PKI - חתימה דיגיטלית-אישור דיגיטלי

כותב המאמר: אדוארדו פרכטנברג , מידען ועדת ענ"א.

הקדמה – תפקיד המידען

בתפקידו מלווה המידען את הפעילות השוטפת של הצוותים המקצועיים במטרה לספק מידע הן כללי והן פרטני (על פי דרישה מקצועית) למען חשיפה יעילה ואמינה של אנשי הצוות למידע רלוונטי ועדכני. אופי הדינמי והקונסטרוקטיבי של התקדמות הפרוייקט בידי הצוות המקצועי מחייב דו-שיח ואינטראקציה בין משתמשי המידע לבין מפיקיה.

ראו את עצמכם רשאים להעביר את הערותיכם והארותיכם בנושא באופן פרטי ובמידענות באופן כללי .

תודה

אדוארדו פרכטנברג

טלפון: 02-5317674 mailto:eduardo@mof.gov.il

How It Works

Assume you were going to send the draft of a will to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

1. You copy-and-paste the will (it's a short one!) into an e-mail note.
2. Using special software, you obtain a message hash (mathematical summary) of the will.
3. You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.
4. The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.)

At the other end, your lawyer receives the message.

1. To make sure it's intact and from you, your lawyer makes a hash of the received message.
2. Your lawyer then uses your public key to decrypt the message hash or summary.
3. If the hashes match, the received message is valid.

Selected Links

- Ronald Rivest's extensive list of links to Cryptography and Security sites is comprehensive.
- http://www.lycos.com/srch/?lpv=1&loc=searchhp&query=digital%20signatue

Sites relating to the overall issues DS/ES related: legislation, products, applications, CA, basic definitions and advanced features, electronic approval. (More than 155.000 sites referred).

- The World Wide Web Consortium (W3C) describes its own Digital Signature Initiative.

- IBM's Cryptography - Quick Overview is a Lotus Freelance presentation that discusses both digital certificates and digital signatures.

---

digital certificate

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticated users can look up other users' public keys.

Selected Links

- IBM's Security Technologies site describes the X.509 certificate and the Public Key Infrastructure.

- VeriSign is the leading certificate authority, providing over 125,000 Web sites with SSL server certificates, mainly for use in e-commerce.

Assistance was provided by Eric Morley.
Last update: October 12, 1999

http://www.youdzone.com/signature.html
מה זה חתימה דיגיטלית.
http://www.state.in.us/digitalsignatures/dsfaq.html
FAQ
http://www.entrust.com/entrust/whatsnew.htm
.מאפיינים,PKI product

http://www.lycos.com/srch/?lpv=1&loc=searchhp&query=digital%20signature

Sites relating to the overall issues DS/ES related: legislation, products, applications, CA, basic definitions and advanced features, electronic approval. (More than 155.000 sites referred).
http://www2.arnes.si/~rzjtopl/usa/elsig.htm

Adjusting technological and legal solutions in electronic commerce.
http://www.zdnet.com/pcmag/stories/reviews/0,6755,394205,00.html
Certificates, Keys and Security. Content:
Solutions for Electronic Signature/Introduction/Certificate Authorities/Digital Certificates/Secure Web Services/Securing E-mail/Clients/ Software Publishing/not just Microsoft/ "Now it's legal to sign electronic documents electronically, but should you?"

Are digital signatures a threat?
Do we need to worry about government tracing and identity theft? A leading technology expert has warned that digital signatures, an increasingly prevalent Internet security technology, could hail a future devoid of privacy.
http://www.msnbc.com/modules/exports/ct_infobeat.asp?/news/467900.asp

http://alpha.qmw.ac.uk/~tl6345/
Review on links related to digital signature issues. Content:

1) Understanding the Technology (Criptography/ Biometrics/Infrastructure)
2) Trusted Third Parties and Certification Authorities(International and Nationals Initiatives)
3) Surveys on Electronic Commerce Law.