



## American National Standard for Financial Services

# X9.59–2006

(R2013)

# 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

This is a preview of "ANSI X9.59-2006 (R20...)". [Click here to purchase the full version from the ANSI store.](#)

# Contents

Page

Foreword .....	vii
Introduction.....	ix
1 Scope .....	1
2 Normative references .....	1
3 Terms and definitions .....	2
4 Symbols and abbreviated terms .....	5
5 Requirements.....	6
6 Clause .....	6
1.1 Business Roles .....	6
1.1.1 The Consumer.....	6
1.1.2 The Merchant .....	7
1.1.3 The Merchant's Financial Institution .....	7
1.1.4 The Consumer's Financial Institution .....	7
1.2 Business Functions .....	7
1.1.5 Authentication of Merchant .....	7
1.1.6 Electronic Shopping experience.....	8
1.1.7 Electronic Payment Negotiation .....	8
1.1.8 Electronic Payment Object Delivery .....	8
1.1.9 Payment or Consideration Acknowledgment.....	8
1.1.10 Interface to Settlement.....	8
1.1.11 Clearing and Settlement .....	8
1.1.12 Account Statement to Consumer.....	8
1.1.13 Electronic Wallet.....	8
1.3 Business Services.....	9
1.1.14 Privacy and Data Confidentiality.....	9
1.1.15 Non-repudiation.....	9
1.1.16 Fraud prevention .....	9
1.4 Schematic Representation .....	9
1.5 Payment Framework .....	10
1.6 Information Interchanged .....	10
1.1.17 Merchant Information.....	10
1.1.18 CFI Information .....	11
1.1.19 Consumer Payment Instructions .....	11
1.1.20 Merchant Authorization/Payment Request .....	11
1.1.21 Payment Ack .....	11
1.1.22 Consideration Ack.....	11
1.1.23 Payment Query .....	12
1.1.24 Consumer Request for Refund .....	12
1.7 Payment Mechanisms to be Supported .....	13
1.1.25 Payment Cards.....	13
6.1.1 Electronic Checks .....	13
1.8 Consumer Client Option Selection .....	13
1.1.26 Payment Option Presentment .....	13
2 Object Content.....	13

**ANSI X9.59**

<b>2.1</b>	<b>Entity Model.....</b>	<b>14</b>
<b>2.2</b>	<b>ASN.1 Definitions.....</b>	<b>14</b>
<b>1.1</b>	<b>Concepts used in the Payment Object .....</b>	<b>19</b>
<b>1.1.1</b>	<b>Link between Consumer and CFI.....</b>	<b>19</b>
<b>1.1.1</b>	<b>Link to Order .....</b>	<b>19</b>
<b>1.1.1</b>	<b>Link between Merchant Certificates .....</b>	<b>20</b>
<b>1.1.1</b>	<b>Certificates .....</b>	<b>20</b>
<b>1.1.1</b>	<b>Locally Unique Identifier (LUID) .....</b>	<b>20</b>
<b>1.1.1</b>	<b>Signature .....</b>	<b>20</b>
<b>1.1.1</b>	<b>Authentication Hash of Order Details.....</b>	<b>21</b>
<b>1.1.1</b>	<b>Payment Routing Code (PRC) .....</b>	<b>21</b>
<b>1.1</b>	<b>Content of the Individual Objects .....</b>	<b>21</b>
<b>1.1.1</b>	<b>Content of the Consumer’s Payment Object .....</b>	<b>21</b>
<b>1.1.1</b>	<b>Content of the Merchant’s Payment Acknowledgment .....</b>	<b>21</b>
<b>1.1.1</b>	<b>Content of the Consideration Acknowledgment .....</b>	<b>22</b>
<b>1.1.1</b>	<b>Content of the Query Object.....</b>	<b>22</b>
<b>1.1.1</b>	<b>Content of the Query Response Object.....</b>	<b>22</b>
<b>1.1.1</b>	<b>Content of the Request for Refund.....</b>	<b>22</b>
<b>1.1</b>	<b>Concrete Syntax.....</b>	<b>22</b>
<b>Annex A</b>	<b>(normative) Message Sequencing .....</b>	<b>23</b>
<b>A.1</b>	<b>Bill Payment .....</b>	<b>23</b>
<b>A.2</b>	<b>Customer Initiated Money Order.....</b>	<b>23</b>
<b>A.3</b>	<b>Payment upon Delivery Transactions.....</b>	<b>23</b>
<b>A.4</b>	<b>Shopping Experience .....</b>	<b>24</b>
<b>Annex B</b>	<b>(Informative) Payment Cards Example .....</b>	<b>25</b>
<b>B.1</b>	<b>Definitions for Payment Card Example .....</b>	<b>25</b>
<b>B.2</b>	<b>Data Elements .....</b>	<b>25</b>
<b>B.3</b>	<b>Description .....</b>	<b>27</b>
<b>B.4</b>	<b>High-Level Flow .....</b>	<b>29</b>
<b>B.5</b>	<b>Considerations.....</b>	<b>30</b>
<b>B.6</b>	<b>Attacks .....</b>	<b>31</b>
<b>B.7</b>	<b>Credit Card Settlement.....</b>	<b>32</b>
<b>Annex C</b>	<b>(Informative) Bank Account Example .....</b>	<b>33</b>
<b>C.1</b>	<b>Definitions for Check Example .....</b>	<b>33</b>
<b>C.2</b>	<b>The Standard Check Model.....</b>	<b>34</b>
<b>C.3</b>	<b>The Z-flow Model.....</b>	<b>34</b>
<b>C.4</b>	<b>Other Models .....</b>	<b>34</b>
<b>C.5</b>	<b>The Check Book.....</b>	<b>34</b>

## Figures

Figure 1 - Framework Schematic .....	10
Figure 2 - Payment Object Schematic (with examples of mechanisms) .....	12
Figure 3 - Entity Model .....	14

**ANSI X9.59**

**Tables**

Table 1 - Business Functions associated with Electronic Payments.....x

Table 2 - Components of ISO 8583 Authorization Request Message..... 27

## 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 too 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**

**ANSI X9.59**

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

Copyright © 2006 ASC X9, Inc.

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without prior written permission of the publisher. Published in the United States of America.



## 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.

**ANSI X9.59**

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**

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

Function & Description	Source of Information
ATM/POS, ACH	Card and clearing association's rules
<b><u>Consumer's Account Maintenance and Control</u></b>	
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
<b><u>Merchant's Cash Register</u></b>	
Merchant's container for payment options and terms for engaging in payment negotiation. This should be contained within a security perimeter.	IOTP
<b><u>Consumer's Trusted Electronic Wallet</u></b>	
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

**ANSI X9.59**

***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:

<b><i>Organization Represented</i></b>	<b><i>Representative</i></b>
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
	Stacy Fitzgerald-Redd
Food Marketing Institute	
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

## **ANSI X9.59**

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

Mr. Richard J. Sweeney, Chairman

### ***Organization Represented***

3PEA Technologies, Inc.  
ACI Worldwide  
American Bankers Association  
American Express Company  
American Financial Services Association  
Bank of America  
Capital One  
Certicom Corporation  
Citigroup, Inc.  
Citigroup, Inc.  
Deluxe Corporation  
DeLap, White, Caldwell and Croy, LLP  
Diebold, Inc.  
Discover Financial Services  
Entrust, Inc.  
Federal Reserve Bank  
Ferris and Associates, Inc.  
Fidelity Investments  
First Data Corporation  
Fiserv  
FSTC, Financial Services Technology Consortium  
FTI Consulting  
Futurex  
Hewlett Packard  
Hypercom  
IBM Corporation  
Identrus  
InfoGard Laboratories  
Ingenico  
Intel Massachusetts, Inc.  
J.P. Morgan Chase & Co  
MagTek, Inc.  
MasterCard International  
Microsoft Corp  
National Institute of Standards and Technology  
National Security Agency  
NCR Corporation  
NTRU Cryptosystems, Inc.  
Orion Security Solutions  
Pi R Squared Consulting LLP  
Pitney Bowes, Inc.  
Proofspace  
RSA Security, Inc.  
Surety, Inc.

### ***Representative***

Mark Newcomer  
Jim Shaffer  
C. Diane Poole  
John Allen  
Mark Zalewski  
Andi Coleman  
Scott Sykes  
Daniel Brown  
Paul Gubiotti  
Mike Halpern  
John Fitzpatrick  
Darlene Kargel  
Bruce Chapa  
Julie Shaw  
Robert Zuccherato  
Neil Hersch  
J. Martin Ferris  
Michael Versace  
Connie Spurgeon  
Bud Beattie  
  
Daniel Schutzer  
Roger Nebel  
Jason Anderson  
Larry Hines  
Scott Spiker  
Todd Arnold  
Mack Hicks  
Tom Caddy  
John Spence  
John Cyr  
Edward Koslow  
Terry Benson  
Ron Karlin  
Niels Ferguson  
Elaine Barker  
Sheila Brand  
David Norris  
William Whyte  
Miles Smid  
Ralph Poore  
Leon Pintsov  
Paul F. Doyle  
James Randall  
Dimitrios Andivahis

**Organization Represented**

TECSEC Incorporated  
 Thales e-Security, Inc.  
 Triton Systems of Delaware, Inc.  
 U.S. Bank  
 University Bank  
 VeriFone, Inc.  
 Verisign, Inc.  
 VECTORsgi  
 VISA  
 Wachovia Bank  
 Wells Fargo Bank

**Representative**

Ed Scheidt  
 James Torjussen  
 Daryll Cordeiro  
 Marc Morrison  
 Stephen Ranzini  
 Dave Faoro  
 Joseph Adler  
 Ron Schultz  
 Richard Sweeney  
 Ray Gatland  
 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**

American Bankers Association  
 American Bankers Association  
 American Express Company  
 American Express Company  
 American Express Company  
 Capital One  
 Certicom Corporation  
 Citigroup, Inc.  
 Discover Financial Services  
 Discover Financial Services  
 Federal Reserve Bank  
 Federal Reserve Bank  
 Federal Reserve Bank

**Representative**

Tom Judd  
 C. Diane Poole  
 Mark Merkow  
 Richard Rodriguez  
 Vicky Sammons  
 Scott Sykes  
 Daniel Brown  
 Bill Burnett  
 Pamela Ellington  
 Jennifer Schroeder  
 Deb Hjortland  
 Dexter Holt  
 Tom Wick

**ANSI X9.59**

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)*