



Can you reliably prevail when your electronic evidence is challenged in court?

In an increasingly paperless world where data can be so easily manipulated, law firms face a new hurdle: proving the authenticity of the electronic evidence presented in support of their client's case. Given that your clients often have the means and the incentive to tamper with their own business records, how do you prove beyond a reasonable doubt that those records are authentic and pristine?

The December 2006 amendments to the Federal Rules of Civil Procedure have caused corporate IT departments to spend huge sums building systems to respond to eDiscovery requests. But if the authenticity of the documents so produced is challenged, that might be money down the drain. As a result, authenticity challenges around electronic records are emerging as a serious problem for attorneys. They can also represent an opportunity, once counsel begins to understand the new litigation tactics that can be used to win cases or drive settlements.

Earlier this year, a partner at a large Minneapolis firm admitted to altering two emails and a memo that he submitted as evidence in a case. Imagine the brand damage that firm faces now. Opposing counsel in future cases will undoubtedly seek opportunities to caution a judge or jury not to trust the records submitted by that firm — as it's known that they've altered their own files in the past. In another case, involving American Express as plaintiff, the judge ruled that the company could not admit its own electronic records as evidence unless they could demonstrate their authenticity. Amex tried and failed three times to demonstrate the authenticity of their electronic records — and eventually lost the case. The winning defendant — a client who didn't have a lawyer — didn't even show up in court.

These scenarios are likely to occur with increasing frequency as courts, clients and regulators become more cynical about the validity of Electronically Stored Information (ESI). They know that virtually any of your — or your clients' — electronic documents can

"If it is critical to the success of your case to admit into evidence computer-stored records, it would be prudent to plan to authenticate the record by the most rigorous standard that may be applied."

— *Honorable Paul W. Grimm*
Chief United States Magistrate Judge
US District Court, Maryland
Lorraine vs. Markel Insurance Company, May 4, 2007

be easily modified, especially by insiders with "admin" access to the applications. Even within modern content management solutions it is easy to alter an email or modify a timestamp. This is because managed systems usually only secure the perimeter — they can't protect individual emails, attachments, spreadsheets, or PDF files from tampering by people inside the organization, or while those documents are in the custody of clients or third parties.

It's a very simple matter to challenge the effectiveness of a company's controls and processes (the typical expert-testimony approach), and as a result create doubt about the authenticity of ESI and cause considerable resources to be allocated to defend the effectiveness of external controls. Vincent Liu, Partner at respected computer forensics firm Stach & Liu says, "For any case that relies on digital forensic evidence, it would be a cakewalk to come in and blow the case up. I can take any machine and make it look guilty, or not guilty. Whatever I want ...the (current) presumption of reliability is unjustified."* In fact, any plaintiff with a plausible story against a corporation can now bury them in production and authenticity expenses to create the leverage needed to drive a settlement.

As a law firm, you may not have control on your client's record-keeping, but you must at a bare minimum be able to prove that nobody has tampered with that evidence since it came into your custody. And you're certainly in the position to save your clients millions going forward, by encouraging them to take records authenticity controls seriously.

Prove document authenticity beyond a doubt

ProofMark solutions for Counsel irrefutably seal electronic records with patented Transient Key™ digital seal and trusted time stamp technology, enabling you to prove the authenticity and pristine state of your evidence to any challenger. Now your records have a tamper-evident seal, a digital equivalent of the delicate plastic protecting a bottle of Tylenol.

ProofMark is a patented, standards-compliant solution for monitoring and proving authenticity — on demand, or totally in the background, depending on the level of control you desire. ProofMark can even help you establish the authenticity of documents that have traveled outside of your organization's control, and it's especially effective at detecting (and therefore deterring) deliberate or inadvertent changes to the records store by trusted parties inside your organization.

ProofMark products offer the strongest possible level of cryptographic integrity assurance and tamper detection technology. And it's available in a variety of packages. Pick the one that's right for your firm!

proofmark™

FOR COUNSEL

ProofDoc™ *FREE trial version at*
www.proofspace.com/proofdoc

COMING
 JAN. 1, 2008!

ProofDoc for Windows XP or Windows Vista is an easy-to-use application that enables you to seal virtually any document or file with a tamper-evident “wrapper” and trusted timestamp, synched to the atomic clocks at the National Institute of Standards and Technology (NIST) and the U.S. Naval Observatory (USNO). Installed on your desktop or on the server, you can configure your solution to automatically support supervisory procedures, such as automatically applying a ProofMark to any document saved to a client folder. Say, for example, you want to seal and timestamp all the records you receive from a client, so you can show they haven’t been tampered with before being submitted in court. With ProofMark you can prove to a judge or arbitrator that you couldn’t have changed a timestamp or inserted a false record, even if you had wanted to.

From \$199 per user. Buy ProofDoc together with any other ProofSpace product and save 10%... Or buy three products and save 25%! ProofDoc is also available as a software developer’s kit (SDK) so that you can achieve a truly seamless integration with your existing systems. Call for pricing..

ProofMail™ *FREE trial version at*
www.proofspace.com/proofmail

COMING
 JAN. 1, 2008!

Email is one of the easiest electronic formats to manipulate — and also the most frequently produced file type during the discovery phase for lawsuits. It’s trivial even for non-technical users to change a date or a timestamp, or to modify the contents of an old email and re-insert it into the stack. That can spell big trouble and get your case thrown out of court. Fortunately, ProofMail makes it easy to digitally seal email communications and their attachments. There’s nothing to download, nothing to install or maintain. You simply BCC our certified ProofMail server on your outgoing mail. If there’s ever any question about one of your communications that somebody else has stored, you can be assured that it would be impossible for them to alter that document without detection. If you prefer, you can even license a local instance of ProofMail and install it adjacent to your current mail server, so that your attorneys can preserve privilege for qualified attorney-client communications.

From \$199 per user. Save 10% when you buy ProofMail with another ProofSpace product, or save 25% when you buy all three together!

ProofMark On-Demand™ *FREE trial version at*
www.proofspace.com/ondemand

ProofMark On-Demand delivers the benefits of ProofMark over the web! You can use it on any computer, be it PC, Mac, Linux or Unix — any platform with a web browser, anywhere you happen to be in the world. ProofMark On-Demand can be implemented rapidly, scales with your organization, and (like all ProofSpace products) includes free upgrades for the duration of your license. ProofMark’s robust service architecture is engineered for high availability, with redundant multiple failover protection and regular backups.

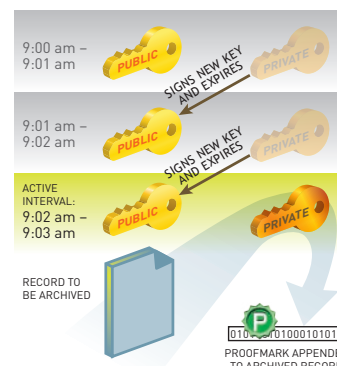
From \$89 per user. Buy ProofMark On-Demand with another ProofSpace product, and save 10%... save 25% when you buy three products together!

Try ProofMark today for FREE! Visit www.proofspace.com/unlimited for a special savings offer.

For more information, call David McClellan, General Manager, at 312-933-8823 or email david@proofspace.com.

The ProofMark Transient Key™ Technology

- In ProofMark’s Transient Key system, each time interval generates its own RSA key pair.
- As records are archived, they are signed by the active time interval’s RSA private key
- When an interval is about to expire, it signs the new interval’s RSA public key; the new keypair goes “on duty” and the old private key is destroyed.



Key Features

- Provides self-validating proof of time with cryptographic tamper detection
- Cryptographically strong chain of events which is virtually impossible to alter after the fact
- No secrets to protect, since private keys are destroyed
- Needs no outside certification authority or trusted 3rd party

For a more detailed technical explanation of patented ProofMark Transient Key technology, download a free whitepaper at www.proofspace.com

ProofMark System Benefits:

- Dramatically reduce court costs during eDiscovery, by minimizing costly manual forensics and expert testimony required for “old-style” email authentication.
- Gain an evidentiary advantage on opposing counsel by using the strongest form of digital records authentication available.
- Quick and easy to use. Embed document integrity safeguards directly into your existing business processes.
- Instantly detect tampering, accidental changes and any other unauthorized modification.
- Virtually eliminates records store integrity threats from insiders, because changes can be immediately detected.
- Long-lasting tamper seals persist on records, even when they travel outside of your organization or to other systems, such as archival, backup, and case-management applications.
- Can be configured to operate almost completely behind the scenes, invisible to your staff and staying out of your way during the normal course of business.
- Provides irrefutable proof of records authenticity that will stand up to regulators, auditors, arbitrators and legal examination.
- Helps firms comply with national standards and specifications including the ANSI X9.95-2005 specification for Trusted Time Stamp Management and Security, Federal E-SIGN legislation and Sarbanes-Oxley.
- Redundant multiple failover protection; regular backups are stored indefinitely in ProofMark’s geographically distributed Forensic Repositories.
- Because you can now prove authenticity of your electronic records, you can start making your office a lot more paperless — and avoid the hassle of tracking down paper “originals”.



proofspace | www.proofspace.com | 900 Clancy Ave NE | Grand Rapids, MI 49503 | (616) 520-3901