



December 2, 2009

## E-Signatures Q&A: Legalize It

Minimize The Risks Of Eliminating External-Facing Paper-Based Processes

by **Bill Nagel**

with Robert Whiteley and Margaret Ryan

### EXECUTIVE SUMMARY

Electronic signatures (e-signatures), with their roots in paperwork elimination initiatives, have been edging into greater prominence due to the greater regulatory, legal, and economic pressures that businesses in many industry verticals are feeling today. The need to shorten sales cycles and reduce turnaround times often runs headlong into the requirement to safeguard valuable transactions and the data associated with them. E-signatures combine secure document signing, workflow automation, and (often) document life-cycle management functions into a package that makes it quicker, more convenient, and safer to execute legally binding agreements online. Forrester recommends that security and risk management professionals get up to speed on e-signature technologies and prepare to answer the top questions business and IT execs will be asking in 2010.

### QUESTIONS

1. How do “electronic signatures” differ from “digital signatures”?
2. Which variations of e-signatures are legally binding?
3. What are organizations using e-signatures for?
4. How can I authenticate customers to be sure that I know who’s signing the transaction?
5. How can I authenticate new or potential customers whom I haven’t yet identified?
6. The e-signing itself seems fairly trivial. Is that all there is to e-signature solutions?
7. How can I ensure that customers correctly sign documents with complex signature requirements?
8. What kind of return on investment can I get from implementing e-signatures?
9. What do I need to do with the signed electronic record?

### ECONOMIC AND REGULATORY FACTORS ARE BRINGING E-SIGNATURES TO THE FOREFRONT

Electronic signatures have become an ever more popular topic of discussion among Forrester clients, which in turn reflects the momentum in the e-signature marketplace.<sup>1</sup> This momentum is partly due to the need for improved governance and security brought on by regulatory requirements. However, several other factors are playing an ever larger role, including the:



#### Headquarters

Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139 USA  
Tel: +1 617.613.6000 • Fax: +1 617.613.5000 • [www.forrester.com](http://www.forrester.com)

- **Pressure from the business to be more efficient.** E-signatures are propelled by a rapidly evolving business process and workflow automation environment.
- **Pressure to adopt cloud computing services.** E-signatures are an important — but often overlooked — element in meeting the increased appetite for moving critical processes to the cloud and consuming them as Web services.
- **Pressure to save money wherever possible.** After a tough start, many companies are showing a demonstrable ROI in their e-signature deployments, saving money in a challenging economic environment.

This document is designed to help security and risk management professionals answer the top questions regarding e-signatures and help jumpstart e-signature projects heading into 2010.

## 1. How do “electronic signatures” differ from “digital signatures”?

The definition of an “electronic signature” in both the US federal E-SIGN Act of 2000 and the European Union’s Electronic Signatures Directive of 1999 is extremely broad.<sup>2</sup> For example, E-SIGN defines an e-signature as “an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record,” whereas the EU directive defines it as “data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.” This exceedingly broad definition encompasses a myriad of potential e-signature techniques, right down to the very simple “Click this button to verify you wish to sign the document.”

In contrast, the term “digital signature” has a very specific meaning: applying asymmetric cryptography — an encryption key plus a signing algorithm — to the contents of a message to generate a “signature” that is then affixed to the message. This signature, which is actually just a calculated mathematical value, is accomplished in the context of a public key infrastructure (PKI). When a document is digitally signed with a private key, only the corresponding public key and signature-verifying algorithm can prove its validity (authenticity and integrity).

In other words, all digital signatures are electronic signatures, but not all electronic signatures are digital signatures. Digital signatures are a subset of electronic signatures — indeed, the most secure form of e-signature available today.

## 2. Which variations of e-signatures are legally binding?

The definitions of “electronic signature” in both the US and EU legislation are intentionally broad and aim to facilitate the uptake of fully electronic document signing by businesses, consumers, and governments. Organizations wishing to eliminate paper-based processes via digitization still need a way to make electronic documents like e-contracts legally binding, and the governments promoting

this paradigm shift — for example, via the Government Paperwork Elimination Act of 1998 in the US — have a vested interest in making this process flexible and easy to adopt.

The practical effect of these expansive definitions of electronic signatures is that any of the signing processes offered by e-signature vendors are legally binding and will be upheld as such in court — the validity of e-signatures is settled law. A more important distinction is whether an electronic signing process is secure or not, and the central question becomes, How can I be sure that the person who signed the document is who she claims to be and that no one can repudiate the e-signature? While only digital signatures can provide true nonrepudiation, authenticating the signer before allowing her to apply the e-signature can greatly mitigate potential fraud issues (see question 4).

### **3. What are organizations using e-signatures for?**

Organizations in both the private and public sectors are using e-signatures to validate a wide variety of internal- and external-facing processes. Most often, this involves signing legally binding contracts, policies, or applications, but e-signatures are also used for more mundane tasks, like securing internal approval to go forward with a sales lead or signing off on SOX-mandated internal controls, that benefit from faster processing times and more convenient workflows.

To date, the primary adopters of external-facing e-signature products have been financial services firms like banks, insurance companies, brokerages, and auto loan and home mortgage companies. These businesses use e-signatures to eliminate costly paper processes and greatly reduce the cycle time for customers to sign and return loan and credit applications, insurance policies, funds transfers, and the like.

The pharmaceutical industry provides a good example of e-signature adoption for a mixture of internal and external processes. Large pharma firms work with dozens of contracting organizations around the globe to carry out functions like developing new drugs and conducting clinical trials — and in the end must submit much of this data to regulatory bodies like the US Food and Drug Administration. E-signatures ensure that all processes are signed in sequence, that all chain of custody requirements are met, and that documents are quickly delivered to the next destination for signature. Finally, some organizations use e-signatures for purely internal approval processes, often taking advantage of a vendor's existing integration with an application like salesforce.com.

### **4. How can I authenticate customers to be sure that I know who's signing the transaction?**

Signer authentication takes on considerably more importance when either the signing process is very simple, the document or process being signed is particularly valuable, or both. Anyone can easily commit fraud by clicking an "I approve" button on a Web page if they're not authenticated, so it's vital that customers be required to authenticate their identity to the document provider before they are allowed to sign anything. In many cases, this authentication takes the form of a user name

and password — assuming the user has established an account with the provider or has set up the desktop e-signing software. Strictly from a security perspective, Forrester recommends this only for low-value transactions or for companies that have strong back-end antifraud measures in place.<sup>3</sup> Otherwise, the sensible path is to implement proper multifactor authentication, although the costs and difficulties associated with distributing and supporting these credentials in a consumer-facing context are well-documented, and as a result many firms still rely on the good old password as the sole means of customer authentication.<sup>4</sup> For very high-value transactions and mission-critical processes, the best practice is to use PKI, which strongly authenticates the user and provides the “gold standard” of the e-signing world: digital signatures.

### **5. How can I authenticate new or potential customers whom I haven't yet identified?**

Verifying the identity of those with whom you haven't already established a business relationship has been one of the biggest chicken-and-egg questions surrounding eCommerce. One of the primary driving forces behind e-signature adoption is the drastic reduction in the time it takes to attract and land a new customer, and for many companies the rush to win a new account trumps all. The plain fact is that most companies that have implemented e-signatures and allow unknown parties to e-sign to open new accounts, apply for a new policy, or secure a new loan use their existing antifraud practices to expose and mitigate potential fraud — trust first, verify later, and swallow a certain level of fraud as a cost of doing business.

For those companies not willing to settle for after-the-fact fraud mitigation, credit bureaus and some authentication vendors offer another method of verifying the identity of new, unknown signers, called “dynamic knowledge-based authentication” (dynamic KBA), which is a stronger twist on the comparatively weak “secret question” method of authentication. Dynamic KBA is offered as a service, and the typical provider (often a credit bureau) has access to a raft of public and private databases potentially containing a significant amount of information about most potential applicants. When a visitor identifies himself to the e-signing Web site, the provider searches through its databases for information about that asserted identity and uses that information to formulate intelligent challenge questions that only the correct person should be able to answer quickly and easily.

### **6. The e-signing itself seems fairly trivial. Is that all there is to e-signature solutions?**

Applying an e-signature is indeed the linchpin of the document legalization process, and lower-end Web-based e-signature solutions don't provide a lot of functionality beyond that. But e-signatures are really primarily about workflow and business process automation. As such, most e-signature solutions act as an orchestration hub that automates and coordinates a number of document life-cycle processes, including generating e-forms, presenting them for dispatch, routing them to and from the signer, executing the signing ceremony, processing the returned document, routing signed records to storage and archiving systems, and logging the entire process for potential audit. The e-signing process orchestration functionality usually needs to be integrated with the organization's

existing content management system (CMS), particularly for on-premises solutions. The degree of integration needed increases with the number of moving parts in the e-signature solution and the number of interfaces required with the CMS. Any company seeking to implement e-signatures needs to first consider what content management pieces it already has in place and whether all of the (paper-based) workflows requiring digitization have already been mapped out.

### **7. How can I ensure that customers correctly sign documents with complex signature requirements?**

What happens if a contract needs to be signed by multiple parties in a particular sequence, or if a document needs to be signed in multiple places? Just as people often don't read documents all the way through before signing them, signers can overlook even the clearest signing instructions without someone there to guide them through the process — and incorrectly or incompletely signed documents have to be returned to the customer for signing, causing inconvenience and sabotaging one of the primary benefits of e-signing: faster turnaround time. To ease the process, many e-signature solutions allow organizations to create custom “signing ceremonies” — automated signing workflows that guide the signer through the document, point out all the places where the document needs to be signed, and even provide instructions for those still clueless. And if the entire e-signature workflow has been defined and automated, then signed documents can be automatically routed to the next signer in the chain.

### **8. What kind of return on investment can I get from implementing e-signatures?**

The cost savings that organizations realize by replacing paper-based processes with fully digital ones incorporating e-signatures can be very significant — Forrester estimates up to 75% of the amount previously spent pushing paper around. Firms implementing e-signatures save considerable amounts of money on materials (chiefly paper and copy supplies) and personnel (to generate, send, receive, process, and store all that paper). But cycle time is also a key component: Even overnight delivery services can't compete with the Internet on speed, price, or convenience to the signer — and the value of this advantage increases exponentially with the number of signers or the number of stages of a multistep signing process involved in completing the execution of a contract. Moreover, the likelihood of customers signing and returning a document within minutes of receipt is far higher when the process does not involve signing, copying, and returning paper. Financial services firms and insurance companies report average contract cycle times falling from one or two weeks to a matter of days — or hours. Finally, firms can increase e-signature ROI by having the document workflows (whether automated or not) worked out well in advance of solution implementation.

### **9. What do I need to do with the signed electronic record?**

In general, the requirements for storage and archiving of signed electronic records depend on the degree of regulation the signed document or process, or the industry of the issuing firm, is subject to. In many cases, companies in industry verticals like financial services, insurance, healthcare, and pharmaceuticals are required to retain signed electronic records for several years. One consequence

is that the integrity of the signature must not be compromised over time. Using digital signatures to e-sign documents provides the highest level of integrity and nonrepudiation over time, but firms adopting digital signatures also need to ensure that the decryption keys are securely stored and well-maintained, so that the plaintext of the signed records can be reproduced on demand.

Companies also need to decide whether they will store the signed electronic records on-site or off. This is rarely a consideration with on-premises solutions, as the records never leave the organization's control except when they are sent out for signature. However, as more and more of the industry moves to a cloud-hosted service model, it's vital for firms to ensure that the signed records will be transferred to their data center efficiently and in a timely manner for storage and archiving, to avoid losing control of documents that are potentially subject to a compliance audit. "The cloud ate my homework" will not be an acceptable excuse. Fortunately, most e-signature vendors have taken this into account and can batch-transfer signed records back to customers' systems on a regular schedule.

## ENDNOTES

- <sup>1</sup> The current economic and regulatory climate has made it more important than ever for firms to find ways of streamlining business processes while maintaining the security and integrity of the associated data. E-signatures combine the security of digital signing with the efficiencies of business process automation to lower the costs of acquiring and transacting with customers while bolstering regulatory compliance. Forrester's IT security and risk management team fielded 4,683 inquiries on a variety of security-related topics between January 2006 and February 2009 — 93 of which came from IT professionals interested in e-signatures. Nearly 60% of the e-signature inquiries asked how firms are using e-signatures; Forrester clients were also interested in which industries are the primary adopters of e-signatures and asked for assistance in navigating the landscape of e-signature vendors. See the April 2, 2009, "[Inquiry Spotlight: E-Signatures, Q2 2009](#)" report.
- <sup>2</sup> The "Electronic Signatures in Global and National Commerce Act" was signed into law in the United States on June 30, 2000. The European Parliament passed "Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures" on December 13, 1999.
- <sup>3</sup> The adoption of strong multifactor authentication (MFA) is on the rise. It's often the first port of call on the journey to a fuller identity and access management implementation; MFA directly addresses the password problem, which is a well-known and well-defined security weakness in many corporate environments. An impressive proportion of enterprises in Europe and North America have implemented MFA, but in reality many of those implementations only cover a small minority of a company's users. As so many organizations have yet to embark on a full MFA rollout, Forrester interviewed several firms that have recently completed the process successfully to learn about the best ways of doing so. Four main themes emerged from these interviews: Understand how your users work; determine what the business needs and be proactive; anticipate and mitigate technology challenges; and develop a strategy to get support in the right places. See the July 23, 2009, "[Best Practices: Implementing Strong Authentication In Your Enterprise](#)" report.

- <sup>4</sup> Security professionals have long known that passwords are no longer sufficient to act as the sole means of gatekeeping access to enterprise network and data resources. Increasingly, they're putting that knowledge into action: More than half of the enterprises surveyed in Forrester's Enterprise And SMB Security Survey, North America And Europe, Q3 2007 have either implemented strong authentication at desktop logon or are planning to start or finish such a project in 2008. While strong multifactor authentication certainly improves security, what's less clear is what end users will accept as a convenient and usable second factor. Reflecting the real-world difficulties security managers have had in keeping users happy with the choice of strong authentication, the vendor landscape is complex and fragmented. Vendors will continue to expand their product lines until enterprise adoption of identity management, including strong authentication, becomes more widespread in the coming years. See the July 16, 2008, "[Market Overview: Strong Authentication For Enterprises In 2008](#)" report.