



# The Digital Signature Paradox

Jeff Stapleton, Paul Doyle, Steven Teppler, Esq.

**Abstract** — “Paradox” is a term often associated with Hollywood’s fanciful time travel; however in the real world a time paradox does, in fact, exist. The system clock is the immediate source of time for any computer, and is the sole source for a time stamp determining when a document was created, modified and printed; or more interestingly when a digital signature was generated. Fraud has already been perpetrated by turning back system clocks, leading to the falsification of information for which individuals have been disbarred or incarcerated. The application of a digital signature would not have resolved these issues; that is because digital signatures are time-insensitive. However, an independent clock source providing a trusted time stamp would and can circumvent individuals taking such illegal liberties. This paper posits that data integrity needs to be redefined within the context of a time-sensitive mechanism.



## Table of Contents

<b>I. Introduction</b>	<b>3</b>
A. Asymmetric Cryptography	3
B. Digital Signatures	3
C. Time Stamping	5
<b>II. Paradox</b>	<b>7</b>
A. Time-Insensitive Digital Signatures	7
B. Trusted Time Stamp	8
C. X9.95 Standard	9
<b>III. Consequences of Time-Based Data Manipulation</b>	<b>10</b>
A. Enron (CFO)	10
B. Rite-Aid (CEO, CFO)	10
C. NextCard (Auditors)	10
D. Autotote (Programmers)	10
E. Sirena Corp (CEO)	10
F. Parmalat (CEO, CFO, and Family)	10
G. Adelphia Communications (executives)	11
<b>IV. Conclusion</b>	<b>11</b>
<b>V. References</b>	<b>12</b>



## I. Introduction

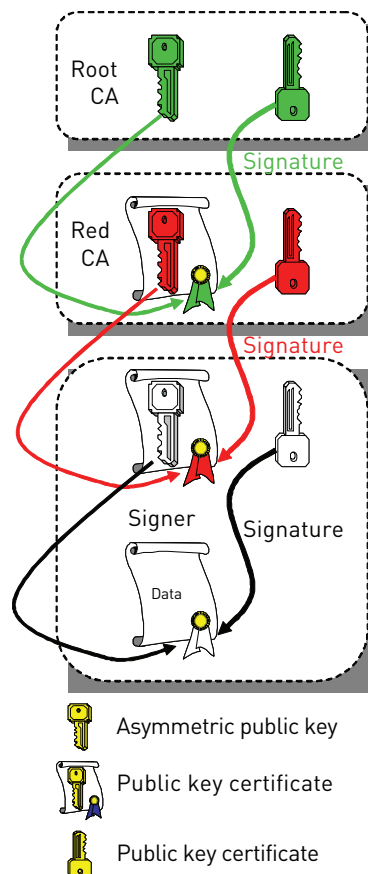
### A. Asymmetric Cryptography

Public key cryptography is the security discipline employing asymmetric cryptography that enables key establishment of symmetric keys and digital signatures. The intrinsic modularity of asymmetric cryptographic algorithms limits their applicability to relatively short data lengths such that they are typically used to establish symmetric cryptographic keys versus operating on the data itself. The established symmetric keys are then used in streaming or block ciphers with practically unlimited data lengths. Key establishment algorithms come in two flavors—key agreement and key transport [X9.44]:

- Key agreement is a key establishment protocol whose secret key is a function of information contributed by two or more participants, so that no party can predetermine the value of the key.
- Key transport is a key establishment protocol under which the secret key is determined by the initiating party.

### B. Digital Signatures

With regard to digital signatures, a hashing function is applied to very long data strings to produce a hash value; and the asymmetric private is applied to the hash value to generate a digital signature. The digital signature can be verified by a relying party using the corresponding asymmetric public key. In a classical public key infrastructure the identity of the signer is provided to the relying party via a public key certificate [X.509] issued by a certification authority (CA). The CA's digital signature on the signer's certificate cryptographically binds the signer's identity to the public key. Similarly, the CA's public key may likewise be encapsulated in another certificate issued by another CA such that a chain of certificates may exist; leading to a root CA. The underlying assumption is that the relying party has and trusts one or more of the certification authorities in the certificate chain.

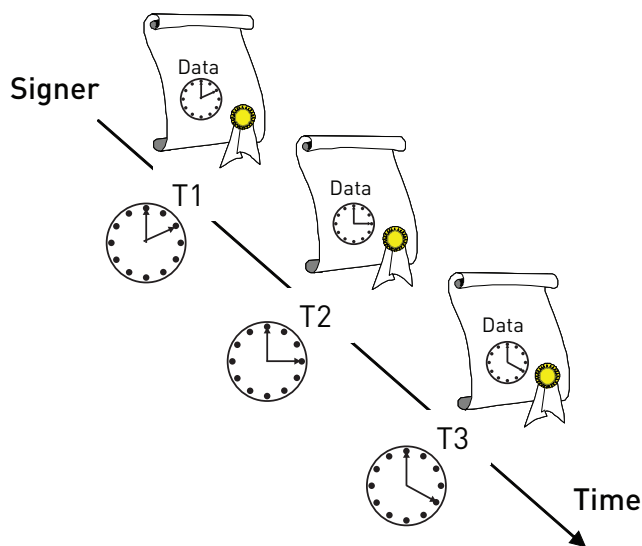


**Figure 1 – Certificate Chain**

As shown in *Figure 1 – Certificate Chain*, the signer generates a digital signature on data. The relying party checks the signer's white certificate and determines that it was issued by the Red CA; the relying party checks the Red CA's certificate and determines that it was issued by the green Root CA. Assuming that the relying party has a trusted copy of the green Root CA's public key, the relying party verifies the green signature on the Red CA's certificate and thus can trust the Red CA public key; the relying party verifies the red signature on the signer's certificate and thus can trust the signer's white public key; the relying party can finally verify the signer's signature on the data.

### C. Time Stamping

Most networks provide a system time such that data can be time stamped with the year, month, day, hour, minute, and second. *Figure 2 – System Time Stamps* shows the relationship between the system clock and the time stamp associated with each piece of signed data.



**Figure 2 – System Time Stamps**

Presumably the time stamp indicates a sequence to the relying party and implies when the digital signatures were generated. However, note that the system generated time stamp *is not independent of the data generation, or the digital signature generation processes.*

The system clock, via the local or wide area network, may be synchronized to a national measurement institute whose clock is calibrated to the international time authority Bureau International des Poids et Mesures (BIPM) located in France. In the United States, the recognized national measurement institutes are the National Institute of Standards and Technology (NIST) and the United States Naval Observatory (USNO).

Figure 3 – US National Measurement Institutes shows the relationship of the various NIST timing services such as the:

- Internet Time Service (ITS),
- Automated Computer Time Service (ACTS),
- Frequency Measurement Analysis Service (FMAS); and the
- Global Positioning System (GPS) operated by the USNO [NIST].

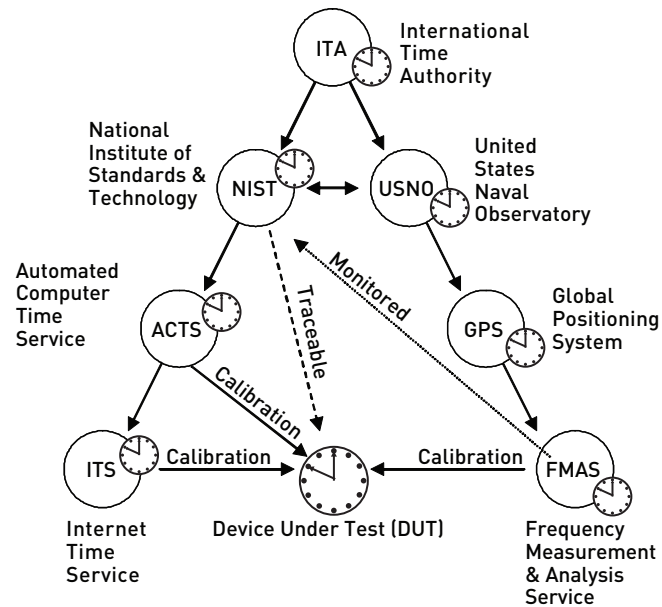


Figure 3 – US National Measurement Institutes

## II. Paradox

### A. Time-Insensitive Digital Signatures

Figure 4 – Digital Signature Paradox below shows the same sequence of signed data; however the system clock has been reset such that the same time stamp is generated at three different times (T1, T2, and T3) for different versions of the same data. The time paradox is that a relying party now has three versions of the same data with the same time stamp; and despite the presence of a legitimate digital signature the relying party can no longer have confidence in the data. Thus digital signatures are time-insensitive.

The relying party has no practical method to distinguish between the three data versions, has no method to prioritize the data versions and has no option but to distrust all three versions. In order for the relying party to distinguish between the data versions and continue to trust the digital signatures, the signer needs to implement a verifiable mechanism such that the time stamp generation is independent of the signature generation. This method is referred to as a trusted time stamp.

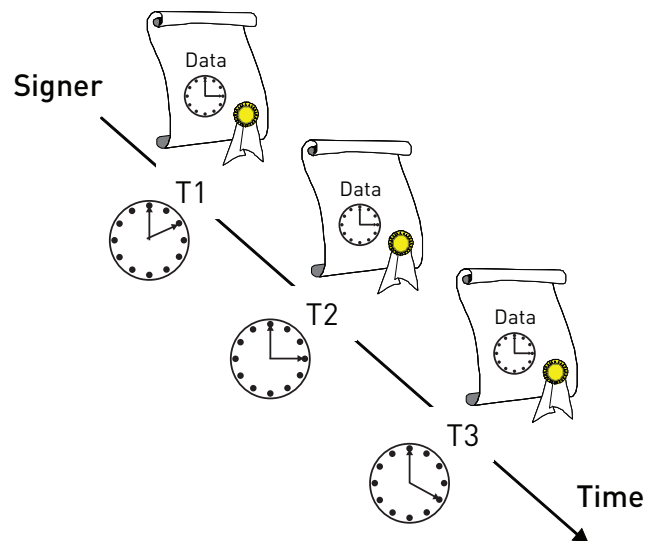


Figure 4 – Digital Signature Paradox

## B. Trusted Time Stamp

In a trusted time stamp scheme, there are five entities: time source entity, time stamp authority, requestor, verifier, and relying party. The relying party can be the requestor or any other third party. The time stamp authority (TSA) calibrates its clock with an upstream time source entity such as Master Clock (MC) or directly with a national measurement institute. The TSA provides a trusted time stamp token to the requestor. The time stamp token can be verified by a third party verifier. *Figure 5 – Trusted Time Stamp* shows the relationship between the time source entities, the TSA, and the requestor.

The requestor generates a digital signature by hashing known data and applying its asymmetric private key to the hash. The digital signature is presented to the TSA as a request for a time stamp token. Note that the TSA only knows the digital signature, not the original source data, and therefore has no liability as to the data content. The TSA appends a time stamp to the requestor's hash and binds them together with a cryptographic method, such as a digital signature [X9.95]. The hash, the time stamp and the crypto are the essential elements of the time stamp token that the TSA returns to the requestor. The requestor can then provide the original data, the requestor's digital signature, and the time stamp token to a relying party.

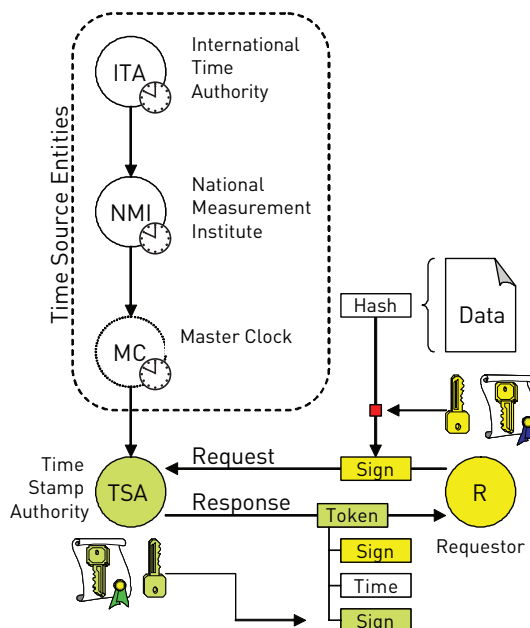
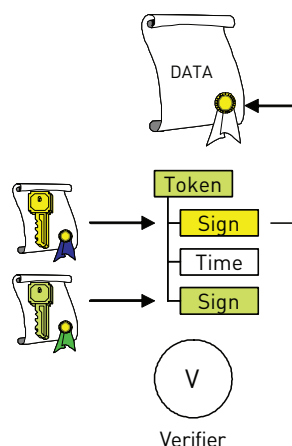


Figure 5 – Trusted Time Stamp



*Figure 6 – Verification* shows how the relying party can then make use of a verification service who (i) verifies that the hash in the time stamp token matches the data, (ii) verifies the TSA's crypto binding, and (iii) verifies the requestor's digital signature — this provides non-reputable evidence of who signed the data (authentication), when it was signed (timeliness) and what data was signed (integrity) provable to an independent third party.



**Figure 6 – Verification**

The definition of data integrity — “a property whereby data has not been altered or destroyed” — must therefore be expanded to embrace time-sensitive mechanisms such as trusted time stamps. A better definition might then be “the continuity of data at a provable point in time.” With this definition a relying party can verify that data integrity is currently contiguous from a previous point in time.

### C. X9.95 Standard

The American National Standard X9.95-2005 Trusted Time Stamps was developed based on RFC 3161 [TSP] and the ISO/IEC 18014 standards [ISO], but goes much further in its analysis and offerings. X9.95 defines time stamp schemes that provide a high assurance level of data integrity and non-repudiation not achievable by digital signatures alone; suitable for regulatory compliance. The standard defines roles, responsibilities, and the management and security requirements for the time source entity, the time stamp authority, the requestor, and the verifier. The standard specifies data objects; message protocol; and trusted time stamp methods, including the digital signature, MAC, linked token, linked and signature, and transient key methods. The standard also provides sample time stamp policy and practice statements along with evaluation compliance criteria suitable for use by a professional practitioner.



### III. Consequences of Time-Based Data Manipulation

#### A. Enron (CFO)

Mr. Fastow, the Chief Financial Officer of Enron, and other members of his executive team made it a habit to engage in time-based data manipulation, i.e., altering or changing financial data to suit whatever it was they wanted the investing public, or governmental authorities, to know or not know. Mr. Fastow pleaded guilty and is now a guest of the federal government.

#### B. Rite-Aid (CEO, CFO)

The CEO and the CFO of this publicly-traded 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.

#### C. NextCard (Auditors)

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.

#### D. Autotote (Programmers)

A senior trusted-insider programmer for 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.

#### E. Sirena Corp (CEO)

The Securities and Exchange Commission fined publicly traded Sirena Corp. 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.

#### F. Parmalat (CEO, CFO, and Family)

In this 18 billion dollar 2003 bankruptcy, the entire CxO level of this multi-national 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 on account. 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.

#### **G. Adelfia Communications (executives)**

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

### **IV. Conclusion**

So — is time-based data manipulation really that much of a problem? It most certainly is: a multi-billion dollar problem, as the case studies above make clear. When given the opportunity, a certain percentage of trusted insiders will always abuse their authority to manipulate records to their advantage. Digital signature-based schemes cannot adequately address this problem, but trusted timestamp technologies might be just what the doctor ordered: a practical, inexpensive and technically robust solution.

## V. References

[X9.44] X9.44 (draft) *Public Key Cryptography for the Financial Services Industry – Key Establishment Using Integer Factorization Cryptography*, Accredited Standards Committee X9, [www.x9.org](http://www.x9.org), October 2003

[X.509] ISO/IEC International Standard 9594-8 | ITUT Recommendation X.509 (1997), Information Technology – Open Systems Interconnections – The Directory: Authentication Framework

[NIST] National Institute of Standards and Technology, Physics Laboratory – Time and Frequency Division, <http://www.boulder.nist.gov/timefreq/index.html>

[X9.95] American National Standard X9.95-2005 Trusted Time Stamps, Accredited Standards Committee X9, [www.x9.org](http://www.x9.org), March 2005

[TPS] Request for Comments (RFC) 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), Internet Engineering Task Force (IETF), C. Adams, P. Cain, D. Pinkas, R. Zuccherato, August 2001

[ISO] ISO/IEC 18014 Information Technology – Security Techniques – Time Stamping Services, ISO/IEC Joint Technical Committee One (JTC1), 2003

*Digital Signature Paradox*, J. Stapleton, P. Doyle, S. Tepler Esq., Proceedings of the 2005 6th IEEE, Workshop on Information Assurance and Security, United States Military Academy, West Point, NY

*Digital Signatures are Not Enough*, J. Stapleton, S. Tepler Esq, THE ISSA JOURNAL , January 2006



ProofSpace  
 900 Clancy Ave NE  
 Grand Rapids, MI 49503  
 (312) 933.8823