

ACCREDITED STANDARDS COMMITTEE X9, INC.,
FINANCIAL INDUSTRY STANDARDS



CATALOG
OF
FINANCIAL INDUSTRY
AMERICAN NATIONAL STANDARDS,
DRAFT STANDARDS FOR TRIAL USE,
TECHNICAL REPORTS and TECHNICAL GUIDELINES

June 2007

ASC X9, Inc.
1212 West Street, Suite 200, Annapolis, Maryland 21401
www.x9.org

TABLE OF CONTENTS
ASC X9 FINANCIAL INDUSTRY STANDARDS



| | |
|--|---------------|
| TABLE OF CONTENTS | PG. 2 |
| HOW TO PURCHASE STANDARDS | PG. 5 |
| TERMS AND DEFINITIONS | PG. 6 |
| X9's CHECK 21 STANDARDS COLLECTION | PG. 7 |
| PAPER CHECK STANDARDS | PG. 8 |
| TR-100 Organization of Standards for Paper-Based and Image-Based Payments | |
| TR-2 Understanding and Designing Checks | |
| TG-6 Quality Control of MICR Documents | |
| TG-8 Check Security Guideline | |
| X9.7 Bank Check Background and Numerical Convenience Amount Field | |
| X9.100-10 Paper Specifications for Checks (formerly X9.18) | |
| X9.100-111 Specifications for Check Endorsements (formerly X9.53) | |
| X9.100-130 Specifications for Universal Interbank Batch/Bundle (formerly X9.64) | |
| X9.100-151 Check Correction Strip Specification (formerly X9.40) | |
| X9.100-160-1 Placement and Location of Magnetic Ink Printing (MICR) (formerly X9.13) | |
| X9.100-160-2 Placement and Location of Magnetic Ink Printing (MICR) Part 2: EPC Field Use (formerly X9.13 Annex A only) | |
| X9.100-161 Creating MICR Document Specification Forms (formerly X9.47) | |
| X9.100-120 Specifications for Bank Deposit Tickets (formerly X9.33) | |
| X9.100-170 Specifications for the Padlock Icon (formerly X9.51) | |
| X9.100-20 Print and Test Specifications for Magnetic Ink Printing (formerly X9.27) | |
| TR-33-2006 Check Image Quality Assurance Standards and Processes | |
| X9.100-40-1 and 2 Specifications for Check Image Tests Part 1: Definition of Elements and Structures; Part 2: Application and Registration Procedures | |
| X9.100-140 Specifications for an Image Replacement Document (IRD) (formerly DSTU X9.90) | |
| ELECTRONIC CHECK PROCESSING STANDARDS | PG. 12 |
| X9.100-171 Specifications for Automated Identification of Security Features | |
| X9.100-180 Specifications for Electronic Exchange of Check and Image Data (formerly DSTU X9.37) | |
| DSTU X9.100-183 Specifications For Electronic Check Adjustments | |
| ELECTRONIC RETAIL, SECURITY AND ELECTRONIC BENEFITS TRANSFER STANDARDS | PG. 13 |
| TG-7 Initial DEA Key Distribution for PIN Entry and Transaction Originating Devices | |
| X9.58 Financial Transaction Messages - Electronic Benefits Transfer (EBT) – Food Stamps | |
| X9.93:1 Financial Transaction Messages - Electronic Benefits Transfer (EBT) – Part 1: Messages | |
| X9.93:2 Financial Transaction Messages - Electronic Benefits Transfer (EBT) – Part 2: Files | |
| X9.104-1 Financial transaction card originated messages – Card acceptor to acquiring host messages Part 1: Messages, data elements and code values | |
| X9.104-2 Financial transaction card originated messages – Card acceptor to acquiring host messages Part 2: Convenience store and petroleum marketing industry | |
| X9.105-1 Financial transaction card originated messages – interchange message specifications – Part 1: Messages, data elements and code values (Identical to ISO 8583-1:2003) | |



- X9.105-3 Financial transaction card originated messages – interchange message specifications – Part 3: Maintenance procedures for messages, data elements and code values (Identical to ISO 8583-3:2003)
- X9.106 Retail Financial Services – Merchant Category Codes (Identical to ISO 18245)
- X9.107 Bank cards – Magnetic stripe data content for track 3 (Identical to ISO 4909)
- DSTU X9.108 Financial transaction messages – Electronic benefits transfer (EBT) – WIC retailer interface standard

CREDIT STANDARDS

PG. 16

- X9.103 Motor Vehicle Retail Sale and Lease Electronic Contracting
- TR-4 Financial Services Technical Report SPeRS – Standards and Procedures for Electronic Records and Signatures

SECURITIES PROCESSING STANDARDS

PG. 17

- TG-10 Signature Guarantee Guideline
- X9.5 Financial Institution Numbering System (FINS)
- X9.6 Securities Identification System
- X9.12 Specifications for Fully Registered Municipal Securities
- X9.14 Specifications for Securities Transaction Interchange Forms X9.20 Securities – Institutional Delivery System
- X9.101 International securities identification numbering system (ISIN) (Identical to ISO 6166)

DATA AND INFORMATION SECURITY STANDARDS

PG. 19

- TG-3 Retail Financial Services Compliance Guideline – Part 1: Online PIN Security and Symmetric Key Management
- TG-7 Initial DEA Key Distribution for PIN Entry and Transaction Originating Devices
- TG-9 Abstract Syntax Notation and Encoding Rules for Financial Industry Standards
- TR-31 Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
- X9.8-1 Personal Identification Number Management and Security – Part 1: PIN Protection Principles and Techniques for Online PIN Verification in ATM & POS Systems
- X9.24-1 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
- X9.24-2 Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
- X9.30:1 Public Key Cryptography, The Digital Signature Algorithm
- X9.30:2 Public Key Cryptography, The Secure Hash Algorithm
- X9.31 Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry
- X9.32 Financial Institution Data Compression (Wholesale)
- X9.42 Public Key Cryptography For The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
- X9.45 Enhanced Management Controls Using Digital Signatures
- X9.49 Secure Remote Access to Financial Services for the Financial Industry
- X9.52 Triple Data Encryption Algorithm Modes of Operation
- X9.55 Public Key Cryptography: Extensions to Public Key Certificates and Certificate Revocation Lists
- X9.57 Public Key Cryptography for the Financial Services Industry, Certificate Management

- X9.62 Public Key Cryptography for the Financial Services ECDSA
- X9.63 Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography



X9.65 Triple Data Encryption Algorithm (TDEA) Implementation
X9.68:2 Digital Certificates for Mobile/Wireless and High Transaction Volume Financial Systems
X9.69 Key Management Extensions
X9.73 Cryptographic Message Syntax
X9.79 Financial Services PKI Policy and Practices Framework
X9.80 Prime Number Generation Primality Testing, and Primality Certificate
X9.84 Biometric Information Management and Security for the Financial Services Industry
X9.95 Trusted Time Stamp Management and Security
X9.96 XML Cryptographic Message Syntax (XCMS)

| | |
|--|---------------|
| MANAGEMENT STANDARDS | PG. 28 |
| X9.99 Privacy Impact Assessment Standard | |
| RETIRED DOCUMENTS | PG. 29 |
| HOW TO JOIN ASC X9, INC. | PG. 30 |
| MEMBERSHIP ENROLLMENT FORM | PG. 32 |



HOW TO PURCHASE STANDARDS ONLINE (*see next page for hard-copy order)

The Accredited Standards Committee X9 (ASC X9) is the only organization accredited by the American National Standards Institute (ANSI)* developing technical standards for the financial services industry. Under agreement with X9, ANSI sells its standards through the ANSI webstore www.ansi.org

Please make your standards selection carefully. X9 is unable to provide refunds nor can we accept returns or cancellations of electronic documents purchased through the X9/ANSI webstore. ALL SALES ARE FINAL. If you are unsure of your selection or if you need further information, please feel free to contact X9 staff before placing your order:

You may access the X9 electronic bookstore in three ways:

- www.x9.org – click on X9 Standards Information then on Standards Store
- www.ansi.org – click eStandards Store
- <http://webstore.ansi.org>

Payment

Standards may be purchased using: MasterCard®, VISA® American Express®.

Free Standards for Accredited Standards Committee X9 members

ASC X9 members in good standing at the X9 membership Category A, B or C levels have full access to X9 standards free of charge. Information about membership in ASC X9 is located beginning on page 26 of this catalog.

Deposit Accounts

ANSI offers a Deposit Account purchase method which enables ANSI customers to purchase individual copies of electronic documents at any time, but will not require use of a credit card to complete the transaction. The Deposit Account option was established in direct response to customer requests for alternate methods of payment via the eSS. An initial deposit of \$200 is required to establish a Deposit Account.

The Deposit Account owner will be able to view the running account balance online. A purchase history will be available via the ANSI Customer Service Department. To establish a Deposit Account you must sign the Deposit Account License Agreement and return the signed agreement with your payment to:

Manager, Customer Services, American National Standards Institute
25 West 43rd Street, New York, NY 10036
Tel: 212-642-4900, Fax: 212-302-1286



HOW TO PURCHASE HARD COPY STANDARDS

If you would like to order a hard copy of a standard, please submit an e-mail order to Global Engineering Documents at global@ihs.com. You may also contact Global Engineering Documents - Customer Service at 800-854-7179 or 303-397-7956 or you may reach the Customer Service Department by fax at 303-397-2740, or by mail:

Global Engineering Documents
15 Inverness Way
East Englewood, CO 80112

Does ANSI Charge Sales Tax?

No. ANSI is a 501 (C) 3, not-for-profit and tax-exempt organization. Thus, they are not required to charge sales tax on purchases.

Prices

Prices are subject to change without notice. All orders will be filled at the current price.

TERMS AND DEFINITIONS

American National Standard

Standards developers accredited by the American National Standards Institute (ANSI) use the "Approved American National Standard" mark and term the standard an American National Standard.

Draft Standard for Trial Use (DSTU)

These are not American National Standards. Draft Standards for Trial may be published by accredited standards developers for trial use and comment in trade or technical journals, or as separate publications for a period of up to three years. The availability of such draft standards shall be registered with ANSI and announced in ANSI's Standards Action, other appropriate media and, if practical, may be listed in ANSI's catalog.

Reaffirmed

An American National Standard that has been reviewed and approved by the consensus body and no changes have been made to it.

Accredited Standards Committee X9, Inc. (ASC X9, Inc.)

Accredited Standards Committee X9, Incorporated, Financial Industry Standards. The ANSI-accredited body that develops national financial industry standards.

American National Standards Institute (ANSI)

A national federation of standards developers. X9 is not ANSI, X9 is accredited by ANSI and each organization has their own separate membership.

International Organization for Standards (ISO)

International Organization for Standardization, or SO/IEC.



Special Pricing

X9's Check 21 Standards Collection II

A newly updated collection to allow persons dealing with payments to meet Check 21 requirements. ASC X9 Check 21 Standards Collection II contains:

X9/TR-100 Organization of Standards for Paper-based and Image-based Payments, Part 1: Organization of Standards for Paper-based and Image-based Payments Organization of Standards

X9/TR-100 Organization of Standards for Paper-based and Image-based Payments, Part 2: Definitions used in Standards

X9/TR-33 Check Image Quality Assurance Standards and Processes

X9.100-40 Specifications for Check Image Tests, Part 1: Definition of Elements and Structures;

X9.100-40 Specifications for Check Image Tests, Part 2: Application and Registration Procedures

X9.100-111 Specification for Check Endorsements, formerly X9.53

X9.7 Bank Check Background and Numerical Convenience Amount Field

DSTU X9.100-183 Specifications for Electronic Check Adjustments, formerly X9.83

X9.100-180 Specifications for Electronic Exchange of Check and Image Data, formerly DSTU.37

X9.100-140 Specifications for an Image Replacement Document (IRD) (formerly DSTU X9.90)

Collection Pricing: \$420.00 (a 40% discount off the retail price of \$700.00)



Paper Check Standards

X9/TR-100 Organization of Standards for Paper-based and Image-based Payments

Part 1: Organization of Standards

X9/TR-100 Organization of Standards for Paper-based and Image-based Payments

Part 2: Definitions used in Standards

Part 1 recommends the numbering scheme for all standards associated with paper-based and image-based payments. The numbering scheme is divided into two sections; core standards and application standards. Core standards cover such items as paper requirements, MICR requirements, optical requirements, and image requirements. Application standards cover such items as check documents, deposit tickets, internal documents, image replacement documents, other documents, MICR, security, and electronic.

Part 2 lists the definitions of industry specific words and phrases required for the understanding of paper-based and image-based payment standards.

Publication Date: 2003 (Revised 2005) Free of Charge Download: www.x9.org or www.ansi.org

X9/TR-2 Understanding, Designing and Producing Checks

Certain elements of check design are specified in X9 American National Standards or are mandated by the Uniform Commercial Code (UCC) and the Federal Reserve Board's Regulation CC. TR-2 presents guidelines for the design and production of a check and describes the proper location of the data elements on the check, along with the rationale for those requirements. Additionally, TR-2 provides a summary of requirements and other optional elements, with references, where appropriate, to standards and legal documents. The guidelines contained in this report are intended to promote greater uniformity in the design and production of checks, which will improve processing and handling throughout the check processing system.

Publication Date: 1990 (Revised 2005)

Price: \$100.00

X9/TG-6 Quality Control of MICR Documents

MICR printers are the audience for this standard related to the production and evaluation of MICR documents and the attainment of broader MICR print specification conformance. TG-6 covers all MICR printing and is intended to improve MICR quality via understanding and uniform interpretation of existing standards and specifications of MICR.

Publication Date: 1995 (Revised 2000)

Price: \$100.00

X9/TG-8 Check Security Guideline

TG-8 is written for all parties concerned in setting up procedures and using preventive technologies to fight the fraudulent use of checks. TG-8 details the receiving, writing and preparation of checks, covering all aspects of where fraud can start, where it occurs, and how all involved can help prevent crime.

Publication Date: 1995 (Revised 2001)

Price: \$100.00



X9.7 Bank Check Background and Numerical Convenience Amount Field

This standard includes “image ready” requirements for vital areas of the check document. It is intended to be the guide for check design as financial institutions adopt image technology systems in the US Payments system. Previously X9.7 addressed only the CAR and MICR areas (which basically remain the same). New requirements focus on legibility of handwriting in binary images in what is called Areas of Interest (AOI). These are: Date, Payee, Legal Amount, and Signature Areas. New measurements have also been added for average background reflectance and “paxel count” which is a quantification of black pixels in binary images. These parameters have been specified to predict legibility and assure that the data will be human readable from stored check images. Reflectance is specified as not less than 40%, averaging all pixels in every 1/8 inch area. Background clutter (as allowed) is specified as a maximum paxel count of 12. This revised specification also contains the design of image based test equipment and image processing performance. It includes (after three years of research) an Image Qualifier reference and procedures that creates a standard binary image and automatically tests for X9.7 conformance.

Publication Date: 1988 (Revised 1999)

Price: \$140.00

***NEWLY REVISED!!* X9.100-10—Formerly X9.18 Paper Specifications for MICR Documents**

This standard establishes paper specifications for the MICR documents that are used in the US Payments System. While checks and deposit tickets are the primary documents considered in these specifications, users of MICR/OCR E-13B font readers will be well served by applying these specifications to internal documents, when intended for use in reader/sorters. This standard gives specifications to those attributes most important and most common both to raw base stock and to finished printed products of MICR documents. When available, methodology for measurements of the various paper attributes shall conform to those of the Technical Association of Pulp and Paper Industry (TAPPI).

Publication Date: 1993 (Revised 2006)

Price: \$60.00

X9.100-111--Formerly X9.53) Specification for Check Endorsements

This standard provides for the legibility and uniformity of the endorsement process. It specifies the parameters for the design elements on the back of the check and the placement and data content of endorsements. This standard includes an informative annex that provides a method for measuring the legibility of endorsements with the use of a legibility gauge. This standard is not intended to modify existing MICR standards for checks.

Publication Date: 1996 (Revised 2004)

Price: \$60.00

***NEWLY REVISED!!* X9.100-130—Formerly X9.64 Specifications for Universal Interbank Batch/Bundle**

This standard facilitates the use of a Universal Interbank Batch/Bundle Ticket as a replacement for non-standard batch tickets and bundle dividers. The Universal Interbank Batch/Bundle Ticket may be used by both a sending and receiving financial institution. A standardized ticket stream- lines check processing operations by eliminating the need to replace a sending bank’s bundle divider tickets with the receiving bank’s batch tickets. The Universal Batch/Bundle Ticket standardizes the MICR line data and ticket design in order to take advantage of the existing automated environment.

Publication Date: 2001 (Revised 2006)

Price: \$60.00



X9.100-151--Formerly X9.40 Check Correction Strip Specification

Design and the functional characteristics of the strip extension (strip) as affixed to a check or other document is covered in this American National Standard. These strips provide a new MICR clear bank area used to modify or correct the MICR line of items for forward collection, returns, rejects, or other banking interchange systems.

Publication Date: 1994 (Reaffirmed 2004)

Price: \$60.00

X9.100-160(formerly X9.13): Part 1, Placement and Location of Magnetic Ink Printing (MICR)

This Part 1 of a two Part standard on financial industry MICR covers design considerations that apply to placement and location of magnetic ink printing on checks, drafts, and other documents intended for automated processing among depository institutions. Other types of documents such as internal control forms are not covered.

Publication Date: 1990 (Revised 2004)

Price: \$100.00

X9.100-160 (formerly X9.13, Annex A only) **Placement and Location of Magnetic Ink Printing (MICR):**

Part 2: EPC Field Use Part 2 of the MICR standard establishes external processing code (EPC) assignments and management, and specifies the MICR characters approved for use in the U.S. Payments System.

Publication Date: 1990 (Revised 2004)

Price: \$60.00

X9.100-161 (formerly X9.47) Creating MICR Document Specification Forms

The contents for MICR Document specification Forms are specified in this X9 American National Standard. It may be used to create specifications for the design and manufacture of checks and deposit tickets, as well as other financial institution MICR documents. The standard is sufficiently flexible to meet the needs of a variety of financial institutions. The standard is not the specification form itself.

Publication date: 2001 (Revised 2004)

Price: \$60.00

X9.100-120 (formerly X9.33) Specifications for Bank Deposit Tickets

This standard was developed to encourage greater uniformity in the design of deposit tickets, which will improve their processing and handling throughout the entire check processing system. This standard specifies certain deposit ticket parameters to provide for the processing of personal size and business size deposit tickets through conventional bank deposit and imaging processes. The location and design of the item listing and total amount data elements are specified. This standard will improve the understanding of deposit tickets by providing background information which may be valuable in the deposit ticket design stages.

Publication Date: 1999 (Revised 2004)

Price: \$60.00

X9.100-170 (formerly X9.51) Specifications for the Padlock Icon

This standard establishes the design and usage requirements of the padlock icon for visually communicating the presence of security features on a check. The standard specifies characteristics of security features that meet the requirements for use of the padlock icon. Information about specific security features can be found in ASC X9/TG-8.

Publication Date: 1999 (Revised 2004)

Price: \$60.00



NEW!! X9.100-20 (formerly X9.27) Print and Test Specifications for Magnetic Ink Printing

The character set includes numerals 0 through 9 and four special symbols. The standard also specifies the shape, dimensions, and tolerances for printed MICR "E-13B" characters and specifications regarding print quality.

Publication Date: 2006

Price: \$140.00

NEW!! X9 TR-33-2006 Check Image Quality Assurance Standards and Processes

Technical Report 33 presents a framework for assuring and assessing image quality to support the exchange of check images between financial institutions. It provides a detailed understanding of the problems and limitations associated with the image capture process, automated methods and systems that might be used to detect check quality problems (i.e., image defects and usability issues).

This report will establish common terminology around check image quality so as to facilitate communication among operations and technical managers at financial institutions.

Publication Date: 2006

Price: \$100.00

NEW!! X9.100-40 Part 1 Specifications for Check Image Tests

Part 1: Definition of Elements and Structures

This Part 1 of ANS X9.100-40 defines the elements and structures for standard check image tests used by the financial industry to assess specific attributes of check images. The specification establishes a framework for defining check image tests, conveying the results from executing a check image test, and conveying any parameters used in executing check image tests.

NEW!! X9.100-40 Part 2 Specifications for Check Image Tests

Part 2: Application and Registration Procedures

Part 2 of ANS X9.100-40 describes the application and registration procedures used to register check image tests that conform to this ANS X9.100-40 Part 1 standard. Check image tests that are submitted to X9 for consideration in accordance with ANS X9.100-40 Part 2 shall be entered in the X9 Registry for Check Image Tests after the Application for a new check image test is approved. In this standard, the term "check" includes checks, substitute checks, and related check-sized financial items such as deposit tickets, cash tickets, and batch headers. Although the initial application for this standard is to support check image tests pertaining to image quality, the standard is applicable to any check image test that has a business purpose and is compatible with the structure defined herein.

Publication Date: 2006

Price: \$140.00 for Parts 1 & 2



Electronic Check Processing Standards

X9.100-140 (formerly DSTU X9.90) Specifications for an Image Replacement Document (IRD)
X9.100-140 establishes the construction, layout, data elements, data content, and printing specifications for Image Replacement Documents (IRD). An IRD is a substitute image copy of a check or a replacement for a previous IRD that includes a machine readable MICR line. An IRD that may under certain legal arrangements be the practical and legal equivalent of the original paper check or a previous IRD. An IRD conforming to these specifications may be used as a Substitute Check in conformance with the Check Clearing for the 21st Century Act (Check 21 Act or Act). Please note that this standard does not address operational, implementation, or settlement issues. These issues may include but are not limited to: the use of security features that are available after imaging, image compression, conversion methods, and IRD printing techniques. The informative annexes within this standard provide information that may prove useful to those implementing the standard.

Publication Date: 2004

Price: \$100.00

X9.100-171 (formerly DSTU X9.85) Specifications for Automated Identification of Security Features
This Standard defines a structure to properly identify security features using automation. The Standard enables the incorporation of standard and proprietary security features into the original check by providing a trigger and identification structure. The Standard provides a means of registering security features for use within this Standard; however it does not specify the aspects of security features.

Publication Date: 2005

Price: \$60.00

NEW!! X9.100-180 (formerly DSTU.37) Specifications for Electronic Exchange of Check and Image Data
The standard was designed to accommodate and work with existing data formats used to transmit check-related data, and to provide flexibility in accommodating future developments in check processing and check product offerings. The use of this standard will enable financial institutions to cut processing costs and fraud losses by reducing the number of times a paper item must be handled, and by shortening the forward presentment and return cycle time frames.

Publication Date: 2006

Price: \$100.00

DSTU X9.100-183 (formerly X9.83) Specifications for Electronic Check Adjustments
This draft standard establishes the file sequences, record types, and field formats to be used in the electronic exchange of check adjustment messages. The standard format supports check related adjustment notices and requests for individual checks, bundles of checks, check cash letters and attachment of images. It supports the full range of adjustment types currently in use by financial institutions and will support web-based or mainframe system transmission. The standard may be used whether or not the particular check, bundle of checks, or cash letter was presented via paper or via an electronic check exchange file. This standard does not address certain operational, implementation, or settlement issues.

Publication Date: 2005

Price: \$60.00



Electronic Retail, Security and Electronic Benefits Transfer (EBT) Standards

X9/TG-7 Initial DEA Key Distribution for PIN Entry and Transaction Originating Devices

This technical guideline provides guidance for the implementation of ANS X9.24 Section 3.5. Included are methods available for distributing the first cleartext key to PIN entry and transaction originating devices used in the retail financial services environment. The procedures and the ancillary equipment required to generate transport, and insert such keys is described. The cryptographic devices include, but are not limited to PIN pads, automatic teller machines (ATM), key generation devices, and key loading devices.

Publication Date: 1995

Price: \$60.00

X9.58 Financial Transaction Messages – Electronic Benefits Transfer (EBT) – Food Stamps

This standard provides all parties involved in Electronic Benefits Transfer (EBT) transactions for Food Stamps with technical specifications for exchanging financial transaction messages between an acquirer and an EBT card issuer processor. It specifies message structure, format and content, data elements and values for data elements used in the Food Stamp program. The method by which settlement takes place is not within the scope of this standard.

Publication Date: 2002

Price: \$60.00

X9.93 Financial Transaction Messages – Electronic Benefits Transfer (EBT)

Part 1: Messages

This part 1 of this two part standard provides all parties involved in EBT transactions with technical specifications for exchanging financial transaction messages. The document standardizes message formats based on the ISO 8583:1993 standard and thereby maximizes EBT productivity for all stakeholders in the industry.

Publication Date: 2002

Price: \$60.00

X9.93 Financial Transaction Messages – Electronic Benefits Transfer (EBT)

Part 2: Files

This part 2 of this two part standard, provides all parties involved in EBT transactions with technical specifications for exchanging financial transaction files for Women, Infants and Children (WIC) program.

Publication Date: 2002 (Revised 2004)

Price: \$60.00



X9.104 Financial transaction card originated messages, card acceptor to acquiring host messages

Part 1: Messages, data elements and code values

Part 1 of this two part standard defines a common interface for the exchange of information between point of sale systems or terminal devices located in a retail establishment and the acquiring host transaction processing system(s). This part of X9.104 is applicable to all aspects of payment processing required by these retail facilities, including the reporting of specific products that are part of a purchase. The standard defines a sufficient number of message types and data elements to facilitate the exchange of all necessary information related to: (1) payment transactions originated by point of sale systems or terminal devices, and (2) automated control of the systems and devices. This standard defines the specific use and additional values of many data elements in the message formats contained in ISO 8583.

Publication Date: 2004

Price: \$100.00

X9.104 Financial transaction card originated messages, card acceptor to acquiring host messages

Part 2: Convenience store and petroleum marketing industry

Part 2 of this two part American National Standard X9.104 provides example of messages used in the convenience store and petroleum marketing industry based on the message formats defined in X9.104 part 1. This part of X9.104 also defines data elements and code values for use in this environment.

Publication Date: 2004

Price: \$100.00

X9.105 (identical to ISO 8583-1:2003) Financial Transaction Card Originated Messages – Interchange Message Specifications

Part 1: Messages, Data Elements and Code Values

Part 1 of this three part American National Standard and identical to its international counterpart of the same name, specifies a common interface by which financial transaction card-originated messages can be interchanged between acquirers and card issuers. The standard specifies message structure, format and content, data elements and values for data elements. The method by which settlement takes place is not within the scope of this part. NOTE: With the proliferation of technology available to financial institutions to offer services to customers, a range of tokens (financial transaction cards, digital certificates etc.) now exist for identifying account relationships. In order to maintain clarity, this part of the standard will continue to refer only to financial transaction cards as the token. However, readers should be aware that the actual token issued by a financial institution may be different.

Publication Date: 2003

Price: \$175.00

X9.105 (identical to ISO 8583-1:2003) Financial Transaction Card Originated Messages – Interchange Message Specifications

Part 3: Maintenance Procedures for Messages, Data Elements and Code Values

Part 3 establishes the role of the maintenance agency (MA) and specifies the procedures for adding messages and data elements to ISO 8583-1 and to codes listed in Annex A of X9.105-1 (Identical to ISO 8583-1). The responsibilities of the MA relate to all message type identifiers and classes, data elements and sub-elements, dataset identifiers and codes within X9.105-1 (Identical to ISO 8583-1), with the exception of Institution Identification Codes.

Publication Date: 2003

Price: \$60.00



X9.106 (identical to ISO 18245) Retail Financial Services – Merchant Category Codes

This American National Standard is an identical adoption of ISO standard 18245 which defines code values used to enable the classification of merchants into specific categories based on the type of business, trade or services supplied. Values are specified only for those merchant categories that are generally expected to originate retail financial transactions. This standard also establishes the procedures for a Registration and Maintenance Management Group (RMMG), which considers requests for new code values, and a Maintenance Agency (MA), which provides the administrative procedures required to maintain an up-to-date list of codes. It is not within the scope of this International Standard to mandate the use of merchant category codes in any given situation.

Publication Date: 2003

Price: \$80.00

X9.107(identical to ISO 4909) Bank Cards – Magnetic Stripe Data Content for Track 3

This American National Standard is an identical adoption of its international counterpart ISO 4909 and establishes specifications for cards issued by or acceptable to the banking industry and is intended to permit interchange based on the use of magnetic stripe encoded information. It specifies the data content and physical location of read/write information on track 3 and is to be used in conjunction with the relevant parts of those documents quoted in clause 2. Using track 3 in conjunction with track 2 is a mode of operation in both on-line and off-line interchange environments.

This mode of operation requires that the original encoded data on track 2 be read; the data on track 3 be read; and, if update is required, all the data on track 3 be rewritten. Independent use of track 3 is an alternative mode of operation permitting both on-line interchange and off-line interchange based on mutual agreement between interested parties. It requires reading only of the data on track 3 and, if update is required, the rewriting of all the data on track 3.

Publication Date: 2003

Price: \$60.00

DSTU X9.108 Financial Transaction Messages – Electronic benefits transfer (EBT) – WIC retailer interface standard

This Draft Standard for Trial Use (DSTU) defines a common set of Application Programming Interface (API) functions to access the WIC benefits on a smart card in the retailer environment; a common method (card discovery mechanism) to identify the issuer of the WIC EBT benefits and the WIC EBT scheme present on the smart card and, an interface to the card reader device that transmits and receives data from the WIC EBT smart card. The reference implementation provided by the WIC authority shall utilize this standard. This standard does not specify the reader driver used by the retailer application but it defines interfaces that may be implemented for the WIC module to access function of the Reader Driver Module (RDM). The use of pseudo Interface Definition Language (IDL) in this standard allows simpler definition of the API functions and their interface in a language independent manner. This standard does not define how WIC-EBT benefits are arranged on the card, the movement of security data or key management.

Publication Date: 2005

Price: \$60.00



Credit Standards

X9.103 Motor Vehicle Retail Sale and Lease Electronic Contracting

The scope of this American National Standard begins at the time of signing the Contract, inclusive of signature capture, and includes the creation, storage and assignment of Electronic Chattel Paper where the assignment will involve establishing control of the Electronic Chattel Paper. This standard addresses both electronically originated Chattel Paper and Tangible Chattel Paper that is subsequently converted to an electronic format. This standard addresses the creation, storage, and assignment of Electronic Chattel Paper where assignment involves establishing "control" of the Electronic Chattel Paper. In addition, this standard addresses retail installment sale and lease contracts in the automotive dealer financing industry. However, it may be useful in establishing a similar process for banks, credit unions, and finance companies that make secured loans directly to buyers to enable them to purchase vehicles.

Publication Date: 2004

Price: \$60.00

TR-4 (companion to X9.103) Financial Services Technical Report SPeR

Standards and Procedures for Electronic Records and Signatures

ASC X9 develops American National Standards that support technological solutions, industry practices, and processes, to provide an enforceable structure for electronic signature and records. ASC X9 Inc approved the inclusion in its collection of the SPeRS document and has registered the document as an X9 Technical Report in an effort to establish a common understanding for consumers and businesses for any interstate and foreign commerce transaction in the use of signatures, contracts or other records in electronic form. SPeRS was prepared by the SPeRS Drafting Committee of the Electronic Financial Services Council in 2003.

X9 TR 4-2004 focuses on five areas:

- Authentication;
- Obtaining Consent to do Business;
- Establishing Agreements Online, and Meeting Notice and Disclosures Requirements;
- Electronic Signatures; and
- Record Retention.

Publication Date: 2004

Price: \$295.00



Securities Processing Standards

X9/TG-10 Signature Guarantee Guideline

TG-10 is meant to educate guarantors to the importance of safekeeping and controlling medallions (hand stamps and/or machine plates) issued to them by their program administrator. Securities Exchange Commission Rule 17Ad-15 dramatically reshaped the method by which financial institutions guarantee signatures and thereby transfer securities. Any financial institution can now guarantee signatures as long as certain protection for transfer agents is provided. Three signature guarantee programs were established following enactment of Rule 17Ad-15 in January, 1992.

Publication Date: 1995

Price: \$100.00

X9.5 Financial Institution Numbering System (FINS)

This American National Standard outlines the industry-wide numerical identification system for banks, broker/dealers, insurance companies, mutual funds and other institutions (FINS) engaged in securities transactions. This standard specifies both the configuration of the number and the meaning attached to each portion. The FINS number will serve as the common denominator in communications among users of completion of transactions and exchange of information.

Publication Date: 1988 (Reaffirmed 2001)

Price: \$100.00

X9.6 Securities Identification System

This American National Standard provides the specification for uniquely identifying securities issues. The standard serves as the common denominator in communications among users for completion of transactions and exchange of information. Both the configuration of the number and the meaning attached to each portion is specified.

Publication Date: 1991 (Reaffirmed 1998)

Price: \$100.00

X9.12 Specifications for Fully Registered Municipal Securities

This standard gives the physical characteristics and format of a registered municipal security including certificate size, content and layout. The standard establishes uniformity among registered municipal securities while addressing the needs of all segments of the municipal securities industry. Printers will be assured of industry acceptance.

Publication Date: 1991 (Reaffirmed 1998)

Price: \$100.00

Specifications for Securities Transaction Interchange Forms (X9.14)

This standard provides specifications for certain forms used by banks, brokers, dealers and other members of the securities industry in the processing of securities transactions. The standard supplies minimum requirements for the physical characteristics of preprinted forms and specifies the design of these forms. Included are three diagrams of forms used for securities processing. The use of standardized forms will foster greater efficiency and provide for a more streamlined processing function.

Publication Date: 1983 (Reaffirmed 2001)

Price: \$100.00



Securities Institutional Delivery System (X9.20)

X9.20 describes a user format that will allow more efficient computer-to-computer processing in a securities transaction. The format followed processes security transactions through the National Delivery System operated by a clearing corporation or depository, and specifies formats to be used by all institutions involved in the securities business such as banks, brokers, and investment and money managers.

Publication Date: 1990 (Revised 1998)

Price: \$100.00

International Securities Identification Numbering System (ISIN) (X9.101) (Identical to ISO 6166)

This American National Standard an identical adoption of the ISO 6166 – Title standard provides a uniform structure for inter-national securities identification numbers (ISINs). It is intended for use in any application in the trading and administration of securities and other financial instruments.

Publication Date: 2003

Price: \$60.00



Data and Information Security Standards

Retail Financial Services Compliance Guideline - Part 1: Online PIN Security and Symmetric Key Management (TG-3)

This Technical Guideline applies to all organizations using the Triple Data Encryption Algorithm (TDEA) for the encryption of PINs used for retail financial services such as POS and ATM transactions, messages among retailers and financial institutions, and interchange messages among acquirers, switches and card issuers. The guideline should be completed by all organizations acquiring or processing transactions containing PINs, from the terminal driving system to the authorizing entity. The guideline questions address security controls from the PIN entry device to the interface delivering the transaction to the authorizing entity. The guideline is not intended to apply to the security procedures and controls of the authorizing entity; however, authorizing processors are not discouraged from using this guideline to perform an internal review of their proprietary security controls. This guideline also does not apply to entities between the terminal and the authorizing entity, which act as 'pass-through' processors, receiving and forwarding the encrypted PIN without decrypting or translating the encrypted information. The 'pass-through' processor does not have knowledge of the encrypting keys used to protect the PIN, nor does it perform any cryptographic processing. This guideline also does not apply to the procedures or controls associated with message authentication or asymmetric cipher systems.

Publication Date: 1997 (*Revised 2004*)

Free of Charge: www.x9.org or www.ansi.org

Initial DEA Key Distribution for PIN Entry and Transaction Originating Devices (X9/TG-7)

This technical paper provides guidance for the implementation of ANS X9.24 Section 3.5. Included are methods available for distributing the first cleartext key to PIN entry and transaction originating devices used in the retail financial services environment. The procedures and the ancillary equipment required to generate transport, and insert such keys is described. The cryptographic devices include, but are not limited to PIN pads, automatic teller machines (ATM), key generation devices, and key loading devices.

Publication Date: 1995

Price: \$60.00

Abstract Syntax Notation and Encoding Rules for Financial Industry Standards (X9/TG-9)

This tutorial guideline helps the user to understand Abstract Syntax Notation One (ASN.1), the international standard language for defining and encoding data elements in the open systems environment. ASN.1 provides for a more precise specification of message fields and other data, improving interoperability and reducing costs. TG-9 familiarizes the reader with the ASN.1 concepts in ISO/IEC 8824, Specification of ASN.1 and ISO/IEC 8825, Specification for Basic Encoding Rules for ASN.1, without requiring the reader to read the international documents.

Publication Date: 1996

Price: \$60.00



Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms (X9/TR-31)

This document describes a method consistent with the requirements of ANS X9.24 Retail Financial Services Symmetric Key Management Part 1 for the secure exchange of keys and other sensitive data between two devices that share a symmetric key exchange key. This method may also be used for the storage of keys under a symmetric key. This method is designed to operate within the existing capabilities of devices used in the retail financial services industry.

This document is not a security standard and is not intended to establish security requirements. It is intended instead to provide an interoperable method of implementing security requirements and policies.

Publication Date: 2005

Price: \$60.00

Personal Identification Number (PIN) Management and Security – Part 1: PIN Protection Principles and Techniques for Online PIN Verification in ATM & POS Systems (X9.8:1)

Part 1 of this two part standard specifies the basic principles and techniques which provide the minimum security measures required for effective international PIN management. These measures are applicable to those institutions responsible for implementing techniques for the management and protection of PINS.

PIN protection techniques applicable to financial transaction card originated transactions in an online environment and a standard means of interchanging PIN data. These techniques are applicable to those institutions responsible for implementing techniques for the management and protection of the PIN at Automated Teller Machines (ATM) and acquirer-sponsored Point-of -Sale (POS) terminals.

Publication Date: 1991 (Revised 2003)

Price: \$100.00

Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques (X9.24-1)

This part 1 of this two part American National Standard covers both the manual and automated management of keying material used for financial services such as point-of-sale (POS) transactions (debit and credit), automated teller machine (ATM) transactions, messages among terminals and financial institutions, and interchange messages among acquirers, switches and card issuers. This part of ANS X9.24:1 deals exclusively with management of symmetric keys using symmetric techniques. Additional parts may be created in the future to address other methods of key management.

Part 1 specifies the minimum requirements for the management of keying material. Addressed are all components of the key management life cycle including generation, distribution, utilization, storage, archiving, replacement and destruction of the keying material. An institution's key management process, whether implemented in a computer or a terminal, is not to be implemented or controlled in a manner that has less security, protection, or control than described herein. It is intended that two nodes, if they implement compatible versions of:

- the same secure key management method:
- the same secure key identification technique approved for a particular method: and
- the same key separation methodologies

Publication Date: 1992 (Revised 2004)

Price: \$140.00



NEW! Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys (X9.24-2)

This part of ANS X9.24 covers the management of keying material used for financial services such as point of sale (POS) transactions, automatic teller machine (ATM) transactions, messages among terminals and financial institutions, and interchange messages among acquirers, switches and card issuers. The scope of this part of X9.24 may apply to Internet-based transactions, but only when such applications include the use of a TRSM (as defined in section 7.2 of ANS X9.24 Part 1) to protect the private and symmetric keys. This part of ANS X9.24 deals with management of symmetric keys using asymmetric techniques and storage of asymmetric private keys using symmetric keys. Additional parts may be created in the future to address other methods of key management.

This part of ANS X9.24 specifies the minimum requirements for the management of asymmetric keying material and TDEA keys used for ensuring the confidentiality and integrity of the private keys of asymmetric key pairs when stored as cryptograms on a database. Addressed are all components of the key management life cycle including generation, distribution, utilization, storage, archiving, replacement and destruction. Requirements for actions to be taken in the event of key compromise are also addressed. This part of ANS X9.24 presents overviews of the keys involved in the key transport and key agreement protocols, referencing other ANSI standards where applicable.

Publication Date: 2006

Price: \$140.00

Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (X9.31)

The standard (adopted from ISO/IEC 9796-2 and ISO/IEC 14888-3 [16]), defines a method for digital signature generation and verification to protect financial messages and data using reversible public key cryptography systems with message recovery. The standard also provides the criteria for the generation of public and private keys required by the algorithm and the procedural controls required for algorithm security. The standard guards against more modern factoring attacks such as the Elliptic Curve Method, the Quadratic Sieve, and the Number Field Sieve, by requiring that the key be sufficiently large to make attacks infeasible.

Publication Date: 1998

Price: \$100.00

Financial Institution Data Compression (Wholesale) (X9.32)

This American National Standard establishes a method for the compression, decompression, and related control functions associated with the electronic transmission of wholesale financial data. Also provided within this standard are techniques to allow for the optimization of the compression function, to detect errors in the compression process, and to prevent the expansion of data.

Publication Date: 1992 (Revised 1998)

Price: \$60.00



Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography (X9.42)

Electronically communicated data is often secured using symmetrically-keyed cryptographic algorithms (e.g., ANSI X9.52 - title, Triple-DEA) in combination with public key cryptography-based key management techniques. This standard defines the secure establishment of symmetric keys using Diffie-Hellman and MQV algorithms. The Diffie-Hellman key agreement mechanism is a widely implemented public key technique that facilitates cost-effective cryptographic key agreement across modern distributed electronic networks such as the Internet. The MQV algorithm is a variation of the Diffie-Hellman algorithm that has more security attributes and may provide better performance over analogous Diffie-Hellman methods. Because the Diffie-Hellman and the MQV techniques are based on the same fundamental mathematics as the Digital Signature Algorithm (DSA) (ANSI X9.30, part 1), additional efficiencies and functionality may be obtained by combining these and other cryptographic techniques.

This standard covers methods of domain parameter generation, domain parameter validation, key pair generation, public key validation, shared secret value calculation, key derivation, and test message authentication code computation for discrete logarithm problem based key agreement schemes. The subroutines defined in this standard are used to build key establishment protocols (e.g., ANSI X9.63). These methods are used by different parties to establish a piece of common shared secret information such as cryptographic keys. The shared secret information may be used with symmetrically-keyed algorithms to provide confidentiality, authentication, and data integrity services for financial information, or used as key-encrypting-keys.

Publication Date: 2001 (Revised 2003)

Price: \$100.00

Enhanced Management Controls Using Digital Signatures and Attribute Certificates (X9.45)

This American National Standard describes the use of attribute certificates and other mechanisms defined in ANSI X9.57, Certificate management [2], to allow the verifier (e.g., recipient) of a signed document or transaction to determine whether the document or transaction can be considered authorized according to the rules and limits agreed to by the parties to the transaction [1,3]. Such rules and limits are embedded in a particular form of attribute certificate, called an authorization certificate. (Other types of attribute certificates may be defined in other X9 standards.) This standard defines a number of specific attributes and data formats for use in various types of authorization certificates. Per-signer information required to make authorization decisions is supplied as signature attributes by the signer. These attributes, along with attributes contained in or extracted from the document, are compared with attributes in the authorization certificates of the signers.

Publication Date: 1999

Price: \$100.00

Secure Remote Access to Financial Services for the Financial Industry (X9.49)

The American National Standard X9.49 is designed to define a minimum level of security requirements for a secure and protected exchange of information between a user and a financial service provider. The standard is intended for use by banks and other payment system groups to implement controls that reduce operational risks in remote access-based financial systems.

When implemented the protection offered will:

- Provide integrity for a message during transmission;
- Provide for secrecy of the message during transmission;
- Identify the correct user and financial service provider to and during data transmission; and
- Prevent repudiation of a message or transaction by user and service provider.

The level of protection provided depends upon the sensitivity of the information exchanged, and could vary among applications.

Publication Date: 1998

Price: \$100.00



Triple Data Encryption Algorithm Modes of Operation (X9.52)

Prudence suggests that financial institutions either using or moving toward the use of Triple DES certify that the algorithm performs according to the X9.52 standard. In addition, the X9 committee is developing a guideline for validating Triple DES implementations. The Technical Guideline-TG19, Part 1: Modes of Operation Validation System for the Triple Data Encryption Algorithm: Requirements and Procedures – defines the methods and procedures for testing Triple DES implementations. National Institute of Standards and Technology (NIST) validation laboratories will provide the service of validation testing for financial institutions and vendors.

Publication Date: 1998

Price: \$100.00

Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) (X9.62)

This American National Standard defines methods for digital signature (signature) generation and verification for the protection of messages and data using the Elliptic Curve Digital Signature Algorithm (ECDSA). ECDSA is the elliptic curve analogue of the Digital Signature Algorithm (ANS X9.30 Part 1).

The ECDSA shall be used in conjunction with the hash function SHA-1 defined in ANS X9.30 part 2. In addition, this ECDSA Standard provides the criteria for the generation of public and private keys that are required by the algorithm and the procedural controls required for the secure use of the algorithm.

Publication Date: 1998

Price: \$100.00

Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography (X9.63)

This American National Standard defines a suite of schemes designed to facilitate the secure establishment of cryptographic data for the keying of symmetrically keyed algorithms (e.g., TDEA). These mechanisms are based on the elliptic curve analogue of the Diffie-Hellman key agreement mechanism (ANSI X9.42). Because the mechanisms are based on the same fundamental mathematics as the Elliptic Curve Digital Signature Algorithm (ECDSA) (ANSI X9.62), additional efficiencies and functionality maybe obtained by combining these and other cryptographic techniques.

This standard specializes ISO/IEC 15946-3 “Cryptographic Techniques Based on Elliptic Curves – Part 3: Key Establishment” for use within the financial services industry. It defines key establishment schemes that employ asymmetric cryptographic techniques. The arithmetic operations involved in the operation of the schemes take place in the algebraic structure of an elliptic curve over a finite field. Both key agreement and key transport schemes are specified. The schemes may be used by two parties to compute shared keying data that may then be used by symmetric schemes to provide cryptographic services, e.g., data confidentiality and data integrity. Supporting mathematical definitions and examples are also provided.

Publication Date: 2002

Price: \$175.00

Triple Data Encryption Algorithm (TDEA) Implementation (X9.65)

This standard specifies methodologies for the implementation of ANS X9.52, Triple Data Encryption Algorithm (TDEA) Modes of Operations for the enhanced cryptographic protection of digital information. The modes of operation defined in ANS X9.52 are specified for both enciphering and deciphering operations. These modes provide a means of extending the effective key space of the ANS X3.92 Data Encryption Algorithm (DEA). ANS X9.52 provides multiple modes of operation. This standard will assist system integrators to select and implement the appropriate mode for their organizations.

Publication Date: 2004

Price: \$60.00



Digital Certificates for Mobile/Wireless and High Transaction Volume Financial Systems (X9.68-2)

This standard defines syntax for a more compact certificate than that defined in ISO 15782-1 and X.509. This syntax is appropriate for use in environments with constraints imposed by mobility and/or limited bandwidth (e.g., wireless communications with personal digital assistants), high volumes of transactions (e.g., Internet commerce), or limited storage capacity (e.g., smart cards). This syntax is also geared towards use in account-based systems such as X9.59.

Publication Date: 2001

Price: \$100.00

Framework for Key Management Extensions (X9.69)

American National Standard X9.69 defines methods for the generation and control of keys used in symmetric cryptographic algorithms. The Standard defines a constructive method for the creation of symmetric keys, by combining two or more secret key components. The Standard also defines a method for attaching a key usage vector to each generated key that prevents abuses and attacks against the key. The two defined methods can be used separately or in combination.

Publication Date: 1998

Price: \$60.00

Cryptographic Message Syntax (X9.73)

This American National Standard specifies a cryptographic message syntax that can be used to protect financial transactions and other documents from unauthorized disclosure and modification. The message syntax has the following characteristics:

- Messages are protected independently. There is no cryptographic sequencing (e.g., cipher block chaining) between messages. There need not be any real-time connection between the sender and recipient of the message. This makes the syntax suitable for use over store-and-forward systems, e.g., Automated Clearing House (ACH). Standard attributes are defined to allow applications to maintain relationships between messages, if desired;
- The syntax is algorithm independent. It supports confidentiality, integrity, origin authentication, and non-repudiation services. Only ASC X9-approved algorithm(s) may be used for message encryption, digital signature, message authentication, and key management;
- Support for biometric security (ANS X9.84), enhanced certificate techniques such as domain certificates (ANS X9.68) and key management extensions such as constructive key management (ANS X9.69) are provided; and
- Selective field protection can be provided by combining multiple instances of this syntax into a composite message.

Publication Date: 2003

Price: \$60.00

Financial Services PKI Policy and Practices Framework (X9.79)

This standard establishes a framework of policy and practices requirements for a PKI including the control objectives to be achieved and the underlying control procedures known to support these control objectives. The control procedures identify (when possible) the applicable requirements from supporting industry standards. The form of both the Certificate Policy and Certification Practice Statement are consistent with industry best practices.

Publication Date: 2001

Price: \$60.00



Prime Number Generation Primality Testing, and Primality Certificates (X9.80)

This standard defines methods for generating large prime numbers as needed by public key cryptographic algorithms. It also provides testing methods for testing candidate primes presented by a third party.

This standard allows primes to be generated either deterministically or probabilistically, where:

- A number shall be accepted as prime when a probabilistic algorithm that declares it to be prime is in error with probability less than 2^{-100} .
- A deterministic prime shall be generated using a method that guarantees that it is prime.

In addition to algorithms for generating primes, this standard also presents primality certificates for some of the algorithms where it is feasible to do so. The syntax for such certificates is beyond the scope of this document. Primality certificates are never required by this standard. Primality certificates are not needed when a prime is generated and kept in a secure environment that is managed by the party that generated the prime.

A requirement placed upon the use of this standard, but out of scope, is as follows:

- When a random or pseudo-random number generator is used to generate prime numbers, an ANSI approved random number (or bit) generator (i.e., one that is specified in an ANSI X9 standard) shall be used. This requirement is necessary to ensure security.

Publication Date: 2001 (Revised 2005)

Price: \$100.00

Biometric Information Management and Security for the Financial Services Industry (X9.84)

This American National Standard specifies the minimum security requirements for effective management of biometric data. Within the scope of this standard the following topics are addressed: Security for the collection, distribution, and processing, of biometric data, encompassing data integrity, authenticity, and non-repudiation; Management of biometric data across its life cycle comprised of the enrollment, transmission and storage, verification, identification, and termination processes; Usage of biometric technology, including one-to-one and one-to-many matching, for the identification and authentication of banking customers and employees; Application of biometric technology for internal and external, as well as logical and physical access control; Encapsulation of biometric data; Techniques for the secure transmission and storage of biometric data; Security of the physical hardware used throughout the biometric data life cycle; Techniques for integrity and privacy protection of biometric data.

Publication Date: 2001 (Revised 2003)

Price: \$100.00



Trusted Time Stamp Management and Security (X9.95)

This American National Standard specifies the minimum security requirements for the effective use of time stamps in a financial services environment. Within the scope of this Standard the following topics are addressed:

- Requirements for the secure management of the time stamp token across its life-cycle, comprised of the generation, transmission and storage, validation, and renewal processes. The requirements in this standard identify the means to securely and verifiably distribute time from a national time source down to the application level.
- Requirements for the secure management of a Time Stamp Authority (TSA)
- Requirements of a TSA to ensure that an independent third party can audit and validate the controls over the use of a time stamp process
- Techniques for the coding, encapsulation, transmission, storage, integrity and privacy protection of time stamp data
- Usage of time stamp technology

Items considered out of scope and not addressed in this standard include the following:

- Requirements for a National Timing Authority imposed by the International Timing Authority
- Application specific requirements and limitations for employing time stamp technology
- The individual's privacy and ownership of time stamp data

Although this standard focuses on the financial services industry, it may be used in other applications where the management and security of time stamps are necessary.

Published Date: 2005

Price: \$100.00

XML Cryptographic Message Syntax (XCMS) (X9.96)

This standard specifies a text based Cryptographic Message Syntax (CMS) represented using XML 1.0 encoding that can be used to protect financial transactions and other documents from unauthorized disclosure and modification. The message syntax has the following characteristics:

1) Protected messages are represented using the Canonical XML Encoding Rules (cXER), and can be transferred as verbose markup text or in a compact, efficient binary representation using the Basic Encoding Rules (BER) or the canonical subset of BER, the Distinguished Encoding Rules (DER).

2) Messages are protected independently. There is no cryptographic sequencing (e.g., cipher block chaining) between messages. There need not be any real-time connection between the sender and recipient of the message. This makes the syntax suitable for use over store-and-forward systems, e.g. Automated Clearing House (ACH) or Society for Worldwide International Funds Transfer (SWIFT). Standard attributes are defined to allow applications to maintain relationships between messages, if desired.

3) The syntax is algorithm independent. It supports confidentiality, integrity, origin authentication, and non-repudiation services. Only X9-approved algorithm(s) may be used for message digest, message encryption, digital signature, message authentication, and key management.

4) Support for biometric security, enhanced certificate techniques such as compact domain certificates and key management extensions such as Constructive Key Management (CKM) are provided.

5) Selective field protection can be provided in two ways. First by combining multiple instances of this syntax into a composite message. And second by using identifier and type markup tag names to select message components to be protected in a single message, which allows reusable message components to be moved between documents without affecting the validity of the signature.

6) Precise message encoding and cryptographic processing requirements are provided.

Publication Date: 2004

Price: \$60.00



Management Standards

Privacy Impact Assessment Standard (X9.99)

This American National Standard recognizes that a Privacy Impact Assessment (PIA) is an important management tool that should be used within an organization or by third parties to identify and mitigate privacy issues and risks associated with processing consumer data using automated, networked information systems. This PIA Standard scope:

- provides references to educate the reader on privacy topics and financial privacy in particular
- describes the privacy impact assessment activity, in general
- defines the common components of a PIA regardless of business system affecting financial institutions, and
- explains how to improve the quality of business-system specific PIAs

A privacy impact assessment (PIA) is different than a privacy compliance audit. A compliance audit determines an institution's current level of compliance with the law and identifies steps to avoid future noncompliance with the law. While there are similarities between PIAs and privacy compliance audits, in that they use some of the same skills and that they are tools used to avoid breaches of privacy, the primary concern of a compliance audit is to just meet the requirements of the law, whereas a PIA should delve much further to identify ways to optimally safeguard privacy. Note: Some laws (e.g. the Gram Leach Bliley act (GLB) address both financial privacy rules and financial security guidelines. X9.99 addresses the privacy aspects, but does not address the security aspects (e.g. the implementation of an information security program (ISP).

This standard recognizes that the choices of system development and risk management procedures are business decisions and as such, the business decision makers must be informed in order to make educated decisions for their institutions. This standard provides a privacy impact assessment structure (e.g., common PIA components, definitions, and informative annexes) for institutions that handle financial information who are seeking to use a PIA as a tool to plan for and to manage privacy issues within business systems that they consider to be

Publication Date: 2004

Price: \$60.00



Retired Documents

This "retired" copyrighted ASC X9, Inc. document has been replaced with an American National Standard. Once retired, ASC X9, Inc. no longer maintains the document and takes no responsibility for errors, omissions or other content of a retired document. Retired Documents may only be purchased through X9. To purchase a retired document, please visit the X9 website at www.x9.org and click on the Standards tab which will reveal the link to Retired Documents.

Formerly DSTU X9.37-2003 Specifications for Electronic Exchange of Check and Image Data (current standard is ANS X9.100-180-2006)

This document, including the normative annexes, establishes the file sequences, record types, and field formats to be used for the electronic exchange of check MICR line, associated check processing data and check images in the form of cash letters.

This document does not address operational, implementation, or settlement issues. These issues may include, but are not limited to a choice of: data and image compression, encryption, and transmission specifications and data representation. The informative annexes attached to this document provide information that may prove useful to those planning on implementation.

Original Publication: 2003

Retired Date: 2006

Price: \$ 60.00



Why not become a Member of ASC X9 today?

ASC X9 standards are widely used and recognized, by banks, companies, organizations, government agencies, consultants, accountants and others. X9 standards are often cited or required by the Federal agencies for use in financial procedures and transactions. In addition, X9 standards continue to be the basis for many international standards used in facilitating global commerce.

ASC X9, Inc. operates under its own procedures and those prescribed by the American National Standards Institute. Presently, ASC X9 operates 4 technical subcommittees and as many as 30 technical working groups developing financial industry technical standards and reports. ASC X9 is the USA Technical Advisory Group (TAG) to the International Technical Committee on Financial Services (TC68) under the International Organization for Standardization (ISO), of Geneva, Switzerland. In this role, X9 holds the USA vote on all ISO standards of TC 68 or its subcommittees SC2, SC4, and SC7.

In 1974, the American National Standards Institute (ANSI) approved the scope of activity for the X9 Standards Committee on Banking, as "Standardization for Facilitating Banking Operations." In June, 1976, the X9 Standards Committee approved expansion of its membership to include vendors, insurance companies, associations, retailers, regulators, and others in the financial services area. With this approval, the name was changed to X9, Financial Services. ANSI first granted X9 official accreditation in 1984. The official committee name became as it remains today, Accredited Standards Committee (ASC) X9, Financial Services. Since this time, ASC X9 was incorporated under a 501 C(6) non-profit designation for associations.

Accredited Standards Committee X9, Inc. members may elect to vote and participate in one or more of the following technical subcommittees:

X9AB – Payments - retail, check, corporate – interfacing with ISO 20022*

X9C - Credit

X9D - Securities Processing

X9F - Data and Information Security

X9 is accredited as the US Technical Advisory Group (TAG) to the ISO committee on Financial Services (TC 68). X9 participates actively in international standards development, supplies votes on TC 68 documents and contributes to the development and adoption of international standards that support the financial industry. X9 approves delegates who represent the US in international meetings and participate in the international development process. In addition, X9 serves as Secretariat to TC 68 and to TC68 SC2 which is the administrator to the TC 68 organization.

* see www.iso20022.org



X9 MEMBERSHIP INFORMATION

Membership in ASC X9 is by organization or company

Category A - Board Membership & Full Voting Privileges

\$8,000

The Category A membership provides an organization with the opportunity to name a representative to the ASC X9's Board of Directors. Category A members belong to and participate in multiple subcommittees and their working groups. The Category A member votes on new work projects, standards, the association's procedures/policies, and directs the work of all subcommittees and working groups. The Category A member receives access to the member section of X9's website. Category A membership allows for free of charge download of all X9 Standards and Technical Guidelines.

Category B - Membership Voting Privileges

\$4,750

Category B membership provides an organization with voting privileges on a single X9 subcommittee and access to that subcommittee's working groups. A Category B member votes on the standards under their subcommittee of choice. Category B members receive member access to X9's website and can download all X9 Standards and Technical Guidelines free of charge.

Category C - Membership Limited Voting

\$2,500

Category C membership is limited in its availability. Category C membership is open to organizations with gross revenues of less than \$1 million and who employ fewer than 100 persons (letter of confirmation required). Category C members voting privileges are for ballots related to a single X9 subcommittee and access to that subcommittee's working groups. Category C members receive member access to X9's website and can download all X9 Standards and Technical Guidelines free of charge.

Category E - Membership Working Group Only

\$400

Category E membership limits participation to a single ASC X9 national/US working (domestic) group. Category E members may participate on multiple working groups at the fee of \$400 per working group. Category E members are provided access to the documents(s) under development in those chosen working group(s). Category E members have no voting privileges.

Information concerning participation in the activities of ASC X9 may be received through direct contact with admin@x9.org.



ACCREDITED STANDARDS COMMITTEE X9, INC. MEMBERSHIP ENROLLMENT APPLICATION

Please indicate the method of payment:

Check enclosed. (Make check payable to Accredited Standards Committee X9, Inc.)

Charge my credit card: Discover VISA MasterCard American Express

Account Number: _____ Expiration Date: _____

Signature: _____ Date: _____

Choose the appropriate category for your organization:

Categories A, B and C have free access to all ASC X9, Inc. Standards on the www.x9.org website.

Category A \$8,000 Category B \$4,750 Category C \$2,500**
Category E \$400 (Per national working group - indicate group(s) below)

** smaller organization

Please indicate Working Group(s)

(e.g., X9F1) _____

*Please choose the Subcommittee(s) that interests you:

X9AB Payments Subcommittee - Electronic Retail, Check and Corporate Financial Transactions X9C Credit
X9D Securities Processing X9F Data and Information Security

Please complete both sections below.
Your Company's Principal Contact

Name _____
Title _____
Organization _____
Address _____
City _____ State _____ Zip Code _____
Phone (_____) _____ Fax (_____) _____ Email _____

Your Company's Alternate Contact

Name _____
Title _____
Organization _____
Address _____
City _____ State _____ Zip Code _____
Phone (_____) _____ Fax (_____) _____ Email _____

We _____ (name of organization) understand that we are making application to join ASC X9, Inc. as a member. We understand that upon receipt of our application and membership dues by ASC X9, Inc. they will provide appropriate access to the member-side of the ASC X9, Inc. website. We have read, understand and will accept ASC X9's Membership Policy.

Signature _____ Date _____

Please return this application form to: Accredited Standards Committee X9, Inc.
P.O. Box 890330 • Charlotte, NC 28289-0330