Technology   Reviews   Discussion Forums   Careers   Tools & Resources   Whitepapers

A Closer Look at E-Signature Laws

LINDA ROSENCRANCE (Computerworld)   06 October, 2000 12:01 | Comments | Like

What do corporations and others have to do to take advantage of the new electronic-signatures law that went into effect Sunday?

Users, analysts and e-commerce experts tried to answer that question this morning at a seminar sponsored by the Massachusetts Software & Internet Council and held in the Boston suburb of Newton, Mass.

The Electronic Signatures in Global and National Commerce Act, which was signed by President Clinton on June 30, allows e-signatures to be as legally binding as handwritten signatures for e-commerce transactions. It doesn't, however, require companies to use such signatures or to keep electronic records. And it also doesn't dictate what technology businesses must use to implement e-signatures.

According to the software council, the legislation is important because acceptance of digital signatures will spur the use of commercial electronic-authentication techniques, such as digital certificates, in the private sector. The techniques also will create significant efficiencies and cost savings for companies, which won't have to keep paper records.

However, companies that have traditionally relied on paper-based processes will have to overcome certain challenges before e-signatures can become a reality in everyday business, said attorney Daniel Greenwood, director of the E-Commerce Architecture Project at MIT.

"The act doesn't tell you how to implement e-signatures or what technology to use," Greenwood said. "We now have a lot of rope to virtually do anything in terms of e-signatures, but we have to be sure we don't hang ourselves with that rope."

Beyond requiring a scalable and manageable infrastructure to support digital signatures, companies face additional challenges, including the lack of interoperability among digital certificate vendors, the complexity of the technology and the costs of deploying the technology.

Digital certificates are encrypted secure codes used to verify the signer of an electronic document. But before there can be widespread use of e-signatures, users will need to overcome some serious interoperability issues related to the public-key infrastructure (PKI) on which digital-signature systems are established (see story). The problem is that there are a number of vendors supplying the technologies, which are often proprietary. It's difficult to certify digital signatures in a PKI where there's a mix of vendor products and certificate authorities involved.

That's about to change, though, said Derek Brink, who heads the customer advisory council for one PKI vendor -- RSA Security Inc. in Bedford, Mass. Brink is also chairman of the PKI Forum, an industry group of vendors and users advocating the use of PKI as an enabler of online business. Brink said the group is working toward interoperabilty of the different vendor products.

In moving toward widespread use of e-signatures, businesses will face a number of data-security issues, including making sure the parties involved

are who they say they are, ensuring that only authorized parties have access to certain information and ensuring that a message hasn't been tampered with in transit, said Sara Greenberg, an attorney at Testa, Hurwitz & Thibeault LLP in Boston.

Arabella Hallowell, an analyst at Gartner Group Inc. in Stamford, Conn., said businesses can use several methods to authenticate e-signatures, including personal identification numbers and passwords, smart cards that can be swiped on a reader attached to a computer, biometrics of physical attributes such as fingerprints or a combination of these methods.

But some of these methods can be expensive. For example, using a smart card could cost anywhere from $30 to $100 per user, including hardware.

Jerry Archer, senior vice president of information security and risk at Fidelity Personal Investments and Brokerage Group, said it could cost his company about $2 billion for its 15 million customers to use digital signatures.

Currently, Fidelity uses a reliable user ID and six-digit password system to make sure a customer is who he says he is, Archer said.

"With this system there's a one-in-a-million chance that someone can figure out the six-digit password and access our system; using a voice-identifier system there's a chance that two people out of 1,000 will gain access," he said.

Bookmark this page

Share this article

Got more on this story? Email Computerworld

Follow Computerworld on

More about: Gartner, Gartner Group, Internet Council, MIT, RSA, The Security Division of EMC

Comments

Post new comment

NAME

EMAIL ADDRESS

The content of this field is kept private and will not be shown publicly.

COMMENT

Users posting comments agree to the Computerworld comments policy.

Post   Preview

Login or register to link comments to your user profile, or you may also post a comment without being logged in.

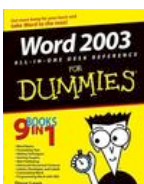Virtualisation: Optimised Power and Cooling to Maximise Benefits

Pulling the Plug on Legacy Log Management
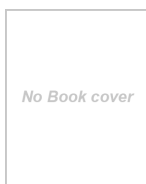
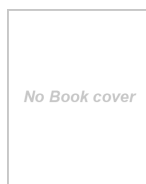PlateSpin Forge: Plug In and Protect Server Workloads

All whitepapers

Word 2003 All-In-One Desk Reference for Dummies

Objects, Data Structures and Abstraction Using C++ with WileyPlus Registration Card

Teach Yourself Visually Photoshop Cs4 with Teach Yourself Visually Flash Cs4 Prof Set

C#

Market Place

Don't let IT/data issues keep you awake at night: Moving Data and its storage is mission critical

Featured White Paper | Pulling the Plug on Legacy Log Management

Power through the disruptions: Uninterruptability from Eaton

Commercial value of software theft exceeds $50B - PC software piracy decreases in Australia by 1% amidst global recession

Virtualising your desktop infrastructure for a more efficient business continuity and disaster recovery

CIO2CIO Research Study | State of the Market: Application Performance Management
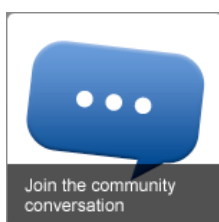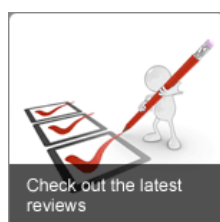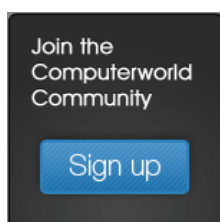
IDG Australia invites you to participate in its 2010 Business Communications survey | Find out more > >

Protect bandwidth from spammers, criminals, hackers, time-wasters and employee misuse.

Strategy Guide | How not to get buried in data

Join the Computerworld Community
Sign up

Check out the latest reviews

Join the community conversation

Editorial Contacts	Events	IT Media Releases
Advertising Information	Whitepapers	Slideshows
Privacy Policy	News	Videos
RSS	Webinars	
Newsletters	Zones	

IDG Sites: PC World | GoodGearGuide | Computerworld Australia | CIO Australia | CSO Online | Techworld | ARN | CIO Executive Council