HỎI - ĐÁP CÔNG NGHỆ

Sử dụng chữ ký số

Hỏi: ***Sử dụng chữ ký số là xu hướng trong các giao dịch sắp tới. Vậy chữ ký số là gì, ai có thể tạo ra nó? Điều gì đảm bảo tính an toàn của chữ ký số? Việt Nam có công nghệ tạo chữ ký số hay không?***

Đáp: Ngày 29/11/2005 Việt Nam đã có Luật Giao dịch điện tử. Ngày 15/02/2007 Chính phủ ban hành Nghị định 26/2007/NĐ-CP quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số (CKS) và dịch vụ chứng thực CKS. Theo đó, khi tiến hành giao dịch điện tử trong hoạt động công cộng, người sử dụng là cá nhân, cơ quan, tổ chức phải sử dụng CKS công cộng do tổ chức cung cấp dịch vụ chứng thực CKS công cộng cấp.

Về căn bản, CKS là thông tin đi kèm dữ liệu nhằm mục đích xác định người chủ của dữ liệu đó. CKS có thể hiểu, và được thừa nhận về mặt pháp lý, như con dấu và chữ ký điện tử của người phát hành văn bản, tài liệu trong giao dịch điện tử. CKS có thể sử dụng trong giao dịch điện tử như hải quan điện tử, giao dịch với ngân hàng, chứng khoán, kê khai thuế qua mạng, ký kết hợp đồng và gửi qua e-mail,…

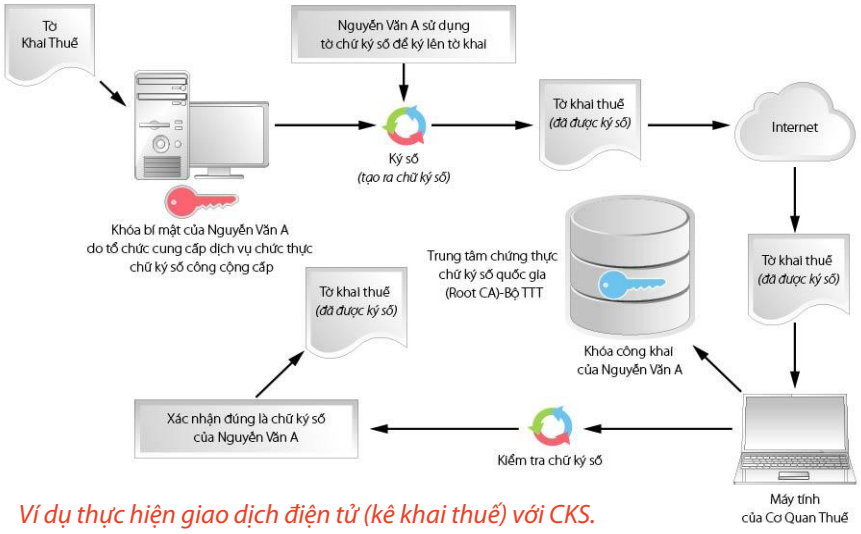
Việc sử dụng CKS bao gồm 2 quá trình:

• ***Tạo chữ ký:*** dùng các ứng dụng hỗ trợ tạo CKS từ khóa bí mật, khóa bí mật do nhà cung cấp dịch vụ chứng thực CKS công cộng cấp được lưu giữ dưới dạng tệp tin (có mật khẩu khi sử dụng), để an toàn và chống copy khóa bí mật một số nhà cung cấp dịch vụ lưu trữ khóa bí mật trong một thiết bị phần cứng chuyên dụng là USB Token hoặc SmartCard.

• ***Kiểm tra chữ ký:*** khi thực hiện giao dịch điện tử, người nhận phải kiểm tra được tính pháp lý của CKS của người giao dịch với mình gửi đến. Việc kiểm tra là so sánh tính đồng nhất của khóa công khai trên CKS của người gửi đến với khóa công khai của Nhà cung cấp dịch vụ chứng thực CKS công cộng lưu trữ trên Hệ thống máy chủ của Trung tâm Chứng thực CKS Quốc gia (thuộc Bộ Thông tin – Truyền thông).

Về mặt kỹ thuật, CKS dựa trên hạ tầng mã hóa công khai (PKI), trong đó phần quan trọng nhất là thuật toán mã hóa công khai RSA. Công nghệ này đảm bảo CKS khi được một người dùng nào đó tạo ra là duy nhất, không thể giả mạo được và chỉ có người sở hữu khóa bí mật mới có thể tạo ra được CKS đó.

USB token.



Ví dụ thực hiện giao dịch điện tử (kê khai thuế) với CKS.

Các ưu điểm của CKS:

• ***Khả năng xác định nguồn gốc:*** để sử dụng CKS, văn bản cần phải được mã hóa hàm băm (giải thuật tạo ra các khóa để phân biệt các khối dữ liệu trong lập trình hướng đối tượng, thường có độ dài cố định và ngắn hơn văn bản), sau đó dùng khóa bí mật của người chủ khóa để mã hóa, lúc này ta có CKS. Khi cần kiểm tra, bên nhận giải mã với khóa công khai 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 đó xuất phát từ người sở hữu khóa bí mật.

• ***Tính không thể phủ nhận:*** trong giao dịch điện tử, CKS gửi kèm với văn bản sẽ là chứng cứ để bên thứ ba giải quyết khi có tranh chấp.

• ***Tính toàn vẹn:*** nội dung văn bản được đảm bảo toàn vẹn, không bị sửa đổi trong quá trình truyền tin. Nếu văn bản bị thay đổi nội dung thì hàm băm cũng sẽ thay đổi và lập tức bị phát hiện. Quy trình mã hóa cũng sẽ ẩn nội dung đối với bên thứ ba.

Thấy được những lợi ích của CKS, các doanh nghiệp Việt Nam đã có nhiều bước đi để hiện thực hóa chữ ký số vào đời sống kinh tế-xã hội. Các nhà khoa học Việt Nam cũng có nhiều đầu tư nghiên cứu xây dựng các phương pháp tạo lập CKS phục vụ cộng đồng. CKS không chỉ dùng cho cá nhân một người ký, mà còn có thể đáp ứng cho nhu cầu ký tên của cả một tập thể. Điển hình là sáng chế của tập thể tác giả Nguyễn Hiếu Minh, Nguyễn Việt Trung, Lưu Hồng Dũng, Nikolay A. Moldovyal., Alexander A. Moldovyal., đã được Cục sở hữu trí tuệ cấp bằng số 1-0008702 ngày 25/10/2010 có tên ***Phương pháp hình thành và kiểm tra CKS tập thể dựa trên đường cong Elliptic để chứng thực các văn bản điện tử***. Sáng chế đề xuất phương pháp hình thành và kiểm tra CKS, bảo đảm khả năng chứng thực các văn bản trong các giao dịch điện tử, cho phép giảm nhỏ kích thước chữ ký tập thể so với chữ ký nếu thực hiện theo từng người ký riêng biệt và độc lập với nhau mà không làm giảm độ tin cậy của CKS.

Mô tả chi tiết sáng chế

Phương pháp hình thành và kiểm tra CKS tập thể dựa trên đường cong Elliptic (EC) để chứng thực các văn bản điện tử được thực hiện như sau:

1. Tạo lập CKS tập thể phía gửi:

• Hình thành các khóa công khai cá nhân $P_1, P_2,\ldots, P_n$ trên EC phù hợp theo công thức $P_i= k_iG$. Ở đây, G là điểm sinh của EC có bậc q, k_i là khóa riêng của các người ký, chúng được chọn ngẫu nhiên, i=1,2,...,n.

• Hình thành khóa công khai tập thể dưới dạng điểm P trên EC. Nó được tạo ra phụ thuộc vào khóa công khai của các người ký trong nhóm ký, theo công thức:

$$P = \sum_{j=1}^{m} w_j P_{\alpha j}$$

Với w_j là giá trị bổ sung, hình thành từ các phần của bản tóm lược h, Paj là khóa công khai của các người ký trong nhóm, j=1, 2,…, m.

• Phát sinh ngẫu nhiên chuỗi số $t_{\alpha 1}, t_{\alpha 2},...,t\alpha m$ từ tập các số tự nhiên, bởi những người ký (mỗi người phát sinh ngẫu nhiên một số).

• Phát sinh m điểm trên EC $R_{\alpha 1}, R_{\alpha 2},...,R_{\alpha m}$ theo công thức: $R_{\alpha 1}=t_{\alpha j}G$, với j=1,2,…m.

• Phát sinh điểm R trên EC theo công thức: $R=\sum_{j=1}^{m} R_{\alpha j}$

• Hình thành phần thứ nhất của chữ ký, theo công thức: $e=(x_Rh) \bmod \delta$. Ở đây, x_R là hoành độ của điểm R, δ là số nguyên tố bổ sung.

• Chọn phù hợp tập khóa riêng của các người ký $k_{\alpha 1}, k_{\alpha 2},...,k_{\alpha m}$ từ tập khóa riêng $k_1, k_2,..., k_m$, m<n. Sau đó phát sinh m dãy số nhị phân (DSNP) $s_{\alpha 1}, s_{\alpha 2},...,s_{\alpha m}$ theo công thức: $s_{\alpha j}=(t_{\alpha j}-ew_jk_{\alpha j}) \bmod q$.

• Phát sinh DSNP s theo cộng thức: $s=\sum_{j=1}^{m} s_{\alpha j} \bmod q$ là phần thứ 2 của chữ ký.

Như vậy, chữ ký số tập thể là cặp DSNP: (e, s).

2. Kiểm tra CKS tập thể, gồm các bước:

• Xác định A theo công thức: $A=x_{R'}h \bmod \delta$. Trong đó, $x_{R'}$ là hoành độ của điểm R' xác định theo công thức: R'=eP+sG;

• Xác định B bằng cách sao chép e, tức là B=e. Nếu A=B, chữ ký được chứng minh là đúng.

Phương pháp này được xây dựng với giả thiết số người tham gia ký vào văn bản chung là m ≥2.

CKS tập thể cũng sẽ rất phổ biến và quan trọng như CKS cá nhân. Trong thực tiễn, chúng ta sẽ gặp các thỏa thuận, các dự án, các công văn cần CKS của một vài đối tác. Khi các tham số phát sinh EC được chọn đủ lớn so với tốc độ tính toán ngày nay, thì các CKS đủ an toàn. Phương pháp mật mã khóa công khai xây dựng trên cơ sở EC là các phương pháp an toàn nhất hiện nay, vì chưa có phương pháp hiệu quả nào để tấn công.

Sáng chế trên giúp giải quyết được những tồn tại ở các phương pháp tạo lập CKS đã có từ trước như:

• Phương pháp tạo CKS theo sáng chế Mỹ số US 4405829 ngày 20/9/1983 có nhược điểm là để CKS được an toàn thì các số nguyên tố p, q hình thành khóa cần chọn phải có giá trị lớn để từ khóa công khai trong thực tế không thể tính ra p, q. Hơn nữa, với tốc độ tính toán ngày càng nhanh, thì giá trị p,q ngày càng phải lớn.

Tìm hiểu các công nghệ vui lòng liên hệ Ban biên tập STINFO, địa chỉ 79 Trương Định, Quận 1, TP. HCM, ĐT: 08 3829 7040 (403), email: stinfo@cesti.gov.vn

• Phương pháp tạo CKS theo sáng chế Mỹ số US 5231668, ngày 27/7/1993 (Digital Signature Algorithm - DSA) và sau đó được Viện Tiêu chuẩn và Công nghệ Quốc gia của Mỹ (National Institute of Standards and Technology - NIST) chấp thuận thành chuẩn CKS DSS (Digital Signature Standard), được mô tả trong FIPS 186, FIPS 186-1, FIPS 186-2, có nhược điểm là quá trình tính toán phức tạp cả khi ký và khi kiểm tra chữ ký. Để bảo độ an toàn tối thiểu cần chọn số nguyên tố hình thành khóa p ≥ 1024 bit.

• Phương pháp hình thành và kiểm tra CKS có bản chất gần nhất với sáng chế này là chuẩn chữ ký số của Cộng hòa Liên bang Nga GOST R 34.10-2001 nhưng nhược điểm là khi cần ký tập thể (có m người), thì chữ ký sẽ dài, xem như gấp m lần chữ ký của một người. ❑

Giới thiệu kết quả nghiên cứu KH&CN tại TP. HCM

✧ **VÂN NGUYỄN**

Xây dựng, áp dụng và đánh giá hiệu quả của chương trình quản lý sử dụng kháng sinh tại Bệnh viện Chợ Rẫy

Chủ nhiệm đề tài: **PGS. Nguyễn Văn Khôi, PGS. Lê Thị Anh Thư**

Cơ quan chủ trì: Bệnh viện Chợ Rẫy

Năm hoàn thành: 2015

Cơ quan quản lý: Sở Khoa học và Công nghệ TP. HCM

Đề kháng kháng sinh là vấn đề quan trọng hiện nay trên thế giới cũng như tại Việt Nam. Theo thống kê của Bộ Y tế trên các bệnh viện toàn quốc, nhiều loại kháng sinh gần như đã bị kháng hoàn toàn. Việc sử dụng kháng sinh không phù hợp là một trong những nguyên nhân quan trọng gây tăng đề kháng kháng sinh, tăng tỷ lệ tử vong, kéo dài thời gian nằm viện và tăng chi phí điều trị. Đề tài được thực hiện nhằm xây dựng, áp dụng và đánh giá hiệu quả của chương trình quản lý sử dụng kháng sinh tại Bệnh viện Chợ Rẫy.

Các tác giả tiến hành nghiên cứu tiền cứu, trước và sau can thiệp, đánh giá hiệu quả của chương trình quản lý sử dụng kháng sinh tại các khoa Ngoại, Nội và Hồi sức tích cực. Tổng số bệnh nhân được đưa vào nghiên cứu là 800 bệnh nhân, 400 trước và 400 sau chương trình, tuổi trung bình là 52,7 (± 20,7), tỷ lệ nam 57,5%. Không có sự khác biệt đặc điểm của bệnh nhân về tuổi, giới, bệnh kèm ở cả hai giai đoạn. Tổng cộng có 2.410 lượt sử dụng kháng sinh, 1.249 trước chương trình và 1.161 sau chương trình.

Kết quả, bước đầu đã xây dựng thành công chương trình quản lý kháng sinh với nhiều nội dung đa chiều, bao gồm: tổ chức ban giám sát sử dụng kháng sinh, kiểm tra bệnh án từng bệnh nhân, đánh giá tính hợp lý, nhắc nhở từng bác sĩ; huấn luyện, đào tạo nhân viên về hướng dẫn sử dụng kháng sinh; xây dựng phần mềm quản lý sử dụng kháng sinh. Chương trình bước đầu cho thấy hiệu quả đáng kể: sau chương trình, tỷ lệ sử dụng kháng sinh không hợp lý giảm có ý nghĩa thống kê ở tất cả các khoa (52,4% xuống còn 22,1%, p<0,001); tỷ lệ dùng đơn trị liệu kháng sinh tăng có ý nghĩa thống kê (từ 30% tăng lên 48,8%, p=0,001); giảm trung bình 3,6 ngày điều trị kháng sinh (DOT), từ 20,4 ngày xuống còn 16,8 ngày; các ngày sử dụng