

What if Your Archives Don't Cut It in Court?

Recent rulings in US Federal Circuit Court make it clear: your electronic archives may not be allowed into evidence unless you can prove their integrity... and "securing the perimeter" isn't good enough anymore.

In a recent federal 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 — who wasn't represented by counsel — didn't even show up for the court date!

This scenario is repeating itself across the country. And the trend may be accelerating. One thing's for sure: the issue of evidence is evolving, and courts are becoming wise to the fact that electronic records can be easily manipulated — from within or without.

The e-Discovery Amendments to the Federal Rules of Civil Procedure, effective December 20, 2006 now require the production of all "responsive" electronic business records upon

"The security industry has been running backwards in our view—starting at the edge (perimeter) and working its way to the data itself. The availability and protection of the data is the core need... but trying to block sessions at the firewall or stripping out malignant emails... completely missed the insider threat problem. Perhaps closest to the core is a small company (ProofSpace) we've seen trying to establish the integrity of the data itself with the non-debatable tag of time."

— Peter Kuper,
Internet Security Analyst,
Morgan Stanley Research Brief
March 15, 2007

request. But the existing Federal Rules of Evidence require legal authentication of all records offered into evidence as a prerequisite for admissibility in a court-of-law! So how will you authenticate your electronic records?

This also begs two questions. First, why is your enterprise spending huge sums to archive electronic records which might not be accepted into evidence in a court of law? Secondly — how can your business prove the authenticity of its electronic records at a given point in time?

The Old Approach to Data Integrity: "Inferred" Authenticity

Using traditional security controls means that, in court, the enterprise will need to try and convince the judge that their electronic records are reliable by inference. In other words, if the perimeter can be shown to be somewhat secure, and the procedures and controls of the enterprise proper, then the electronic records of the enterprise should be assumed to be reliable. This approach is costly, time-consuming and (in the end) often doesn't work. That's because data change is almost always possible no matter how strong the controls may be. For example, insiders with unlimited access privileges almost always exist, and data often moves from strongly controlled environments to areas of weaker control during its life cycle. Increasingly, when confronted with these realities of computing, judges distrust such electronic records and will not admit them as evidence.

Today's courtrooms are less trusting of corporate America than ever. Options backdating scandals, mutual fund late-trading debacles and frequent earning restatements have made judges more than a little skeptical about the authenticity of electronic records offered into evidence. Today's bench understands that company insiders frequently have the means — and the motive — to manipulate the archive to their benefit. So now, enterprises using "inferred" authentication of their data find that their records are easily (and increasingly) challenged in court. Once so challenged, these companies have to resort to complex (and very expensive) arguments to ensure their records are not rejected as evidence. They have to demonstrate a reliable chain-of-custody, effective security controls, and verifiable audit trails. Even after months of painstaking forensics work and the testimony of expert witnesses, inferred authenticity is still easily challenged.

Just ask American Express.

The ProofMark Approach: Intrinsic Authenticity

You need a legally airtight system that thwarts fraud, provides an undeniable record of good enterprise conduct, and repudiates false legal claims against your company.

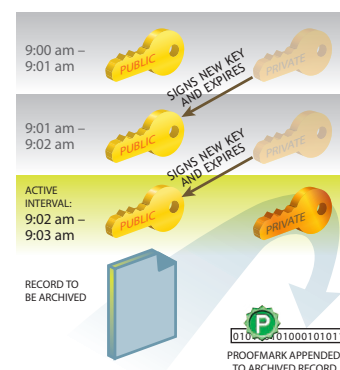
ProofMark for Financial Services is the solution. ProofMark's patented Transient Key technology tags your electronic business records with a self-validating cryptographic seal that acts as a "tamper indicator" based on a true and provable time-reference datum, impossible to manipulate, even by trusted insiders. ProofMark irrefutably proves that the content of a record has not changed since the ProofMark was applied, no matter where the data resides or who controls it.

ProofMark's underlying Transient Key technology is recognized within the American National Standard X9.95-2005 ("Trusted Time Stamp Management and Security") published by ANSI ASC X9, the accredited standards body for the financial services industry. ProofMark is the only method recognized by the ANSI X9.95 standard that can be deployed entirely as software inside your enterprise, within your line-of-business, without depending on an external trusted third party.

The ProofMark System is easy to deploy, enabling you to apply tamper indicators to any electronic records placed into short-term or long-term enterprise storage, based on business rules you define. ProofMarks are persistent and can be verified independently by anyone, eliminating the need for trusted third parties or expensive public-key certification hierarchies. ProofMark seals are portable, self-contained, independent and indelible, giving you the highest level of assurance over the authenticity of your electronic business records.

The ProofMark Transient Key SM 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
- No secrets to protect, since private keys are destroyed
- Cryptographically strong chain of events which is virtually impossible to alter after the fact
- 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

Issues Addressed by ProofMark:

- ↓ Archival and eDiscovery Authentication (e.g. under Symantec Enterprise Vault)
- ↓ Trade Order Management Systems Integrity.
- ↓ Mitigating Mutual Fund Late Trading
- ↓ Options Backdating Financial Reporting and SOX Compliance

ProofMark System Benefits:

- ↓ Provides irrefutable proof of records authenticity that will stand up in a court of law, resulting in lower legal and forensics costs.
- ↓ Enables compliance with national standards and specifications including the ANSI X9.95-2005 specification for Trusted Time Stamp Management and Security, HIPAA and Sarbanes-Oxley.
- ↓ Virtually eliminates archive integrity threats from insiders, because changes can be immediately detected. No third-party dependency on expensive external Certification Authorities.

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