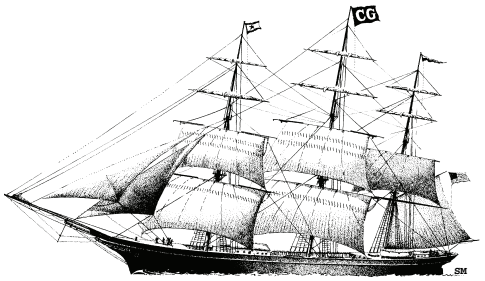
THE CLIPPER GROUP
Navigator™



Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2007076 July 17, 2007

Assuring the Validity of Data with *AbsoluteProof*

Analyst: Anne MacFarland

Management Summary

Electronic data is inherently more mutable than stuff written in ink. If you have created something of value, getting certifiable proof of *what you have done* and *when you did, it* can be of prime importance. For some ideas, a copyright is an appropriate vehicle, but getting a copyright takes years and costs a lot. For more prosaic creations, something simpler is needed. For businesses, the need to document corporate actions can extend across document/records management, financial transactions, internal accounting, and even to documentation of provided services, depending on the responsibilities involved and the risk of contention or litigation that the business faces.

There is also an increasing need to prove that electronic images have not been altered. In news footage, there is a tradition of trying to make things dramatic – but alteration crosses the line between fact and fiction. In scientific imaging, playing with the contrast to better invalidate one variable may invalidate its use for the illustration of other variables. More generally, image alteration can range from innocent touch-ups of blemishes to outright fraud. It is good to have a provable original image.

A company called Surety, LLC, based in Reston, VA, can provide the trusted timestamp to make the proof stand up in court. As an independent third party, its proof is not tainted by affiliation, as enterprise IT system logs might be perceived. As a digital notary, they provide a service that will be of interest to any organization that wishes to preserve its intellectual property or wants a defensible system of record when confronted by litigation. Surety's *AbsoluteProof* timestamp can be attached to any binary object without touching the content or changing the record. Its value is documentation of the creation of intellectual property, contracts, and other important documents and the assurance that they have not been changed in any way. *AbsoluteProof* is not a digital signature or certificate system. It gives a provable timestamp that digital signatures do not. It is not part of an encryption scheme, like digital certificates. It is simply an authentication system, independent of an organization, like a notary, that retains its power and value for years.

Use of Surety's *AbsoluteProof* can reduce risk and prevent litigation. It can be a simple way to document what the enterprise needs documented. If you live in a world of *trust – but verify*, you will want to know more. To do so, please read on.

IN THIS ISSUE

The Role of a Notary

Since ancient Rome, a notary was a person who could check the identity of signatories and attest that their signatures on a document were valid. The notary would affix a stamp and record the signatories in a register. Such notary authentication was important in the Dark Ages when other forms of law were noticeably lacking, for claims had to be verifiable as to who signed them, and when, and where. Most notaries cannot attest documents with any blanks – so the notarization also authenticated the contents.

In an electronic age, the need for some kind of electronic services has expanded. The chain of custody of a physical document has points of peril, but the chain of custody of an electronic document is many times more perilous. In many cases, you want the document to be disseminated – and even changed. You just also want the original and when it was created to be provable beyond a doubt. This ability is important to life science, manufacturing, and other organizations as well as to writers, artists, researchers, scientists and anyone whose reputation rests on a litany of any provable acts of creation.

Surety *AbsoluteProof*

Surety, LLC, has been in business 12 years. Its notary service has been accepted in courts. Its platform partners and resellers include well-known names like Hitachi Data Systems, Open Text, and FileNet, as well as more specialized partners like Symyx Systems and KineMatik.

The *AbsoluteProof* Server that seals a document or image is installed at a customer site in three ways.

- It can be **installed on a desktop**, say that of a researcher, as a tool. The pricing for this method is $250/seat/year for unlimited use. This is attractive to small organizations with a limited number of users who need notary services.
- It can be **delivered as a software development kit** (SDK), which allows an IT department to integrate it into the relevant applications. The Writers Guild of America has used this approach. The Software Development Kit costs $1,000 and the charge is waived in favor of a per-use model, in many cases.
- The Surety system can be delivered as a **modular software service** that makes sealing documents a part of a workflow. Surety's partners and resellers do the integration. In this case, the pricing is a tiered transaction model, with a discount for higher volumes of use.

When the sealing action is invoked, a hash of the electronic record is sent to Surety via secure HTTPs. The small (788 bytes) hash is entered into the *AbsoluteProof Database*[1]. Using two absolute clocks[2], Surety documents when the hash was received in the *AbsoluteProof Universal Registry*, and produces a timestamp.

This action kicks out a token, the *Surety Integrity Seal*. It contains the hash, timestamp, and location of the entry in the Database. The Surety Integrity Seal is sent back to the source of the invocation, and kept with the document that is sealed, or in a database, as the customer wishes.

Once a day, Surety concatenates the hash chain of all the hashes it has received, creating a summary value. This is published every Wednesday in the *New York Times Commercial Section* (a widely used public record). This patented *widely-witnessed* process becomes an independent path of verification of the timestamp.

Surety, like Adobe, offers an *Integrity Viewer* via free download. Lawyers, regulators, and other interested parties may use this to validate Surety Integrity Seals.

Surety's Seals are both ANSI and ISO compliant. Its AbsoluteProof service uses a dual hash for its authentication. Currently this is *SHAH256* and *RIPEMD-160*. Over

[1] The database is two mirrored databases in a highly secure datacenter. Surety does not store the document in its database – it only stores the hash. Enterprise security is not compromised. Surety does not amass a huge database, but instead provides a highly scalable solution that keeps costs down for customers.

[2] A corrupt institution can backdate timestamps. Using an independent third party, and independently derived time gives the seal great validity.

the years, the hashes will change to keep up with advances in security[3].

Surety's AbsoluteProof is a service. If a customer is uncomfortable with having the proof held by an outside party, Surety will augment the Seal with the summary value published in the New York Times. With this amendment, customers do not have to authenticate through a third party, and do not have to worry about the longevity of Surety.

How This Differs from Other Approaches

- Surety's approach is independent of an enterprise's IT systems. Five years in the future, when you are in litigation over a piece of intellectual property, a comparison of the customer's Seal with that held by Surety, if they are the same, shows that the document in question was created at a certain time, and has not changed since then. As a third party is involved, it has greater legal weight than a timestamp created by a customer's IT system.
- AbsoluteProof differs from a digital signature process. Digital signatures simulate the intent of a written signature, and have legal significance. They can authenticate the sources of a message and that it has not been altered in transmission, but they do not inherently provide proof of *when* the document was sent or signed.
- The AbsoluteProof process uses cryptography, but it does not encrypt a document. It simply assures its validity in everyday and widespread use. People can also use PKI[4] encryption if they want – but that is an independent process.

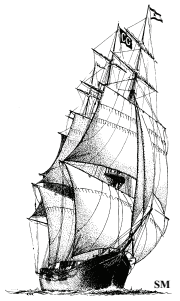
Digital signatures and timestamps are separate but complementary technologies. If you only need to assure the *who,* digital signatures work. If you only need the *when*, timestamps will suffice. However, when you need both *who* and *when*, both technologies are required.

Like the notaries that validate the signing of contracts – not reading the contracts, but by stamping and/or embossing the paper, Surety provides a notary service. They offer proof that something was done, and that it was done at a certain time. Their value lies in organizational documentation, in intellectual property management, and in risk and litigation avoidance.

Conclusion

Organizations that benefit from the ease of communications and immediacy of collaboration of IT systems must also be aware of the limitations of the corporate documentation that IT systems afford. They may have a need for more explicit, disciplined forms of organizational documentation. Enterprises now facing more forms of regulatory compliance may find the need to make certain kinds of routine actions provable and incorruptible. Surety offers a way to take a variety of enterprise risks off the table, while providing the comfort of provability to those who capture and create valuable documents and files.

Take a moment to think of how your enterprise could benefit from electronic notary services. The benefits are often a matter of risk avoidance – but, for many, the biggest benefit may be peace of mind.



[3] The AbsoluteProof service includes a Renewal option should current hashes be compromised in the future (as past ones have). New Seals will be linked to the old tokens and a time value issued to provide a continuous and uncontestable chain of proof.

[4] Public Key Infrastructures are used as part of encryption. There are three algorithms in a Public Key Infrastructure – the first generates the key pair, the second produces a "signature", and the third certifies the "signature" at the other end. A separate authority is required to keep the association of users with keys secure. The method is similar to Surety's, but the purpose is encryption, not documentation.

About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

Anne MacFarland **is Director of Data Strategies and Information Solutions for The Clipper Group.** Ms. MacFarland specializes in strategic business solutions offered by enterprise systems, software, and storage vendors, in trends in enterprise systems and networks, and in explaining these trends and the underlying technologies in simple business terms. She joined The Clipper Group after a long career in library systems, business archives, consulting, research, and freelance writing. Ms. MacFarland earned a Bachelor of Arts degree from Cornell University, where she was a College Scholar, and a Masters of Library Science from Southern Connecticut State University.

- ***Reach Anne MacFarland via e-mail at Anne.MacFarland@clipper.com or at 781-235-0085 Ext. 128. (Please dial "128" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group Captain's Log**, **The Clipper Group Voyager**, **Clipper Notes**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and *"teraproductivity"* are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.