

Explore the TechTarget Network at [SearchTechTarget.com](#).

[Activate your FREE membership today](#) | [Log-In](#)



Search this site and the Web

Powered by Google

[HOME](#) [NEWS](#) [TOPICS](#) [ITKNOWLEDGE EXCHANGE](#) [TIPS](#) [ASK THE EXPERTS](#) [WEBCASTS](#) [WHITE PAPERS](#) [PRODUCTS](#) [CAREERS](#) [SITE MAP](#)

ADVERTISEMENT

ADVERTISEMENT

[whatis.com](#) searchSecurity.com Definitions - digital signature

[EMAIL THIS PAGE TO A FRIEND](#)

searchSecurity.com Definitions - powered by whatis.com

BROWSE WHATIS.COM DEFINITIONS: [A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#) <#> [BROWSE ALL CATEGORIES](#)

Search [whatis.com](#) for: - OR - Search this site:

digital signature

powered by whatis.com

The term you selected is being presented by searchSecurity.com, a TechTarget site for Security professionals.

SITE SPONSOR

A digital signature (not to be confused with a [digital certificate](#)) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent

is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

How It Works

Assume you were going to send the draft of a contract 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 contract (it's a short one!) into an e-mail note.
2. Using special software, you obtain a message hash (mathematical summary) of the contract.
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

EXPLORE THIS AREA: RICH-MEDIA ADVERTISEMENT

WHAT'S NEW

on searchSecurity

1. [McAfee Security Center](#)
2. [Simplify the challenge of securing email](#)
3. [Security School - Free CISSP Training](#)
4. [IT Knowledge Exchange](#)

Information Security Magazine [Information Security Magazine](#)

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.

Also see [hashing](#) and [Digital Signature Standard](#).

>> [Find products and vendors related to digital signature.](#)

Read more about it:

- >> [SearchCIO.com offers information about the use of digital signatures in Internet commerce.](#)
- >> [The American Bar Association provides guidelines for the use of digital signatures.](#)
- >> [The World Wide Web Consortium \(W3C\) describes its own Digital Signature Initiative.](#)
- >> [SearchSecurity.com provides links to more information about digital signatures.](#)
- >> [SearchCRM.com has information about the use of digital signatures in customer relationship management.](#)

RELEVANT SPONSORED LINKS

[Digital Signature](#)

Easy to use digital signature software or signature service.

www.alphatrust.com

[Digitally Sign and Seal](#)

Easily e-sign with any application
Expedite processes & increase ROI

www.arx.com

[Digital Signature](#)

Encryption, Signatures & Privacy
Download our white papers now!

www.rsasecurity.com

[Electronic Signature Tech](#)

Electronic signature pads and free software tools, plug-ins, and demos

www.topazsystems.com

[Electronic Signatures](#)

Lenders go paperless now with eSigning & eVaulting Software

www.eOriginal.com

Last updated on: Apr 16, 2001

<< [Back to previous page](#) [Go to whatis.com home page](#) >>



[View this month's issue and subscribe today.](#)



[Apply online for free conference admission.](#)



- HOME
- NEWS
- TOPICS
- ITKNOWLEDGE EXCHANGE
- TIPS
- ASK THE EXPERTS
- WEBCASTS
- WHITE PAPERS
- PRODUCTS
- CAREERS
- SITE MAP

[About Us](#) | [Contact Us](#) | [For Advertisers](#) | [For Business Partners](#) | [Reprints](#)

SEARCH

SearchSecurity.com is part of the TechTarget network of industry-specific IT Web sites

WINDOWS

- [SearchExchange.com](#)
- [SearchVB.com](#)
- [SearchWin2000.com](#)
- [SearchWindowsSecurity.com](#)
- [Labmice.net](#)
- [MyITForum.com](#)

APPLICATIONS

- [SearchCRM.com](#)
- [SearchSAP.com](#)

ENTERPRISE IT MANAGEMENT

- [SearchCIO.com](#)
- [SearchSmallBizIT.com](#)

CORE TECHNOLOGIES

- [SearchDatabase.com](#)
- [SearchEnterpriseVoice.com](#)
- [SearchMobileComputing.com](#)
- [SearchNetworking.com](#)
- [SearchOracle.com](#)
- [SearchSecurity.com](#)
- [SearchStorage.com](#)
- [SearchWebServices.com](#)
- [WhatsIs.com](#)

PLATFORMS

- [Search390.com](#)
- [Search400.com](#)
- [SearchDomino.com](#)
- [SearchEnterpriseLinux.com](#)



[TechTarget Expert Answer Center](#) | [TechTarget Enterprise IT Conferences](#) | [TechTarget Corporate Web Site](#) | [Media Kit](#)

Explore [SearchTechTarget.com](#), the guide to the TechTarget network of industry-specific IT Web sites.

All Rights Reserved, Copyright 2000 - 2004, TechTarget

[Read our Privacy Statement](#)