ỨNG DỤNG CỦA PKI TRONG KÝ SỐ VÀ BẢO MẬT DỮ LIỆU

Mai Thị Hoa Huệ*

ABSTRACT

Public key infrastructure is the basic framework for building a security and privacy model in e-commerce. Learn the role of digital certificates in public key infrastructure. The role of digital certificates in online transactions. Users, in addition to the usual security such as a password, must also use a personal digital certificate to confirm their identity, confirm their transaction activities with banking, e-commerce services. testing, securities trading, etc. Digital authentication will help managers ensure that customers cannot disprove their transactions, once they have used digital certificates. Thereby posing problems (issuance, authentication) revocation and re-issuance of digital certificates.

Keywords: *Public, key infrastructure*

Ngày nhận bài: 9/5/2021; Ngày phản biện: 11/5/2021; Ngày duyệt đăng: 3/6/2021

1. Đặt vấn đề

Hạ tầng khóa công khai là bộ khung cơ bản để xây dựng mô hình an ninh, bảo mật trong thương mại điện tử. Tìm hiểu vai trò của chứng thực số trong hạ tầng khóa công khai. Vai trò của chứng thực số trong các giao dịch trực tuyến. Người sử dụng, ngoài hình thức bảo mật thông thường như mật khẩu, cũng phải dùng một chứng thực số cá nhân để khẳng định danh tính của mình, xác nhận các hoạt động giao dịch của mình với dịch vụ ngân hàng, thương mại điện thử, giao dịch chứng khoán... Chứng thực số sẽ giúp nhà quản lý đảm bảo rằng khách hàng không thể chối cãi các giao dịch của mình, khi họ đã dùng chứng thực số. Từ đó đặt ra các vấn đề (cấp phát, xác thực) thu hồi và cấp phát lại chứng thư số. Trong bài này tôi sẽ trình bày các vấn đề xoay quanh vấn đề hạ tầng khóa công khai (PKI) trong kí số và bảo mật dữ liệu.

2. Nội dung nghiên cứu

Khái niệm Mã hóa

Lợi ích đầu tiên của chứng thư số là tính bảo mật thông tin. Khi người gửi đã mã hóa thông tin bằng khóa công khai của bạn, chắc chắn chỉ có bạn mới giải mã được thông tin để đọc. Trong quá trình truyền thông tin qua Internet, dù có đọc được các gói tin đã mã hóa này, kẻ xấu cũng không thể biết được trong gói tin có thông tin gì. Đây là một tính năng rất quan trọng, giúp người sử dụng hoàn toàn tin cậy về khả năng bảo mật thông tin. Những trao đổi thông tin cần bảo mật cao, chẳng hạn giao dịch ngân hàng, ngân hàng điện tử, thanh toán thẻ tín dụng, đều phải có chứng thư số để đảm bảo an toàn.

2.2. Chống giả mạo

Khi bạn gửi đi một thông tin, có thể là một dữ liệu hoặc một email, có sử dụng chứng thư số, người nhận sẽ kiểm tra được thông tin của bạn có bị thay đổi hay không. Bất kỳ một sự sửa đổi hay thay thế nội dung của thông điệp gốc đều sẽ bị phát hiện. Địa chỉ mail của bạn, tên domain... đều có thể bị kẻ xấu làm giả để đánh lừa người nhận để lây lan virus, ăn cắp thông tin quan trọng. Tuy nhiên, chứng thư số thì không thể làm giả, nên việc trao đổi thông tin có kèm chứng thư số luôn đảm bảo an toàn.

2.3. Xác thực

Khi bạn gửi một thông tin kèm chứng thư số, người nhận – có thể là đối tác kinh doanh, tổ chức hoặc cơ quan chính quyền – sẽ xác định rõ được danh tính của bạn. Có nghĩa là dù không nhìn thấy bạn, nhưng qua hệ thống chứng thư số mà bạn và người nhận cùng sử dụng, người nhận sẽ biết chắc chắn đó là bạn chứ không phải là một người khác. Xác thực là một tính năng rất quan trọng trong việc thực hiện các giao dịch điện tử qua mạng, cũng như các thủ tục hành chính với cơ quan pháp quyền. Các hoạt động này cần phải xác minh rõ người gửi thông tin để sử dụng tư cách pháp nhân. Đây chính là nền tảng của một Chính phủ điện tử, môi trường cho phép công dân có thể giao tiếp, thực hiện các công việc hành chính với cơ quan nhà nước hoàn toàn qua mạng. Có thể nói, chứng thư số là một phần không thể thiếu, là phần cốt lõi của Chính phủ điện tử.

2.4. Chống chối bỏ nguồn gốc

Khi sử dụng một chứng thư số, bạn phải chịu trách nhiệm hoàn toàn về những thông tin mà chứng thư số đi kèm. Trong trường hợp người gửi chối cãi, phủ nhận một thông tin nào đó không phải do mình gửi (chẳng hạn một đơn đặt hàng qua mạng), chứng thư số mà người nhận có được sẽ là bằng chứng khẳng định người gửi là tác giả của thông tin đó. Trong trường hợp chối cãi, CA cung cấp chứng thư số cho hai bên sẽ

* Khoa CNTT, Trường Đại học Hạ Long

chịu trách nhiệm xác minh nguồn gốc thông tin, chứng tỏ nguồn gốc thông tin được gửi.

2.5. Chữ ký điện tử

Những thông điệp có thể gửi đi qua Internet, đến những khách hàng, đồng nghiệp, nhà cung cấp và các đối tác. Tuy nhiên, tài liệu rất dễ bị tổn thương bởi các hacker. Những thông điệp có thể bị đọc hay bị giả mạo trước khi đến người nhận.

Bằng việc sử dụng chứng thư số cá nhân, bạn sẽ ngăn ngừa được các nguy cơ này. Với chứng thư số cá nhân, bạn có thể tạo thêm một chữ ký điện tử vào tài liệu như một bằng chứng xác nhận của mình. Chữ ký điện tử cũng có các tính năng xác thực thông tin, toàn vẹn dữ liệu và chống chối cãi nguồn gốc.

2.6. Bảo mật website

Khi Website của bạn sử dụng cho mục đích thương mại điện tử hay cho những mục đích quan trọng khác, những thông tin trao đổi giữa bạn và khách hàng của bạn có thể bị lộ. Để tránh nguy cơ này, bạn có thể dùng chứng thư số để bảo mật cho Website của mình.

Chứng thư số sẽ cho phép bạn lập cấu hình Website của mình theo giao thức bảo mật SSL (Secure Sockets Layer). Loại chứng thư số này sẽ cung cấp cho Website của bạn một định danh duy nhất nhằm đảm bảo với khách hàng của bạn về tính xác thực và tính hợp pháp của Website. Chứng thư số SSL Server cũng cho phép trao đổi thông tin an toàn và bảo mật giữa Website với khách hàng, nhân viên và đối tác của bạn thông qua công nghệ SSL mà nổi bật là các tính năng: Thực hiện mua bán bằng thẻ tín dụng. Bảo vệ những thông tin cá nhân nhạy cảm của khách hàng. Đảm bảo hacker không thể dò tìm được mật khẩu.

2.7. Code Signing

Nếu bạn là một nhà sản xuất phần mềm, chắc chắn bạn sẽ cần những "con tem chống hàng giả" cho sản phẩm của mình. Đây là một công cụ không thể thiếu trong việc áp dụng hình thức sở hữu bản quyền. Chứng thư số Nhà phát triển phần mềm sẽ cho phép bạn ký vào các applet, script, Java software, ActiveX control, các file dạng EXE, CAB, DLL... Như vậy, thông qua chứng thư số, bạn sẽ đảm bảo tính hợp pháp cũng như nguồn gốc xuất xứ của sản phẩm. Hơn nữa người dùng sản phẩm có thể xác thực được bạn là nhà cung cấp, phát hiện được sự thay đổi của chương trình (do vô tình hỏng hay do virus phá, bị crack và bán lậu...).

Với những lợi ích về bảo mật và xác thực, chứng thư số hiện đã được sử dụng rộng rãi trên thế giới như một công cụ xác minh danh tính của các bên trong giao dịch thương mại điện tử. Đây là một nền tảng công nghệ mang tính tiêu chuẩn trên toàn cầu, mặc dù ở mỗi nước có một số chính sách quản lý chứng thực số khác nhau. Mỗi quốc gia đều cần có những CA bản địa để chủ động về các hoạt động chứng thực số trong nước. Nhưng ngoài ra, nếu muốn thực hiện TMĐT vượt ra ngoài biên giới, các quốc gia cũng phải tuân theo các chuẩn công nghệ chung, và thực hiện chứng thực chéo, trao đổi và công nhận các CA của nhau. Đây cũng là những yếu tố quan trọng đối với một quốc gia đang trong quá trình phát triển TMĐT như Việt Nam.

2.8. Chứng thực điện tử

Phân biệt với chữ kí số (digital signature), chứng thực điện tử (digital certification) được xem như là một chứng thư, con dấu điện tử, dùng để chứng tỏ danh tính của bạn khi tham gia một công việc kinh doanh nào đó thông qua mạng. Nó sẽ chứa tên của bạn, các thông tin cá nhân, số serial, ngày hết hạn, một bản sao của của khóa công khai (public key – sử dụng cho việc mã hóa các thông điệp và chữ kí điện tử của bạn), và chữ kí điện tử của tổ chức cung cấp để cho người nhận có thể nhận biết chứng thực này là hợp lệ.

Chứng thực điện tử cũng như giấy tờ xe, để biết được nó là hợp lệ thì phải cần một tổ chức có thẩm quyền xác nhận bằng cách đóng dấu và kí ở đằng sau nó. Tổ chức này được gọi là Certificate Authority (CA). Các tổ chức trung gian CA có trách nhiệm xem xét tất cả những văn kiện giấy tờ được yêu cầu về chứng thực điện tử, "đóng dấu" và gắn thêm chữ kí điện tử của họ lên nó cho mỗi lần xác nhận đúng, bảo đảm các chứng từ này là hợp lệ.

3. Kết luận

Với các đặc điểm nổi bật như không thể giả mạo, chứng thực nguồn gốc xuất xứ, các quốc gia phát triển đề đã sử dụng chứng thực số như một bằng chứng pháp lý từ rất sớm. Đây là yếu tố quan trọng để có thể phát triển thương mại điện tử, vì không ai dám mạo hiểm, khi họ chưa chắc chắn được rằng các hoạt động đó có được đảm bảo, và có được pháp luật công nhận hay không.

Nghiên cứu này được hỗ trợ bởi Trường Đại học Hạ Long, Quảng Ninh, Việt Nam

Tài liệu tham khảo

1. Hồ Văn Hương, Hoàng Chiến Thắng, *Ký số và xác thực trên nền tảng web*, Tạp chí An toàn thông tin, số 2 (026) năm 2013,

2. Hồ Văn Hương, Nguyễn Quốc Uy,*Giải pháp bảo mật cơ sở dữ liệu*, Tạp chí An toàn thông tin, số 3 (027) năm 2013.

3. Hồ Văn Hương, Hoàng Chiến Thắng, Nguyễn Quốc Uy, *Giải pháp bảo mật và xác thực thư điện tử*, Tạp chí An toàn thông tin số 04 (028), 2013.