



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

e-Signatures: A signature that can be trusted?

Written by: Brent Gifford

October 1, 2000

I. Introduction

In June 2000, President Clinton signed into law the Electronic Signatures in Global and National Commerce Act. The new law, which will go into effect on October 1, 2000, “clears the way for people to use digital signatures to sign online contracts, agree to software licenses, and secure business-to-business transactions.”¹ “The new Electronic Signatures Act, passed in June, was crafted to be technology-neutral. Our lawmakers know that a technology-specific law can become outdated quickly. But by refusing to place limits on e-signature technology for future considerations, they’ve allowed for the use of any current technology that fits the law.”²

“The law’s biggest impact primarily will be one of perception. Federal approval should make people and business more comfortable with the concept of accepting e-signatures – but it doesn’t mean they’ll take off right away.”³

“Although digital signatures may appear to solve many consumer worries, Brands believes that they raise equally pressing questions over liberties”²

II. The desired outcome

“When the federal e-signature law goes into effect Sunday, proponents are hoping it will usher in a new era of clickable contracts, people sailing through airports without lines, and establishing brokerage accounts with the push of a button.”³ “The law basically states that a signature cannot be turned down simply because it takes electronic form. Thus, a click of a mouse, a press of a telephone touch pad button, or a swipe of a smart card are as binding as your John Hancock on paper.”³

Just about every industry that relies on a face-to-face human interaction to transact business is anxiously working towards simplifying and making the process more efficient. If a person does not have to be physically present to participate in a transaction, but can legally effect the transaction remotely by a digital signature, the new process would dramatically simplify and make more efficient any given transaction. “Soothing consumer fears, Digital signatures provide an Internet user with a unique identity document protected by encryption keys which serve to assure a third party that a document, a message, or a transaction comes from who is says it does. The technology may help to soothe consumer fears about the dangers posed by computer hackers and the risks of using credit cards online or sending messages securely.”²

“However, down the road McNeese sees e-signatures being used for everything from signing an insurance form to updating medical records.

His company also is in talks with major airlines to develop a single electronic mechanism that would let people pay for a ticket, prove their identity, check luggage, and log frequent flyer mileage at the airport without rifling through their wallet multiple times.

Right now, I might produce five pieces of plastic from the moment I get out of the limo to when I get on the plane, McNees said.

The company also expects the technology to smooth the road for industries that have had trouble selling their goods online. Take, for example, the wine industry. Right now, most states don't allow wine sales because the companies can't prove their customer is over 21. However, a secure digital technology that would confirm a buyer's age could overcome the problem.

The financial sector has taken the lead on the e-signature front, followed by the insurance industry. It's also expected to take hold in the government and medical sectors as well as industries where sales of big-ticket items and parts have traditionally required a pen-and-paper signature.

Thomas J. Smedinghoff, an attorney with Baker and McKenzie in Chicago, said he has several traditional brick-and-mortar clients from the auto and manufacturing sectors looking to take advantage of e-sigs.³

The new law will speed contract execution, allowing for signatures in cyberspace at cyberspeed. "One private bank, National City Bank, uses digital signature software to sign up new banking customers. The bank claims e-signatures cut transaction processing time in half and increased its customer base by 1,200 percent."⁴

As a gesture of acceptance and encouragement to comply with the law, the United States Federal Government has imposed a deadline of 2003 for making its services available online to contractors and business.

III. The potential problems

A. Usability

"A bigger problem, said McGraw, is that the technology is still not easy to use.

There has been a lot of money pumped into cryptography, but the problem is that there has not been enough effort to hide the technology away from the user, he said.

With such usability and security problems unresolved, digital signatures may have a long road ahead to acceptance, even with the go-ahead from the U.S. government."¹

B. Lack of standards

“The Commonwealth of Massachusetts' definition of a signature is perhaps the most general: any mark on paper made with an instrument that the person creating the mark claims is his or hers. To call this an open definition is an understatement, and the interpretation of e-signatures seems to be headed in the same direction. What will likely pass as an e-signature is any set of bits that some vendor can demonstrate to be uniquely tied to a person.”⁵

“Implementation problems and legal challenges will limit the law's impact on e-commerce for at least five years, said analyst Prince in a report.”⁶

C. Government tracking

“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.

Speaking at the International Forum on Surveillance by Design in London, senior cryptographer Dr. Stefan Brands, with specialists in anonymous Internet technology Zero Knowledge Systems Inc., warned that digital signatures might lead to widespread government tracing and identity theft.

Brands warned that digital signatures could lead to a future where the online movements of citizens can be traced by governments.

These identity signatures are a very dangerous trend, said Brands. Everything you do can be traced automatically. In the near future identity certificates may be built into anything that contains a computer such as phones and watches.”²

D. Identity theft

“Before electronic signatures can offer full security, they must overcome several technological hurdles, warn experts.

They caution that once you add unproven servers, a variety of software and the quirks of individual users into the equation, any assumptions about the bedrock security of the system are open to question.

Once you sign with a digital signature, (that signature is) going to be equated with you, said Adam Shostack, director of technology for privacy-enhanced software maker Zero-Knowledge Systems Inc. Unfortunately, the computing base is not that secure. Someone could get access to the keys on your machine and sign documents in your name.

Another issue is the need for third-party authentication, which is essential for most biometric technologies. Your biometric template must be stored on a server out of your control. If that server is compromised, your template may be compromised, too.”¹

“But not everyone is cheering the law. Some consumers groups have complained that e-signatures will open the door to fraud and identity theft and allow companies to change digital contracts at will. Such concerns are likely to keep lawyers busy for years to come, as e-signatures become more popular.

Fraud is nothing new, Smedinghoff said. We've had fraud in the paper world, and we'll have fraud in the electronic world.”³

E. Retention

“One pressing concern is document retention. A piece of paper or microfilm can be filed for years, and the courts have accepted the authenticity of such stored documents. But how will we establish adequate evidential trails for electronic documents?

We need two facts to establish the evidential trail of a document: The first is validity of the signature; the second is the time of the signature. The validity of ink signatures is established through notaries and expert analysis; the validity of electronic signatures is established through mathematical and computational principles. It has been well documented that an electronic signature that is computationally sound today will not be so in a number of years. Although cryptographers debate the details, no one denies the basic fact.

Electronic signatures are used primarily for purchasing agreements with relatively short life spans. Just a few years is typical for document retention, and little or no archiving is done. In these cases, signature-validation credibility is not an issue. Perhaps this is why quick implementation for general usage of electronic signatures is allowed under the new law.

Financial and medical documents present a different set of issues. Many of these documents are archived for a few decades at least. By law, some must be archived for years after the signer's death. Not even conservative estimates provide any trust when detecting forged electronic signatures--created with today's keys--in some distant future. Therein lies the concern. Thirty years from now, just about anyone could produce an electronically signed financial instrument, using the key you got during the dawn of electronic signatures, and claim payment. Your only protection would be to demand the evidential trail. It doesn't matter if you used your private key to sign only short-lived purchasing documents. You need have signed only one for some yet-to-be-born hacker to regenerate your private key with a futuristic personal digital assistant.

Our only protection against the inevitable advances in computing power is to insist that any system using long-lived electronically signed documents maintain an unspoofable evidentiary trail. Even today's time-stamping services will be forgeable tomorrow. Organizations wishing to implement such electronic-signature-based systems have until that day in March not only to develop archival systems with the necessary evidential trail, but to develop

the accreditation methods to show the digital certificate owners that the systems will work.

I do not believe this inevitable future of forgeable electronic signatures means we dare not use them today. Some archival systems already can accommodate the needs of electronically signed documents. Use of CDs in offsite vaulting with proper witnessing is a perfect example of a process we can build upon as a trusted archive. Evidential trails can be established today for any system requiring long-term archiving of signed documents, so insist on it.

Unquestionably, e-signatures are held to a higher standard than ink signatures are. In this digital age, we should endeavor to hold everything to a higher standard because the risks are as great as ever.”⁷

IV. Conclusion

Although e-signatures promise a future that is more efficient and simple when it comes to transacting business, the future may still be farther off than we anticipate. Until a set of standards is developed that clearly defines the electronic transaction, the liabilities of each party, the security needed, the method of dispute, and the appropriate retention methodology, you might want to hold on to your signature. In our technology pursuit we have come along ways, but we are at the edge of the digital signature frontier. Let the early adopters settle the wilderness for us so that the rest of us can settle in a civilized and cultivated digital signature community.

¹ Lemos, Rob “Lingering questions on e-sign security”. 9/28/2000. URL: <http://www.zdnet.com/zdnn/stories/news/0,4586,2634180,00.html> (10/10/2000)

² Knight, Will “Digital signatures a security threat?”. 9/26/2000. URL: <http://www.zdnet.com/zdnn/stories/news/0,4586,2633544,00.html?chkpt=zdhnews01> (10/01/2000)

³ Bowman, Lisa M. “E-signatures: Signed, sealed, delivered”. 9/28/2000. URL: <http://www.zdnet.com/zdnn/stories/news/0,4586,2634368,00.html> (10/01/2000)

⁴ Charny, Ben “Banks, brokers first to adopt e-sgin” 9/27/2000. URL: <http://www.zdnet.com/zdnn/stories/news/0,4586,2633546,00.html> (10/01/2000)

⁵ Moskowitz, Robert “What’s ‘E’ about signatures?”. 9/18/2000. URL: http://www.nwc.com/1118/1118colmoskowitz.html?Is=NCJS_NL162 (10/01/2000)

⁶ Shim, Richard “Making money from e-signatures”. 9/28/2000. URL: <http://www.zdnet.com/zdnn/stories/news/0,4586,2633629,00.html> (10/01/2000)

⁷ Moskowitz, Robert “Tracking Digital Signatures”. 08/21/2000 URL: <http://www.nwc.com/1116/1116colmoskowitz.html> (10/01/2000)

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event