WIKIPEDIA

Chữ ký số

Bách khoa toàn thư mở Wikipedia

Chữ ký số là một tập con của chữ ký điện tử[1][2][3][4]. Có thể dùng định nghĩa về *chữ ký điện tử* cho *chữ ký số*:

> Chữ ký điện tử là thông tin đi kèm theo dữ liệu (văn bản, hình ảnh, video...) nhằm mục đích xác định người chủ của dữ liệu đó[5]. Cũng có thể sử dụng định nghĩa rộng hơn, bao hàm cả mã nhận thực, hàm băm và các thiết bị bút điện tử.

Chữ ký số khóa công khai (hay *hạ tầng 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 có thể ký các văn bản điện tử cũng như trao đổi các thông tin mật. Khóa công khai thường được phân phối thông qua chứng thực khóa công khai. Quá trình sử dụng chữ ký số bao gồm 2 quá trình: tạo chữ ký và kiểm tra chữ ký.

Khái niệm *chữ ký điện tử* - mặc dù thường được sử dụng cùng nghĩa với *chữ ký số* nhưng thực sự có nghĩa rộng hơn. *Chữ ký điện tử* chỉ đến bất kỳ phương pháp nào (không nhất thiết là mật mã) để xác định người chủ của văn bản điện tử. Chữ ký điện tử bao gồm cả địa chỉ telex và chữ ký trên giấy được truyền bằng fax.

Mục lục

Lịch sử

Con người đã sử dụng các hợp đồ`ng dưới dạng điện tử từ hơn 100 năm nay với việc sử dụng mã Morse và điện tín. Vào năm 1889, tòa án tố´i cao bang New Hampshire (Hoa kỳ) đã phê chuẩn tính hiệu lực của chữ ký điện tử. Tuy nhiên, chỉ với những phát triển của khoa học kỹ thuật gâ`n đây thì chữ ký điện tử mới đi vào cuộc sô´ng một cách rộng rãi [6].

Vào thập kỷ 1980, các công ty và một sô´ cá nhân bă´t đầ`u sử dụng máy fax để truyê`n đi các tài liệu quan trọng. Mặc dù chữ ký trên các tài liệu này vẫn thể hiện trên giấ´y nhưng quá trình truyê`n và nhận chúng hoàn toàn dựa trên tín hiệu điện tử.

Hiện nay, chữ ký điện tử có thể bao hàm các cam kế´t gửi bă`ng email, nhập các sô´ định dạng cá nhân (PIN) vào các máy ATM, ký bă`ng bút điện tử với thiế´t bị màn hình cảm ứng tại các quầ`y tính tiê`n[7], chấ´p nhận các điê`u khoản người dùng (EULA) khi cài đặt phầ`n mê`m máy tính, ký các hợp đồ`ng điện tử online[8]...

Các ưu điểm của chữ ký số

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

Khả năng xác định nguồn gốc

Các hệ thố´ng mật mã hóa khóa công khai cho phép mật mã hóa văn bản với khóa bí mật mà chỉ có người chủ của khóa biế´t. Để sử dụng chữ ký sô´ thì văn bản cầ`n phải được mã hóa bă`ng hàm băm (văn bản được "băm" ra thành chuỗi, thường có độ dài cố´ định và ngắ´n hơn văn bản) sau đó dùng khóa bí mật của người chủ khóa để mã hóa, khi đó ta được chữ ký sô´. Khi cầ`n kiểm tra, bên nhận giải mã (với khóa công khai) để lấ´y lại chuỗi gố´c (được sinh ra qua hàm băm ban đầ`u) và kiểm tra với hàm băm của văn bản nhận được. Nế´u 2 giá trị (chuỗi) này khớp nhau thì bên nhận có thể tin tưởng rằ`ng văn bản xuấ´t phát từ người sở hữu khóa bí mật. Tấ´t nhiên là chúng ta không thể đảm bảo 100% là văn bản không bị giả mạo vì hệ thố´ng vẫn có thể bị phá vỡ.

Vấ´n đề` nhận thực đặc biệt quan trọng đố´i với các giao dịch tài chính. Chẳng hạn một chi nhánh ngân hàng gửi một gói tin vê` trung tâm dưới dạng *(a,b)*, trong đó *a* là sô´ tài khoản và *b* là sô´ tiề`n chuyển vào tài khoản đó. Một kẻ lừa đảo có thể gửi một sô´ tiề`n nào đó để lấ´y nội dung gói tin và truyề`n lại gói tin thu được nhiề`u lầ`n để thu lợi (tấ´n công truyề`n lại gói tin).

Tính toàn vẹn

Cả hai bên tham gia vào quá trình thông tin đề`u có thể tin tưởng là văn bản không bị sửa đổi trong khi truyề`n vì nế´u văn bản bị thay đổi thì hàm băm cũng sẽ thay đổi và lập tức bị phát hiện. Quá trình mã hóa sẽ ẩn nội dung của gói tin đố´i với bên thứ 3 nhưng không ngăn cản được việc thay đổi nội dung của nó. Một ví dụ cho trường hợp này là tấ´n công đồ`ng hình (homomorphism attack): tiế´p tục ví dụ như ở trên, một kẻ lừa đảo gửi 1.000.000 đồ`ng vào tài khoản của a, chặn gói tin *(a,b)* mà chi nhánh gửi về` trung tâm rồ`i gửi gói tin (a,b^3) thay thế´ để lập tức trở thành triệu phú!Nhưng đó là vấ´n đề` bảo mật của chi nhánh đố´i với trung tâm ngân hàng không hẳn liên quan đế´n tính toàn vẹn của thông tin gửi từ người gửi tới chi nhánh, bởi thông tin đã được băm và mã hóa để gửi đế´n đúng đích của nó tức chi nhánh, vấ´n đề` còn lại vấ´n đề` bảo mật của chi nhánh tới trung tâm của nó

Tính không thể phủ nhận

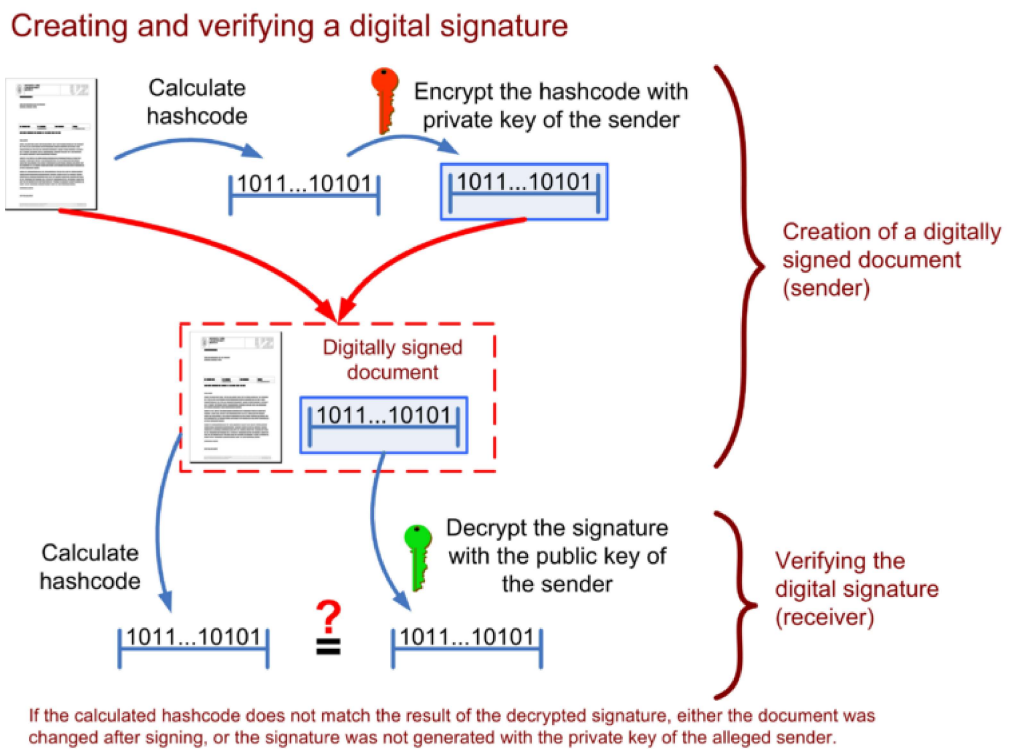
Trong giao dịch, một bên có thể từ chối nhận một văn bản nào đó là do mình gửi. Để ngăn ngừa khả năng này, bên nhận có thể yêu cầu bên gửi phải gửi kèm chữ ký số với văn bản. Khi có tranh chấp, bên nhận sẽ dùng chữ ký này như một chứng cứ để bên thứ ba giải quyết. Tuy nhiên, khóa bí mật vẫn có thể bị lộ và tính không thể phủ nhận cũng không thể đạt được 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 có một cặp khóa: một công khai và một bí mật. Khóa công khai được công bố rộng rãi còn khóa bí mật phải được giữ kín và không thể tìm được khóa bí mật nếu chỉ biết khóa công khai.

Toàn bộ quá trình gồm 3 thuật toán:

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



Sơ đồ tạo và kiểm 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 kiểm tra sự thống nhất giữa bản tin và chữ ký bằng thuật toán kiểm tra sử dụng khóa công cộng của Bob. 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 phép thử 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 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 mặc dù xác suất rất thấp.

Một vài thuật toán chữ ký số

- Full Domain Hash, RSA-PSS..., dựa trên RSA
- DSA
- ECDSA
- ElGamal signature scheme
- Undeniable signature
- SHA (thông thường là SHA-1) với RSA

Tình trạng hiện tại - luật pháp và thực tế

Tất cả các mô hình chữ ký số cần phải đạt được một số yêu cầu để có thể được chấp nhận trong thực tế:

- Chất lượng của thuật toán: một số thuật toán không đảm bảo an toàn;
- Chất lượng của phần mềm/phần cứng thực hiện thuật toán;
- Khóa bí mật phải được giữ an toàn;
- Quá trình phân phối khóa công cộng phải đảm bảo mối liên hệ giữa khóa và thực thể sở hữu khóa là chính xác. Việc này thường được thực hiện bởi hạ tầng khóa công cộng (PKI) và mối liên hệ khóa↔người sở hữu được chứng thực bởi những người điều hành PKI. Đối với hệ thống PKI *mở*, nơi mà tất cả mọi người đều có thể yêu cầu sự chứng thực trên thì khả năng sai sót là rất thấp. Tuy nhiên các PKI thương mại cũng đã gặp phải nhiều vấn đề có thể dẫn đến những văn bản bị ký sai.
- Những người sử dụng (và phần mềm) phải thực hiện các quá trình đúng thủ tục (giao thức).

Chỉ khi tất cả các điều kiện trên được thỏa mãn thì chữ ký số mới là bằng chứng xác định người chủ (hoặc người có thẩm quyền) của văn bản.

Một số cơ quan lập pháp, dưới sự tác động của các doanh nghiệp hy vọng thu lợi từ PKI hoặc với mong muốn là người đi tiên phong trong lĩnh vực mới, đã ban hành các điều luật cho phép, xác nhận hay khuyến khích việc sử dụng chữ ký số. Nơi đầu tiên thực hiện việc này là bang Utah (Hoa kỳ). Tiếp theo sau là các bang Massachusetts và California. Các nước khác cũng thông qua những đạo luật và quy định và cả Liên hợp quốc cũng có những dự án đưa ra những bộ luật mẫu trong vấn đề này. Tuy nhiên, các quy định này lại thay đổi theo từng nước tùy theo điều kiện về trình độ khoa học (mật mã học). Chính sự khác nhau này làm bối rối những người sử dụng tiềm năng, gây khó khăn cho việc kết nối giữa các quốc gia và do đó làm chậm lại tiến trình phổ biến chữ ký số.

> *Xem thêm*: Các nguyên tắc chữ ký số ABA

Khía cạnh pháp luật

Một số quy định liên quan tới giá trị pháp lý của chữ ký số:

Trung quốc

- Luật chữ ký điện tử của Trung quốc (tiếng Trung quốc) (http://www.cin.gov.cn/law/other/2005040803.htm) - Mục tiêu hướng tới thống nhất việc thực hiện, khẳng định tính pháp lý và bảo vệ quyền lợi hợp pháp của các bên liên quan tới việc thực hiện chữ ký điện tử.

Brazil

- Medida provisória 2.200-2 (tiếng Bồ Đào Nha) (http://www.presidencia.gov.br/CCIVIL_03/MPV/Antigas_2001/2200-2.htm) - Luật Brazil thừa nhận tính pháp lý của văn bản số nếu được chứng nhận bởi **ICP-Brasil** (PKI chính thức của Brazil) hoặc một PKI khác nếu các bên đồng ý.

Liên hiệp châu Âu

- EU đã thiết lập khung pháp lý cho chữ ký điện tử:
  - Hướng dẫn số 1999/93/EC của Quốc hội châu Âul (http://eur-lex.europa.eu/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf) ngày 13 tháng 12 năm 1999 về khung pháp lý của chữ ký điện tử.
  - Quyết định 2003/511/EC (http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf) sử dụng 3 thỏa thuận tại hội thảo CEN làm tiêu chuẩn kỹ thuật.
- Các luật ban hành: Một số quốc gia đã thực hiện quyết định 1999/93/EC.

- Áo
  - Luật chữ ký, 2000 (http://www.a-sit.at/signatur/rechtsrahmen/SigG_incl_Novelle2000.pdf)
- Anh, Scotland và Wales
  - Luật thông tin điện tử, 2000 (http://www.legislation.hmso.gov.uk/acts/acts2000/20000007.htm#7)
- Đức
  - Luật chữ ký, 2001 (http://www.bsi.de/esig/basics/legalbas/sigg2001.pdf)
- Lithuania
  - Luật chữ ký điện tử, 2002 (http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=204802)
- Nauy
  - Luật chữ ký điện tử, 2001 (http://www.lovdata.no/all/hl-20010615-081.html) (tiếng Nauy).
- Tây Ban Nha
  - Ley 59/2003, de 19 de diciembre, de firma electrónica (tiếng Tây Ban Nha) (http://www.google.com/url?sa=t&ct=res&cd=1&url=http%3A//www.aeat.es/descarga/ley59_2003.pdf).
- Thụy Điển
  - Qualified Electronic Signatures Act (SFS 2000:832) (tiếng Thụy Điển) (http://rixlex.riksdagen.se/htbin/thw?%24%7BOOHTML%7D=SFST_DOK&%24%7BSNHTML%7D=SFSR_ERR&%24%7BBASE%7D=SFST&BET=2000%3A832&%24%7BTRIPSHOW%7D=format%3DTHW).
  - SFS 2000:832 bản dịch tiếng Anh (http://www.pts.se/Archive/Documents/SE/engelsk%20oversattning%20av%20lag%20elektroniska%20signaturer.pdf)

Ấn Độ

- Luật Công nghệ thông tin, 2000 (http://www.mit.gov.in/it-bill.asp)

New Zealand

- Luật Giao dịch điện tử, 2003 điều 22-24 (http://www.legislation.govt.nz/)

Luật thương mại quốc tế của Ủy ban Liên hiệp quốc

- UNCITRAL Luật mẫu về chữ ký điện tử (2001), bộ luật có ảnh hưởng lớn. (http://www.uncitral.org/english/texts/electcom/ecommerceindex.htm)

Hoa kỳ

- Uniform Electronic Transactions Act (UETA)
- Electronic Signatures in Global and National Commerce Act (E-SIGN), at 15 U.S.C. 7001 (http://www4.law.cornell.edu/uscode/15/7001.html) et seq.

Thụy Sĩ

- Luật liên bang về dịch vụ chứng thực liên quan tới chữ ký điện tử, 2003 (http://www.admin.ch/ch/f/rs/c943_03.html)

Uruguay

Luật pháp Uruguay bao gồm cả chữ ký điện tử và chữ ký số:

- Liên quan tới mật khẩu và các hành động tương đương trong công nghệ thông tin (http://www.parlamento.gub.uy/Leyes/Ley16736.htm#art695)
- Liên quan tới chữ ký số, chữ ký điện tử và PKI (http://www.parlamento.gub.uy/Leyes/Ley17243.htm#art25)

Việt Nam

- Luật Giao dịch điện tử[9][10] - có hiệu lực từ ngày 1 tháng 3 năm 2006.

[11]

Tham khảo

1. ^ University of Virginia (http://www.itc.virginia.edu/virginia.edu/fall00/digsigs/home.html)
2. ^ State of WI (http://enterprise.state.wi.us/home/strategic/esig.htm)
3. ^ National Archives of Australia (http://www.naa.gov.au/recordkeeping/er/Security/6-glossary.html)
4. ^ CIO (http://www.cio.com/archive/101500/et.html)
5. ^ US ESIGN Act of 2000 (http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf)
6. ^ Electronic Signatures - Understanding the Origins, Laws and Affects (https://privasign.com/whitepaper-esign.asp)
7. ^ Digital pen pad solutions (http://www.integrisign.com/products/index.html)
8. ^ Online electronic signatures (https://privasign.com)
9. ^ Hệ thống văn bản quy phạm pháp luật của chính phủ (http://qppl.egov.gov.vn/congbao.nsf/9e6a1e4b64680bd247256801000a8614/85256f620062656c852570ee007187b8?OpenDocument)
10. ^ Cổng thông tin điện tử chính phủ (http://tintuc.egov.gov.vn/tintuc.nsf/0/751DCC029906CEC44725716B0038ABA2?OpenDocument&fullmode)
11. ^ Trung tâm Chứng thực kỹ thuật số - Bộ KH-CN (http://www.most.gov.vn/chukydientu/default.asp)

Xem thêm

- Chữ ký điện tử
- Hạ tầng khóa công khai
- RSA (mã hóa)

Liên kết ngoài

- An introduction to Digital Signatures (http://www.youdzone.com/signature.html)

Mật mã hóa khóa công khai

Thuật toán: Cramer-Shoup | DH | DSA | ECDH | ECDSA | EKE | ElGamal | GMR | MQV | NTRUEncrypt | NTRUSign | Paillier | Rabin | Rabin-Williams | RSA | Schnorr | SPEKE | SRP | XTR

Lý thuyết: Logarithm rời rạc | Mật mã đường cong elíp | Bài toán RSA

Tiêu chuẩn: ANS X9F1 | CRYPTREC | IEEE P1363 | NESSIE | NSA Suite B **Vấn đề khác:** Chữ ký điện tử | PKI | Mạng lưới tín nhiệm | Độ lớn khóa