



## SURETY PATENTS AND SEMINAL RESEARCH

### METHOD FOR SECURE TIME-STAMPING OF DIGITAL DOCUMENTS

**U.S. Patent No. 5,136,647, issued August 4, 1992.**

**U.S. Patent Re. 34,954, reissued May 30, 1995.**

The initial patent issue covers a variety of fundamental technology and algorithmic components of digital time-stamping. More specifically, the claims cover:

- The linking of timestamp requests in a sequence
- The “random-witness” method that uses the document being time-stamped to pseudo-randomly choose time-stamping witnesses

The subsequent reissue of the patent added some additional claims which were supported by the original specification. The additional claims cover:

- The use of a single hash value to represent a timestamp request for an “accumulation” or “collection” of digital documents
- A time-stamping process that does not explicitly require the use of a digital signature

### DIGITAL DOCUMENT TIME-STAMPING WITH CATENATE CERTIFICATE

**U.S. Patent No. 5,136,646, issued August 4, 1992.**

The claims of this patent cover the use of one-way hash functions to form an unalterable linked list of timestamp certificates. This makes it effectively impossible for anyone, including the time-stamping service, to retrospectively fake part of the chain. In the current implementation of Surety’s Digital Notary<sup>®</sup> Service, this linking method is how the sequence of “root hash values” are linked to form the chain of “super hash values.”

### METHOD OF EXTENDING THE VALIDITY OF A CRYPTOGRAPHIC CERTIFICATE

**U.S. Patent No. 5,373,561, issued December 13, 1994.**

This patent covers the use of time-stamping to renew or to extend the validity of cryptographic certifications of authenticity such as timestamp certificates and digital signatures. This use enables a digitally signed record to retain its validity even if the signer’s private key is later compromised, or the key’s digital certificate has expired. As long as the timestamp for the record indicates that it was signed prior to the compromise of the key, or during the digital certificate’s validity period, the signature is still trustworthy.

This patent also covers the parallel use of multiple hash functions in a time-stamping system. Surety currently uses a combination of RSA’s RIPEMD-160 hash function and the NIST’s Secure Hash Algorithm SHA-256.

### DIGITAL DOCUMENT AUTHENTICATION SYSTEM

**U.S. Patent No. 5,781,629, issued July 14, 1998.**

This patent covers Surety’s current method for assigning SureID numbers to documents. A SureID number is a short, unique, cryptographically secure identifier produced for any digital document, record, or message that is notarized by the Surety Digital Notary Service. The patent also covers several extensions to the use of SureID numbers that Surety has not yet implemented, and provides additional claim coverage to protect Surety’s time-stamping methods.

### METHOD AND APPARATUS FOR SELF-AUTHENTICATING DIGITAL RECORDS

#### Patent Pending

This patent covers a method of creating a self-authenticating document by combining a signed document with evidence that the corresponding certificate was valid at the time of signing (e.g., CRL, OCSP response), and applying at least one trusted timestamp to the aggregate. This method produces a self-contained signed document with a signature that can rely upon even if a corresponding certificate is subsequently revoked or expired.