Chương 1. Tổng quan về thuế và thuế điện tử

1.1. Những vấn đề cơ bản về thuế

1.1.1. Định nghĩa thuế

Thuế là số tiền thu của các công dân, hoạt động và đồ vật (như giao dịch, tài sản) nhằm huy động tài chính cho chính quyền, nhằm tái phân phối thu nhập, hay nhằm điều tiết các hoạt động kinh tế-xã hội.

1.1.2. Các nguyên tắc chung về thuế

Các sắc thuế đều cần thỏa mãn bằng nguyên tắc chung sau đây:

Trung lập: sắc thuế không được bóp méo các hoạt động sản xuất, dẫn tới phúc lợi xã hội (tổng hiệu dụng) của nền kinh tế bị giảm đi.

Đơn giản: việc thiết kế sắc thuế và tiến hành trưng thu thuế phải không phức tạp và không tốn kém.

Công bằng: sắc thuế phải đánh cùng một tỉ lệ vào các công dân có điều kiện như nhau. Giữa các công dân có điều kiện khác nhau, thì thuế suất cũng cần khác nhau (vì thông thường người có điều kiện tốt hơn có xu hướng tiêu dùng hàng hóa công cộng nhiều hơn).

Riêng các sắc thuế địa phương còn cần thỏa mãn một số nguyên tắc nữa:

Cơ sở thuế phải bất biến: nghĩa là công dân, hoạt động và đồ vật phải tương đối cố định, không hay di chuyển giữa các địa phương. Nguyên tắc này nhằm đảm bảo địa phương này không đánh thuế lên công dân, hoạt động và đồ vật vốn là của địa phương khác.

Nguồn thu ổn định: nghĩa là quy mô dân số địa phương và quy mô các hoạt động, đồ vật không nên biến động thường xuyên. Nguyên tắc này nhằm đảm bảo thu ngân sách của địa phương không bị biến động.

Nguồn thu phân bố đồng đều giữa các địa phương. Nguyên tắc này nhằm đảm bảo nguồn thu ngân sách giữa các địa phương không quá chênh lệch.

Chính quyền địa phương phải có trách nhiệm tài chính. Nguyên tắc này nhằm

đảm bảo chính quyền địa phương không lạm dụng quyền hạn thuế của mình để đánh thuế quá mức.

Trong thực tế, khó có sắc thuế nào đảm bảo đầy đủ các nguyên tắc đòi hỏi cho nó. Vì thế, theo nguyên tắc về "cái tốt thứ hai", sắc thuế nào càng thỏa mãn nhiều nguyên tắc, thì càng xứng đáng là một sắc thuế tốt. Việc ban hành phần lớn các sắc thuế thường cần phải được quốc hội phê chuẩn và phải có luật về sắc thuế đó.

1.1.3. Phân loại thuế

Thuế trực thu và thuế gián thu

Các sắc thuế khi phân loại theo hình thức thu sẽ gồm hai loại là thuế trực thu và thuế gián thu. Thuế trực thu là thuế mà người, hoạt động, đồ vật chịu thuế và nộp thuế là một. Ví dụ như một người nhập hàng hóa từ nước ngoài về và tiêu dùng luôn, hay như thuế thu nhập doanh nghiệp hay thu nhập cá nhân, nhà đất... Thuế gián thu là thuế mà người chịu thuế và người nộp thuế không cùng là một. Chẳng hạn, chính quyền đánh thuế vào công ty (công ty nộp thuế) và công ty lại chuyển thuế này vào chi phí tính vào giá hàng hóa và dịch vụ, do vậy đối tượng chịu thuế là người tiêu dùng cuối cùng. Ví dụ: thuế VAT, thuế tiêu thụ đặc biệt...

Thuế nội địa và thuế quan

Thuế nội địa: là thuế đánh vào công dân, hoạt động, tài sản trong nước. Có rất nhiều sắc thuế nội địa đánh vào cá nhân (thuế thu nhập, thuế tiêu thụ), đánh vào công ty (thuế pháp nhân, thuế môn bài, ...), đánh vào các hoạt động (thuế giao dịch tài chính, thuế mua bán nhà đất, thuế thừa kế, ...), thuế đánh vào đồ vật (thuế tài sản, lệ phí phòng cháy chữa cháy, lệ phí đăng ký ô tô xe máy, lệ phí công chứng, ...). Lưu ý lệ phí thực chất là thuế; ở Việt Nam gọi chúng là "các loại phí mang tính chất thuế".

Thuế quan: là thuế đánh vào hàng hóa di chuyển giữa các quốc gia/lãnh thổ (nên còn gọi là thuế xuất nhập khẩu).

Một số hàng hóa nhập khẩu sẽ vừa phải chịu thuế nhập khẩu khi đi qua biên giới, vừa phải chịu thuế nội địa khi được bán lại ở thị trường nội địa.

Thuế định ngạch và thuế định lệ

Thuế định ngạch: là đánh một lượng cố định vào tất cả các đối tượng thu của sắc thuế. Ví dụ: thuế cầu đường, lệ phí sử dụng dịch vụ sân bay, …

Thuế định lệ: là thuế đánh vào đối tương thu của sắc thuế theo tỉ lệ nhất định. Thuế định lệ lại có loại thuế lũy tiến (tỉ lệ tăng dần) và loại thuế tỉ lệ đồng đều.

Thuế thông thường và thuế đặc biệt

Thuế thông thường: là thuế nhằm các mục đích chính là thu ngân sách và điều tiết thu nhập, chứ không nhằm mục đích đặc biệt nào khác.

Thuế đặc biệt: là thuế nhằm các mục đích đặc biệt, ví dụ thuế tiêu thụ đặc biệt đánh vào rượu bia, thuốc lá nhằm hạn chế cá nhân tiêu thụ các hàng hóa này, hay phí thủy lợi nhằm huy động tài chính cho phát triển, duy tu hệ thống thủy lợi địa phương.

Thuế phụ thu

Bên cạnh thuế chính thức còn có thể có thuế phụ thu. Thuế này không nhằm điều tiết trực tiếp đối tượng thu mà chỉ lợi dụng đối tượng thu để huy động một nguồn tài chính phục vụ mục đích nào đó không nhất thiết liên quan đến đối tượng thu. Ví dụ: chính phủ Pháp đánh thế phụ thu đối với người đi máy bay ở Pháp (thu thuế này khi họ mua vé máy bay) để có nguồn tài chính tài trợ cho các hoạt động phòng chống dịch bệnh, nhất là HIV/AIDS, ở các nước nghèo.

Đánh thuế theo khả năng và theo lợi ích

Đánh thuế theo khả năng: là cách đánh thuế có phân biệt theo khả năng nộp thuế. Người có thu nhập nhiều hơn sẽ phải đóng thuế nhiều hơn người có thu nhập thấp. Thông thường, các sắc thuế quốc gia áp dụng nguyên tắc đánh thuế này.

Đánh thuế theo lợi ích: là cách đánh thuế có phân biệt theo mức độ sử dụng hàng hóa công cộng nhiều hay ít. Người sử dụng hàng hóa công cộng nhiều hơn thì phải đóng thuế nhiều hơn. Thông thường, các sắc thuế địa phương áp dụng nguyên tắc đánh thuế theo lợi ích.

"Thuế" mà không phải thuế

Thuế lạm phát: do lạm phát làm thu nhập của cá nhân giảm tương đối giống như khi bị đánh thuế, nên có thuật ngữ "thuế lạm phát" hàm ý một trong những hậu quả của lạm phát.

Thuế thời gian: khi thời gian là tiền bạc, thì việc mất thời gian do những thủ tục hành chính rắc rối gây ra cũng có tác động như khi người ta bị đánh thuế.

Một số loại thuế và sắc thuế phổ biến

- Thuế tiêu thụ
- VAT
- Thuế thu nhập
- Thuế cổ tức
- Thuế môn bài
- Thuế tài sản
- Thuế chuyển nhượng
- Thuế thừa kế
- Thuế xuất nhập khẩu
- Thuế khoán

1.2. Thuế điện tử

1.2.1. Chính phủ điện tử

Chính phủ Điện tử là ứng dụng công nghệ thông tin để các cơ quan của Chính quyền từ trung ương và địa phương đổi mới, làm việc có hiệu lực, hiệu quả và minh bạch hơn; cung cấp thông tin, dịch vụ tốt hơn cho người dân, doanh nghiệp và các tổ chức; và tạo điều kiện thuận lợi hơn cho người dân thực hiện quyền dân chủ và tham gia quản lý Nhà nước.

Chức năng của chính phủ điện tử

Mặc dù còn có những quan niệm khác nhau, song có thể hiểu một cách đơn giản: Chính phủ điện tử là sự ứng dụng công nghệ thông tin – truyền thông để các cơ quan chính phủ đổi mới, làm việc hiệu lực, hiệu quả và minh bạch hơn, cung cấp thông tin, dịch vụ tốt hơn cho người dân, doanh nghiệp và các tổ chức; đồng thời tạo điều kiện thuận lợi hơn cho người dân thực hiện quyền dân chủ của mình trong việc tham gia quản lý Nhà nước. Nói cách ngắn gọn, Chính phủ điện tử là chính phủ hoạt động hiệu lực, hiệu quả hơn, cung cấp dịch vụ tốt hơn trên cơ sở ứng dụng công nghệ thông tin – truyền thông.

Chính phủ điện tử với các đặc trưng:

- Thứ nhất, Chính phủ điện tử đã đưa chính phủ tới gần dân và đưa dân tới gần chính phủ.
- Thứ hai, Chính phủ điện tử làm minh bạch hóa hoạt động của chính phủ, chống tham nhũng, quan liêu, độc quyền
- Thứ ba, Chính phủ điện tử giúp chính phủ hoạt động có hiệu quả trong quản lý và phục vụ dân (cải cách hành chính và nâng cao chất lượng dịch vụ công)

1.2.2. Tiến tới thuế điện tử

Trong xu hướng tiến tới Chính phủ điện tử, việc xây dựng một hệ thống thuế điện tử được xem là một việc vô cùng quan trọng và cấp thiết. Đó sẽ là một hệ thống thông tin về thuế phục vụ nội bộ và cung cấp dịch vụ cho các tổ chức, cá nhân bên ngoài ngành thuế. Các dịch vụ điện tử thuế sẽ bao gồm: cung cấp thông tin tham khảo, đối thoại hỏi đáp trực tiếp, đăng ký thuế, nộp tờ khai và kê khai, nộp thuế. Với tầm quan trọng trên, để hướng tới mô hình Chính phủ điện tử, thuế điện tử sẽ phải trở thành một thành phần trong Chính phủ điện tử ở Việt Nam.

Tuy nhiên, việc phát triển mô hình Chính phủ điện tử ở Việt Nam lại đang gặp rất nhiều khó khăn và vướng mắc. Các cơ quan Nhà nước mạnh ai nấy xây dựng các trang web theo nhu cầu của mình mà chưa có sự kết nối cũng như chưa có cơ quan đầu mối. Do đó, các thông tin, dịch vụ điện tử cũng chưa thực sự phát huy được sức mạnh tổng hợp. Trong khi đó, Việt Nam lại đang còn thiếu một hành lang pháp lý cho các giao

dịch điện tử.

Theo Phó giám đốc Trung tâm Tin học-Thống kê (Tổng cục Thuế), ngành thuế cần thiết phải xây dựng một lộ trình triển khai thuế điện tử trong đó bắt đầu bằng hệ thống nghiệp vụ. Trong giai đoạn đầu của lộ trình, thuế điện tử sẽ bắt đầu bằng các công việc đơn giản như tuyên truyền, phổ biến chính sách, chế độ thuế hiện hành; hướng dẫn các thủ tục về thuế như đăng ký thuế, kê khai, nộp thuế, quyết toán thuế...; giải đáp các vấn đề thường gặp trong lĩnh vực thuế và cung cấp các thông tin tham khảo về mã số thuế.

Trong giai đoạn tiếp theo, sẽ tiến tới việc cung cấp các dịch vụ trả lời về chính sách, chế độ thuế trực tiếp qua mạng Internet, dịch vụ nhận bảng kê hóa đơn điện tử, dịch vụ đăng ký thuế điện tử, dịch vụ kê khai thuế điện tử, dịch vụ nộp thuế qua mạng Internet và cuối cùng là quản lý thu thuế đối với các giao dịch thương mại điện tử.

Về tổ chức, trong quá trình tiến tới thuế điện tử, ngành này sẽ hình thành bộ máy tổ chức hỗ trợ người nộp thuế từ trung ương tới địa phương, quy định về chức năng nhiệm vụ, quy trình hoạt động. Người nộp thuế cũng sẽ được hỗ trợ thông qua nhiều hình thức khác nhau, qua hình thức thuế điện tử và thông qua việc đa dạng hóa môi trường hoạt động, tăng cường áp dụng công nghệ thông tin và viễn thông.

Để triển khai được mô hình này, ngành thuế cũng đòi hỏi phải có một cơ sở hạ tầng công nghệ thông tin và viễn thông gồm một hệ thống ứng dụng thống nhất toàn ngành, đảm bảo cập nhật thông tin kịp thời chính xác; nối mạng Internet với tốc độ và dung lượng cao; hệ thống thiết bị, phần mềm an toàn, bảo mật và ổn định. Ngoài ra, cũng cần phải có một đội ngũ cán bộ tin học đủ về số lượng và năng lực, đảm bảo vận hành, duy trì, bảo trì hệ thống ứng dụng.

Mô hình trên dự kiến sẽ được triển khai theo 2 giai đoạn. Trong giai đoạn triển khai thí điểm, mô hình này sẽ được triển khai tại một số cơ quan thuế, triển khai một số dịch vụ trực tuyến và xây dựng giải pháp đóng gói triển khai. Tiếp theo, mô hình này sẽ được triển khai rộng với việc xây dựng mô hình ứng dụng xử lý tập trung tại các cục thuế tỉnh, thành phố và tổng cục thuế dựa trên hạ tầng truyền thông. Sau đó, ngành này sẽ triển khai hệ thống ứng dụng tại tất cả các cơ quan thuế trong cả nước.

Để thực hiện thành công mô hình thuế điện tử, Phó giám đốc Trung tâm tin học-

thống kê Nguyễn Minh Ngọc cho rằng: trước hết cần phải có sự chỉ đạo thống nhất của Chính phủ và hình thành một Portal của Chính phủ. Ngoài ra, cũng cần có sự gắn kết nội dung các dịch vụ điện tử của các ngành, đơn vị; thiết lập giao dịch điện tử giữa các quốc gia, khu vực trên thế giới và hoàn thiện khung pháp lý về giao dịch điện tử của Việt Nam.

Riêng đối với ngành thuế, cần thiết phải cải cách công tác quản lý hành chính, tin học hóa các quy trình nghiệp vụ quản lý thuế, cung cấp các dịch vụ giao dịch điện tử với doanh nghiệp và với các cơ quan khác đồng thời tham gia đề xuất xây dựng khung pháp lý về trao đổi thông tin, giao dịch điện tử trên Internet.

Về vấn đề pháp lý đối với thuế điện tử, cần có quy định người nộp thuế phải cung cấp thông tin dạng điện tử (số hóa) và có quy định về sử dụng thông tin điện tử của các cơ quan có liên quan tới thuế. Đối với giao dịch điện tử nói chung, cần phải có hệ thống xác thực sử dụng và có môi trường thuận tiện, an toàn và đa dạng.

Theo định hướng của ngành thuế, trong khi chưa có khung pháp lý về giao dịch điện tử của Việt Nam, ngành này sẽ phát triển dịch vụ cung cấp thông tin một chiều cho người nộp thuế và người dân, thí điểm các dịch vụ trực tuyến về nộp tờ khai và nộp bảng kê hóa đơn, phát triển cơ sở hạ tầng kỹ thuật và xây dựng đội ngũ cán bộ kỹ thuật vững mạnh.

Khi đã có khung pháp lý về giao dịch điện tử, ngành thuế sẽ phát triển các dịch vụ trao đổi thông tin hai chiều giữa cơ quan thuế và người nộp thuế, triển khai rộng các dịch vụ trực tuyến về nộp tờ khai, bản kê hóa đơn.

Bên cạnh đó, ngành này cũng sẽ phối hợp với Bộ Kế hoạch và Đầu tư, ngân hàng, kho bạc, hải quan... cải tiến phương pháp đăng ký thuế, nộp thuế qua hệ thống máy tính nối mạng đồng thời tiếp tục nâng cấp cơ sở hạ tầng và xây dựng đội ngũ kỹ thuật.

1.2.3. Hiện trạng thuế điện tử ở Việt Nam và thế giới

Việt Nam

Theo bản báo cáo về công tác cải cách hành chính và hiện đại hóa ngành thuế ngày 30-11-2009 của Bộ tài chính, việc hiện đại hóa công tác quản lý thuế đã đạt được

những kết quả khả quan.:

- Xây dựng và triển khai dự án "Người nộp thuế nộp hồ sơ khai thuế qua mạng Internet"

Nhằm tạo điều kiện thuận lợi hơn nữa cho người nộp thuế trong việc nộp hồ sơ khai thuế, giảm chi phí về thời gian đi lại, chi phí in ấn và lưu trữ tờ khai bằng giấy cho người nộp thuế; đồng thời, giảm áp lực cho cơ quan thuế trong những ngày cao điểm tiếp nhận tờ khai thuế và giảm nhân lực nhập dữ liệu, lưu trữ hồ sơ tại cơ quan thuế, Tổng cục Thuế đã xây dựng và triển khai thí điểm dự án "Người nộp thuế nộp hồ sơ khai thuế qua mạng Internet".

Tổng cục thuế đã ban hành "Quy trình quản lý đăng ký, nộp tờ khai thuế qua mạng" và phối hợp với công ty VDC thuộc VNPT triển khai hoạt động cấp chứng thư số công cộng tạo điều kiện cho việc cấp chữ ký điện tử cho người nộp thuế thực hiện nộp tờ khai thuế qua mạng, đã triển khai việc nộp hồ sơ khai thuế qua mạng cho 411 doanh nghiệp tại các địa bàn thực hiện thí điểm (TP.HCM, Hà nội, Bà rịa-Vũng tàu, Đà nẵng). Kết quả bước đầu được các doanh nghiệp đánh giá tốt. Tổng cục Thuế đang tổng hợp ý kiến, rút kinh nghiệm để mở rộng thực hiện dự án trong năm 2010.

- Mở rộng triển khai dự án hiện đại hóa quy trình quản lý thu nộp thuế giữa cơ quan Thuế, Hải quan, Kho Bạc và Tài chính (dự án Hiện đại hoá thu ngân sách Nhà nước)

Đã hoàn thành việc triển khai dự án tại 34 tỉnh, thành phố; 103 quận huyện. Đang tiếp tục triển khai giai đoạn mở rộng giai đoạn 1 với 2 tỉnh và 108 quận, huyện.

- Xây dựng và triển khai dự án "Nộp thuế qua ngân hàng"

Tổng cục Thuế đã phối hợp với Kho bạc Nhà nước và một số ngân hàng (ngân hàng Công thương, ngân hàng Nông nghiệp, ngân hàng Đầu tư) trong hợp tác thanh toán, ký kết Thoả thuận phối hợp thu thuế qua hệ thống ngân hàng. Việc thực hiện thoả thuận này sẽ giúp thông tin về số thuế phải thu, đã thu sẽ được cập nhật, đối chiếu đầy đủ, nhanh chóng, chính xác tại kho bạc Nhà nước, cơ quan thuế, ngân hàng; đồng thời giảm thiểu khối lượng nhập liệu cho cán bộ kho bạc Nhà nước và cơ quan thu do dữ liệu về số phải thu sẽ được cơ quan thuế truyền sang cho Kho bạc và ngân hàng; sau đó, ngân hàng sẽ truyền lại dữ liệu về số đã thu cho kho bạc Nhà nước và cơ quan thuế

(cán bộ kho bạc Nhà nước và cán bộ thuế không phải nhập lại chứng từ giấy, kể cả bằng tiền mặt và chuyển khoản).

Đối với người nộp thuế, dự án này sẽ tạo thuận lợi hơn trong việc nộp thuế và đảm bảo tính chính xác trong quá trình thu thuế vào ngân sách Nhà nước: Khi nộp thuế trực tiếp tại kho bạc hoặc nộp qua hệ thống ngân hàng, người nộp thuế không phải viết Giấy nộp tiền vào ngân sách Nhà nước, không cần phải nhớ và ghi mục lục ngân sách trên Giấy nộp tiền. người nộp thuế chỉ cần lập bảng kê nộp tiền, ghi tên, mã số thuế và khoản tiền nộp. Địa điểm nộp thuế cũng mở rộng hơn, tại tất cả các nơi có chi nhánh ngân hàng đã được kết nối. Thời gian nộp thuế cũng được kéo dài hơn, việc nộp thuế qua ngân hàng có thể thực hiện cả trong và ngoài giờ hành chính; Đặc biệt, nếu người nộp thuế thực hiện nộp thuế qua thẻ ATM thì thời gian nộp thuế có thể kéo dài đến tận 23 giờ tất cả các ngày trong tuần.

- Xây dựng và chuẩn bị thí điểm triển khai hoạt động "Trung tâm hỗ trợ người nộp thuế qua điện thoại"

Để góp phần đưa công tác hỗ trợ người nộp thuế được chất lượng, hiệu quả, học tập kinh nghiệm của các nước, Tổng cục thuế đã xây dựng và chuẩn bị thí điểm triển khai hoạt động "Trung tâm hỗ trợ người nộp thuế qua điện thoại". Qua đó, người nộp thuế có thể liên hệ với cơ quan thuế qua một số điện thoại tập trung duy nhất để được hướng dẫn giải đáp vướng mắc về thuế. Đến nay đã hoàn thành giải pháp ứng dụng và đang triển khai xây dựng hạ tầng kỹ thuật, đang chuẩn bị kiểm thử để nghiệm thu hệ thống.

- Nghiên cứu, xây dựng cơ sở sở dữ liệu thông tin về người nộp thuế đáp ứng yêu cầu quản lý thuế theo rủi ro:

Phối hợp với Tổng cục Hải quan xây dựng các Thông tư liên tịch về trao đổi thông tin phục vụ quản lý thuế, hải quan giữa Bộ Tài chính và một số Bộ, ngành. Đến nay, đã ban hành được 01 Thông tư liên tịch giữa Bộ Tài chính với Bộ Kế hoạch- Đầu tư và Bộ Công Thương, 02 dự thảo đang trong giai đoạn ký luân phiên để ban hành (thông tư liên tịch với Bộ Giao thông vận tải, Bộ Thông tin - truyền thông; thông tư liên tịch với Toà án nhân dân tối cao, Viện kiểm sát nhân dân tối cao), 2 dự thảo đang lấy ý kiến thẩm định của Vụ Pháp chế (thông tư liên tịch với Ngân hàng Nhà nước; thông tư liên tịch với Bộ Công an, Bộ Quốc phòng).

Đang triển khai dự án tập trung cơ sở dữ liệu về người nộp thuế tại Tổng cục Thuế để hỗ trợ cho triển khai các đề án quản lý thuế theo rủi ro. Theo đó, khi dự án triển khai, toàn ngành thuế sẽ có một cơ sở dữ liệu thông tin về người nộp thuế trên phạm vi toàn quốc với những thông tin chủ yếu về tình hình thực hiện nghĩa vụ thuế để hỗ trợ công tác phân tích, khai thác thông tin, đánh giá hồ sơ phân loại người nộp thuế theo mức độ tuân thủ pháp luật, từ đó, tập trung nguồn lực vào nhóm người nộp thuế có mức độ tuân thủ thấp để thực hiện các biện pháp quản lý hiệu quả như tiến hành thanh tra, kiểm tra, cưỡng chế nợ thuế...

Hiện tại kê khai thuế điện tử là nội dung trọng tâm mà ngành thuế đang cố gắng hoàn thiện, các phần mềm và hướng dẫn chi tiết có thể tìm thấy tại trang web kê khai thuế của ngành thuế.

Sau gần 5 năm, việc triển khai thuế điện tử ở Việt Nam được đánh giá là đã đi đúng hướng và bài bản, nhưng tiến độ còn quá chậm, chủ yếu là do quá trình triển khai cơ sở hạ tầng khóa công khai (PKI) và chứng thực điện tử (CA).

Ngày 3/9/2009, Cục Ứng dụng CNTT, Bộ Thông tin và Truyền thông, đã tổ chức cuộc họp tổng kết sau 5 năm triển khai và đề ra phương án phát triển các bước tiếp theo để Việt Nam dần hoàn thành mục tiêu ứng dụng CNTT rộng rãi trong mọi lĩnh vực.

Cách đây 5 năm, Trung tâm Hợp tác Quốc tế về Tin học hóa Nhật Bản (CICC) và Diễn đàn Cơ sở hạ tầng khóa công khai của Nhật Bản (PKI-J) đã tổ chức khóa học về chứng thực điện tử với đối tượng tham gia là các doanh nghiệp, tổ chức chính phủ của Việt Nam. Sau đó luật Giao dịch điện tử được thông qua mở ra một cánh cửa mới cho các doanh nghiệp, tổ chức thực hiện các giao dịch, dịch vụ công thay vì thông qua phương thức truyền thống thì đều áp dụng cơ chế mới bằng giao dịch điện tử.

Hiện nay, có hai hạ tầng chính phát triển hệ thống PKI Quốc gia là Bộ Thông tin và Truyền thông và Ban Cơ yếu Chính phủ. Tới thời điểm hiện tại, thống kê của Bộ Thông tin và Truyền thông cho thấy giao dịch điện tử B2C, B2B chiếm tới 2,5% GDP với những con số rõ nét là 9.300 trang web với doanh thu từ mua sắm trực tuyến, điện thoại... lên tới 450 triệu USD và 3000 doanh nghiệp có doanh thu khoảng 1,5 tỉ USD. Song song với việc đó, nhiều dịch vụ hành chính công nay đã từng bước áp dụng công cụ trực tuyến có sử dụng chữ ký điện tử như E-Tax của Tổng cục thuế, E-Banking của

Ngân hàng Nhà nước...

Ban Cơ yếu Chính phủ là tổ chức đầu tiên của Nhà nước áp dụng và đưa ra các giải pháp quản lý PKI nhằm mục đích phục vụ cho các cơ quan thuộc hệ thống chính trị. Cho tới nay, đã triển khai được trên nhiều bộ, ban, ngành như Bộ Công an, Bộ Ngoại giao và các cơ quan đảng. Mục tiêu phấn đấu trong thời gian tới, đơn vị này sẽ triển khai áp dụng lên toàn bộ các đơn vị hành chính, tạo tiền đề phát triển cho chính phủ điện tử.

Bộ Tài chính đề xuất nhân rộng mô hình triển khai PKI, theo đó các cơ quan Nhà nước khi giao dịch với cá nhân, tổ chức bên ngoài thì sử dụng dịch vụ chứng thực chữ ký điện tử công cộng, còn giao dịch trong nội bộ thì sử dụng hệ thống chứng thực điện tử chuyên dùng của Chính phủ. Đại diện Bộ, ông Trần Nguyên Vũ, Cục trưởng Cục Tin học và Thống kê tài chính cho biết: "Với việc nhân rộng mô hình này, sẽ tạo thuận tiện cho cá nhân, tổ chức khi giao dịch với các cơ quan Nhà nước (sử dụng một chứng thư số giao dịch được với nhiều cơ quan khác nhau). Ngoài ra, nó còn góp phần tăng cường các hoạt động tuyên truyền đào tạo nâng cao nhận thức của xã hội về tác dụng của chữ ký điện tử".

Đến nay, Bộ Tài chính đã ra quyết định sử dụng hệ thống chứng thực chữ ký điện tử của VNPT cho giai đoạn thí điểm "Người nộp thuế nộp hồ sơ khai thuế qua mạng Internet". Ngoài ra, ngày 14/08/2009 vừa qua, Tổng cục Thuế cũng bắt đầu triển khai thí điểm chương trình này tại TP Hồ Chí Minh, áp dụng ban đầu cho 100 doanh nghiệp lựa chọn, sau đó sẽ mở rộng cho phép tất cả các doanh nghiệp trên địa bàn thành phố được đăng ký sử dụng. Tiếp đó sẽ triển khai tại Hà Nội, Đà Nẵng và sẽ có báo cáo tổng kết vào cuối năm nay để từ đó chuẩn bị mở rộng hệ thống ra cả nước trong năm 2010.

Về phía khối hệ thống ngân hàng, ông Phan Thái Dũng, Cục CNTT ngân hàng Nhà nước cũng cho biết, kế hoạch phát triển trong thời gian tới sẽ nâng cấp và hoàn thiện phần mềm CA. Bên cạnh đó tích hợp các nghiệp vụ khác như Kế toán giao dịch; Thị trường mở và Hệ thống báo cáo thống kê. Từ đó hoàn thiện hệ thống của khối ngân hàng theo cơ sở pháp lý.

Nhìn chung, việc phát triển cơ sở hạ tầng khóa công khai (PKI) cũng như chứng thực điện tử (CA) đang triển khai đúng hướng và bài bản. Tuy nhiên bên cạnh đó cũng không tránh khỏi những rào cản về pháp lý, nhận thức dẫn tới việc tiến độ triển khai

đại trà mô hình này vẫn còn chậm. Trong thời gian tới, cần có sự kết hợp chặt chẽ giữa các bộ, ban ngành, các tổ chức chính phủ và các doanh nghiệp để từ đó thắt chặt sự liên kết, giao dịch, hình thành một hạ tầng vững chắc, tạo tiền đề thúc đẩy thương mại điện tử và chính phủ điện tử phát triển.

Hiện tại đã có 4 doanh nghiệp đăng kí cung cấp dịch vụ chữ ký số. Theo thông tin từ Bộ Thông tin và Truyền thông, đến nay đã VDC và NacenComm xin cấp phép cung cấp dịch vụ chữ ký điện tử, và hai công ty khác là Viettel và Bkis đang rục rịch chuẩn bị.

Ngày 3/9/2009, Bộ Thông tin và Truyền thông đã phối hợp với Ban Cơ yếu Chính phủ tổ chức hội thảo "Hiện trạng hạ tầng khóa công khai và kế hoạch phát triển" nhằm đánh giá hiện trạng, xây dựng cơ sở hạ tầng khóa công khai tại Việt Nam; đồng thời đưa ra các khuyến nghị, giải pháp nhằm đáp ứng yêu cầu thực tế sử dụng chữ ký điện tử trong các hoạt động giao dịch điện tử.

Ngoài kê khai thuế điện tử, đối với các nội dung khác như đăng ký thuế, nộp thuế, hoàn thuế… hiện vẫn đang gặp nhiều khó khăn do điều kiện thực hiện, cần phải có sự phối hợp của các cơ quan khác như đơn vị quản lý đăng ký kinh doanh, Kho bạc, Ngân hàng, do đó sẽ cần có các quy trình nghiệp vụ tương ứng, có tính liên kết giữa cơ quan Thuế và các đơn vị có liên quan.

Thế giới

Từ nhiều năm nay các nước trên thế giới đều coi đây là một cuộc cách mạng, người ta nói đến "Cuộc cách mạng Chính phủ điện tử". Nước Mỹ trong nhiều tài liệu có nêu rằng: Chính phủ điện tử là cuộc cách mạng tiếp theo của nước Mỹ. Vì việc đưa tài liệu về tình hình triển khai Chính phủ điện tử tại các nước sẽ quá dài, em xin chỉ đưa ra đây sắp xếp mức độ triển khai Chính phủ điện tử của 20 quốc gia do Ngân hàng thế giới tổng kết để cùng tham khảo: Mỹ, Singapore, Ôxtrâylia, Canada, Pháp, Anh, Hồng Kông, Niudilân, Nauy, Tây Ban Nha, Đức, Hà Lan, Nam Phi, Italia, Nhật Bản, Ireland, Mêhicô, Bỉ, Malayxia, Brazil.

Gần chúng ta có Singapore đã triển khai Chính phủ điện tử từ khá lâu (1990) và đến nay đã đạt được những thành tựu lớn. Riêng về thuế điện tử, quy trình thế ở Singapore đã gần như hoàn thiện, mọi việc đều có thể thực hiện qua Internet và điện

thoại. Trên trang web của ngành thuế Singapore có các hướng dẫn cụ thể và chi tiết cho từng đối tượng người nộp thuế, từ việc nhận hóa đơn, tính thuế, kê khai thuế, nộp thuế, …

Chương 2. Tổng quan về an toàn thông tin

2.1. Định nghĩa an toàn thông tin

2.1.1. Định nghĩa

An toàn thông tin nghĩa là thông tin được bảo vệ, các hệ thống và dịch vụ có khả năng chống lại những sự can thiệp, lỗi và những tai họa không mong đợi, các thay đổi tác động đến độ an toàn của hệ thống là nhỏ nhất. Hệ thống không an toàn là hệ thống tồn tại những điểm: thông tin bị rò rỉ ra ngoài - thông tin dữ liệu trong hệ thống bị người không được quyền truy nhập lấy và sử dụng, thông tin bị thay đổi - các thông tin trong hệ thống bị thay thế hoặc sửa đổi làm sai lệch một phần hoặc hoàn toàn nội dung...

Giá trị thực sự của thông tin chỉ đạt được khi thông tin được cung cấp chính xác và kịp thời, hệ thống phải hoạt động chuẩn xác thì mới có thể đưa ra những thông tin có giá trị cao. Mục tiêu của an toàn bảo mật trong công nghệ thông tin là đưa ra một số tiêu chuẩn an toàn và áp dụng các tiêu chuẩn an toàn này vào chỗ thích hợp để giảm bớt và loại trừ những nguy hiểm có thể xảy ra. Ngày nay với kỹ thuật truyền nhận và xử lý thông tin ngày càng phát triển và phức tạp nên hệ thống chỉ có thể đạt tới một mức độ an toàn nào đó và không có một hệ thống an toàn tuyệt đối. Ngoài ra khi đánh giá còn phải cân đối giữa mức độ an toàn và chất lượng của dịch vụ được cung cấp. Khi đánh giá độ an toàn thông tin cần phải dựa trên nội dung phân tích các rủi ro có thể gặp, từ đó tăng dần sự an toàn bằng cách giảm bớt những rủi ro. Các đánh giá cần hài hoà với đặc tính, cấu trúc hệ thống và quá trình kiểm tra chất lượng.

2.1.2. Các yêu cầu an toàn bảo mật thông tin

Ngày nay, với sự phát triển rất nhanh của khoa học công nghệ, các biện pháp tấn công ngày càng tinh xảo hơn, độ an toàn của thông tin có thể bị đe dọa từ nhiều nơi, theo nhiều cách khác nhau, chúng ta cần phải đưa ra các chính sách đề phòng thích hợp. Các yêu cầu cần thiết của việc bảo vệ thông tin và tài nguyên:

- Đảm bảo tính tin cậy (Confidentiality): Thông tin và tài nguyên không thể bị truy cập trái phép bởi những người không có quyền hạn.

- Đảm bảo tính toàn vẹn (Integrity): Thông tin và tài nguyên không thể bị sửa đổi, bị thay thế bởi những người không có quyền hạn.
- Đảm bảo tính sẵn sàng (Availability): Thông tin và tài nguyên luôn sẵn sàng để đáp ứng sử dụng cho người có quyền hạn.
- Đảm bảo tính không thể chối bỏ (Non-repudiation): Thông tin và tài nguyên được xác nhận về mặt pháp luật của người cung cấp.

2.2. Chữ ký số

2.2.1. Định nghĩa

Chữ ký số khóa công khai là mô hình sử dụng các kỹ thuật mật mã để gắn với mỗi người sử dụng một cặp khóa công khai - bí mật và qua đó người sử dung, doanh nghiệp, tổ chức có thể ký các văn bản điện tử cũng như trao đổi các thông tin cần độ an toàn cao với nhau. Khóa công khai thường được phân phối thông qua một nhà cung cấp chứng thực khóa công khai. Quá trình sử dụng chữ ký số bao gồm 2 bước: tạo chữ ký và thẩm tra chữ ký.

2.2.2. Lịch sử

Con người đã sử dụng các hợp đồng dưới dạng điện tử từ hàng trăm năm nay với việc sử dụng mã Morse và điện tín. Vào năm 1889, tòa án tối cao bang New Hampshire (Hoa Kỳ) đã phê chuẩn tính hiệu lực của chữ ký điện tử. Tuy nhiên, chỉ với những phát triển vượt bậc của khoa học kỹ thuật nói chung và công nghệ thông tin nói riêng gần đây thì chữ ký điện tử mới đi vào cuộc sống một cách rộng rãi.

Vào thập kỷ 1980, các công ty, tổ chức và một số cá nhân bắt đầu sử dụng máy fax để trao đổi các tài liệu quan trọng. Mặc dù chữ ký trên các tài liệu này vẫn thể hiện trên giấy tờ nhưng quá trình truyền và nhận chúng hoàn toàn dựa trên tín hiệu điện tử.

Hiện nay, chữ ký điện tử có thể bao hàm các cam kết gửi bằng thư điện tử, nhập các số định danh cá nhân (PIN) vào các máy ATM, ký bằng bút điện tử với thiết bị màn hình cảm ứng tại các quầy tính tiền, chấp nhận các điều khoản người dùng (EULA) khi cài đặt phần mềm máy tính, ký các hợp đồng điện tử trực tuyến...

2.2.3. Các ưu điểm của chữ ký số

Việc sử dụng chữ ký số mang lại một số lợi điểm sau:

Khả năng xác định nguồn gốc

Các hệ thống mật mã hóa khóa công khai cho phép mật mã hóa văn bản với khóa bí mật mà chỉ có người chủ của khóa có. Để sử dụng chữ ký số thì văn bản cần phải được mã hóa hàm băm (thường có độ dài cố định và ngắn hơn nhiều so với văn bản) sau đó dùng khóa bí mật của người chủ khóa để mã hóa, khi đó ta được chữ ký số. Khi cần kiểm tra, bên nhận sử dụng khóa công khai của bên gửi thực hiện giải mã để lấy lại hàm băm và kiểm tra với hàm băm của văn bản nhận được. Nếu hai giá trị này khớp nhau thì bên nhận có thể tin tưởng rằng văn bản được gửi đi từ người sở hữu khóa bí mật. Tất nhiên chúng ta không thể đảm bảo 100% là văn bản không bị giả mạo vì hệ thống vẫn có thể bị truy cập và giả mạo.

Vấn đề xá hàm băm c thực đặc biệt quan trọng đối với các giao dịch tài chính. Chẳng hạn một chi nhánh ngân hàng gửi một gói tin A về trung tâm trong đó chứa thông tin về số tài khoản và số tiền gửi. Kẻ gian có thể thực hiện một giao dịch, sau đó bắt lấy nội dung gói tin A và truyền lại gói tin thu được nhiều lần hoặc thay đổi nội dung gói tin để thu lợi (tấn công truyền lại gói tin).

Tính toàn vẹn

Cả hai bên tham gia vào quá trình trao đổi thông tin đều có thể tin tưởng là văn bản không bị sửa đổi trong quá trình truyền truyền vì nếu văn bản bị thay đổi dù là cực nhỏ thì giá trị hàm băm cũng sẽ thay đổi theo và việc này sẽ bị phát hiện. Nếu chỉ có quá trình mã hóa thì chỉ có thể ẩn nội dung của gói tin nhưng không thể ngăn cản được việc thay đổi nội dung của nó. Một ví dụ cho trường hợp này là tấn công đồng hình (homomorphism attack): tiếp tục ví dụ như ở trên, một kẻ lừa đảo gửi 500.000 Đồng vào tài khoản Z, sau đó bắt gói tin A mà chi nhánh gửi về trung tâm sau đó gửi gói tin B có giá trị hơn để sinh lợi. Đây là vấn đề bảo mật của chi nhánh đối với trung tâm ngân hàng không hẳn liên quan đến tính toàn vẹn của thông tin từ người gửi tới chi nhánh, bởi thông tin đã được băm và mã hóa để gửi đến đúng đích của nó tức chi nhánh ngân hàng, vấn đề còn lại vấn đề bảo mật của chi nhánh ngân hàng tới trung tâm của nó.

Tính không thể chối bỏ

Trong khi trao đổi thông tin, một bên có thể không nhận thông tin là do mình gửi đi. Để chống lại khả năng này, bên nhận có thể yêu cầu bên gửi phải gửi kèm chữ ký số với thông tin. Khi có tranh chấp xảy ra, bên nhận sẽ dùng chữ ký này như một chứng cứ để bên thứ ba giải quyết. Tuy nhiên, bằng cách nào đó khóa bí mật vẫn có thể bị lộ và tính không thể chối bỏ cũng không phải là hoàn toàn.

Thực hiện chữ ký số khóa công khai

Chữ ký số khóa công khai dựa trên nền tảng mật mã hóa khóa công khai. Để có thể trao đổi thông tin trong môi trường này, mỗi người sử dụng cần tạo, hoặc đăng ký cho mình cặp khóa: một khóa bí mật và một khóa công khai. Khóa bí mật phải được bảo quản kĩ lưỡng, không được để lộ, khóa công khai sẽ được công bố rộng rãi qua nhà phân phối chứng thực khóa công khai hoặc qua được riêng. Nếu chỉ biết khóa công khai thì không thể dò ngược lại được để tìm khóa bí mật.

Quá trình này gồm ba thuật toán:

- Thuật toán tạo khóa
- Thuật toán tạo chữ ký số
- Thuật toán thẩm tra chữ ký số

Xét ví dụ sau: Bob muốn gửi thông tin cho Alice và muốn Alice biết thông tin đó thực sự do chính Bob gửi. Bob gửi cho Alice bản tin kèm với chữ ký số. Chữ ký này được tạo ra với khóa bí mật của Bob. Khi nhận được bản tin, Alice sử dụng khóa công khai của Bob để kiểm tra nguồn gốc của văn bản. Bản chất của thuật toán tạo chữ ký đảm bảo nếu chỉ cho trước bản tin, rất khó (gần như không thể) tạo ra được chữ ký của Bob nếu không biết khóa bí mật của Bob.

Nếu quá trình kiểm tra cho kết quả đúng thì Alice có thể tin tưởng rằng bản tin thực sự do Bob gửi.Thông thường, Bob không mật mã hóa toàn bộ bản tin với khóa bí mật mà chỉ thực hiện với giá trị băm của bản tin đó. Điều này khiến việc ký trở nên đơn giản, thực hiện nhanh hơn và chữ ký ngắn hơn. Tuy nhiên nó cũng làm nảy sinh vấn đề khi hai bản tin khác nhau lại cho ra cùng một giá trị băm. Đây là điều có thể xảy ra khi sử dụng các thuật toán hàm băm mặc dù xác suất rất thấp.

Các bước mã hoá và ký

Bước 1: Ở bước này, sử dụng hàm băm để đảm bảo tính toàn vẹn của thông điệp. Các thuật toán hàm băm không làm thay đổi thông điệp mà chỉ dùng để tạo ra một chuỗi băm riêng của thông điệp. Sau đó bước 3 sẽ sử dụng thông điệp và chuỗi băm của thông điệp để thực hiện mã hóa. Bước này có thể dùng SHA hoặc MD5.

Bước 2: Mã hóa chuỗi băm của thông điệp bằng khóa bí mật của người gửi ở bước 1. Quá trình này thường dùng các thuật toán như RSA, DSA, 3DES,... Kết quả thu được chính là chữ ký số của thông điệp ban đầu.

Bước 3: Sử dụng khóa công khai của người nhận để mã hoá thông tin cần gửi đi.

Bước 4: Gộp chữ ký số vào thông điệp đã được mã hoá và gửi đi. Như vậy sau khi đã ký nhận chữ ký số vào thông điệp đã được mã hoá, mọi sự thay đổi trên thông điệp sẽ bị phát hiện trong giai đoạn thẩm tra. Ngoài ra, việc ký nhận này cho phép người nhận xác định được chính xác người gửi tin.

Các bước kiểm tra

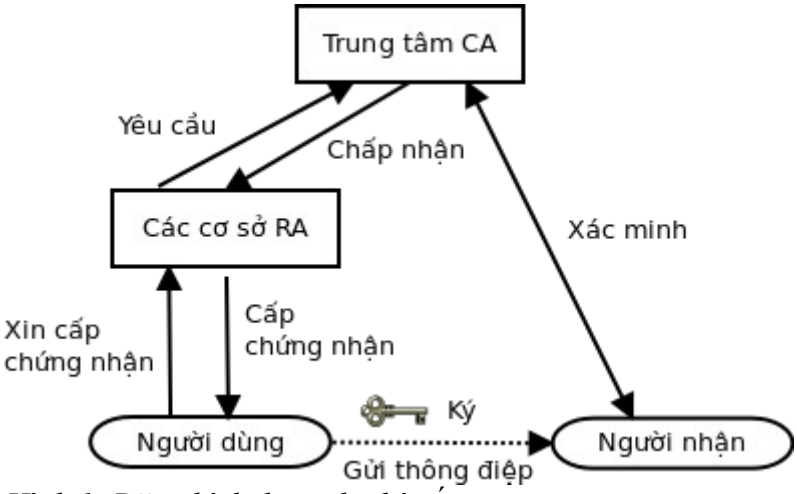
Bước 1: Người nhận dùng khóa bí mật của mình để giải mã thông tin nhận được gồm hai phần: phần thông điệp và phần chữ ký người gửi.

Bước 2: Dùng khóa công khai của người gửi (khoá này được phát hành qua một nhà chứng nhận khóa công khai) để giải mã chữ ký số của thông điệp, ta được chuỗi băm của thông điệp.

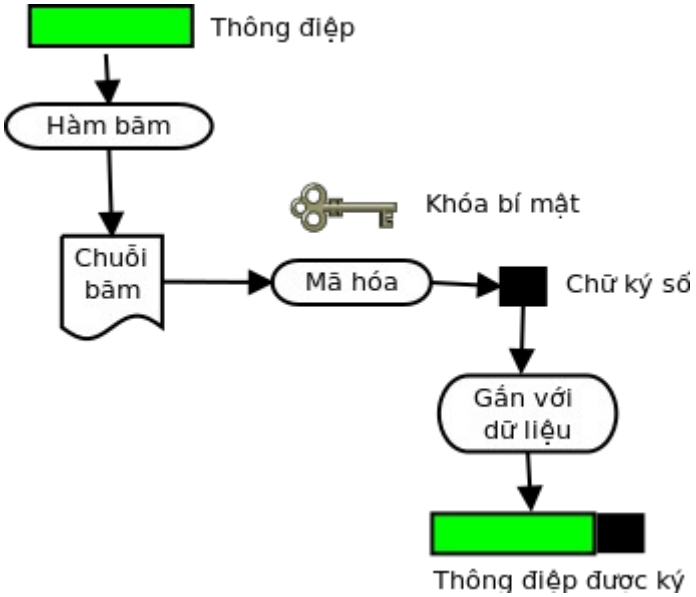
Bước 3: Dùng giải thuật MD5 (hoặc SHA) băm thông điệp đính kèm ta có chuỗi băm của thông điệp nữa.

Bước 4: So sánh kết quả thu được ở bước 2 và 3 nếu trùng nhau, ta kết luận thông điệp này không bị thay đổi trong quá trình truyền và thông điệp này là của người gửi.

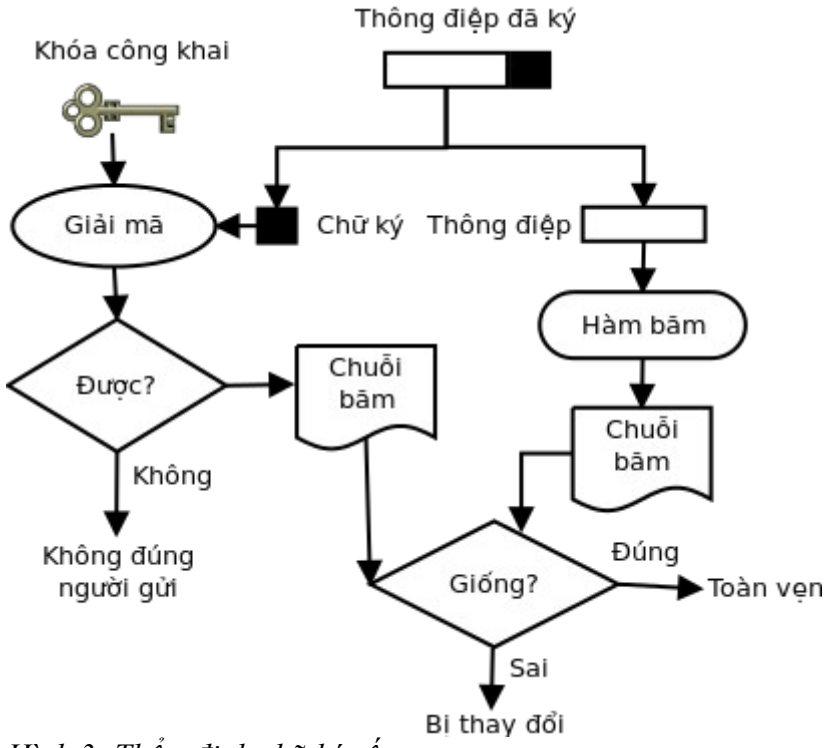
2.2.4. Đăng ký, sử dụng và thẩm tra chữ ký số



Hình 1: Đăng kí dịch vụ chữ ký số



Hình 2: Ký vào thông điệp



Hình 3: Thẩm định chữ ký số

2.2.5. Một vài thuật toán dùng trong chữ ký số

RSA

Trong mật mã học, RSA là một thuật toán mật mã hóa khóa công khai. Đây là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử đồng thời với việc mã hóa. Nó đánh dấu một sự tiến bộ vượt bậc của lĩnh vực mật mã học trong việc sử dụng khóa công khai. RSA đang được sử dụng phổ biến trong thương mại điện tử và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.

Thuật toán được Ron Rivest, Adi Shamir và Len Adleman mô tả lần đầu tiên vào năm 1977 tại Học viện Công nghệ Massachusetts (MIT). Tên của thuật toán lấy từ ba chữ cái đầu của tên ba tác giả.

Trước đó, vào năm 1973, Clifford Cocks, một nhà toán học người Anh, đã mô tả một thuật toán tương tự. Với khả năng tính toán tại thời điểm đó thì thuật toán này không khả thi và chưa bao giờ được thực nghiệm. Tuy nhiên, phát minh này chỉ được công bố vào năm 1997 vì được xếp vào loại tuyệt mật.

Thuật toán RSA được MIT đăng ký bằng sáng chế tại Hoa Kỳ vào năm 1983 (Số đăng ký 4.405.829). Bằng sáng chế này hết hạn vào ngày 21 tháng 9 năm 2000. Tuy nhiên, do thuật toán đã được công bố trước khi có đăng ký bảo hộ nên sự bảo hộ hầu như không có giá trị bên ngoài Hoa Kỳ. Ngoài ra, nếu như công trình của Clifford Cocks đã được công bố trước đó thì bằng sáng chế RSA đã không thể được đăng ký.

Thuật toán RSA có hai khóa: khóa công khai và khóa bí mật. 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 đều có thể mã hóa nhưng chỉ có người biết khóa bí mật mới có thể giải mã được.

Tạo khóa

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

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

Một số lưu ý:

- Các số nguyên tố thường được chọn bằng phương pháp thử xác suất.
- Các bước 4 và 5 có thể được thực hiện bằng giải thuật Euclid mở rộng (xem thêm: số học môđun).
- Bước 5 có thể viết cách khác: Tìm số tự nhiên *x* sao cho $d = \frac{x(p-1)(q-1)+1}{e}$ cũng là số tự nhiên. Khi đó sử dụng giá trị *d mod*

(p – 1)(q - 1) .

- Từ bước 3, PKCS#1 v2.1 sử dụng $\lambda = LCM(p-1, q-1)$ thay cho $\varphi = (p-1)(q-1)$.

Khóa công khai bao gồm:

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

Khóa bí mật bao gồm:

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

Một dạng khác của khóa bí mật bao gồm:

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

Dạng này cho phép thực hiện giải mã và ký nhanh hơn với việc sử dụng định lý số dư Trung Quốc. Ở dạng này, tất cả thành phần của khóa bí mật phải được giữ bí mật.

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

Mã hóa

Giả sử Bob muốn gửi đoạn thông tin *M* cho Alice. Đầu tiên Bob chuyển *M* thành một số $m < n$ theo một hàm có thể đảo ngược (từ *m* có thể xác định lại *M*) được thỏa thuận trước.

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

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

Giải mã

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

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

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

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

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

$$m^{ed} \equiv m \bmod p \quad \text{và} \quad m^{ed} \equiv m \bmod q$$

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

$$m^{ed} \equiv m \bmod pq. \quad \text{hay} \quad c^d \equiv m \bmod n.$$

Ví dụ

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

Lấy:

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

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

n = *pq* = 3233 - môđun (công bố công khai)

e = 17 - số mũ công khai

d = 2753 - số mũ bí mật

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

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

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

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

với *c* là văn bản mã.

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

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

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

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

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

Chuyển đổi văn bản rõ

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

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

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

255^3 nhỏ hơn giá trị *n* chấp nhận được. Những bản mã này sẽ dễ dàng bị phá mã.

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

Một số tiêu chuẩn, chẳng hạn như PKCS, đã được thiết kế để chuyển đổi bản rõ trước khi mã hóa bằng RSA. Các phương pháp chuyển đổi này bổ sung thêm bít vào *M*. Các phương pháp chuyển đổi cần được thiết kế cẩn thận để tránh những dạng tấn công phức tạp tận dụng khả năng biết trước được cấu trúc của bản rõ. Phiên bản ban đầu của PKCS dùng một phương pháp đặc ứng (ad-hoc) mà về sau được biết là không an toàn trước tấn công lựa chọn bản rõ thích ứng (adaptive chosen ciphertext attack). Các phương pháp chuyển đổi hiện đại sử dụng các kỹ thuật như chuyển đổi mã hóa bất đối xứng tối ưu (Optimal Asymmetric Encryption Padding - OAEP) để chống lại tấn công dạng này. Tiêu chuẩn PKCS còn được bổ sung các tính năng khác để đảm bảo an toàn cho chữ ký RSA (Probabilistic Signature Scheme for RSA – RSA-PSS).

DSA

Giải thuật ký số (Digital Signature Algorithm, viết tắt DSA) là chuẩn của chính phủ Mỹ hoặc FIPS cho các chữ ký số.

Tạo khoá

- Chọn số nguyên tố 160 bit q.
- Chọn 1 số nguyên tố L bit p, sao cho p=qz+1 với số nguyên z nào đó, $512 \leq L \leq 1024$, L chia hết cho 64.
- Chọn h, với $1 < h < p - 1$ sao cho $g = h^z \bmod p > 1$. ($z = (p-1) / q$)
- Chọn x ngẫu nhiên, thoả mãn $0 < x < q$.
- Tính giá trị $y = g^x \bmod p$.
- Khoá công là (p, q, g, y). Khoá riêng là x.

Hầu hết các số h đều thoả mãn yêu cầu, vì vậy giá trị 2 thông thường được sử dụng.

Ký

- Tạo 1 số ngẫu nhiên với mỗi thông điệp, giá trị k thỏa mãn $0 < k < q$
- Tính $r = (g^k \bmod p) \bmod q$
- Tính $s = (k^{-1}(\text{SHA-1}(m) + x*r)) \bmod q$, ở đây SHA-1($m$) là hàm băm mã hoá SHA-1 áp dụng cho thông điệp m
- Tính toán lại chữ ký trong trường hợp không chắc chắn khi r=0 hoặc s=0
- Chữ ký là (r,s)

Giải thuật Euclid mở rộng có thể được sử dụng để tính toán biểu thức $k^{-1} \bmod q$.

Xác nhận

- Loại bỏ chữ ký nếu hoặc 0< r <q hoặc 0< s <q không thỏa mãn.
- Tính $w = (s)^{-1} \bmod q$
- Tính $u1 = (\text{SHA-1}(m)*w) \bmod q$
- Tính $u2 = (r*w) \bmod q$
- Tính $v = ((g^{u1}*y^{u2}) \bmod p) \bmod q$
- Chữ ký là có hiệu lực nếu $v = r$

Sự đúng đắn của giải thuật

Lược đồ ký số là đúng đắn có ý nghĩa khi người xác nhận luôn chấp nhận các chữ ký thật. Điều này có thể được chỉ ra như sau:

Từ $g = h^z \bmod p$ suy ra $g^q \equiv h^{qz} \equiv h^{p-1} \equiv 1 \pmod p$ bởi định lý Fermat nhỏ. Bởi vì $g>1$ và q là số nguyên tố suy ra g có bậc q.

Người ký tính

$$s = k^{-1}(SHA-1(m) + xr) \bmod q.$$

Như vậy

$$k \equiv SHA-1(m)s^{-1} + xrs^{-1} \equiv SHA-1(m)w + xrw \pmod{q}.$$

Bởi vì g có bậc q chúng ta có

$$g^k \equiv g^{SHA-1(m)w} g^{xrw} \equiv g^{SHA-1(m)w} y^{rw} \equiv g^{u1} y^{u2} \pmod{p}.$$

Cuối cùng, tính đúng đắn của DSA suy ra từ

$$r = (g^k \bmod p) \bmod q = (g^{u1} y^{u2} \bmod p) \bmod q = v.$$

SHA

SHA (Secure Hash Algorithm hay thuật giải băm an toàn) là năm thuật giải được chấp nhận bởi FIPS dùng để chuyển một đoạn dữ liệu nhất định thành một đoạn dữ liệu có chiều dài không đổi với xác suất khác biệt cao. Những thuật giải này được gọi là "an toàn" bởi vì, theo nguyên văn của chuẩn FIPS 180-2 phát hành ngày 1 tháng 8 năm 2002:

"for a given algorithm, it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest. Any change to a message will, with a very high probability, result in a different message digest."

Tạm dịch đại ý là:

"1) Cho một giá trị băm nhất định được tạo nên bởi một trong những thuật giải SHA, việc tìm lại được đoạn dữ liệu gốc là không khả thi. 2) Việc tìm được hai đoạn dữ liệu nhất định có cùng kết quả băm tạo ra bởi một trong những thuật giải SHA là không khả thi. Bất cứ thay đổi nào trên đoạn dữ liệu gốc, dù nhỏ, cũng sẽ tạo nên một giá trị băm hoàn toàn khác với xác suất rất cao."

Năm thuật giải SHA là SHA-1 (trả lại kết quả dài 160 bit), SHA-224 (trả lại kết quả dài 224 bit), SHA-256 (trả lại kết quả dài 256 bit), SHA-384 (trả lại kết quả dài 384 bit), và SHA-512 (trả lại kết quả dài 512 bit). Thuật giải SHA là thuật giải băm mật được phát triển bởi cục an ninh quốc gia Mĩ (National Security Agency hay NSA) và được xuất bản thành chuẩn của chính phủ Mĩ bởi viện công nghệ và chuẩn quốc gia Mĩ (National Institute of Standards and Technology hay NIST). Bốn thuật giải sau

thường được gọi chung là SHA-2.

SHA-1 được sử dụng rộng rãi trong nhiều ứng dụng và giao thức an ninh khác nhau, bao gồm TLS và SSL, PGP, SSH, S/MIME, và IPSec. SHA-1 được coi là thuật giải thay thế MD5, một thuật giải băm 128 bit phổ biến khác.

Hiện nay, SHA-1 không còn được coi là an toàn bởi đầu năm 2005, ba nhà mật mã học người Trung Quốc đã phát triển thành công một thuật giải dùng để tìm được hai đoạn dữ liệu nhất định có cùng kết quả băm tạo ra bởi SHA-1. Mặc dù chưa có ai làm được điều tương tự với SHA-2, nhưng vì về thuật giải, SHA-2 không khác biệt mấy so với SHA-1 nên nhiều nhà khoa học đã bắt đầu phát triển một thuật giải khác tốt hơn SHA.

2.3. PKI

Để triển khai được chữ ký số, việc cần thiết nhất là phải xây dựng được hệ thống PKI hoàn chỉnh, thuận tiện với người sử dụng.

2.3.1. Tổng quan về PKI

Public Key Infrastructure (PKI) là một cơ chế để cho một bên thứ ba (thường là nhà cung cấp chứng thực số) cung cấp và xác thực thông tin định danh các bên tham gia vào quá trình trao đổi thông tin. Cơ chế này cho phép gán cho mỗi người sử dụng trong hệ thống một cặp khóa bí mật/khóa công khai. Hệ thống này thường bao gồm một phần mềm ở trung tâm, và các chi nhánh ở những địa điểm khác nhau của người dùng. Khoá công khai thường được phân phối dựa trên cơ sở hạ tầng khóa công khai – hay Public Key Infrastructure.

Khái niệm hạ tầng khoá công khai thường được dùng chỉ toàn bộ hệ thống bao gồm cả nhà cung cấp chứng thực số (CA) cùng các cơ chế liên quan đồng thời với toàn bộ việc sử dụng các thuật toán mã hoá công khai trong trao đổi thông tin. Trên thực tế một hệ thông PKI không nhất thiết phải sử dụng phương pháp mã hóa khóa công khai.

2.3.2. Các thành phần của PKI

PKIs thông thường bao gồm các thành phần chính sau:

- Chứng thực và đăng ký mật mã đầu cuối

- Kiểm tra tính toàn vẹn của khoá công khai
- Chứng thực yêu cầu trong quá trình bảo quản các khoá công khai
- Phát hành khoá công khai
- Huỷ bỏ khoá công khai
- Duy trì việc thu hồi các thông tin về khoá công khai (CRL)
- Đảm bảo an toàn về độ lớn của khoá

Chứng nhận khóa công khai

Mục tiêu của việc trao đổi khoá bất đối xứng là phát một cách an toàn khoá công khai từ người gửi (mã hoá) đến người nhận (giải mã). PKI hỗ trợ tạo điều kiện cho việc trao đổi khoá an toàn để đảm bảo xác thực các bên trao đổi với nhau.

Chứng nhận khóa công khai được phát bởi nhà cung cấp chứng nhận số (CA). Để nhà cung cấp chứng nhận số cấp phát chứng nhận cho người dùng thì việc đầu tiên là phải đăng ký. Quá trình đăng ký gồm: đăng ký, kích hoạt, và chứng nhận của người dùng với PKI (CAs và RAs).

Quá trình đăng ký như sau:

- Người dùng đăng ký với CA hoặc RA. Trong quá trình đăng ký, người dùng đưa ra cách nhận biết đến CA. CA sẽ xác thực đầu cuối, phát khóa công khai đến người sử dụng.
- Các đầu cuối bắt đầu khởi tạo phase bằng cách tạo ra một cặp khóa và khóa công khai của cặp khóa được chuyển đến CA.
- CA viết mật hiệu lên chứng nhận khóa công khai cùng với khóa bí mật để tạo một chứng nhận khóa công khai cho mật mã đầu cuối.

Lúc này các người dùng có thể yêu cầu và nhận chứng thực khóa công khai từ người sử dụng khác. Chúng có thể sử dụng khóa công khai của CAs để giải mã chứng nhận khóa công khai để thu được khoá tương ứng.

Trong nhiều trường hợp, CA sẽ cung cấp tất cả các dịch vụ cần thiết của PKI để quản lý các khóa công khai bên trong mạng. Tuy nhiên có nhiều trường hợp CA có thể

uỷ nhiệm làm công việc của RA. một số chức năng mà CA có thể uỷ nhiệm thay thế cho RA như:

- Kiểm tra mật mã đầu cuối đã đăng ký khóa công khai với CA để có khóa bí mật mà được dùng để kết hợp với khóa công khai.
- Phát cặp khóa được dùng để khởi tạo phase của quá trình đăng ký.
- Xác nhận các thông số của khóa công khai.
- Phát gián tiếp các danh sách thu hồi chứng nhận (CRL).

Phát hành chứng nhận số

CA dùng để cấp phát chứng nhận, xác thực PKI khách, và khi cần thiết thu hồi lại chứng nhận. CA đại diện cho nguồn tin cậy chính của PKI. Vì CA là yếu tố duy nhất trong PKI mà có thể phát chứng thực khóa công khai đến những người sử dụng. CA cũng luôn đáp ứng cho việc duy trì CRL. PKI không phải chỉ có một CA mà PKI có thể thiết lập nhiều CAs khác nhau.

Các CA giúp dễ dàng xác nhận và lấy thông tin của những người thực hiện trao đổi thông tin với nhau. Các CA không chỉ chứng nhận cho những người dùng mà còn có thể chứng nhận những CA khác bằng cách cấp phát chứng nhận cho chúng. Những CA đã được chứng nhận lại có thể chứng nhận tiếp cho những CA khác, cứ như vậy cho đến khi các thực thể có thể ủy nhiệm cho nhau trong quá trình giao dịch.

2.3.3. Mục tiêu và các chức năng của PKI

PKI cho phép những người tham gia xác thực lẫn nhau và sử dụng các thông tin từ các chứng thực khoá công khai để mã hoá và giải mã thông tin trong quá trình trao đổi.

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 trao đổi các thông tin bảo mật từ trước.

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

- Mã hoá Email hoặc xác thực người gửi Email
- Mã hoá hoặc chứng thực văn bản
- Xác thực người dùng ứng dụng
- Các giao thức truyền thông an toàn

Chương 3. Xây dựng biện pháp an toàn trong thuế điện tử

3.1. Vấn đề

Theo cách thông thường để nộp thuế người nộp thuế phải đi đến rất nhiều văn phòng để hoàn tất các thủ tục vào giao dịch với các nhân viên ở cơ quan thuế. Những thủ tục này bao gồm những việc từ đăng kí nộp thuế, lấy mã số thuế, nộp thuế, nhận giấy tờ chứng nhận,... ngay cả việc nộp phiếu kê khai thuế. Người nộp thuế sẽ thấy đây là cả một hệ thống nặng nề, đòi hỏi nhiều quá trình rắc rối. Thuế điện tử ra đời với mục đích nâng cao chất lượng dịch vụ, đơn giản hóa những thủ tục, giao dịch.

Triển khai dịch vụ thuế điện tử cần phải có những tính chất như: tin cậy, toàn vẹn, chống chối bỏ, công minh. Tuy vậy để có thể thành công, việc vô cùng quan trọng là cần có sự thống nhất, liên kết giữa các thành phần, các cơ quan, giúp cho cả hệ thống lớn có thể giao tiếp, làm việc ăn khớp với nhau.

Về khía cạnh an toàn, các thủ tục, giao dịch cần được thực sự chú trọng, đặc biệt cho việc xác thực người dùng trên cổng thông tin thuế. Việc này liên quan đến nhiều vấn đề như nền tảng, công nghệ được sử dụng, phần mềm triển khai, những chức năng mà mỗi cơ quan cần... nó yêu cầu các tổ chức phải ngồi cùng nhau, cùng đưa ra ý kiến và đưa ra thông tin một cách đầy đủ nhất để có thể sử dụng cổng thông tin thuế như là một nơi duy nhất cung cấp dịch vụ cho người nộp thuế.

3.2. Giải pháp

Như đã trình bày về chữ ký số và PKI ở các chương trước, triển khai thuế điện tử việc khó khăn nhất, cũng là việc cần thực hiện nhất đó là xây dựng được một hệ thống PKI hoàn chỉnh. Ngoài ra, không kém phần quan trọng là xây dựng một cổng thông tin thuế với đầy đủ chức năng, an toàn, thân thiện với người nộp thuế. Để dễ dàng cho người sử dụng chúng ta cần giới thiệu, quảng bá về những nền tảng dùng để phát triển hỗ trợ tất cả các dịch vụ đang có trên cổng thông tin, về những cơ chế an toàn của việc xác thực số cho người dân và doanh nghiệp. Người nộp thuế sẽ có một trung tâm liên lạc với cơ quan thuế, qua đó họ có thể tìm thông tin, truy cập tài liệu mà vài năm trước khó có thể xem được đồng thời có thể hoàn thành những thủ tục, giao dịch của mình chỉ trong vài giờ. Hơn nữa từ cổng thông tin này, các cơ quan con của ngành thuế có

thể cung cấp những dịch vụ mới cho người dùng, đây sẽ là nơi cung cấp thông tin riêng theo từng cấu trúc, phân mục phù hợp.

Trong dự án này vấn đề giải quyết và điều chỉnh những vấn đề liên quan đến trao đổi và sử dụng thông tin ở hiện tại cũng như trong tương lai là rất quan trọng. Theo đó chúng ta cần xây dựng những hướng dẫn, quy tắc trong việc triển khai những dịch vụ công cộng sao cho có thể sử dụng thông tin một cách an toàn. Nền tảng dựng lên phải chứa những yêu cầu rõ ràng, khắt khe liên quan một cách trực tiếp tới các vấn để tổ chức, thủ tục và công nghệ của xác thực số đối người nộp thuế dựa trên thông tin có trong mỗi giao dịch. Hệ thống sẽ sử dụng PKI và chứng nhận số để xác thực người sử dụng và đảm bảo an toàn, chính xác cho mỗi giao dịch. Với những chức năng mạnh mẽ sẵn có của PKI, cổng thông tin đảm bảo sự an toàn của cá nhân và những thông tin nhạy cảm mà người sử dụng trao đổi sẽ được bảo vệ bằng cả hai biện pháp: gia tăng mức độ bảo mật trong các thủ tục xác thực và mã hóa dữ liệu, giao dịch.

Chúng ta có thể chia dự án này thành hai dự án con:

- Hệ thống xác thực: Hệ thống định danh số cho cá nhân, đơn vị nộp thuế và cho các dịch vụ cung cấp bởi các cơ quan thuế
- Hệ thống các dịch vụ: Được thiết kế để người nộp thuế có thể dễ dàng truy cập và sử dụng các dịch vụ thuế

3.2.1. Hệ thống xác thực

Hệ thống này được thiết kế không chỉ để chứa các chứng nhận xác thực cần thiết của các thiết bị định danh người dùng (USB hoặc thẻ thông minh) mà còn để cho các thiết bị, hệ thống hạ tầng khác có thể đọc và thẩm tra những thiết bị định danh đó. Những thành phần cơ bản của một hệ thống xác thực bao gồm:

- Một hệ thống thẩm tra định danh - Hệ thống này bằng một phương pháp xác thực nào đó sẽ xác định người chủ của thiết bị định danh với độ tin cậy cao.
- Một cơ sở dữ liệu - Là nơi lưu trữ toàn bộ dữ liệu cần thiết của hệ thống
- Một thiết bị định danh - Có thể là USB hoặc thẻ thông minh chứa những thông tin thực tế để xác thực người dùng. Trong trường hợp này có thể

dùng để chứa khóa bí mật.

- Một hệ thống thẩm tra thiết bị định danh - Dùng để đọc và xác nhận thông tin của các thiết bị định danh.
- Các chính sách - Nó lưu lại sự sử dụng hệ thống diễn ra lúc nào, như thế nào, bao gồm cả sự giám sát và quản lý của cơ quan có thẩm quyền. Nó cho phép dò tìm những giao dịch và hành động của người sử dụng.
- Khả năng mở rộng - Giải pháp triển khai phải cho phép ứng dụng có thể nâng cấp, sử dụng một cách linh hoạt và cho nhiều mục đích. Có thể trong tương lai sẽ phát triển và gộp tất cả lại trong một thiết bị định danh duy nhất, hệ thống cần đủ linh hoạt để thực hiện những việc này.

Không chỉ cung cấp các phương thức tiện lợi, hệ thống cần phải là một thành phần thực sự đáng tin cậy giữa người sử dụng (ở đây là người nộp thuế) và cơ quan chức năng (ở đây là cơ quan thuế). Ngoài ra các vấn đề về quyền riêng tư cũng cần được chú trọng.

Một phần quan trọng của hệ thống là là thiết bị định danh người dùng. Nó là một thiết bị có thể chứa thông tin, có thể cập nhật thông tin, và có thể thực hiện những việc này một cách cực kì an toàn. Tại sao không sử dụng những đặc điểm cá nhân như vân tay (hay những đặc điểm sinh học khác)? Khó khăn là cần phải có một trung tâm chứa tất cả những mẫu vân tay hợp lệ, điều này gia tăng sự nguy hiểm như là giả mạo hoặc trộm cắp bởi vì tất cả các thông tin được lưu trữ ở cùng một địa điểm. Hơn nữa công nghệ để xác nhận vân tay cho cả triệu người dùng công cộng chưa được triển khai nhiều, và chưa phù hợp với thực tế. Giải pháp sẽ là USB hoặc thẻ thông minh kết hợp dữ liệu người dùng với những thông tin xác thực khác, các mẫu thông tin nhận dạng tương ứng cũng được lưu trong chính thiết bị này. Đối với những thủ tục, giao dịch thực sự cần xác thực, nó sẽ được dùng. Còn đối với những thủ tục đơn giản những thông tin này sẽ được bỏ qua.

Theo trình tự để thiết bị định danh có thể đi vào sử dụng, các thiết bị đọc phải được đặt ở mọi vị trí mà cần dùng đến thiết bị. Đối với các thiết bị USB thì việc này khá dễ dàng do đa phần các máy tính hiện nay đều có cổng USB, các thiệt bị khác như thẻ thông minh cũng đã được sử dụng khá phổ biến hiện nay. Đối với Việt Nam hiện

nay, để triển khai nhanh, sử dụng USB làm thiết bị định danh là hợp lý.

3.2.2. Hệ thống các dịch vụ

Một dịch vụ thuế tiên tiến phải là dịch vụ có khả năng phục vụ người nộp thuế truy cập 24 giờ một ngày và 7 ngày trong tuần. Các dịch vụ này phải luôn luôn chính xác và có độ an toàn cao. Một thử thách thực tế khi chuyển từ thủ tục truyền thống sang thuế điện tử là khả năng triển khai các giải pháp đưa ra với một giao diện thân thiện, dễ sử dụng đối với một lượng rất lớn người sử dụng bao gồm đủ các lứa tuổi và tầng lớp. Các dịch vụ này cũng cần chú ý tới vấn đề cá nhân như bảo quản quyền riêng tư và các dữ liệu nhạy cảm.

Nhìn chung hầu hết các dịch vụ nên tập trung vào những chức năng cơ bản như kê khai thuế, hỗ trợ mẫu nhập liệu và chuyển thành các định dạng điện tử thông dụng.

Việc triển khai thuế điện tử, mở rộng ra là chính phủ điện tử đã được thực hiện thành công ở nhiều nước, hệ thống PKI cũng chứng tỏ tính khả thi và có thể phục vụ một lượng lớn người dùng với sự tin cậy và độ an toàn cao. Vì vậy việc triển khai thuế điện tử ở Việt Nam chỉ còn là vấn đề thời gian.

3.3. Triển khai

Mục này trình bày các giải pháp, công nghệ được sử dụng để triển khai trong thực tế xoay quanh nền tảng PKI.

3.3.1. VPN

Hầu hết các ứng dụng PKI hiện nay hỗ trợ việc sử dụng VPN. VPN cung cấp các giải pháp kinh tế, an toàn cho phép người dùng điều khiển, giao tiếp với các thiết bị an toàn. Sử dụng PKI trong VPN cho hiệu quả cao hơn và tăng khả năng hữu ích của VPN. Điểm cần quan tâm chính của sử dụng VPN là làm cách nào hành động người dùng được quản lý. Có thể sử dụng một số giải pháp VPN như IPSec VPN và SSL VPN.

- IPSec (Internet Protocol Security) là giao thức mạng về bảo mật và thường được liên kết với VPN. IPSec cho phép việc truyền tải dữ liệu được mã hóa an toàn ở lớp mạng (Network Layer) theo mô hình OSI thông qua

mạng công cộng như Internet. VPN lớp mạng đề cập đến những thách thức trong việc dùng Internet như là một môi trường truyền đưa các lưu lượng đa giao thức và nhạy cảm.

- Thuật ngữ SSL VPN được dùng để chỉ một dòng sản phẩm VPN mới và phát triển nhanh chóng dựa trên giao thức SSL. Cũng cần nói rõ là bản thân giao thức SSL không mới nhưng liên kết SSL với VPN là mô hình mới. Dùng SSL VPN, kết nối giữa người dùng từ xa và tài nguyên mạng công ty thông qua kết nối HTTPS ở lớp ứng dụng thay vì tạo "đường hầm" ở lớp mạng như giải pháp IPSec. SSL VPN cung cấp các ứng dụng trên nền Web (Web-based application), các ứng dụng thư điện tử (POP3/IMAP/SMTP). Các máy khách chỉ cần dùng trình duyệt có hỗ trợ SSL thực hiện kết nối VPN mà không cần cài đặt phần mềm riêng cho VPN. Đa số các giải pháp SSL VPN không cung cấp các ứng dụng dùng cổng TCP động như FTP hay VoIP.

Hiện tại thị phần VPN đang tăng lên rất nhanh đặc biệt là SSL VPN, có các tên tuổi lớn như: NetScreen (đã bị Juniper mua lại năm 2004), F5, Aventail, Nokia.

3.3.2. Ký văn bản

Một trong những ứng dụng thuế được dùng nhiều trong PKI là ký vào văn bản. Ký văn bản có thể được nhìn dưới hai cách:

- Ký vào những văn bản độc lập rồi gửi chúng theo những phương thức truyền thống ví dụ như thư điện tử.
- Như là một phần của một chuỗi các hành động, trong đó có bước ký vào văn bản.

Sử dụng việc ký văn bản cũng cần xác định chính xác mục đích sử dụng là nội bộ hay là cả từ bên ngoài. Các quá trình nội bộ có thể được quản lý sử dụng chứng nhận tự ký (self-signed certificates). Các quá trình liên quan đến bên ngoài hầu hết yêu cầu chứng nhận một CA công cộng, điều này có nghĩa là mỗi người dùng cần có một chứng nhận trước khi có thể sử dụng các ứng dụng. Nhìn chung việc ký văn bản có hai mục tiêu chính:

- Làm đơn giản và tăng tính hiệu quả cho quy trình
- Tăng sự ràng buộc pháp lý của các văn bản đã ký

Trong trường hợp các mẫu văn bản cần được ký và hoàn thành mà không có kết nối Internet, việc ký các văn bản độc lập là giải pháp tốt. Giải pháp này có thể sử dụng phần mềm của bên thứ ba như: Adobe, Silanis,... Những ứng dụng này cho phép ký lên các dạng tài liệu phổ biến như pdf, Microsoft Word, AutoCAD,...

Để phát triển các ứng dụng ký điện tử riêng một cách nhanh chóng có thể sử dụng một số bộ thư viện phát triển phần mềm của một số nhà cung cấp như InfoMosaic, Xetex,... InfoMosaic cung cấp giải pháp ký điện tử dựa trên XML, sản phẩm của họ được gọi là SecureXML, nó cung cấp một loạt các giải pháp từ phía người sử dụng cho đến phía người cung cấp. Dựa trên bộ thư viện phần mềm của họ chúng ta có thể xây dựng một phần mềm riêng biệt, phù hợp. Xetex cung cấp hàng loạt các sản phẩm liên quan đến PKI. Một sản phẩm đặc trưng của họ là cung cấp một bộ điều khiển ActiveX cho ký văn bản.

3.3.3. An toàn thư điện tử

Giải pháp an toàn trong việc sử dụng thư điện tử có thể chia làm hai loại: có sử dụng chương trình khách (client) trên máy người dùng và chỉ sử dụng trình duyệt web. Giải pháp sử dụng chương trình thư điện tử trên máy người dùng có thể cung cấp nhiều tính năng hơn, còn giả pháp sử dụng trình duyệt có lợi thế là gọn nhẹ, rẻ và dễ triển khai. Sử dụng giải pháp nào phụ thuộc vào mục đích riêng của mỗi tổ chức.

Sử dụng chương trình khách

Có thể sử dụng một số phần mềm thư điện tử nổi tiếng, các phần mềm này được tích hợp hoàn toàn với chứng nhận số. Phần mềm cho phép người sử dụng có thể gửi một thư điện tử không mã hóa, mã hóa, được ký, hoặc vừa ký vừa mã hóa. Các phần mềm được sử dụng rộng rãi hiện nay như:

- Microsoft Outlook Express
- Mozilla Thunderbird

Sử dụng dịch vụ web

Hầu hết các dịch vụ thư điện tử trên nền web đều không đi kèm các dịch vụ chứng thực. Tuy vậy chúng ta có thể tích hợp các phần bổ sung cho phép ký và mã hóa thư điện tử vào trình duyệt để sử dụng cùng với các dịch vụ thư điện tử trên nền web. Một số phần bổ sung cho trình duyệt Firefox như:

- Gmail S/MIME
- WiseStamp Email Signature

3.3.4. An toàn mạng không dây

Nói đến xây dựng PKI không dây dường như là không thể. Khi làm việc với môi trường không dây, vì một vài lý do PKI sẽ gặp rất nhiều khó khăn khi triển khai. Điều cần nói nhất là giới hạn về sức mạnh bộ xử lý và bộ nhớ trong của các thiết bị di động. Tuy vậy có một vài cách tiếp cận được phát triển để vượt qua những giới hạn đó. Hai trong số những giải pháp chính cho phép triển khai trên các thiết bị di động là:

- Chứng nhận Wireless Transport Layer Security (WTLS) - cách tiếp cận này đã thay đổi chứng nhận X.509 cho phép sử dụng được những thiết bị di động với bộ vi xử lý và bộ nhớ trong nhỏ hơn.
- Wireless Public Key Infrastructure (WPKI) - Hiện tại vấn đề ủy nhiệm của các thiết bị di động đã được giải quyết qua WPKI. WPKI bao gồm những thành phần tương tự với PKI chuẩn như CA, RA, thực thể cuối; hơn nữa WPKI cũng có thể sử dụng cổng thông tin PKI truyền thống bằng cách chuyển qua lại giữa WAP trên di động và mạng Internet CA.

Certicom

Certicom cung cấp nhiều giải pháp trong lĩnh vực không dây, xoay quanh từ giải pháp WLAN tới PKI cho các thiết bị di động. Certicom cũng cung cấp máy chủ PKI CA của chính họ và cổng thông tin WPKI để phát hành chứng nhận số cho các thiết bị như PDA và điện thoại di động. Thêm nữa, Certicom cũng cung cấp đường VPN cho các thiết bị di động gọi là movianVPN.

Openware

Một trong những tiên phong trong lĩnh vực không dây, Openware có nhiều sản

phẩm tương thích với hàng loạt các dịch vụ xác thực. Sản phẩm đáng kể đến nhất là microbrowser (một trình duyệt cho di động) hỗ trợ chứng nhận WTLS.

3.3.5. Đăng nhập một lần (Single Sign-On)

Đăng nhập một lần (SSO) có lẽ là giải pháp đáng nói nhất trong ngành công nghiệp bảo mật. Về cơ bản, đăng nhập một lần cho phép người sử dụng định danh một lần duy nhất và sau đó sử dụng sự xác nhận này để truy cập hàng loạt tài nguyên. Hiện nay có rất nhiều cách giúp thực hiện những giải pháp xung quanh SSO. Nếu không sử dụng SSO, người dùng sẽ phải định danh họ với nhiều hệ thống rời rạc, phức tạp. Việc xác thực nhiều lần, lặp lại có thể gây nhiều phiền hà và cả những mối nguy hiểm về bảo mật bởi vì rất nhiều người sử dụng các mật khẩu dễ đoán ở một vài hệ thống. Có hai giải pháp chính cho SSO, cả hai đều khá đắt tiền:

Giải pháp tích hợp

Cung cấp khả năng tích hợp với việc đăng nhập của một hệ điều hành riêng biệt, như vậy có thể vận dụng khả năng an toàn của hệ điều hành kết hợp với việc bổ sung xác thực, và thông tin xác thực được cung cấp bởi một bên thứ ba. Ví dụ việc đăng nhập vào các hệ điều hành như Windows, GNU/Linux cho phép người dùng sử dụng sự xác thực này để truy cập vào các dịch vụ khác.

Giải pháp lai

Dựa vào sự thật là có sự kết hợp của nhiều công nghệ trong thực tế, bao gồm cả những vật định danh. Nó cho phép SSO có thể đạt được bằng cách bắt trước đầu vào người dùng như là tài khoản và mật khẩu. Giải pháp sẽ lưu trữ những ủy nhiệm (mật khẩu, PIN, chứng nhận) trong phần mềm "ví" hoặc vật định danh và người dùng có thể sử dụng những ủy nhiệm này để định danh và sử dụng tài nguyên. Giải pháp này ít tốn kém hơn giải pháp tích hợp, ngoài ra nó còn dễ dàng mở rộng và phát triển.

3.3.6. Máy chủ web

Tất nhiên một máy chủ web có thể dễ dàng sử dụng cho các ứng dụng dựa trên sự tím nhiệm. Hầu hết các trang web thương mại hiện nay được sử dụng qua những phương pháp an toàn nào đó, nhưng hầu hết tất cả đều dựa vào sử dụng chứng nhận Secure Socket Layer (SSL). Chứng nhận SSL là một trong những ứng dụng sớm nhất

của công nghệ PKI. Chứng nhận SSL cho phép tạo ra một đường truyền an toàn giữa trình duyệt web và máy chủ web của các tổ chức. Một trong những lý do chứng nhận SSL phát triển như là một ứng dụng cốt lõi cho việc ủy nhiệm là để cho các công ty xác thực và lấy chứng nhận SSL từ một bên thứ ba - một nhà cung cấp PKI. Việc này rất tiện dụng cho người dùng vì chứng nhận của các nhà cung cấp đã có sẵn trong hầu hết các trình duyệt hiện nay.

Có hai loại máy chủ web là hệ thống dựa trên phần mềm hoặc phần cứng:

Phần mềm máy chủ web

Máy chủ web có thể được triển khai như là một phần mềm dựa trên phần cứng sẵn có. Bổ sung bảo mật là việc khá đơn giản vì hầu hết phần mềm máy chủ web hiện nay đều có những công cụ để thêm chứng nhận SSL. Hai phần mềm máy chủ web đang chiếm hầu hết thị phần hiện nay là:

- Apache với mod_ssl
- Microsof IIS

Máy chủ web dựa trên phần cứng

Với khả năng xây dựng phù hợp với trung tâm dữ liệu, đơn giản hóa việc cấu hình, dạng máy chủ web này được rất nhiều tập đoàn lớn sử dụng. Một số máy chủ web như:

- Sun Cobalt
- Net Integrator
- UVNetworks WebBox

3.3.7. Thẻ thông minh

Thẻ thông minh là những con chíp máy tính được tích hợp trên các thẻ cứng. Ứng dụng của thẻ thông minh bao gồm từ việc lưu trữ những dữ liệu đơn giản (như chứng nhận) tới những giao dịch phức tạp như những giao dịch về tài chính. Phần này sẽ tập trung vào việc sử dụng thẻ thông minh liên quan đến những vấn đề xác thực các giao dịch. Trong hoàn cảnh này chúng ta chỉ dùng những thẻ thông minh đơn giản là nơi lưu trữ dữ liệu khóa như là khóa bí mật cho các chứng nhận điện tử. Nó có thể phục vụ

cho hai mục đích:

- Tăng tính bảo mật bởi vì thẻ thông minh (và cả khóa bí mật) có thể hủy bỏ vật lý và nó là riêng biệt đối với từng máy tính.
- Tăng tính cơ động cho khóa bí mật, cho phép người sử dụng có khả năng dùng chúng ở nhiều nơi.

Có nhiều loại thẻ thông minh, mỗi loại sẽ có chức năng và ứng dụng riêng vì vậy tùy mục đích mà sử dụng loại thẻ thích hợp. Khi sử dụng giải pháp thẻ thông minh cần chú ý đến những điểm chính sau:

- Giá cả - Thẻ giá rẻ hầu như chỉ sử dụng để chứa dữ liệu, những thẻ nhiều chức năng hơn sẽ đắt hơn và có thêm những phần mềm bổ sung.
- Dung lượng lưu trữ - Tùy vào loại thẻ, những thẻ công nghệ thấp có thể chứa hai hoặc ba chứng nhận số, những thẻ công nghệ cao có thể chứa nhiều hơn 128K dữ liệu.
- Bảo mật - Một vài đầu đọc có bàn phím để nhập PIN nhúng trong nó, việc này tránh được những chương trình ăn cắp mã PIN khi người dùng mở khóa thẻ thông minh để truy cập thông tin. Những thẻ công nghệ thấp hầu như không có tính năng bảo mật.

3.3.8. Bảo vệ kho dữ liệu

Với sự phát triển của mạng lưới lưu trữ và những dạng lưu trữ điện tử khác, dữ liệu cần được cất giữ một cách an toàn và được bảo vệ chặt chẽ. Việc này không chỉ áp dụng cho các máy chủ trong cơ sở hạ tầng mà còn cho cả máy tính của người sử dụng. Nếu là máy tính xách tay, nếu bị mất cắp, thiệt hại sẽ giảm đi rất nhiều nếu ổ cứng được mã hóa toàn bộ. Cũng như vậy với các cơ quan, mạng lưới lưu trữ cần phải an toàn hơn, nhất là trong quá trình sao lưu dữ liệu. Có hai lĩnh vực chính mà các giải pháp ủy nhiệm PKI có thể áp dụng cho mạng lưới lưu trữ:

- An toàn trong cơ cấu - Xác thực định danh của các bộ chuyển đổi (switch) trước khi cho phép nó vào mạng lưới lưu trữ.
- An toàn từ người quản lý - Bảo vệ an toàn dữ liệu từ bản điều khiển của

người quản lý tới các thành phần của mạng lưới lưu trữ. Công nghệ PKI được dùng để cung cấp một cơ chế mã hóa bao gồm cả xác thực những lệnh đến từ người quản lý.

Brocade

Cung cấp rất nhiều nền tảng bảo mật, các giải pháp an toàn được tích hợp trong mỗi thành phần trong mạng lưới lưu trữ, mỗi thành phần có thể giao tiếp với những thành phần khác một cách an toàn và cung cấp đủ xác thực để tránh những thành phần lừa đảo từ các hệ thống được kết nối vào. Mỗi bộ chuyển đổi được gắn một chứng nhận số trong thời gian chế tạo, chứng nhận này sẽ được người quản trị mạng lưới lưu trữ và các phần mềm kiểm tra xem nó có đủ chứng thực để tham gia mạng lưới không. Bằng việc sử dụng chứng nhận số, tên của bộ chuyển đổi cũng có thể được xác thực, và tên này được giữ cho nguyên vẹn.

3.4. Kết luận

Chương này đã đưa ra và để xuất các giải pháp xung quanh PKI để triển khai thuế điện tử. Với một hệ thống lớn, phức tạp, cần độ an toàn cao và nhiều người sử dụng, việc lựa chọn đúng giải pháp công nghệ là rất cần thiết. Cần phải xác định rằng hệ thống thuế điện tử cần mở rộng trong tương lai, có thể do thay đổi chính sách hoặc do cơ chế luật pháp, thêm nữa là cần được tích hợp với các hệ thống khác trong chính phủ điện tử, vì vậy hệ thống cũng cần mềm dẻo, linh động, dễ dàng nâng cấp.

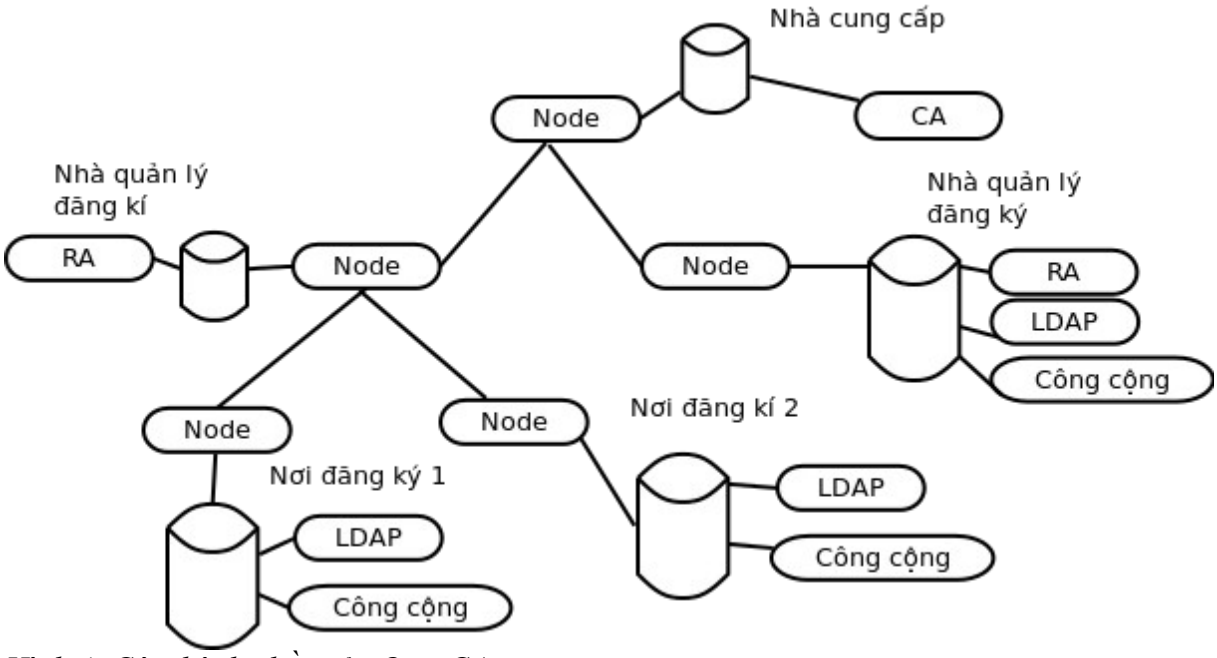
Chương 4. Phần mềm PKI

4.1. Giới thiệu về OpenCA

OpenCA cung cấp một hạ tầng PKI hoàn chỉnh cho các nhà cung cấp chứng chỉ số. Dự án OpenCA bắt đầu từ năm 1999. Ý tưởng ban đầu bao gồm 3 phần chủ yếu - giao diện web bằng Perl, sử dụng OpenSSL cho phần xử lý các hành động mã hóa và một cơ sở dữ liệu. Ý tưởng đơn giản này vẫn là phương châm hiện tại của OpenCA. Gần như tất cả các hành động có thể thực hiện qua giao diện web. OpenCA có 6 giao diện được cấu hình trước và có thể tạo thêm nhiều nữa tùy yêu cầu. Phần mã hóa phía sau vẫn là OpenSSL, phần cơ sở dữ liệu chứa tất cả những thông tin về các đối tượng mang tính mã hóa của người dùng như Certificate Signing Requests (CSRs), Certificates, Certificate Revocation Requests (CRRs) and Certificate Revocation Lits (CRLs). Hiện tại OpenCA hỗ trợ rất nhiều thành phần:

- Giao diện công cộng
- Giao diện LDAP
- Giao diện RA
- Giao diện CA
- SCEP
- OCSP
- Bộ lọc ip cho giao diện
- Role Based Access Control
- Cung cấp CRL
- Cảnh báo cho chứng nhận sắp hết hạn
- Hỗ trợ các trình duyệt mới

OpenCA không chỉ là giải pháp phục vụ các nghiên cứu nhỏ và trung bình, mà mục tiêu là hỗ trợ linh hoạt nhất cho các tổ chức lớn như các trường đại học, các mạng lưới doanh nghiệp.



Hình 4: Các thành phần của OpenCA

Node

Giao diện này quản lý cơ sở dữ liệu và điều khiển tất cả các chức năng xuất và nhập. OpenCA có thể tạo tất cả các bảng cơ sở dữ liệu nhưng nó không thể tự tạo ra dữ liệu bởi vì có sự khác nhau giữa các nhà đăng ký. Vì vậy ở đây cần một cơ sở dữ liệu với các quyền truy cập thích hợp và một cơ sở dữ liệu mới. Giao diện này bao gồm vài chức năng thực hiện sao lưu và khôi phục cho node. Không có một cơ chế mặc định ở OpenCA để sao lưu khóa bí mật. Chức năng xuất và nhập cũng được quản lý tại đây. Chúng ta có thể cấu hình các luật khác nhau cho sự đồng bộ giữa node với các cơ sở cao hơn và thấp hơn.

CA

Giao diện CA có tất cả chức năng cần thiết để tạo chứng nhận và danh sách thu hồi chứng nhận (CRLs). CA cũng bao gồm tất cả các chức năng để thay đổi cấu hình qua một giao diện web. Không thể thay đổi cấu hình này qua một giao diện web khác.

RA

Một RA của OpenCA có thể quản lý tất cả các loại yêu cầu. Nó bao gồm những

việc như: yêu cầu chỉnh sửa, yêu cầu chấp nhận, tạo khóa bí mật với thẻ thông minh, xóa yêu cầu sai và thư điện tử người dùng.

LDAP

Giao diện LDAP được triển khai riêng biệt để quản lý hoàn toàn LDAP. Việc này cần thiết vì có rất nhiều chức năng riêng cho LDAP mà người quản trị cần, nhưng người dùng không cần đến nó.

Công cộng

Phần giao diện công cộng bao gồm tất cả những chức năng người dùng cần:

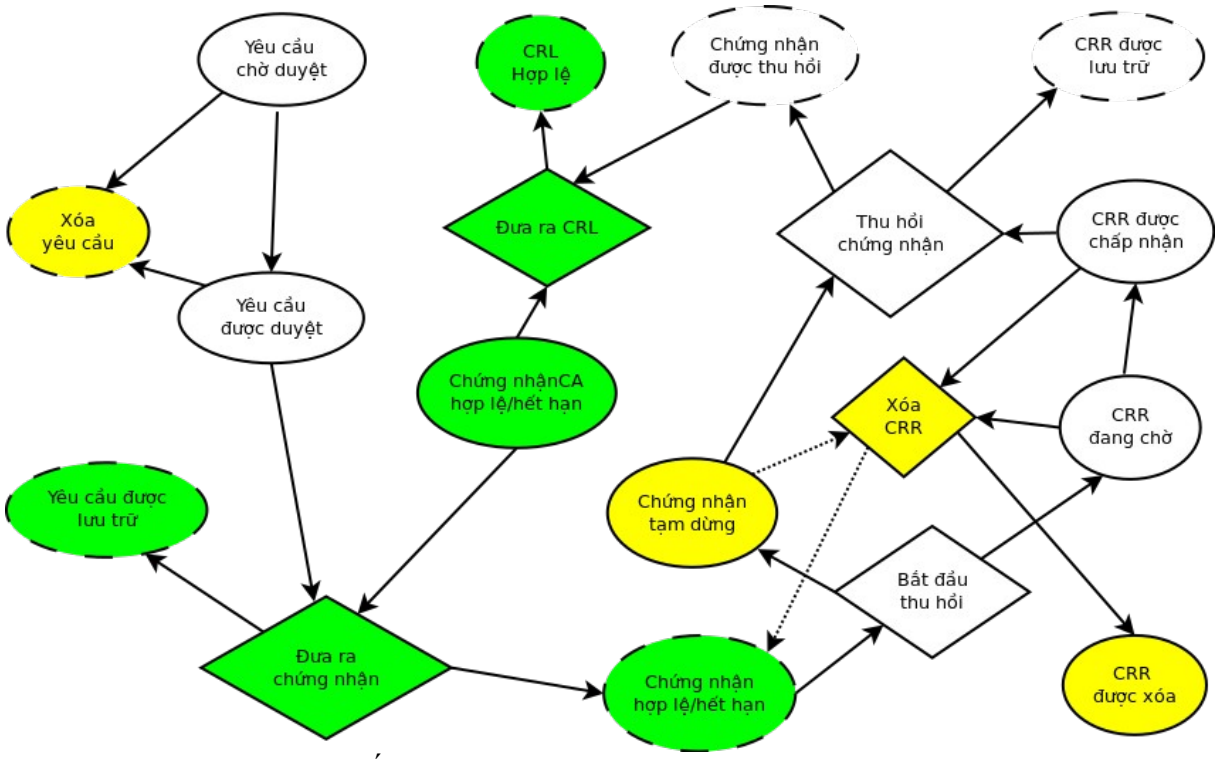
- Tạo CSRs (các yêu cầu kí xác nhận) cho IE, Mozilla,...
- Tạo các khóa bí mật
- Nhận yêu cầu PKCS#10 dưới dạng PEM từ máy chủ
- Nạp các chứng nhận
- Nạp CRLs
- Tìm kiếm chứng nhận
- Thử chứng nhận trong trình duyệt

4.2. Cài đặt

Chuẩn bị

OpenCA không phải là một hệ thống có thể chạy riêng lẻ, nó sử dụng một số sản phẩm từ các dự án nguồn mở khác như: Apache, mod_ssl, OpenSSL, OpenLDAP. Ngoài ra OpenCA còn cần khá nhiều Mô-đun của Perl như:

Authen::SASL, CGI::Session, Convert::ASN1, Digest::HMAC, Digest::MD5 Digest::SHA1, Encode::Unicode, IO::Socket::SSL, IO::stringy, MIME::Base64, MIME::Lite, MIME-tools, MailTools, Net-Server, Parse::RecDescent, URI X500::DN, XML::Twig, libintl-perl, perl-ldap



Hình 5: Vòng đời của một đối tượng OpenCA

OpenCA có thể chạy trên bất kì hệ thống nào hộ trợ Apache, mod_ssl, OpenSSL and Perl. Vì vậy nếu chúng ta có một hệ điều hành Linux, hiển nhiên có thể cài đặt và chạy OpenCA trên đó.

Cài đặt

Việc cài đặt được tiến hành trên máy chủ cài hệ điều hành Ubuntu GNU/Linux phiên bản 10.04. Để cài đặt, chuyển sang người dùng root:

sudo -i

Cài đặt các phần mềm cần thiết:

apt-get install gpg ftp links make unzip openssl libexpat-dev httpd mod_ssl mysql-server gcc

Cài đặt các Mô-đun cần thiết của Perl:

perl -MCPAN -e shell (Vào chế độ dòng lệnh của CPAN)

install CGI::Session

install Convert::ASN1

install Digest::MD5

install Digest::SHA1

install Encode::Unicode

install IO::Socket::SSL

install IO::Stringy

install MIME::Base64

install MIME::Lite

install MIME::Tools

install MailTool

install Net::Server

install URI

install XML::Twig

install XML::SAX::Base

Tạo cơ sở dữ liệu cho OpenCA

Tạo người dùng openca với mật khẩu openca:

CREATE USER 'openca'@'localhost' IDENTIFIED BY 'openca';

Đặt quyền cho người dùng openca (ở đây đặt cho có tất cả các quyền):

GRANT ALL PRIVILEGES ON *.* TO 'openca'@'localhost';

Tạo cơ sở dữ liệu cho openca:

CREATE DATABASE openca;

Cài đặt OpenCA

Phiên bản mới nhất của OpenCA là 1.1.0 tên mã là *samba*. Dưới đây là quá trình cài đặt OpenCA từ mã nguồn.

Cài đặt gói OpenCA Tool:

cd /usr/src

wget http://www.openca.org/alby/download?target=openca-tools-1.3.0.tar.gz

tar xvf openca-tools-1.3.0.tar.gz

cd openca-tools-1.3.0

./configure

make

make install

Cài đặt gói OpenCA:

wget http://www.openca.org/alby/download?target=openca-base-1.1.0.tar.gz

tar xvf openca-base-1.1.0.tar.gz

cd openca-base-1.1.0

./configure –with-httpd-fs-prefix=/var/www

make

make install-offline (Cài đặt ca và node)

make install-online (Cài đặt ra, ldap, pub, scep và node)

Như vậy là OpenCA đã được cài đặt vào thư mục /usr/local

Tạo mã lệnh khởi động cho OpenCA:

cd /etc/init.d

ln -s /usr/local/etc/init.d/openca

Tiếp theo là chỉnh tệp cấu hình của OpenCA, mở tệp :

/usr/local/etc/openca/confix.xml và chỉnh sửa các thông số:

Tên tổ chức:

ca_organization

UET

Tên nước:

<name>ca_country</name>

<value>VI</value>

Chỉnh sửa dịch vụ gửi thư điện tử:

<name>sendmail</name>

<value>/usr/lib/sendmail -t </value>

Địa chỉ thư điện tử:

<name>service_mail_account</name>

<value>ca@vnu.edu.vn</value>

Liên kết tới trang chính sách của CA:

<name>policy_link</name>

<value>http://</value>

Cấu hình cơ sở dữ liệu với người dùng là root và mật khẩu đặt ở trên.

```
<option>
    <name>dbmodule</name>
    <!-- you can use DB or DBI -->
    <value>DBI</value>
</option>
<option>
    <name>db_type</name>
    <value>mysql</value>
</option>
<option>
    <name>db_name</name>
    <value>openca</value>
</option>
```

<option>

<name>db_host</name>

<value>localhost</value>

</option>

<option>

<name>db_port</name>

<value>3306</value>

</option>

<option>

<name>db_user</name>

<value>openca</value>

</option>

<option>

<name>db_passwd</name>

<value>database_password</value>

</option>

Tắt LOAS (Levels of Authentication)

<option>

<name>USE_LOAS</name>

<value>no</value>

</option>

Sau khi chỉnh sửa cập nhật cấu hình cho OpenCA

cd /usr/local/etc/openca

./configure_etc.sh

Khi cấu hình hệ thống sẽ yêu cầu nhập mật khẩu cho người dùng admin.

Để cấu hình sử dụng https hay http, chỉnh sửa tệp cấu hình trong thư mục cài đặt OpenCA tương ứng với dịch vụ. Ví dụ chỉnh RA chạy ở dịch vụ http thường, chỉnh sửa tập tin etc/openca/access_control/ra.xml

```
<channel>
    <type>mod_ssl</type>
    <protocol>http</protocol>
    <source>.*</source>
    <asymmetric_cipher>.*</asymmetric_cipher>
    <asymmetric_keylength>0</asymmetric_keylength>
    <symmetric_cipher>.*</symmetric_cipher>
    <symmetric_keylength>0</symmetric_keylength>
</channel>
```

Tại đây cũng có thể cấu hình mật khẩu đăng nhập, hoặc thêm bớt người dùng có quyền đăng nhập hệ thống.

Sau khi cấu hình khởi động dịch vụ OpenCA bằng lệnh:

```
/etc/init.d/openca start
```

4.3. Sử dụng

4.3.1. Khởi tạo ban đầu

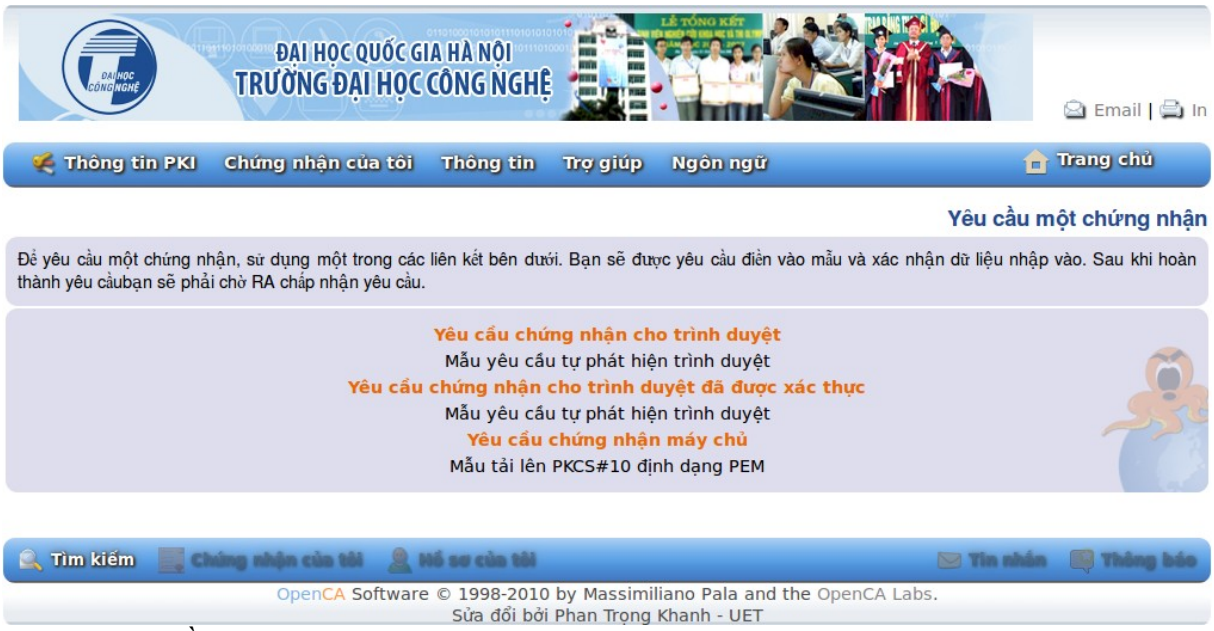
Khởi tạo ban đầu của CA bao gồm ba bước và chỉ có thể thực hiện một lần. Bước đầu tiên là bắt buộc. Nó khởi tạo chính CA. Bước hai và ba là tùy chọn. Chúng tạo hai chứng nhận đầu tiên. Bước hai tạo một chứng nhận cho một người điều hành và bước ba tạo chứng nhận cho máy chủ web.

Hình 6: Khởi tạo OpenCA

Bước đầu tiên khởi tạo của OpenCA được dùng để cài đặt tất cả các cơ chế mã hóa cần thiết để chạy CA. Nó bao gồm khóa bí mật, yêu cầu chứng nhận chữ ký (CSR), chứng nhận CA và quy trình chứng nhận của CA. Sau khi bước này được thực hiện thành công, CA sẽ sẵn sàng đi vào sử dụng. Bước này gồm các phần: khởi tạo cơ sở dữ liệu, tạo cặp khóa cho CA, cài đặt chứng nhận cho CA,...

Hình 7: Khởi tạo CA

4.3.2. Yêu cầu một chứng nhận

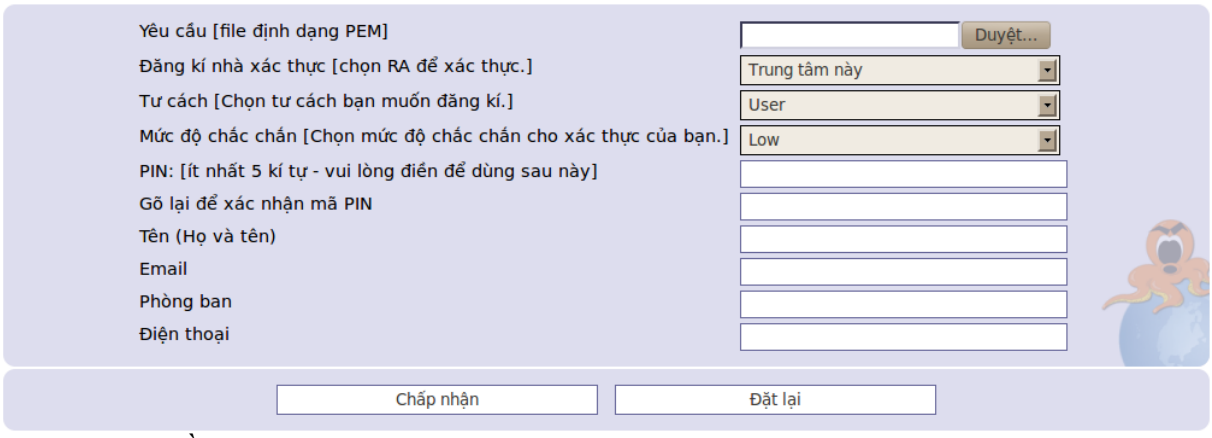


Hình 8: Yêu cầu một chứng nhận

Tại trang công cộng, vào trình đơn Chứng nhận của tôi → Yêu cầu một chứng nhận để chọn yêu cầu chứng nhận phù hợp.

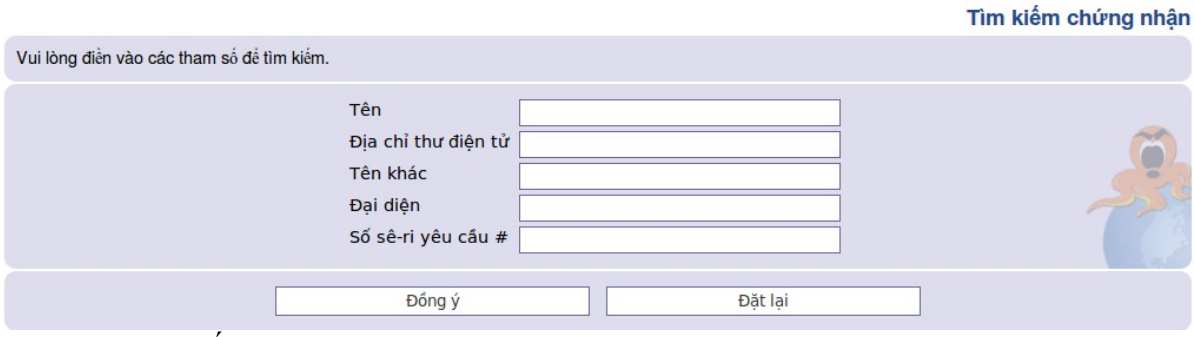
Giả sử người sử dụng đã có khóa bí mật, và tập tin pem dùng để yêu cầu các CA

chứng nhận. Chọn Yêu cầu chứng nhận máy chủ để tải lên tập tin pem:



Hình 9: Yêu cầu chứng nhận từ tệp PEM

Sau khi điền đầy đủ thông tin và tập tin yêu cầu chứng nhận được thông báo là hợp lệ, yêu cầu sẽ được gửi lên RA. Sau khi RA đồng ý và phát hành chứng nhận, người dùng sẽ nhận được thư điện tử kèm theo những thông tin liên quan đến chứng nhận của mình như số sê-ri, nội dung chứng nhận,.... Ngoài ra người dùng có thể yêu cầu chứng nhận cho trình duyệt của mình sử dụng hai lựa chọn đầu tiên của trang yêu cầu chứng nhận.

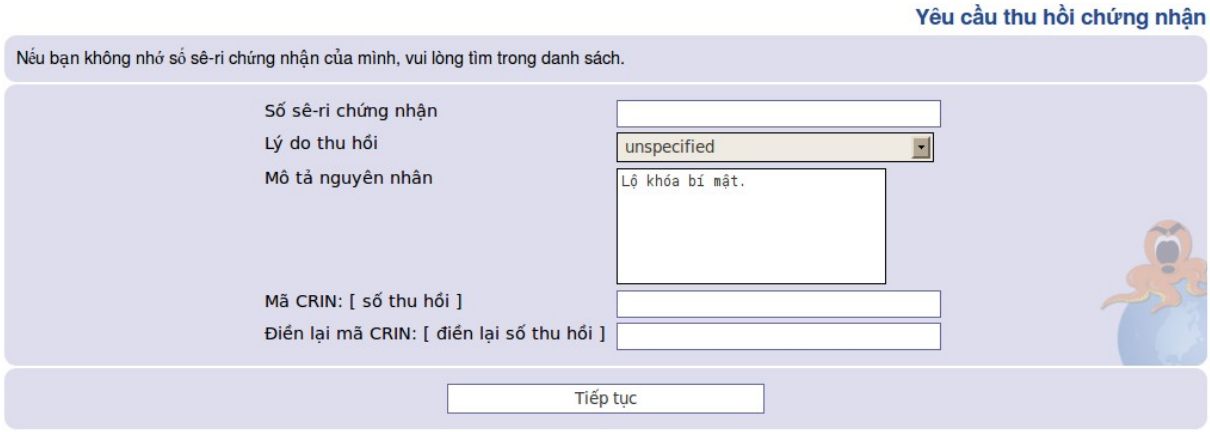


Hình 10: Tìm kiếm chứng nhận

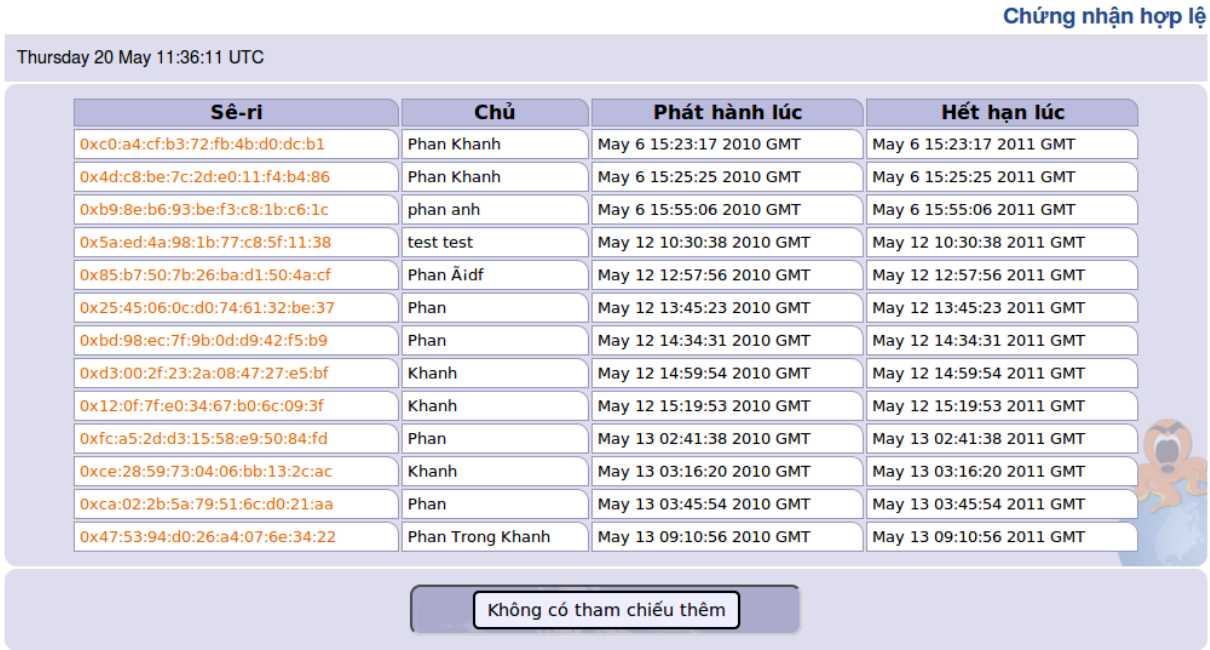
Sau khi chứng nhận được phát hành, những người dùng khác có thể tìm kiếm chứng nhận trên trang công cộng của OpenCA và sử dụng chứng nhận này để lấy khóa công khai, thông tin về người dùng. Sử dụng những thông tin này để xác nhận người cần liên lạc, để mã hóa thông tin khi liên lạc hoặc để giải mã, thẩm tra chữ ký khi nhận thông tin từ người kia.

4.3.3. Thu hồi chứng nhận

Vì một lý do nào đó, cơ quan, tổ chức, người sử dụng không muốn sử dụng chứng nhận đã đăng ký, có thể thực hiện yêu cầu thu hồi chứng nhận. Quá trình này yêu cầu điền đầy đủ thông số về chứng nhận và mã CRIN (mật mã dùng thu hồi chứng nhận) nhận được khi đăng ký chứng nhận.



Hình 11: Yêu cầu thu hồi chứng nhận



Sê-ri	Chủ	Phát hành lúc	Hết hạn lúc
0xc0:a4:cf:b3:72:fb:4b:d0:dc:b1	Phan Khanh	May 6 15:23:17 2010 GMT	May 6 15:23:17 2011 GMT
0x4d:c8:be:7c:2d:e0:11:f4:b4:86	Phan Khanh	May 6 15:25:25 2010 GMT	May 6 15:25:25 2011 GMT
0xb9:8e:b6:93:be:f3:c8:1b:c6:1c	phan anh	May 6 15:55:06 2010 GMT	May 6 15:55:06 2011 GMT
0x5a:ed:4a:98:1b:77:c8:5f:11:38	test test	May 12 10:30:38 2010 GMT	May 12 10:30:38 2011 GMT
0x85:b7:50:7b:26:ba:d1:50:4a:cf	Phan Ãidf	May 12 12:57:56 2010 GMT	May 12 12:57:56 2011 GMT
0x25:45:06:0c:d0:74:61:32:be:37	Phan	May 12 13:45:23 2010 GMT	May 12 13:45:23 2011 GMT
0xbd:98:ec:7f:9b:0d:d9:42:f5:b9	Phan	May 12 14:34:31 2010 GMT	May 12 14:34:31 2011 GMT
0xd3:00:2f:23:2a:08:47:27:e5:bf	Khanh	May 12 14:59:54 2010 GMT	May 12 14:59:54 2011 GMT
0x12:0f:7f:e0:34:67:b0:6c:09:3f	Khanh	May 12 15:19:53 2010 GMT	May 12 15:19:53 2011 GMT
0xfc:a5:2d:d3:15:58:e9:50:84:fd	Phan	May 13 02:41:38 2010 GMT	May 13 02:41:38 2011 GMT
0xce:28:59:73:04:06:bb:13:2c:ac	Khanh	May 13 03:16:20 2010 GMT	May 13 03:16:20 2011 GMT
0xca:02:2b:5a:79:51:6c:d0:21:aa	Phan	May 13 03:45:54 2010 GMT	May 13 03:45:54 2011 GMT
0x47:53:94:d0:26:a4:07:6e:34:22	Phan Trong Khanh	May 13 09:10:56 2010 GMT	May 13 09:10:56 2011 GMT

Hình 12: Danh sách chứng nhận

Nếu không nhớ số sê-ri có thể tìm trong danh sách chứng nhận hợp lệ, danh sách này cũng dùng để tìm kiếm và tra cứu thông tin về chứng nhận. Sau khi yêu cầu thu hồi chứng nhận được người quản trị CA chấp nhận, chứng nhận sẽ xuất hiện ở danh sách thu hồi chứng nhận CRL.

Kết luận

Nội dung của khóa luận trình bày những kiến thức cơ bản nhất về các biện pháp an toàn và triển khai Thuế điện tử, từ đó có thể mở rộng ra với Chính phủ điện tử.

Kết quả chính của khóa luận:

- Có được hiểu biết cơ bản về thuế và thuế điện tử, đồng thời cũng cố thêm kiến thức về chữ ký số, PKI.
- Nắm được các công nghệ an toàn xoay quanh hệ thống PKI, từ đó có thể vận dụng để xây dựng một hệ thống thuế điện tử hoàn chỉnh.
- Sử dụng và cài đặt PKI qua phần mềm mã nguồn mở OpenCA

Những ưu điểm của PKI là không thể phủ nhận, và là phần lõi không thể thiếu của hệ thống Chính phủ điện tử nói chung và Thuế điện tử nói riêng.

Từ những kiến thức thu được trong khóa luận, hướng nghiên cứu tiếp theo có thể áp dụng các biện pháp an toàn cần thiết vào OpenCA để triển khai được một hệ thống thuế điện tử thực tế. Hoặc nghiên cứu về vấn đề tích hợp các dịch vụ liên quan tới thuế vào OpenCA biến nó trở thành một cổng thông tin của ngành Thuế.

Tài liệu tham khảo

Tiếng Anh

[1] Andreas Mitrakas, “Secure E-government web services”, Idea Group Inc (IGI), 2007, pp. 1-15, 29-44.

[2] Norbert Pohlmann, Helmut Reimer, Wolfgang Schneider, “ISSE 2009 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2009 Conference”, Vieweg+Teubner Verlag, 2009, pp. 109-115.

[3] Stig F.Mjølsnes, Sjouke Mauw, Sokratis K. Katsikas, “Public Key Infrastructure: 5th European PKI Workshop: Theory and Practice, EuroPKI 2008 Trondheim, Norway, June 16-17, 2008, Proceedings”, Springer, 2008, pp. 1-110.

Tiếng Việt

[4] Báo cáo công tác cải cách hành chính - hiện đại hoá ngành thuế, hải quan năm 2009 và phương hướng công tác năm 2010, tài liệu của Bộ tài chính.

[5] Giải pháp an toàn thông tin trong môi trường điện tử, tài liệu trình bày tại Tuần lễ Tin học Hà Nội 2004 về Chứng thực điện tử & Chữ ký điện tử.

[6] Tài liệu của Tổng cục thuế - http://gdt.gov.vn