



## Cryptography Rides to the Notaries' Rescue

By [Larry Seltzer](#)  
May 1, 2006



▶ 5 comments posted

▶ [Add your opinion](#)

**Opinion: It's amazing that it took this long, and it's still in early stages, but public key cryptography is emerging as the notarization stamp of the future.**



**eWEEK.com Special Report:**  
Piracy and Counterfeiting

To those who grew up in the electronic age, notarization

of documents has the odor of antiquity and obsolescence.

[Telelogic's Popkin Purchase Prepares the Way for SOA When PKIs Learn to Connect](#)  
[nCipher Aids PKI Portability](#)  
[Popkin Partners With Lanner](#)  
[Popkin, Intalio Team on Biz Processes](#)

It is an ancient practice, but ironically it serves purposes directly analogous to many of high priority for modern electronic documents. And now modern security techniques are bringing notarization to the electronic realm, to the benefit of both.

Think of notaries as an old-world authentication and accreditation system.

In the United States, they are accredited by the state, and similar positions are supported by governments the world over.

They witness the signature of documents, authenticate the signatories, and accredit the signatures through a physical mark attached to the paper: an ink stamp, a crimp, even a physical seal (how's that for old world?).

There are lots of problems with this system, but let's focus on two of them: 1) paper notarization only works for paper documents, and the world is going digital, and 2) the paper notarizations are subject to fraud of various kinds.

Of course, traditional notarization has never really been about any actual security created by the process.

Its true meaning is in the formality of the process, telling the signers that they are committing an official act of some sort and underscoring their risk of legal penalty for perjury or fraud.

The centrality of the symbolic aspect is basically still true of electronic notarization, but the authentication aspect of the process becomes more genuine.

The world of paper documents will continue to have these problems and be totally symbolic, but strong notarization tools increase the incentive for official document recording to go electronic.



**eWEEK.com Special Report:**  
Enterprise, Gov't. Team Security

Therefore **the NNA (National Notary Association)** has been pushing for states to embrace e-notarization, or electronic notarization of electronic documents.

It has been adopted to varying degrees by seven states (California, Colorado, Florida, Michigan, Pennsylvania, Texas and Utah), but Pennsylvania has emerged as the poster child for widespread adoption.

According to the NNA, it is the only state where all the important actors have signed on.

Over the next year the Pennsylvania Department of State is conducting Phase I of its **Electronic Notarization Initiative** and expects all counties to begin accepting e-notarized documents.

E-notarization is a specialized form of public key signing.

**To become an e-notary (here in PDF form)**, one must, first of all, be a commissioned notary of the conventional sort.

The applicant files **an application**, which, if accepted, allows the applicant to receive an "Electronic Notary Seal" and their contact information is forwarded to the NNA. The applicant pays a \$24.95 fee to the NNA.

At this point, the applicant has to appear in person before a participating county Recorder of Deeds (**there are four of them right now, explained here in PDF form**) and present their approval letter and satisfactory ID.

The Recorder will then enter the notary's ID information into the shared Electronic Notary Seal database.

Only at this point does the NNA contact the notary and tell them how to download their Electronic Notary Seal, which is an x.509 v3 certificate.

Cumbersome, isn't it? Don't expect an Amazon one-click version of this process any time soon. And don't assume that electronic notarization can be done remotely through a Web site.

E-notarization still requires the notary to physically witness the signatories sign the document, albeit to apply their signatures electronically.

As the Pennsylvania site says, "...the personal appearance rule must be strictly followed. In addition, the signer of the electronic document must be positively identified and screened for awareness and willingness."

When I say the signatories "sign the document," I refer to signatures in the more conventional sense, not to digital signatures.

Probably the most common way this would be done is with a stylus on a tablet PC or an attached device similar to the ones used in stores for electronically signing credit card receipts.

## Cryptography Rides to the Notaries' Rescue



**eWEEK.com Special Report:**  
Politics Meets IT

How to  
the actual  
software  
procedure  
s work for  
e-  
notarizing

Telelogic's Popkin Purchase Prepares the Way for SOA  
When PKIs Learn to Connect  
nCipher Aids PKI Portability  
Popkin Partners With Lanner  
Popkin, Intalio Team on Biz Processes

document? The Pennsylvania and NNA sites are not very specific about it. One very popular way is to use Adobe Acrobat, which has good support for digital signing.

There are also a number of vertical software companies that have had to contend with the notarization process and which are excited at the possibility to provide for electronic notarization directly in their products.

Consider **Simplifile**, which makes products for electronic document recording at counties, or **Tyler Technologies**, which makes products for (among other things) property appraisal and assessment.

It's also possible to use any free, off-the-shelf software that supports x.509 certificates (**Microsoft has some for free download**).

These might be inconvenient, in that you might have to separately track a file with a signature in it, as opposed to using a format like PDF that supports signatures intrinsically.

No matter how they are made, if they follow established PKI x.509 standards the notary's certificate can be checked by anyone not only for authenticity with the certificate authority (**GeoTrust**, under contract to the NNA), but check to see if their authority has been revoked or expired. Try doing that with a conventional notary.

The PKI infrastructure thus makes notarization much more secure than in the paper world, where it's too easy to photocopy a stamp or seal and duplicate it.

It's a pretty radical change, though, for a practice that has been pretty stable for hundreds, arguably thousands of years.

And it's not just a matter of getting individual notaries to embrace the electronic approach; there are state-to-state and international legal issues.

What happens when someone tries to use in one state a legal document electronically notarized in another that doesn't yet have electronic notarization?

The NNA says that such a case is in the courts in Michigan now and that they have filed an amicus brief in it in support of electronic notarization.

The Constitution requires that states grant "full faith and credit" to the legal decisions and procedures of others, but to an old-fashioned state facing an e-notarization, it must surely seem as if the Martians have landed.

As widespread as PKI is in computing, I have to think it's been substantially a failure for not reaching so many areas to which it can bring value.

Notarization could be a bellwether for the movement of PKI into mainstream applications where strong authentication and accreditation are needed.

If it can't be made accessible and compelling enough, people will resist it, and that would be to everyone's loss.

*Security Center Editor Larry Seltzer has worked in and written about the computer industry since 1983. He can be reached at [larryseltzer@ziffdavis.com](mailto:larryseltzer@ziffdavis.com).*