



Digital Signatures Are Not Enough

By Jeff Stapleton and Steven Tepler

jeff.stapleton@innove-us.com; stepler@timecertain.com

Information Assurance History

Pre-1950s virtually all information was paper-based. In the 1950s and 1960s data entry operators using computers converted the same paper-based information to digitally encoded electronic data. In the 1970s and into the 1980s users began to generate digital data directly using software such as spreadsheets and word processors. This trend has continued such that today virtually all information now originates as digital data and ironically paper-based documents are generated from digital data.

Historically, paper was the authoritative record with intrinsic physical and chemical ink characteristics that provided an acceptable degree of integrity. Already today, and traversing into the future, digital electronic data has no such characteristics; data bits can be duplicated, copied, manipulated, and counterfeited at will. Digital signatures can provide cryptographically valid data integrity and authenticity; however without a trusted time source, the integrity for all practical purposes can only be relied upon by the original signer.

Digital Signature Fundamentals

Recall that a digital signature is a cryptographic value generated by an asymmetric private key and validated by the corresponding public key certificate. Figure 1 shows the basic processing steps. The signer entity inputs the message (1) into to a HASH algorithm (2) which produces a hash value (3); the hash value and the private key are input to a SIGN algorithm (4) which generates the signature (5). The message (1) and signature (5) are sent by the signer to a relying party. The relying party inputs the message (6) into the same HASH algorithm (7) which produces the same hash value (8); inputs the signature (9), the hash value (7) and the public key from the certificate into the VERIFY algorithm (10) to validate the signature with the message. If either the message (1) or the signature (5) is modified in transit, the relying party

knows that the signature will not validate. However, prior to the relying party trusting the public key in the certificate, the relying party must validate the certificate.

Figure 2 shows the basic validation process. The relying party presumably knows that the signer is the subject of the certificate, checks the issuer name to determine the subject certificate was issued by the Sub CA, and checks that issuer name to determine the Sub CA certificate was issued by the Root CA. The relying party then verifies the Root CA self-signed certificate using the Root CA public key; verifies the Sub CA certificate using the Root CA public key, and ultimately verifies the subject certificate using the Sub CA public key.

The validation of the subject certificate and the verification of the message digital signature provide a degree of authenticity to the relying party but do not necessarily impart data integrity. Because the message content and the system clock are both under the control of the signer, there is a risk that the signer can reset the system clock, change the message content, and sign the modified message. The relying party would then be unable to distinguish between the original message and the modified message, as both display the same time stamp and valid digital signatures. Genuine data integrity requires a cryptographic-based integrity mechanism (e.g. digital signature) and an independent verifiable time stamp.

Trusted Time Stamps

The American National Standard X9.95-2005 Trusted Time Stamps describes the roles, responsibilities and requirements for users of trusted time stamps—time source entities, time stamp authorities, time stamp requestors, and time stamp relying parties. The standard also specifies data objects, processing flows, error handling, and message formats as well as defines technology methods for digital signature, message authentication code, linked-token and transient key. In addition, the standard offers a comprehensive set of time stamp control objectives to validate a trusted time stamp system for use by a professional audit practitioner. It also provides sample time stamp policy and time stamp practice statements. The benefit of trusted time stamp technology is in its ability to verify managed data integrity against a reliable time source provable to any third party.

Hash-Based Time Stamp Tokens

Figure 3 shows the time source entities for a Time Stamp Authority (TSA); and the transaction schema for the issuance of a Time Stamp Token (TST) by a TSA to a Requestor (R). The TSA system clock is calibrated to a regional master clock or a national measurement institute (NMI) whose clock is calibrated to the international time authority (ITA) Bureau International des Poids et Mesures (BIPM) located in France. In the United States, the national measurement institutes (NMI) are the National Institute of Standards and Technology (NIST) and the United States Naval Observatory (USNO).

The requestor (R) inputs the data into a HASH algorithm which produces a hash value; the hash value is sent to the RSA in a Request message. The TSA returns a Time Stamp Token (TST) to the requestor, consisting of the (i) original hash value, (ii) a timestamp from the TSA trusted clock, and (iii) a digital signature generated by the TSA using its private key. A relying party, having received the original data and the TST from the Requestor (R), can verify the TSA digital signature using the TSA public key certificate. The relying party also regenerates a hash value from the

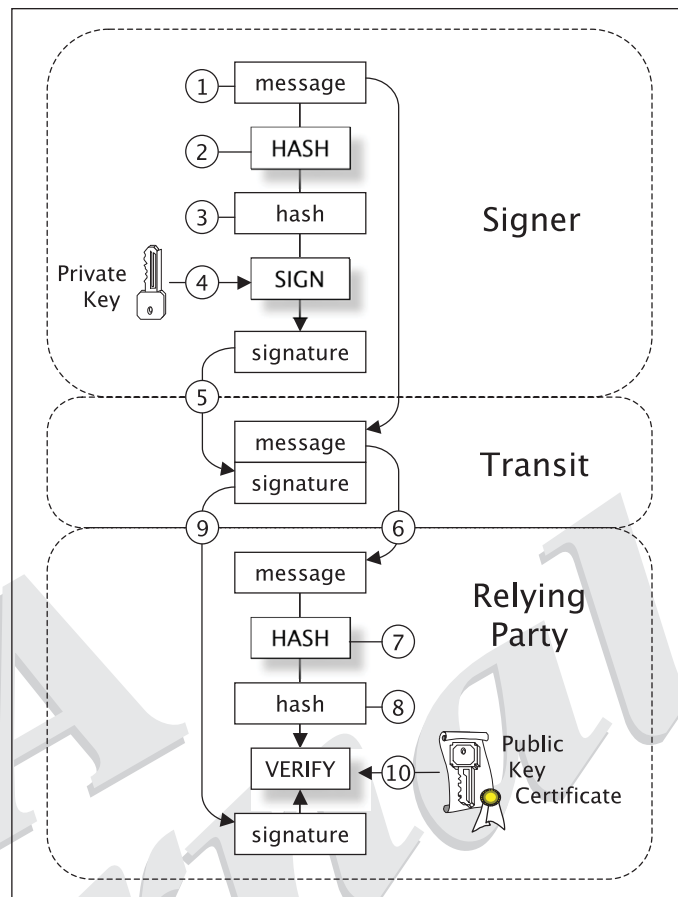


Figure 1: The basic processing steps

original data and validates that it matches the hash value in the TST. The validated TST provides a high degree of assurance of the data integrity at the time indicated per the TST timestamp.

Signature-Based Time Stamp Tokens

The trusted time stamp method described in Figure 3 can be combined with a requestor's digital signature to provide an even higher degree of assurance of the data integrity and authenticity. Figure 4 shows the same time source entities and TSA with the requestor submitting a digital signature of the data in the Request message instead of a hash. The TSA generates and returns the TST to the Requestor as normal, containing the digital signature. In this case, the TSA is not cognizant and does not need to know whether a hash or digital signature was sent in the Request message, and incurs no liability of the Requestor's digital signature.

The inclusion of the Requestor digital signature (in lieu of the plain hash value) in the TST provides the Relying Party with a higher degree of assurance of the data integrity and that the data was digitally signed by the Requestor at the time indicated per the TST timestamp. The risk scenario described above is not theory, and in fact has several real-world occurrences.

Real-World Occurrences

Enron

Mr. Fastow, the Chief Financial Officer and other members of the Enron executive team made it a habit to engage in time-based data

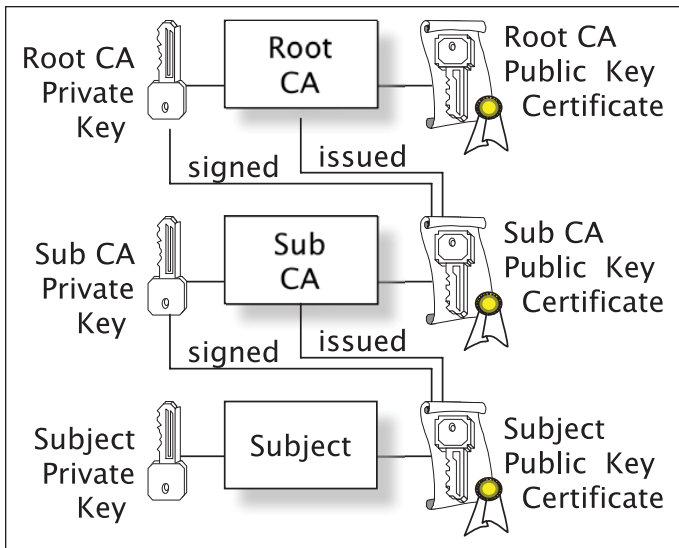


Figure 2: The basic validation process

manipulation, i.e., to alter or change financial data to suit whatever it was they wanted the investing public, or governmental authorities to know, or not know. Mr. Fastow has pleaded guilty and is now a guest of the federal government.

Nancy Temple was the Arthur Andersen attorney assigned to the **Enron** matter. When asked by a Congressional committee whether any data had ever been altered or changed after the fact, she responded that no final reports were ever altered or changed. The clarity of her response (and the admission by implication that everything prior to those final papers was altered by time-based data manipulation) earned her a disbarment from the practice of law.

Rite Aid

The CEO and the CFO of the publicly traded **Rite Aid** company backdated compensation grant letters to enrich themselves by millions of dollars. They then attempted to remove any evidence of their wrongdoing by dumping the computer they used to backdate the documents into the Atlantic Ocean. These gentlemen are now guests of the federal government.

NextCard

The now defunct **NextCard** was the largest issuer of Internet MasterCard and Visa credit cards. Executives of this former high-flying public company fraudulently and illegally re-characterized loan losses, thereby reducing the amount of cash reserves required. Assisting in no small way in this billion-dollar flameout, auditors from Ernst & Young perpetuated the company's fraud by backdating their work papers and their final reports to conform to the fraudulent representations by company executives. These auditors are also currently guests of the federal government. The SEC attorney investigating this matter lamented that the real crime here was that there was no way to ascertain or recover the real, or the true data, because of the time-based data manipulation of these insiders.

Autotote

A senior trusted programmer for **Autotote**, the largest electronic wagering organization in the United States, back-dated data to create a 6-million-dollar winning ticket in the Maryland Breeder's Cup race. This gentleman is now a guest of the state.

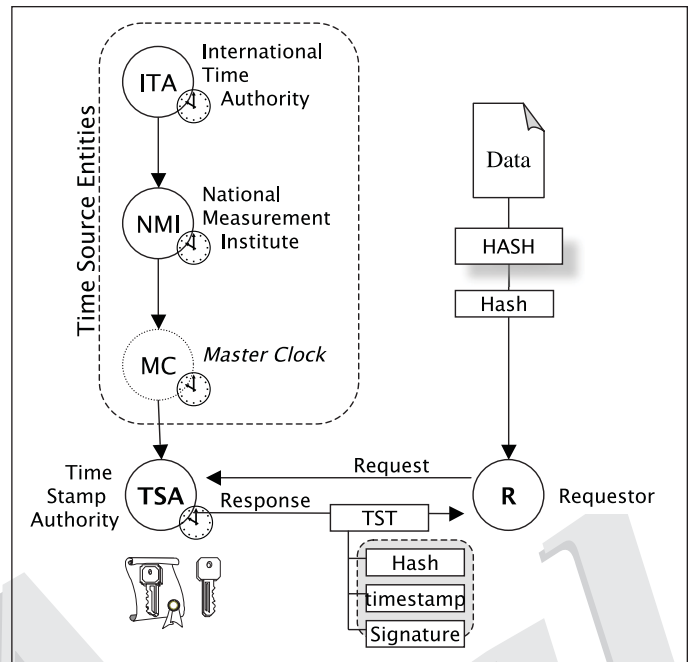


Figure 3: TST with Digital Signature

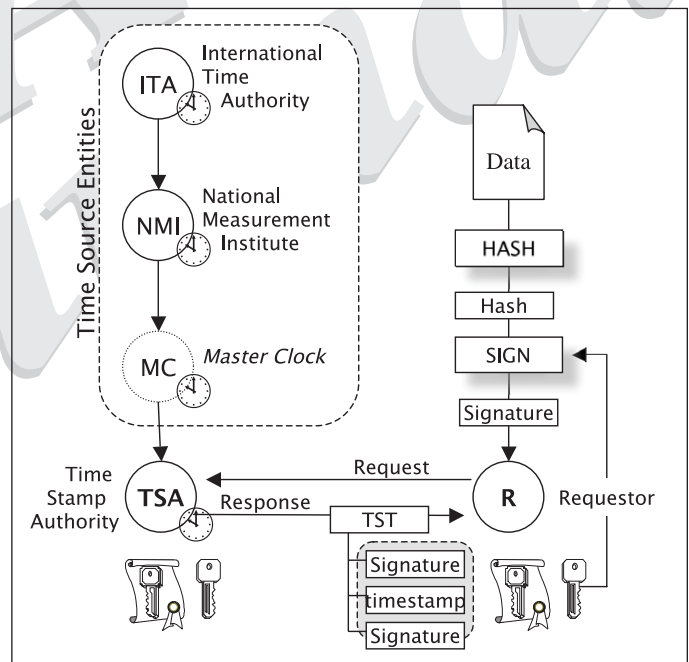


Figure 4: TST with Digital Signature with the requestor submitting a digital signature of the data in the Request message instead of a hash

Sirena

The Securities and Exchange Commission fined publicly traded **Sirena** Corporation for holding the quarter open for days after the end of that quarter in order to squeeze additional revenues to meet analysts' projections. Sirena eventually declared bankruptcy.

Parmalat


In this 18-billion-dollar 2003 bankruptcy, the entire CxO level and family of the multi-national **Parmalat** conglomerate engaged in time-based data manipulation by creating an authentic-appearing confirmation by Bank of America, on Bank of America Letterhead, and signed by a Bank of America Vice President, to the effect that there existed an offshore bank

account holding 5 billion euro. In reality both the funds and the account were non-existent, and the alleged Bank of America letter used by the Company to raise billions in the public credit market was pieced together by the company executives using a scanner and Adobe Photoshop, from three totally unrelated sources. The signature of the Bank of America VP was from the information technology department. There are currently at least three lawsuits, including two class actions, pending in various courts around the world.

Adelphia

Once one of the largest cable providers in the United States, the top executives of **Adelphia** engaged in time-based data manipulation to hide the theft of more than 400 million dollars from the company. Adelphia subsequently entered bankruptcy, its top executives were tried (and two convicted), and the company is now being acquired by one of its competitors.

Conclusion

In each of these examples, trusted time stamp technology would have provided data integrity assurance of financial reports, grant letters, loan reports, securities transactions, financial audit reports, software releases, letters of credit, and financial transactions. 

Jeff Stapleton is the Chief Cryptography Architect with Innové LLC (www.innové-us.com), an emerging company focused systems engineering and technical risk management services and solutions primarily for the military.

Steven W. Tepler is an inventor, attorney, as well as the Chairman and founder of TimeCertain, LLC.