April 2013

American National Standards –

Role of Standard

American National Standard – X9.59
X9.59 Electronic Commerce for the Financial Services Industry: Account Based Secure Payments Objects
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 -
Publication Date: 2006

X9.8-1 Personal Identification Number (PIN) Management and Security Part 1: PIN Protection Principles and Techniques for Online PIN Verification in ATM & POS Systems
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: 2003

X9.24-1 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
This part of this 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 this standard deals exclusively with management of symmetric keys using symmetric techniques. This part of this standard 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

in accordance with this part of this standard will be interoperable at the application level. Other characteristics may be necessary for node interoperability; however, this part of this standard does not cover such characteristics as message format, communications protocol, transmission speed, or device interface.
Publication Date: 2009

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

X9.42 Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
This standard specifies schemes for the agreement of symmetric keys using Diffie-Hellman and MQV algorithms. It 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. These methods may be 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 a key-encrypting key with other ASC X9 key management protocols.
Publication Date: 2003

X9.44 Public Key Cryptography for the Financial Services Industry: Key Establishment Using Integer Factorization Cryptography
This Standard specifies key establishment schemes using public-key cryptography based on the integer factorization problem. Both key agreement and key transport schemes are specified. The schemes may be used by two parties to transport or agree on shared keying material. The keying material may be used to provide other cryptographic services that are outside the scope of this Standard, e.g. data confidentiality, data integrity, and symmetric-key-based key establishment. The key pair generators may be used in other Standards based on the integer factorization problem.
Publication Date: 2007

X9.62 Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)
This 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). The ECDSA shall be used in conjunction with an Approved hash function, as specified in X9 Registry Item 00003, Secure Hash Standard (SHS). The hash functions Approved at the time of publication of this document are SHA-1 (see NOTE), SHA-224, SHA-256, SHA-384 and SHA-512. This ECDSA Standard provides methods and criteria for the generation of public and private keys that are required by the ECDSA and the procedural controls required for the secure use of the algorithm with these keys. This ECDSA Standard also provides methods and criteria for the generation of elliptic curve domain parameters that are required by the ECDSA and the procedural controls required for the secure use of the algorithm with these domain parameters.
Publication Date: 2005

X9.63 Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography
This Standard specializes ISO/IEC 11740-3 “Information Technology - Security Techniques - Key Management - Part 3: Mechanisms using asymmetric techniques” for use by the financial services industry. This Standard 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.
Publication Date: 2011

X9.69 Framework for Key Management Extensions
This Standard 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: 2007

X9.73 Cryptographic Message Syntax – ASN.1 and XML

This Standard specifies a cryptographic syntax scheme which can be used to protect financial transactions, files and other messages from unauthorized disclosure and modification. The cryptographic syntax scheme is based on an abstract Cryptographic Message Syntax (CMS) schema whose concrete values can be represented using either a compact, efficient, binary encoding, or as a flexible, human-readable, XML markup format.
Publication Date: 2010

X9.79-4 Public Key Infrastructure – Part 4: Asymmetric Key Management

This project addresses the necessary revision of two withdrawn American National Standards (X9.57 and X9.55) and the unacceptability of an international standard (ISO 15782) into an existing American National Standard (X9.79). X9.57-1997 Certificate Management was internationalized as ISO 15782 Certificate management for financial services Part 1: Public key certificates; however the X9F4 working group has determined that the USA cannot adopt ISO 15782-1 due to the numerous inconsistencies with USA practices including the removal of certificate revocations.
Publication Date: 2013

X9.80 Prime Number Generation Primality Testing and Primality Certificates

In the current state of the art in public key cryptography, all methods require, in one way or another, the use of prime numbers as parameters to the various algorithms. This document presents a set of accepted techniques for generating primes. It is intended that ASC X9 standards that require the use of primes will refer to this document, rather than trying to define these techniques on a case-by-case basis. Standards, as they exist today, may differ in the methods they use for parameter generation from those specified in this document. It is anticipated that as each existing ASC X9 standard comes up for its 5-year review, it will be modified to reference this document instead of specifying its own techniques for generating primes. 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.
Publication Date: 2005

X9.82-1 Random Number Generation Part 1: Overview and Basic Principles

This Standard defines techniques for the generation of random numbers that shall be used whenever ASC X9 Standards require the use of a random number or bit string for cryptographic purposes.
Publication Date: 2006

X9.82-3 Random Number Generation Part 3: Deterministic Random Bit Generators
This part of ANS X9.82 (Part 3) defines mechanisms for the generation of random bits using deterministic methods.
Publication Date: 2007

X9.82-4 Random Number Generation Part 4: Random Bit Generator Constructions
This Standard defines techniques for the generation of random numbers that shall be used whenever ASC X9 Standards require the use of random number or bitstring for cryptographic purposes. Part 4 specifies how to build complete random bit generators from the mechanisms in X9.82 Part 2 and Part 3.
Publication Date: 2011

X9.84 Biometric Information Management and Security for the Financial Services Industry
This Standard describes the security framework for using biometrics for authentication of individuals in financial services. It introduces the types of biometric technologies and addresses issues concerning their application. This standard also describes the architectures for implementation, specifies the minimum security requirements for effective management, and provides control objectives and recommendations suitable for use by a professional practitioner.
Publication Date: 2010

X9.95 Trusted Time Stamp Management and Security
This 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.
Published Date: 2012

X9.92-1 Public Key Cryptography for the Financial Services Industry Digital Signature Algorithms Giving Partial Message Recovery Part 1: Elliptical Cure Pintsov-Vanstone Signatures (ECPVS)
This Standard defines methods for digital signature generation and verification for the protection of messages and data giving partial message recovery. This document is Part 1 of this Standard, and it defines the Elliptic Curve Pintsov-Vanstone Signature (ECPVS) digital signature algorithm. Part 2 of this Standard defines the Finite Field Pintsov-Vanstone Signature (FFPVS) digital signature algorithm. ECPVS is a signature scheme with low message expansion (overhead) and variable length recoverable and visible message parts. ECPVS is ideally suited for short messages, yet is flexible enough to handle messages of any length. The ECPVS shall be used in conjunction with an Approved hash function and an Approved symmetric encryption scheme. In addition, this ECPVS Standard provides the criteria for checking the message redundancy. Supporting examples are also provided.
Publication Date: 2009

X9.97-1 Financial Services - Secure Cryptographic Devices (Retail) Part 1: Concepts, Requirements and Evaluation Methods
This part of ANS X9.97 specifies the requirements for Secure Cryptographic Devices which incorporate the cryptographic processes defined in ISO 9564, ISO 16609 and ISO 11568. This part of ANS X9.97 has two primary purposes: 1) to state the requirements concerning both the operational characteristics of SCDs and the management of such devices throughout all stages of their life cycle, 2) to standardize the methodology for verifying compliance with those requirements. Appropriate device characteristics are necessary to ensure that the device has the proper operational capabilities and provides adequate protection for the data it contains. Appropriate device management is necessary to ensure that the device is legitimate, that it has not been modified in an unauthorized manner, e.g., by "bugging", and that any sensitive data placed within the device (e.g., cryptographic keys) has not been subject to disclosure or change.
Publication Date: 2009

X9.98 Lattice-Based Polynomial Public Key Encryption Algorithm Part 1: Key Establishment: Part 2: Data Encryption
This Standard specifies the cryptographic functions for establishing symmetric keys using a lattice-based polynomial public key encryption algorithm and the associated parameters for key generation. The mechanism supported is *key transport*, where one party selects keying material and conveys it to the other party with cryptographic protection. The keying material may consist of one or more individual keys used to provide other cryptographic services outside the scope of this Standard, e.g. data confidentiality, data integrity, or symmetric-key-based key establishment. It also specifies key pair generators and corresponding key pair validation methods supporting the key transport schemes.
Publication Date: 2010

X9.97-2 (Identical to ISO 13491-2: 2005) Banking - Secure cryptographic devices (retail) Part 2: Security compliance checklists for devices used in financial transactions

This part of the standard specifies checklists to be used to evaluate secure cryptographic devices (SCDs) incorporating cryptographic processes, as specified in parts 1 and 2 of ISO 9564, ISO 16609 and parts 1 to 6 of ISO 11568, in the financial services environment. IC payment cards are subject to the requirements identified in this part of ISO 13491 up until the time of issue, after which they are to be regarded as a "personal" device and outside of the scope of this document.

Publication Date: 2009

X9.102 Symmetric Key Cryptography for the Financial Services Industry - Wrapping of Keys and Associated Data

This standard specifies four key wrap mechanisms based on ASC X9 approved symmetric key block ciphers whose block size is either 64 bits or 128 bits. The key wrap mechanisms can provide assurance of the confidentiality and the integrity of data, especially cryptographic keys or other specialized data.

Publication Date: 2008

X9.111 Penetration Testing Within the Financial Services Industry

This standard specifies recommended processes for conducting penetration testing with financial service organizations. This standard describes a framework for specifying, describing and conducting penetration testing, and then relating the results of the penetration testing. This standard allows an entity interested in obtaining penetration testing services to identify the objects to be tested, specify a level of testing to occur, and to set a minimal set of testing expectations.

Publication Date: 2011

X9.112-1 Wireless Management and Security Part 1: General Requirements

In today's world, both private and public sectors depend upon information technology systems to perform essential and mission-critical functions. In the current environment of increasingly open and interconnected systems and networks, network and data security are essential for the effective use of information technology. Privacy and regulatory requirements highlight this need. For example, systems that perform electronic commerce must protect against unauthorized access to confidential records and unauthorized modification of data. Wireless technologies are rapidly emerging as significant components of these networks. As such, data classification and risk assessments should be performed to determine the sensitivity of, and risk to, data transmitted over wireless networks. Various methods and controls should be considered for data that is sensitive, has a high value, or represents a high value if it is vulnerable to unauthorized disclosure or undetected modification during transmission over wireless networks. These methods and controls support communications security, for example by encrypting the communication prior to transmission and decrypting it at receipt. Note that data classification and risk assessments, regardless of whether data transmission is over wired or wireless environments, should be part of an organization's general security policy and best practices. Refer to Annex A Wireless Validation Control Objectives for further details. Part 1 of this Standard provides an

overview of wireless radio frequency (RF) technologies and general requirements applicable to all wireless implementations for the financial services industry. Subsequent parts of this Standard will address specific applications to wireless technology and associated risks, as well as technologies, methods and controls that mitigate those risks.
Publication Date: 2009

X9.117 Secure Remote Access Mutual Authentication

The financial services industry relies on several time-honored methods of electronically identifying, authorizing, and authenticating entities and protecting financial transactions. These methods include, but are not limited to: Personal Identification Numbers (PINs) and Message Authentication Codes (MACs) for retail and wholesale financial transactions, user IDs and passwords for network and computer access, and key management for network connectivity. Over the last forty years banks, investment, and insurance companies have developed risk management processes and policies to support the use of these technologies in financial applications.
Publication Date: 2012

X9.119-1 Retail Financial Services – Requirements for Protection of Sensitive Payment Data – Part 1: Using Encryption Methods

Theft of sensitive card data during a retail payment transaction is increasingly becoming a major source of financial fraud. Besides an optional encrypted PIN, this data includes magnetic stripe track 2 data: PAN, expiration date, card verification value, and issuer private data. While thefts of this data at all segments of the transaction processing system have been reported, the most vulnerable segments are between the point of transaction device capturing the magnetic stripe data and the processing systems at the acquirer. This document would standardize the security requirements and implementation for a method for protecting this sensitive card data over these segments. Several implementations exist to address this situation. This document would provide guidance for evaluating these implementations.
Publication Date: 2013

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

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: 1995

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

This standard 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 asymmetric key. 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: 2010

X9/TR-39 (formerly TG-3) Retail Financial Services Compliance Guideline Part 1: PIN Security and Key Management
This guideline applies to all organizations using the Triple Data Encryption Algorithm - TDEA (Reference 7) 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 Control Objectives address security controls from the PIN entry device to the interface delivering the transaction to the authorizing entity. When this guideline is completed by a device manufacturer, the Control Objectives are intended to evaluate the manufacturing environment and the device's ability to be implemented in a manner compliant with X9.8 and X9.24 (all parts).
Publication Date: 2009

X9/TR-39 FAQ
Publication: 2009

DATA AND INFORMATION SECURITY STANDARDS

X9.59 Electronic Commerce for the Financial Services Industry: Account Based Secure Payments Objects
X9/TG-9 Abstract Syntax Notation and Encoding Rules for Financial Industry Standards
X9/TR-31 Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
X9/TR-39 Retail Financial Services Compliance Guideline Part 1: PIN Security and Key Management (formerly TG-3)
X9/TR-39 FAQ
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
X9.42 Public Key Cryptography For The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
X9.44 Public Key Cryptography for the Financial Services Industry: Key Establishment Using Integer Factorization Cryptography
X9.62 Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)

X9.63 Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography
X9.69 Framework for Key Management Extensions
X9.73 Cryptographic Message Syntax - ASN.1 and XML
X9.79-4 Public Key Infrastructure – Part 4: Asymmetric key Management
X9.80 Prime Number Generation Primality Testing, and Primality Certificates
X9.82-1 Random Number Generation, Part 1: Overview and Basic Principles
X9.82-3 Random Number Generation, Part 3: Deterministic Random Bit Generators
X9.82-4 Random Number Generation, Part 4: Random Bit Generator Constructions
X9.84 Biometric Information Management and Security for the Financial Services Industry
X9.92-1 Public Key Cryptography for the Financial Services Industry Digital Signature Algorithms Giving Partial Message Recovery Part 1: Elliptic Curve Pintsov-Vanstone Signatures (ECPVS)
X9.95 Trusted Time Stamp Management and Security
X9.97-1 Financial services - Secure Cryptographic Devices (Retail) Part 1: Concepts, Requirements
and Evaluation Methods
X9.97-2 Identical to ISO 13491-2: 2005 Banking - Secure cryptographic devices (retail) Part 2: Security compliance checklists for devices used in financial transactions
X9.98 Lattice-Based Polynomial Public Key Encryption Algorithm Part 1: Key Establishment: Part 2: Data Encryption
X9.102 Symmetric Key Cryptography For the Financial Services Industry - Wrapping of Keys and Associated Data
X9.111 Penetration Testing Within the Financial Services Industry
X9.112-1 Wireless Management and Security Part 1: General Requirements
X9.117 Secure Remote Access Mutual Authentication
X9.119-1 Retail Financial Services – Requirements for Protection of Sensitive Payment Data Part 1: Using Encryption Methods

Additional x9 Security Standards under Development

X9.122 Secure Consumer Authentication for Internet Payments
X9.123 Implicit Certificates
X9.124 Formal Preserving Encryption
X9.125 Cloud Services Compliance Data Standard