American National Standard
for Financial Services

X9.59–2006

Electronic Commerce for the Financial Services Industry: Account Based Secure Payment Objects

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: May 24, 2006

American National Standards Institute

Contents

Figures

Tables

Foreword

Electronic payments are susceptible to fraud unless there are methods applied to reduce or eliminate that fraud. This standard defines a “secure payment object” in the area of consumer electronic payments that enables creation and movement of a secure digital signature in conjunction with a consumer electronic purchase or payment. This “secure payment object” contains the digital signature and several elements of the electronic transaction that may not be captured in the current environment that insure the uniqueness of the transaction, enabling the relying party to validate the digital signature and therefore verify the authenticity of the transaction, including origin identification, data integrity and signer non-repudiation. When used in interchange, this “secure payment object” is a separate data element (Example: see X9.105-1:2003, Section 6.5.1, Table 9, bit 34, Dataset identifier 71.) which after creation by the transaction initiator, can be carried from the transaction acquirer to the issuer, and there validated as part of the authentication process preceding an authorization request. The degree to which transactions are thus protected with digital signatures have a direct correlation to the amount of fraud reduction. Heretofore, methods of creating digital signatures applied to retail situations were far to cumbersome or “infrastructure heavy”. X9.59 provides some examples of implementation of digital signatures in a very efficient manner, in fact, efficient enough to scale to all electronic retail transactions.

Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretation should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

NOTE The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights.

By publication of this standard, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. Details may be obtained from the standards developer.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken to reaffirm, revise, or withdraw this standard no later than five years from the date of approval.

Published by

Accredited Standards Committee X9, Incorporated

Financial Industry Standards
1212 West Street, Suite 200
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

Introduction

Business practice has changed with the introduction of computer-based technologies. The substitution of electronic transactions for their paper-based predecessors has reduced costs and improved efficiency. Trillions of dollars in funds and securities are transferred daily by telephone, wire services, and other electronic communication mechanisms. The high value or sheer volume of such transactions within an open environment exposes the financial community and its customers to potentially severe risks from accidental or deliberate alteration, substitution or destruction of data. This risk is compounded by interconnected networks, and the increased number and sophistication of malicious adversaries.

Some of the conventional “due care” controls used with paper-based transactions are unavailable in electronic transactions. Examples of such controls are safety paper which protects integrity, and hand-written signatures or embossed seals which indicate the intent of the originator to be legally bound. In an electronic-based environment, controls must be in place that provides the same degree of assurance and certainty as in a paper environment. The financial community is responding to these needs.

This Standard ANSI X9.59–2006 Electronic Commerce for the Financial Services Industry: Account Based Secure Payment Objects defines electronic payment objects used in consumer-oriented, account-based transactions. This standard is mute about other payment mechanisms, such as stored value cards. Since the goal was as simple a standard as possible, no features were included in this standard unless a valid business case could be made for the feature.

These secure payment objects use standard cryptographic tools and techniques to offer authentication, integrity, and prevention of replay. When used within a complete payment certification infrastructure, digital signatures can help to prevent the consumer from successfully repudiating the payment order. When used with signed acknowledgment objects, they will likewise prevent the merchant from successfully repudiating the receiving of a valid payment object. Thus the consumer’s Financial Institution wants to be assured that its customer intended to make the payment and that the merchant is accurately identified on the account statement sent to the consumer.

Any of the entities receiving signed objects during the payment transaction can be assured that the signed information has been protected from alteration. In particular, the settlement systems must assure that the data contained in the payment object gets back to the consumer’s financial institution so that it can validate the digital signatures made by the consumer.

It is expected that other groups will work to embed these objects within appropriate specifications and protocols for the Internet and other transport media. The scope statement should help these groups by defining the boundary inside of which these objects will operate. The intended audience for this standard is developers of payment systems and the applications that use payments.

Future message standards may be required to accommodate other message flows, such as that from the merchant, to the consumer and then on to the issuing financial institution.

Three fundamental principles have been identified that can result in a successful payment system:

- Authentication techniques are separated from techniques that provide privacy,
- Authentication without encryption, is sufficient to ensure integrity of the financial payment transactions,
- Privacy can be provided by other methods outside the scope of this document.

These are some of the design decisions that followed from these principles, some intended, and some not:

- The routing code, defined in this standard, is not required to be encrypted, and so must not be used in transactions that are not digitally signed,
- A smaller number of private key operations are required, reducing the cost over combined methods,
- The interchange protocol is outside the scope of the standard,
- Export problems become much less difficult to accommodate since encryption is not required,
- Current clearing systems will be able to support this standard by adding some new data fields.

While the techniques specified in this Standard are designed to maintain the integrity of payment objects and provide a service that can be used in non-repudiation, the Standard does not guarantee that a particular implementation is secure. It is the responsibility of the financial institution to put an overall process in place with the necessary controls to ensure that the process is securely implemented. Furthermore, the controls should include the application of appropriate audit tests in order to verify compliance with this Standard.

During the investigative stage, this committee examined the work of a large number of extant payment systems and standards organizations. In the table below, we have tried to list the sources of the information that was used. These functions are further defined in Section 3 of the standard.

Table 1 - Business Functions associated with Electronic Payments

Function & Description	Source of Information
Authentication of Merchant	
Should occur before purchasing activity. May also occur when payment is made if the MFI supplies a merchant certificate	ITU-T X.509
Shopping Experience	
Selection of goods, building of invoice, transport of invoice for approval, conditions of delivery	X12, IOTP, OFX
Payment Negotiation	
Listing of payment options and selection by consumer or negotiation with merchant	W3C (JEPI & UPP), IOTP
Payment Object Delivery	
Creation of secure payment objects and transport to merchant and on to payment system.	X9.59, SET, e-check, ACH, and stored value
Payment or Consideration Ack	
Acknowledgment sent from Merchant to Consumer and from Consumer to Merchant.	X9.59, IOTP
Interface to Settlement	
Gateways between payment delivery channel and existing settlement networks	SET, FSTC – BIPS, ISO 8583-1:2003/X9.105-1:2003
Clearing and Settlement	

Function & Description	Source of Information
ATM/POS, ACH	Card and clearing association's rules
Consumer's Account Maintenance and Control	
Interface between the Consumer and the CFI. Statements, transaction, and control documents are currently paper, they could move to web page data base	X9.49, BAI, OFX, BIPS
Merchant's Cash Register	
Merchant's container for payment options and terms for engaging in payment negotiation. This should be contained within a security perimeter.	IOTP
Consumer's Trusted Electronic Wallet	
Consumer's container for payment options and terms for engaging in payment negotiation. This should be contained within a security perimeter.	OFX, IOTP

The responsibility for the success of any collegial effort like this one is always so diffuse as to be nearly indecipherable. The editor would like to explicitly acknowledge some of the fine work that fed directly into this document: including: the FSTC electronic check project and the Visa/MasterCard SET pilot. He was pleased to be able to liberally apply their learning by adopting many of their structures directly.

The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. To date, no such claims have been identified.

By publication of this standard, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant a license under these rights on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain such a license- Details may be obtained from **Accredited Standards Committee X9, Incorporated, Financial Industry Standards, 1212 West Street, Suite 200, Annapolis, MD 21401 USA**

Suggestions for the improvement or revision of this Standard are welcome. They should be sent to the X9 Committee Secretariat **Accredited Standards Committee X9, Incorporated, Financial Industry Standards, 1212 West Street, Suite 200, Annapolis, MD 21401 USA**
.

This Standard was processed and approved for publication by the Accredited Standards Committee on Financial Services, X9 Inc. Committee approval of the Draft Standard does not necessarily imply that all the committee members voted for its approval.

At the time this standard was approved, it had the following X9 Board Members (Consensus Body)

Vincent DeSantis, X9 Vice Chairman
Cynthia Fuller, Executive Director
Isabel Bailey, Managing Director

Organization Represented	*Representative*
ACI Worldwide	Jim Shaffer
American Bankers Association	C. Diane Poole
American Express Company	John Allen
American Financial Services Association	Mark Zalewski
Bank of America	Daniel Welch
Capital One	Scott Sykes
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Mike Halpern
Deluxe Corporation	John Fitzpatrick
Diebold, Inc.	R. David Nein
Discover Financial Services	Jennifer Schroeder
Federal Reserve Bank	Dexter Holt
First Data Corporation	Connie Spurgeon
Fiserv	Skip Smith
FSTC, Financial Services Technology Consortium	Daniel Schutzer
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker
iStream Imaging/Bank of Kenney	Ken Biel
IBM Corporation	Todd Arnold
Identrus	Mack Hicks
Ingenico	John Spence
Intuit, Inc.	Jana Hocker
J.P. Morgan Chase & Co	Jacqueline Pagán
KPMG LLP	Mark Lundin
MagTek, Inc.	Carlos Morales
MasterCard International	William Poletti
National Association of Convenience Stores	Gray Taylor
National Security Agency	Sheila Brand
NCR Corporation	Steve Stevens
SWIFT/Pan Americas	Malene McMahon
The Clearing House	Vincent DeSantis
U.S. Bank	Marc Morrison
University Bank	Stephen Ranzini
VeriFone, Inc.	Brad McGuinness
VECTORsgi	Ron Schultz
VISA	Richard Sweeney
Wachovia Bank	Ray Gatland
Wells Fargo Bank	Ruven Schwartz

The X9A subcommittee on Retail Electronic Payments had the following members:

Organization Represented	***Representative***
ACI Worldwide	Cindy Rink
American Bankers Association	C. Diane Poole
American Express Company	John Allen
American Financial Services Association	Mark Zalewski
Bank of America	Andi Coleman
Capital One	Scott Sykes
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Bill Burnett
Deluxe Corporation	John Fitzpatrick
Diebold, Inc.	Bruce Chapa
Federal Reserve Bank	Dexter Holt
First Data Corporation	Connie Spurgeon
Fiserv	Skip Smith
Food Marketing Institute	Stacy Fitzgerald-Redd
FSTC, Financial Services Technology Consortium	Daniel Schutzer
GTECH Corp	Mirek Kula
Hypercom	Scott Spiker
Identrus	Mack Hicks
Ingenico	John Spence
J.P. Morgan Chase & Co	Edward Koslow
MasterCard International	Ron Karlin
Maximus, Inc.	Peter Relich
National Association of Convenience Stores	Gray Taylor
National Security Agency	Sheila Brand
Navy Federal Credit Union	Joan Wood
NCR Corporation	Steve Stevens
Texas EBT	Doug Walker
The Clearing House	Vincent DeSantis
U.S. Bank	Marc Morrison
University Bank	Michael Talley
VeriFone, Inc.	Brad McGuinness
VECTORsgi	Ron Schultz
VISA	Richard Sweeney
Wachovia Bank	Ray Gatland
Wells Fargo Bank	Salley Hoopes

The X9F subcommittee on Data and Information Security had the following members:

Mr. Richard J. Sweeney, Chairman

Organization Represented	***Representative***
3PEA Technologies, Inc.	Mark Newcomer
ACI Worldwide	Jim Shaffer
American Bankers Association	C. Diane Poole
American Express Company	John Allen
American Financial Services Association	Mark Zalewski
Bank of America	Andi Coleman
Capital One	Scott Sykes
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Paul Gubiotti
Citigroup, Inc.	Mike Halpern
Deluxe Corporation	John Fitzpatrick
DeLap, White, Caldwell and Croy, LLP	Darlene Kargel
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Julie Shaw
Entrust, Inc.	Robert Zuccherato
Federal Reserve Bank	Neil Hersch
Ferris and Associates, Inc.	J. Martin Ferris
Fidelity Investments	Michael Versace
First Data Corporation	Connie Spurgeon
Fiserv	Bud Beattie
FSTC, Financial Services Technology Consortium	Daniel Schutzer
FTI Consulting	Roger Nebel
Futurex	Jason Anderson
Hewlett Packard	Larry Hines
Hypercom	Scott Spiker
IBM Corporation	Todd Arnold
Identrus	Mack Hicks
InfoGard Laboratories	Tom Caddy
Ingenico	John Spence
Intel Massachusetts, Inc.	John Cyr
J.P. Morgan Chase & Co	Edward Koslow
MagTek, Inc.	Terry Benson
MasterCard International	Ron Karlin
Microsoft Corp	Niels Ferguson
National Institute of Standards and Technology	Elaine Barker
National Security Agency	Sheila Brand
NCR Corporation	David Norris
NTRU Cryptosystems, Inc.	William Whyte
Orion Security Solutions	Miles Smid
Pi R Squared Consulting LLP	Ralph Poore
Pitney Bowes, Inc.	Leon Pintsov
Proofspace	Paul F. Doyle
RSA Security, Inc.	James Randall
Surety, Inc.	Dimitrios Andivahis

Organization Represented	***Representative***
TECSEC Incorporated	Ed Scheidt
Thales e-Security, Inc.	James Torjussen
Triton Systems of Delaware, Inc.	Daryll Cordeiro
U.S. Bank	Marc Morrison
University Bank	Stephen Ranzini
VeriFone, Inc.	Dave Faoro
Verisign, Inc.	Joseph Adler
VECTORsgi	Ron Schultz
VISA	Richard Sweeney
Wachovia Bank	Ray Gatland
Wells Fargo Bank	Ruven Schwartz

Under ASC X9 procedures, a working group may be established to address specific segments of work under the ASC X9 Committee or one of its subcommittees. A working group exists only to develop standard(s) or guideline(s) in a specific area and is then disbanded. The individual experts are listed with their affiliated organizations. However, this does not imply that the organization has approved the content of the standard or guideline. The X9A10 working group that developed this standard had the following members:

Organization Represented	***Representative***
American Bankers Association	Tom Judd
American Bankers Association	C. Diane Poole
American Express Company	Mark Merkow
American Express Company	Richard Rodriguez
American Express Company	Vicky Sammons
Capital One	Scott Sykes
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Bill Burnett
Discover Financial Services	Pamela Ellington
Discover Financial Services	Jennifer Schroeder
Federal Reserve Bank	Deb Hjortland
Federal Reserve Bank	Dexter Holt
Federal Reserve Bank	Tom Wick

First Data Corporation	Curt Beeson
First Data Corporation	Connie Spurgeon
Fiserv	Mary Bland
Fiserv	Dan Otten
Food Marketing Institute	Stacy Fitzgerald-Redd
Food Marketing Institute	Jennifer Hatcher
FSTC, Financial Services Technology Consortium	Christine Nautiyal
GTECH Corp	Mirek Kula
GTECH Corp	Steve Lupo
Hypercom	Scott Spiker
Identrus	Alan Asay
Identrus	Mack Hicks
J.P. Morgan Chase & Co	Paul Simon
Maximus, Inc.	Peter Relich
Pitney Bowes, Inc.	Leon Pintsov
University Bank	Stephen Ranzini
University Bank	Michael Talley
VeriFone, Inc.	Brad McGuinness
VeriFone, Inc.	Brenda Watlington
VECTORsgi	Jerry Bowman
VECTORsgi	Ron Schultz
VISA	Richard Sweeney

ANSI X9.59 – Electronic Commerce for the Financial Services Industry: Account-Based Secure Payment Objects –2006

1 Scope

This standard addresses the following:

A) Payment Model Description

This standard describes a model of account based electronic payments. It identifies the roles played by different components of the payment process and the flow of information between those roles. The roles are the consumer, who wishes to make a payment, a merchant which provides value, and their respective Financial Institutions, the consumer financial institution and the merchant financial institution.

B) Secure Object Specifications

This standard specifies a collection of electronic payment objects and references digital signature techniques to secure their content. The objects are all defined in terms of how they need to be constructed, signed and verified in computing machinery that is acting on behalf of a consumer and a merchant. A concrete syntax is specified in order that the signature can be constructed or verified at any location that has access to the consumer's public key and associated data. A business recommendation is made that the payment routing code (or PAN) used in conjunction with secure payment objects defined by this standard is not accepted as valid in non-authenticated transactions. Several usage scenarios are given to show examples of real applications where the standard objects may be applicable.

Confidentiality for the payment information may be desired and is neither required, nor precluded, by this standard. Prudent implementers may choose to conduct a risk assessment to determine the need for confidentiality. Also policy issues, including terms and conditions of the agreements between the parties, are not covered in this standard. . While some of the information described in the standard must survive interchange between cooperating financial institutions, the syntax of how it appears in any particular payment protocol is not specified.

2 Normative references

The following standards contain provisions that, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Accredited Standards Committee X9 (ASC X9) maintains a register of currently valid financial industry standards.

ANSI X9.24-1: 2004, *Retail Financial Services Symmetric Key Management – Part 1: Using Symmetric Techniques*

ANSI X9.30-2: 1997, *Public Key Cryptography Using Irreversible Algorithms – Part 2: The Secure Hash Algorithm (SHA-1)*

ANSI X9 31: 1998*, Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry (rDSA)*