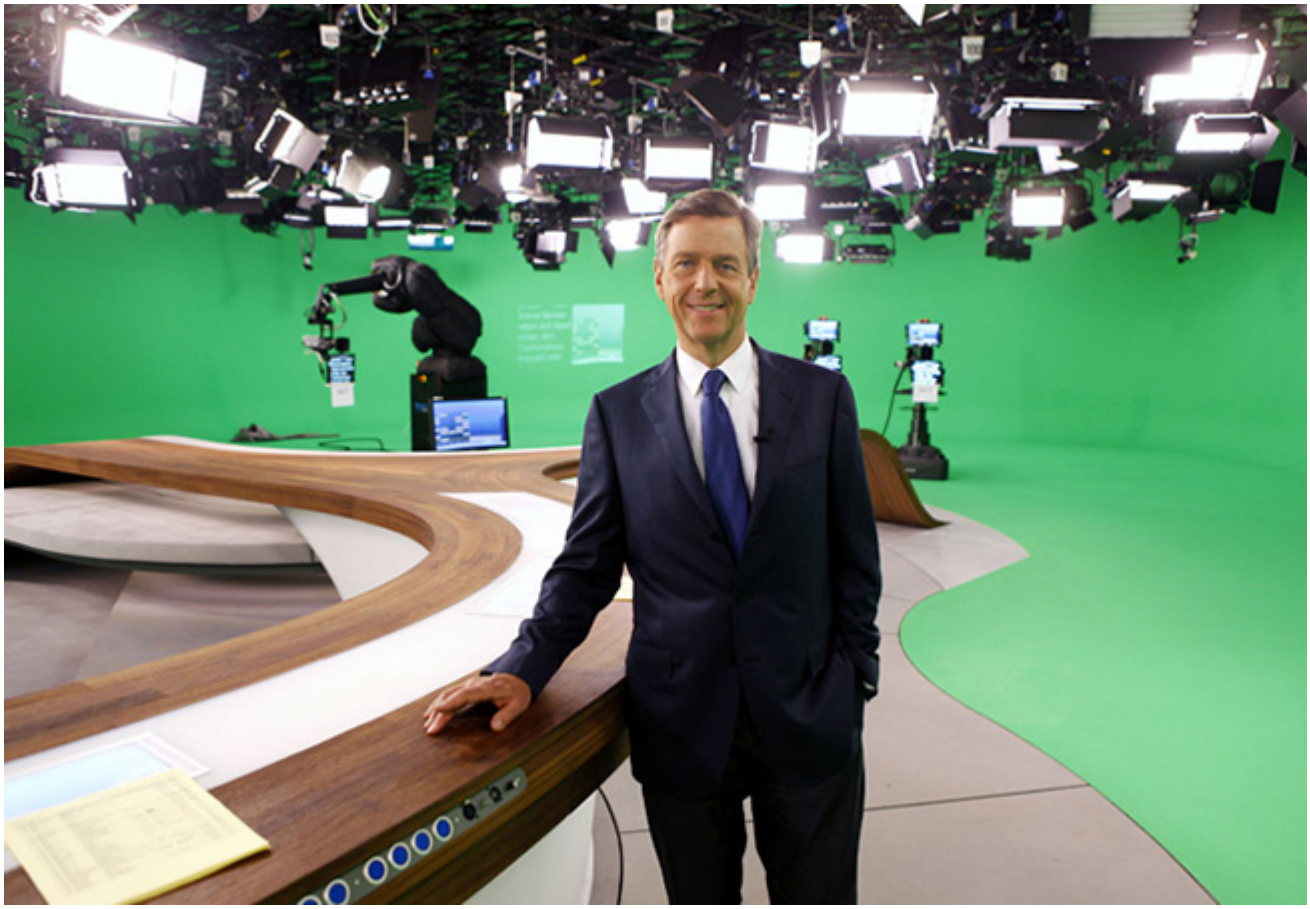
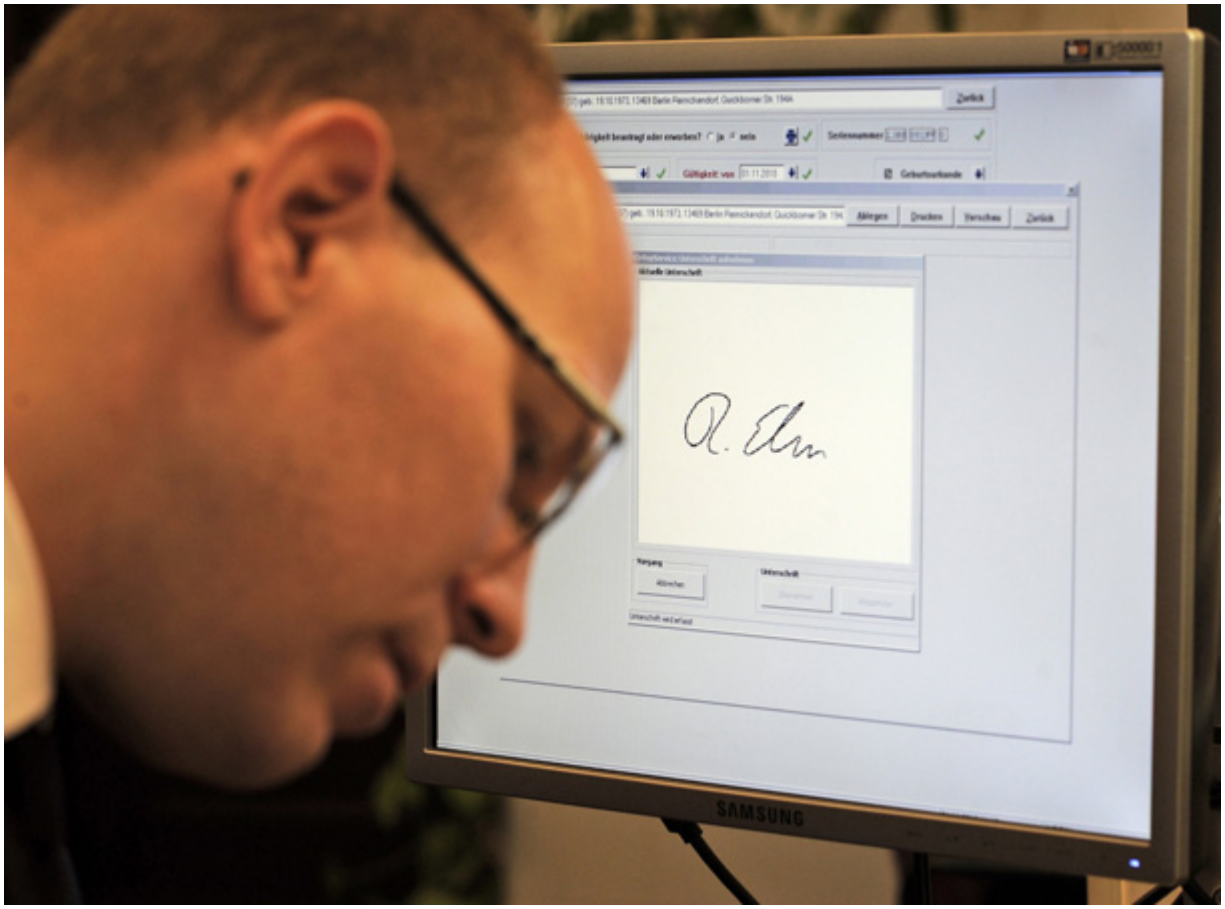
Digital Signatures

Computer Sciences. 2nd ed. 2013.

Full Text:





A digital signature is an identifier that can be used to authenticate the sender of an electronic message (e-mail) or the signer of an electronic document. This technology can also be used to ensure the integrity of the message or document (that no alterations have been made since it was signed) as well as to date/time-stamp the document at signing. Finally, the signatory cannot easily repudiate or refuse to acknowledge his digital signature, nor can the document be easily forged.

Due to these criteria, a digital signature can be trusted and used like a written signature. On October 1, 2000, the Electronic Signatures in Global and National Commerce Act (known as the E-Signature Act) became effective in the United States. This act basically states that a signature cannot be denied simply because it is electronic, and an electronic signature must be considered as legally valid as a written signature. Not all electronic signatures, however, are digital signatures, so it is worth noting the following electronic signature examples that are *not* digital signatures:

a biometric identifier;
a written signature on a document that has been scanned into an electronic file; or
a signature on a document that has been faxed (transmitted by facsimile).

So what *is* a digital signature? A digital signature uses cryptographic cryptographic technology to create an electronic identifier, but it can be used with any message, whether the message is encrypted encrypted or not. Thus, digital signatures can accompany an unencrypted or an encrypted message. For example, the Computer Emergency Response Team (CERT) broadcasts messages of computer vulnerabilities in clear text (unencrypted) to everyone on its mailing list. To allow its recipients to verify that these messages come from the CERT and are not spoofed (counterfeited into looking like messages from CERT) or modified in transit, the CERT signs all of its messages with its digital signature. Yet a government employee protecting classified information or a company employee protecting trade secrets would not only digitally sign his document but would encrypt the base message as well.

Many different software packages can be used to create a digital signature, from freeware to PC-based, shrink-wrapped software to large server-based systems, also known as public key infrastructures (PKIs). The process for sending a digitally signed unencrypted message is the same regardless of the package used as follows. A user creates a digital signature with a private key that he keeps to himself. He then attaches this signature to a document and sends it to others. His private key is mathematically linked to a public key that he posts on a public key server. He then tells the recipient(s) where his public key is stored. The recipient can then retrieve the sender's public key and reverse the process to determine the authenticity of the document.

The process for sending a digitally signed encrypted message is similar. In this case, the sender must retrieve the recipient's public key from a public key server. She then uses it to encrypt the message and send it to the recipient. The recipient then uses her own private key to decrypt the document, and the sender can be sure that only the recipient can read it.

Although there are many advantages to using digital signatures, several problems also exist:

> Anyone can create a public/private key pair and contact the recipient, claiming to be the sender. Without knowing the sender by voice or another method, there is no way to guarantee that the owner of the key is indeed the person sending the document.
> If someone other than the owner of the computer has had physical or logical access to the computer that houses the encryption software, malicious code could be inserted into this software to enable other actions, such as collecting the owner's private key and mailing it to the author of the code.
> A computer may legitimately have a person's digital signature resident on it, but if that computer is stolen or used by another and the private key guessed, then a document created on that computer may not have been "signed" by the digital signature's owner.

In other words, the integrity of a digital signature can be compromised if someone gains improper access to the computer that runs the encryption software.

Regardless of the problems, digital signatures have great potential. However, for electronic business to reach its full potential, the end user must feel secure in signing or receiving a document electronically. Digital signature technology has the potential to create that level of trust.

What is a Digital Signature?

A digital signature can be trusted and used like a written signature. Not all electronic signatures, however, are digital signatures.

Federal Government Saves Paper and Lowers Costs with Digital Signature

According to the U.S. Government Printing Office (GPO), in 2008 the Federal government's Budget for fiscal year 2009 was transmitted electronically. According to GPO head Robert C. Tapella, the GPO provided "authentication for the Budget via digital signature. This authentication verifies to anyone who downloads the Budget that the content has not been changed or altered. GPO's authentication capability ushers in a new era for Federal publications in terms of digital capability. Along with ongoing programs for the use of recycled paper and vegetable-based ink, digital also helps promote environmental sustainability in the Government's publishing and information dissemination activities." People can still obtain printed versions of each year's Federal Budget, but they must pay a fee to do so.

Words to Know

cryptographic
of the science of understanding codes and ciphers and their application

encrypted
coded, usually for purposes of security or privacy

public key infrastructures (PKIs)
the supporting programs and protocols that act together to enable public key encryption/decryption

Books

Katz, Jonathan. *Digital Signatures*. 2nd ed. New York: Spring Publishing, 2010.

Web Sites

US-Cert. "Understanding Digital Signatures." http://www.us-cert.gov/cas/tips/ST04-018.html (accessed September 24, 2012).

Source Citation (MLA 8th Edition)
Smith, Cindy. "Digital Signatures." *Computer Sciences*, edited by K. Lee Lerner and Brenda Wilmoth Lerner, 2nd ed., Macmillan Reference USA, 2013. *Science In Context*, http://link.galegroup.com/apps/doc/CV2642250214/SCIC?u=txshracd2598&sid=SCIC&xid=741bf12c. Accessed 30 Apr. 2018.

Gale Document Number: GALE|CV2642250214