PKI VÀ THỰC TRẠNG ỨNG DỤNG TẠI VIỆT NAM

Nguyễn Hữu Việt
Trung tâm Tin học, Bộ KH&CN

Hạ tầng khóa công khai (Public Key Infrastructure - PKI) là hạ tầng kỹ thuật thông tin, cho phép người dùng trên Internet trao đổi thông tin một cách riêng tư và bảo mật thông qua việc sử dụng cặp khóa public và private của riêng họ. Với sự phát triển không giới hạn của công nghệ thông tin và nhu cầu của xã hội hiện đại, PKI đã được triển khai ở các nước phát triển từ cuối thế kỷ XX. Ở nước ta, PKI đã và đang được triển khai ứng dụng ngày càng rộng rãi. Đây là một trong những giải pháp để phát triển thành công chính phủ điện tử và đảm bảo cho các giao dịch thương mại điện tử được an toàn, thông suốt.

PKI là gì?

Hạ tầng khóa công khai (PKI) thương mại đầu tiên trên thế giới bảo đảm cho hoạt động của dịch vụ chứng thực điện tử (CTĐT) ra đời vào năm 1994 do hãng Entrust thực hiện. Tuy vậy, phải đến cuối thập niên 90 của thế kỷ XX thì công nghệ PKI mới được triển khai rộng rãi và phát triển hoàn thiện để đóng vai trò là một bên thứ ba tin cậy có thẩm quyền chứng thực cho hoạt động CTĐT của các thuê bao hay người sử dụng đầu cuối.

Hoạt động CTĐT không chỉ là cung cấp dịch vụ chữ ký số (CKS) đơn thuần, dịch vụ bảo mật thông tin điện tử (TTĐT) sử dụng kết hợp mật mã khóa công khai và khóa đối xứng mà còn cung cấp các dịch vụ khác như gắn tem thời gian, cung cấp trạng thái trực tuyến của chứng thư số (CTS). Tất cả những yêu cầu này là nhằm làm cho CKS có giá trị như chữ ký và con dấu của cấp có thẩm quyền trên văn bản giấy truyền thống. Vì vậy cần phải có một hạ tầng PKI hoạt động trực tuyến thường trực. Việc tích hợp hạ tầng PKI đã được sử dụng rộng rãi ở các nước như Mỹ, Nga, Nhật Bản, cộng đồng châu Âu, Hàn Quốc... để xác thực trong mọi giao dịch điện tử nói chung, trong thương mại điện tử nói riêng. Đảm bảo được cho khóa công khai của từng người sử dụng không bị sai lệch hay giả mạo, người ta đã dùng công nghệ CTS. Để có được các dịch vụ an toàn của CTĐT, người ta sử dụng hai chức năng an toàn nguyên thủy của CTS là lập mã, giải mã TTĐT và ký số, kiểm tra hợp lệ của CKS trên TTĐT. Dịch vụ CTĐT được ứng dụng trong hai khu vực khác nhau đối với hầu hết các quốc gia. Đó là khu vực dịch vụ công cộng cho thông tin kinh tế - xã hội và khu vực chuyên dùng cho lĩnh vực an ninh quốc phòng của mỗi quốc gia.

Tại châu Âu, 80% các nước đã cung cấp dịch vụ CKS cho người dân và doanh nghiệp, Estonia là một trong số các quốc gia đứng đầu về chính phủ điện tử (trong năm 2002 bắt đầu cấp chứng minh thư điện tử cho người dân, năm 2005 tiến hành bầu cử điện tử lần đầu tiên trên thế giới). Tại Hàn Quốc, năm 1999 Chính phủ đã ban hành Luật giao dịch điện tử. Tới năm 2002, 12,8 triệu CTS với 22,9 tỷ USD được chuyển qua internet banking sử dụng CTS. Tại Singapore, Luật giao dịch điện tử ra đời năm 1998, năm 1999 ban hành quy định về việc thành lập các nhà cung cấp tích hợp dịch vụ PKI...

Thực trạng ứng dụng tại Việt Nam

Việt Nam ứng dụng dịch vụ CTĐT muộn hơn các quốc gia khác trên thế giới. Đi tiên phong là ngành ngân hàng tài chính với các ứng dụng thử nghiệm từ đầu những năm 2000 cho đến năm 2005 khi Luật giao dịch điện tử

được thông qua. Đến năm 2007, 2008 các tổ chức chuyên trách về dịch vụ CTĐT được thành lập tại khu vực công và khu vực chuyên dùng chính phủ. Tiếp đó, Thủ tướng Chính phủ đã ban hành các văn bản chỉ đạo như Chỉ thị 897/CT-TTg ngày 10/6/2011 về đảm bảo an toàn thông tin số; Chỉ thị 15/CT-TTg ngày 22/5/2012 về tăng cường sử dụng văn bản điện tử trong hoạt động của cơ quan nhà nước. Đảng và Nhà nước đã và đang quyết tâm ứng dụng mạnh mẽ công nghệ thông tin trong hoạt động quản lý, điều hành, nhằm thúc đẩy phát triển chính phủ điện tử. Trong bối cảnh đó, Ban Cơ yếu Chính phủ được giao nhiệm vụ triển khai tích hợp hạ tầng PKI vào hạ tầng công nghệ thông tin tại các cơ quan nhà nước từ trung ương tới địa phương nhằm đảm bảo an toàn, an ninh thông tin. Năm 2012, Ban Cơ yếu Chính phủ đã cung cấp gần 4.500 CTS phục vụ cho hoạt động CTĐT của các bộ/ngành và địa phương, tăng 50% so với năm 2011. Đến đầu năm 2013 đã có 30% các bộ/ngành (22 bộ/ngành và 5 tổ chức chính trị), 17% các tỉnh, thành phố ứng dụng CKS. Đến tháng 4/2015, đã có khoảng 30.000 CTS được cấp phát cho các cơ quan Đảng và Nhà nước.

Hiện nay Cục Chứng thực số và Bảo mật thông tin (Ban Cơ yếu Chính phủ) đã triển khai tích hợp hạ tầng PKI các cho cơ quan của Nhà nước, như các Bộ: Công an, Ngoại giao, Tài chính, Nội vụ, Quốc phòng, Giao thông vận tải, Văn phòng Chính phủ... Trước tình hình trên, ngay từ năm 2010, Trung tâm Tin học (Bộ KH&CN) đã thực hiện đề tài nghiên cứu cấp bộ "Triển khai áp dụng thí điểm hệ thống chữ ký điện tử và CTĐT". Đây là nền tảng tạo tiền đề để năm 2016 Trung tâm tiếp tục thực hiện đề tài "Nghiên cứu triển khai dịch vụ tích hợp hạ tầng PKI vào hạ tầng kỹ thuật công nghệ thông tin của Bộ".

Tính đến thời điểm hiện tại, Bộ KH&CN đã hoàn thành việc tích hợp dịch vụ hạ tầng PKI do Ban Cơ yếu Chính phủ cung cấp vào hạ tầng công nghệ thông tin của Bộ, giúp đồng bộ hóa các quy trình và đảm bảo tính bảo mật cho người sử dụng. Các dịch vụ được sử dụng gồm: *i) Có thể ký số/xác thực thư điện tử:* xác thực danh tính người sử dụng thư điện tử; có thể mã hóa/giải mã văn bản thư điện tử; đảm bảo tính toàn vẹn và chính xác của các văn bản liên quan đến thủ tục hành chính; *ii) Có thể ký số/xác thực cho module văn bản quy phạm pháp luật, một số dịch vụ công:* xác thực danh tính người ký số; đảm bảo tính toàn vẹn và chính xác của các văn bản liên quan đến thủ tục hành chính; *iii) Có thể ký số/xác thực CKS cho Lãnh đạo Bộ, Lãnh đạo các đơn vị, chuyên viên cũng như văn thư;* tăng cường xác thực nguồn gốc thông tin, đảm bảo cho văn bản không bị sửa đổi; quy trách nhiệm cho cá nhân đã ký số, phát hành tài liệu.

Tóm lại, trong kỷ nguyên của công nghệ thông tin, tính phổ biến rộng rãi của Internet một mặt đem lại nhiều ứng dụng tiện lợi, thú vị và dần thay thế các hoạt động truyền thống trong thế giới thực, mặt khác nó đặt ra các vấn đề về sự an toàn, tính tin cậy của những giao dịch trên Internet. PKI có thể đáp ứng, giải quyết những vấn đề cơ bản nhất cho những yêu cầu trên. Dựa trên các dịch vụ cơ bản về chứng thực số và CKS, một PKI chính là bộ khung của các chính sách, dịch vụ và phần mềm mã hóa, đáp ứng nhu cầu bảo mật của người sử dụng. Với các đặc điểm nổi bật như không thể giả mạo, chứng thực nguồn gốc xuất xứ, các quốc gia phát triển đều đã sử dụng chứng thực số như một bằng chứng pháp lý từ rất sớm. Việc các cơ quan, tổ chức ở nước ta triển khai áp dụng PKI là yếu tố rất quan trọng để có thể phát triển thành công chính phủ điện tử và các hoạt động thương mại điện tử trong tương lai