

ABSTRACT

This paper identifies the developmental, technical and operational differences between the American National Standard X9.95-2005 Trusted Time Stamp, the International Standard ISO 18014 and the IETF specification RFC 3161; and provides guidance on how to use X9.95 as a Time Source Entity, a Time Stamp Authority, a Time Stamp Requestor or a Time Stamp Verifier. Trusted time stamping methods are the only cryptography based technology that provides data integrity verifiably to a reliable point in time.

1	Introduction.....	1
2	Organizations	1
2.1	ISO.....	1
2.2	JTC1	2
2.3	ANSI	2
2.4	ASC X9.....	2
2.5	IETF	2
3	Roles and Responsibilities.....	3
3.1	Time Source Entity	3
3.2	Time Stamp Authority	3
3.3	Time Stamp Requestor	3
3.4	Time Stamp Verifier	3
4	Requirements	3
5	Time Stamp Methods	3
5.1	Digital Signature Method.....	3
5.2	MAC Method.....	4
5.3	Linked Token Method	4
5.4	Transient Key Method.....	4
5.5	Archive Method.....	4
6	Time Stamp Objects	4
7	Time Stamp Message Flows	4
8	Audit Control Objectives	4
9	Policy and Practices	5
10	Conclusions	5

1 INTRODUCTION

Data integrity mechanisms are not reliable unless they are (i) verifiable to a point in time and (ii) the time source controls are independent of the data content provider. Digital signatures¹ and other mechanisms do not provide time control independence. Trusted time stamping methods are the only cryptography based technology that provides data integrity verifiably to a reliable point in time.

The American National Standard X9.95-2005 Trusted Time Stamp was developed by the X9F4 Cryptographic Protocol and Application Security working group, which operates under the auspices of the Accredited Standards Committee X9 Inc. X9.95

¹ Digital Signature Paradox, 6th IEEE Information Assurance Workshop, Jeff Stapleton, Paul Doyle, Steven Tepler Esquire, June 2005

provides a rich set of technical and operational requirements, methods and control objectives not afforded by other standards. This paper identifies the differences between X9.95 and the other standards and provides guidance on how to use X9.95. The discussions presented in this paper are summarized in Table 2 – Standards Comparison.

2 ORGANIZATIONS

National bodies such as the United States use their own domestic standards when an international (ISO) standard is either not available or it conflicts with national practices. In many cases, a national standard is developed for a specific industry, such as financial services, when an existing standard is either too broad or incomplete for use in such an industry. This section provides an overview of the related organizations that develop or accredit standards developers.

The decision to rely upon a standard or a proprietary solution is a challenge to many businesses. The reliability of proprietary solutions is based upon the vendor’s credibility, experience and stability. Standards are developed and peer reviewed by experts from the industrial, technical and business sectors; and a standard will outlast any one vendor.

The decision to rely upon an ISO or a domestic standard is often another challenge. The scope of one’s business, domestic only or international, a specific industry segment or cross-industry markets, are contributing decision factors. Further, the market acceptance, maturity, and applicability of any standard are other contributing decision factors.

2.1 ISO

ISO² is a non-governmental network of the national standards institutes of 157 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO is made up of its members who are divided into three categories:

- A *member body* of ISO is the national body "most representative of standardization in its country". Only one such body for each country is accepted for membership of ISO.
- A *correspondent member* is usually an organization in a country which does not yet have a fully-developed national standards activity.
- *Subscriber membership* has been established for countries with very small economies.

² www.iso.org

Many think "ISO" is an acronym, but it is not, rather that is its actual name. Because "International Organization for Standardization" would have different abbreviations in different languages ("IOS" in English, "OIN" in French for *Organisation internationale de normalisation*), it was decided at the outset to use a word derived from the Greek isos, meaning "equal". Therefore, whatever the country, whatever the language, the short form of the organization's name is always ISO.

2.2 JTC1

ISO and the International Electrotechnical Commission (IEC) established the Joint Technical Committee One (JTC1)³ for developing information technology standards. ISO/IEC JTC1 develops generic standards that are agnostic to industry segments unlike the ones developed by ISO technical committees. JTC1 operates under a slightly different set of rules than ISO, but similarly recognizes national standards bodies as members. Specifically, ISO 18014 was developed by subcommittee (SC) 27 IT Security Techniques.

During the development of the three parts of ISO/IEC 18014 in SC27, there were contributions from many National Bodies (USA, Germany, Spain, and others). ISO/IEC 18014 Part 1 and ISO/IEC 18014 Part 2 were published in 2002, and ISO/IEC 18014 Part 3 was published in 2004. The USA contribution was provided through the International Committee for Information Technology (IT) Standards⁴ (INCITS) T4 IT Security Techniques technical committee. Note that T4 has since been superseded by the Cyber Security (CS) 1 technical committee.

2.3 ANSI

The American National Standards Institute⁵ (ANSI) coordinates the development and use of voluntary consensus standards in the United States and represents the needs and views of U.S. stakeholders in standardization forums around the globe. ANSI is the official U.S. representative to ISO, the International Electrotechnical Commission (IEC), ISO/IEC JTC1 and a member of the International Accreditation Forum (IAF). ANSI itself does not develop standards; rather it accredits other US domestic organizations as standards developers.

2.4 ASC X9

The Accredited Standards Committee X9⁶ (ASC X9), accredited by ANSI, has the mission to develop, establish, maintain, and promote standards for the Financial Services Industry in order to facilitate

delivery of financial services and products. Under this mission ASC X9 fulfills the objectives of supporting existing standards, facilitates the development of new standards based upon consensus, and participates in and promotes the development of international (ISO) standards. Specifically X9.95 was developed by the X9F4 Cryptographic Protocol and Application Security working group.

During the development of the X9.95 standard, the X9F4 working group had in its roster over 40 members, listed in alphabetical order: American Express Company, American Financial Services Association, Bank of America, BB and T, Cable & Wireless America, Certicom Corporation, Diebold, Inc., Discover Financial Services, Diversinet Corporation, Entrust, Inc., Federal Reserve Bank, First Data Corporation, Fiserv, Griffin Consulting, Hewlett Packard, Hypercom, IBM Corporation, Identrus, InfoGard Laboratories, Ingenico, Innové LLC, Inovant, International Biometric Group, KPMG LLP, MasterCard International, National Security Agency, NCR Corporation, NEC Solutions America, NTRU Cryptosystems, Orion Security Solutions, Proofspace, RSA Security, Sun Microsystems, Surety Inc., TECSEC Incorporated, Thales e-Security, Inc., TimeCertain LLC, Unisys Corporation, University Bank, VeriFone, Inc., VECTORsgi and Wells Fargo Bank.

Following the publication of X9.95 several of the X9F4 members including Innové LLC, Orion Security Solutions, ProofSpace, Surety Inc, and TimeCertain LLC established the Information Assurance Consortium⁷ to promote X9.95 so that commercial entities, government organizations, and individuals can conduct their affairs in a secure, confident, efficient, and verifiable manner. Since that time, the consortium has added the ISSA⁸, CSIA⁹, GAISP¹⁰, ABA-ISC¹¹ and SNIA¹² as liaison members.

2.5 IETF

The Internet Engineering Task Force¹³ (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The IETF Mission Statement is documented in RFC 3935. The IETF is not affiliated with ISO or ANSI; rather the IETF is a self-accredited standards body, although it is internationally well recognized. Individuals from any

³ www.jtc1.org

⁴ www.incits.org

⁵ www.ansi.org

⁶ www.x9.org

⁷ www.infoassurance.org

⁸ www.issa.org

⁹ www.csialliance.org

¹⁰ www.issa.org/gaisp

¹¹ www.abanet.org/dch/committee.cfm?com=ST230002

¹² www.snia.org

¹³ www.ietf.org

company and any country can be a member of the IETF. Specifically, RFC 3161 was developed by the Network Working Group.

During the development of RFC 3161, the focus was on the definition of a time stamp request protocol and of the related data types. Subsequently, additional work was done by the European Telecommunications Standards Institute¹⁴ (ETSI) on a profile for RFC 3161 which was subsequently reissued as RFC 3628 Policy Requirements for Time-Stamping Authorities. The profile limits the number of options by placing additional constraints on the protocol elements for purposes of promoting interoperability.

3 ROLES AND RESPONSIBILITIES

X9.95 identifies four roles: Time Source Entity (TSE), Time Stamp Authority (TSA), Time Stamp Requestor (TSR) and the Time Stamp Verifier (TSV); and addresses the responsibilities for each role. In contrast, RFC 3161 and ISO 18014 only address the TSA role and responsibilities. The TSR and TSV are referred in RFC 3161 and ISO 18014 as entities participating in the trusted time stamp request, response and verification processes; however specific responsibilities for each entity are not provided. Further, neither standard includes the TSE in its scope.

3.1 TIME SOURCE ENTITY

The Time Source Entity (TSE) is any National Measurement Institute (e.g., NIST¹⁵, USNO¹⁶) upstream from a TSA that provides time calibration services. The time source for any National Measurement Institute (NMI) is the International Time Authority (ITA) designated as the Bureau International des Poids et Mesures (BIPM) near Paris, France is the official ITA who calibrates the clocks of each NMI. Another uniqueness of X9.95 is the proffered Time Calibration Report (TCR). The TCR used between the TSA and the TSE provides an audit trail of the time calibration event.

3.2 TIME STAMP AUTHORITY

The Time Stamp Authority (TSA) is any entity that issues Time Stamp Tokens (TST) that can be internal to a financial institution (e.g. cryptographic hardware) or an external 3rd party service provider. An internal TSA means that the financial institution controls the TSA operations.

3.3 TIME STAMP REQUESTOR

The Time Stamp Token Requestor (TSR) is any entity (e.g., client, server) that submits a request and receives a Time Stamp Token (TST) response from a

TSA. The request contains a hash value of the data to be time stamped. The TST is composed of the TSA time stamp info object (containing the submitted hash value, the time stamp, and other data) and a cryptographic binding between the hash value and the time stamp, which provides authentication of the TSA to the TSR and any TSV.

3.4 TIME STAMP VERIFIER

The Time Stamp Verifier (TSV) is any entity that verifies a TST. The verifier may be the TSR or any other third party such as a relying party needing to validate the TST and consequently the data content. All relying parties are verifiers, but not all verifiers are necessarily relying parties. A relying party by presumption has a financial liability related to the validity of the TST. For example, a verifier could be a regulatory body needing to validate the TST as part of an investigation. Note that verifiers can perform the TST validation or employ trusted third party verification service providers.

4 REQUIREMENTS

X9.95 identifies mandatory requirements as “shalls” and recommendations as “shoulds” for each of the four roles: TSE, TSA, TSR and TSV. RFC 3161 and ISO 18014 provide some technical requirements with regard to the structure and processing of data objects, but neither addresses the operational requirements as provided in X9.95. X9.95 identifies over 150 technical and operational requirements. In contrast, ISO 18014 Part 1 Framework provides nine requirements and RFC 3161 provides twenty-two requirements. All of the ISO and RFC requirements are included in X9.95; hence X9.95 is considered to be a much more stringent and richer standard.

5 TIME STAMP METHODS

Table 1 - Methods compares the trusted time stamp methods for each standard. X9.95 supports digital signature, message authentication code (MAC), Linked Tokens and Transient Key methods. In contrast, ISO 18014 does not support the Transient Key method, and supports the Archived method not supported by X9.95; and RFC 3161 only supports the digital signature method.

Table 1 - Methods

X9.95	ISO 18014	RFC 3161
Digital Signature	Digital Signature	Digital Signature
MAC	MAC	-
Linked Tokens	Linked Tokens	-
-	Archive	-
Transient Key	-	-

5.1 DIGITAL SIGNATURE METHOD

The digital signature method is where the TSA uses the private key of an asymmetric key pair to digitally sign the time stamp info object encapsulated in the

¹⁴ www.etsi.org

¹⁵ <http://tf.nist.gov/>

¹⁶ <http://www.usno.navy.mil/>

Time Stamp Token (TST). The TST verification is carried out by performing signature verification using the corresponding public key, presumably contained in the TSA certificate. This method assumes the existence of a PKI such that the relying party can validate the TSA certificate issued by a trusted Certification Authority (CA).

5.2 MAC METHOD

The MAC method is where the TSA uses a secret symmetric key to cryptographically bind the time stamp info object encapsulated in the Time Stamp Token (TST) with a message authentication code (MAC). The TST verification is done by authenticating the MAC. The TSA is needed to carry out the verification as a trusted third party verifier.

5.3 LINKED TOKEN METHOD

The linked token method is where the TSA uses hash functions to link and cryptographically bind the time stamp info object encapsulated in a the TST with previously issued time stamp tokens. The TSA maintains values from its linking operations for subsequent time-stamp token verification and auditing. Each time stamp token contains a cryptographic binding that authenticates its participation in the TSA's linking operations for the time stamp in the TST. The TST verification is done by computing a value from this cryptographic binding and matching it with the equivalent value maintained by the TSA. The TSA is needed to carry out the verification as a trusted third party verifier. The TSA further publishes data derived from the output values of its linking operations, and TSTs may be extended to the published data and subsequently verified independently of the issuing TSA.

An alternative to the linked token method is the linked and signed method where the TSA uses the linked token method as described above and in addition the TSA signs the time stamp info object encapsulated in the TST.

5.4 TRANSIENT KEY METHOD

The transient key method is where the TSA uses asymmetric key pairs that are generated and used for a predefined interval of time to sign the time stamp info object encapsulated in the TST, and is used to sign the public key of the next interval. The previous interval private key is always destroyed. The TST verification is carried out by any relying party by performing signature verification using the corresponding public key for the given time interval. Further, the signing of the public key can be cross certified by other transient key TSAs.

5.5 ARCHIVE METHOD

The archive method is where the TSA returns a time-stamp token that only has reference information to

bind the time-stamp to the hash value in the TST. The TSA archives locally enough information to verify that the time-stamp is correct.

The archive method was intentionally omitted in X9.95 during its 2004 development. Upon discovery that IBM had originally submitted the archive method to JTC1/SC27 in 2001 but had no plans to support the method; ASC X9 issued a letter to IBM notifying IBM of the X9F4 working group's decision to omit the method. IBM accepted the decision and the method was formally withdrawn.

6 TIME STAMP OBJECTS

X9.95 provides Abstract Syntax Notation One (ASN.1) and Extensible Markup Language (XML) definitions for the following objects: Time Calibration Report, Time Stamp Request and Response, Time Stamp Token, Verification Request and Response; and provides a description for creating an Audit Log. In contrast, ISO 18014 provides ASN.1 for the Time Stamp Request and Response, Time Stamp Token, Verification Request and Response; and RFC 3161 provides ASN.1 for the Time Stamp Request and Response, Time Stamp Token, and does allude to an audit log.

Neither ISO 18014 nor RFC 3161 support XML data structures, whereas X9.95 not only provides XML objects, it even provides a summary of the OASIS¹⁷ Digital Signature Services XML Time Stamp.

7 TIME STAMP MESSAGE FLOWS

X9.95 provides detailed processing flows, error handling and retry logic for Time Calibration, Time Stamp Acquisition and Time Stamp Verification messages. In contrast, ISO 18014 and RFC 3161 only define error codes. In fact, in developing the message flows, the X9F4 working group identified additional error codes which were included in X9.95 and subsequently conveyed to JTC1/SC27 and IETF as US submissions.

8 AUDIT CONTROL OBJECTIVES

The goal of any organization should be to meet or exceed industry standard practices when using technology in a responsible manner by imposing proper controls. Compliance to policies, standards, and procedures can only be assured by verification of the controls via an *audit*. There are two primary types of security review audits: internal audits performed by an internal audit group or out-sourced to an external audit firm; and external audits performed by an independent third party, such as an accounting or audit firm. The control objectives provided in X9.95 represent recommended practices for business, operational, and technical use against which a time

¹⁷ www.oasis-open.org

stamp entity may be evaluated or audited. In contrast neither ISO 18014 nor RFC 3161 include in their scope control objectives or evaluation criteria.

The control objectives and evaluation criteria in X9.95 are organized by IT environmental controls, key management controls, and time management controls. The specific evaluation criteria applicable to each of the four roles (TSE, TSA, TSR and TSV) are organized into three broad categories: IT Environmental control objectives, Key Management control objectives, and Time Management control objectives. The control objectives and criteria are written in audit approved language and adapted from similar standards with comparable objectives and evaluation criteria:

- ANS X9.79-2001 PKI Policy and Practices Framework
- AICPA/CICA WebTrust Program for Certification Authorities¹⁸
- ANS X9.84-2003 Biometric Information Management and Security

Altogether there are eleven IT Environmental control objectives with 144 specific evaluation criteria statements; six Key Management control objectives with 61 evaluation criteria statements; and five Time Management control objectives with 32 evaluation criteria statements.

9 POLICY AND PRACTICES

Similar to the industry accepted conventions for a Certification Authority needing a Certificate Policy (CP) and Certificate Practice Statement (CPS); and while emphasizing that a TSA is not a CA; the TSA needs a Time Stamp Policy (TSP) and a Time Stamp Practice Statement (TSPS). X9.95 provides sample Time Stamp Policy (TSP) and Time Stamp Practice Statement (TSPS) material. In contrast, ISO 18014 and RFC 3161 do not address this topic.

The Time Stamp Policy (TSP) states the goals of “what” is to be achieved, whereas the Time Stamp Practice Statement (TSPS) states the performance of “how” the goals will be fulfilled. Furthermore, the TSP is considered a public document, certainly available to anyone upon request, whereas the TSPS contain more sensitive information and may be restricted to customers, business partners or prospective clients. Each time stamp entity (TSE, TSA, TSR, and TSV) is expected to have some Time Stamp Policy declarations, whereas only the TSA is expected to produce a TSPS. Further, each time stamp entity is also expected to have detailed time stamp procedures that are internal to the organization.

The Time Stamp Policy (TSP) declares what assertions the Time Stamp Authority (TSA) is making. It specifies what warranties the TSA offers that these assertions are true, and what liabilities will be assumed or allocated by the TSA in the event that an assertion is discovered to be untrue. It also specifies any limitations to these liabilities, the maximum liabilities per time stamp token (TST) or per transaction, and specifies the types of transactions in which the warranties are in effect. The TSP also specifies procedures for submission of claims and for resolution of disputes, and it specifies any conditions the participants should fulfill or actions a Verifier should perform before being authorized to rely on a TST and its assertions.

The purpose of the Time Stamp Practice Statement (TSPS) is to clearly define the general procedures and practices performed by the TSA in fulfilling the roles and functions of the TSA. The TSPS may take the form of a declaration by the TSA of the details of its trustworthy system and the practices it employs in its operations to securely issue and manage its time stamp tokens (TST). Portions of a Time Practice Statement may also be included as part of the contract between the TSA and the Requestor.

10 CONCLUSIONS

Data integrity mechanisms are not reliable unless they are (i) verifiable to a point in time and (ii) the time source controls are independent of the data content provider. Trusted time stamping methods are the only cryptography based technology that provides data integrity verifiably to a reliable point in time.

As summarized in Table 2 – Standards Comparison the X9.95 standards offers a more comprehensive set of conditions and constraints. X9.95 includes more roles, requirements, objects, control objectives and evaluation criteria than other ISO 18014 or RFC 3161 and can therefore be used as follows:

- The X9.95 standard can be used as input to help define an organization’s business and technology requirements for information integrity.
- The X9.95 standard can be used during an organization’s design and development phases to implement data integrity controls.
- The X995 standard can be used to determine an organization’s pre and post deployment compliance to trusted time stamping.

Further, X9.95 segregates requirements, control objectives and evaluation criteria for each of the four roles, the Time Source Entity (TSE), the Time Stamp Authority (TSA), the Time Stamp Requestor (TSR), and the Time Stamp Verifier (TSV). The X9.95 standard also provides example policy and practice statements for the TSA.

¹⁸ www.webtrust.org/certauth_fin.htm

Table 2 – Standards Comparison

Roles and Responsibilities	ANS X9.95	ISO 18014	RFC 3161
▪ Time Source Entity	TSE	-	-
▪ Time Stamp Authority	TSA	TSA	TSA
▪ Time Stamp Requestor	Requestor	Requestor	-
▪ Time Stamp Verifier	Verifier	verifier	-

Requirements	ANS X9.95	ISO 18014	RFC 3161
▪ Approximate count	150+	22	9

Time Stamp Objects	ANS X9.95	ISO 18014	RFC 3161
▪ Time Calibration Report	ASN.1 and XML	-	-
▪ Time Stamp Request	ASN.1 and XML	ASN.1	ANS.1
▪ Time Stamp Response	ASN.1 and XML	ASN.1	ANS.1
▪ Time Stamp Token	ASN.1 and XML	ASN.1	ANS.1
▪ Verification Request	ASN.1 and XML	ASN.1	-
▪ Verification Response	ASN.1 and XML	ASN.1	-
▪ Audit Log	<i>described</i>	-	<i>mentioned</i>

Time Stamp Methods	ANS X9.95	ISO 18014	RFC 3161
▪ Digital Signature	Digital Signature	Digital Signature	Digital Signature
▪ MAC	MAC	MAC	-
▪ Linked Tokens	Linked Tokens	Linked Tokens	-
▪ Archive	<i>eliminated</i>	Archive	-
▪ Transient Key	Transient Key	-	-

Time Stamp Message Flows	ANS X9.95	ISO 18014	RFC 3161
▪ Time Calibration	Calibration	-	-
▪ Time Stamp Acquisition	Request / Response	-	-
▪ Time Stamp Verification	Request / Response	-	-

Policy and Practice Statements	ANS X9.95	ISO 18014	RFC 3161
▪ Time Stamp Policy	22 Examples	-	-
▪ Time Stamp Practice	<i>Sample Statements</i> 22 Examples	-	-

Audit Control Objectives	ANS X9.95	ISO 18014	RFC 3161
▪ IT Controls	11 Control Objectives 144 Evaluation Criteria	-	-
▪ Key Management Controls	6 Control Objectives 61 Evaluation Criteria	-	-
▪ Time Stamp Controls	5 Control Objectives 32 Evaluation Criteria	-	-