Accredited Standards Committee X9
Title: X9-Financial Services
Accredited by the
American National Standards Institute

Date September 8, 2000

WORKING DRAFT

ACCREDITED STANDARDS COMMITTEE X9
TR-1 - 2000

TECHNICAL GUIDE FOR ABA/ASC X9 STANDARDS DEFINITIONS, ACRONYMS AND SYMBOLS

Notice -- Warning to readers of this document

This document is intended to serve as a reference for the standardization of definitions, acronym's and symbols to be used in ABA/ASC X9 standards. This document will change on an ongoing basis, in order to maintain currency with developing and published standards being produced by the various work groups who comprise the X9F organization.

Secretariat: American Bankers Association
Standards Department
1120 Connecticut Ave., N.W.
Washington, DC 20036

Contents

1 SCOPE

This technical reference (TR) is intended to provide a standardized list of definitions, acronyms and symbols found in existing, published standards or to be used as the appropriate definition to be used for developing standards. New definitions, acronyms, or symbols incorporated into new standards or technical guidelines will be added to this list on an on-going base.

2 REFERENCES

This document contains the standard definitions listed in the following published and draft ANSI Standards and Technical Guidelines:

Reference Number	Title
X3.92	Data Encryption Algorithm
X3.106	DEA Modes of Operation
X9.8	Personal Identification Number (PIN) Management and Security
X9.9(W)	Financial Institution Message Authentication (Wholesale)
X9.17-85(W)	Financial Institution Key Management (Wholesale)
X9.17-95(W)	Financial Institution Key Management (Wholesale)
X9.19	Financial Institution Retail Message Authentication
X9.23(W)	Encryption of Wholesale Financial Messages
X9.24	Financial Institution Retail Key Management
X9.26(W)	Financial Institution Secure Sign-On Authentication For Wholesale Financial Services
X9.28(W)	Multiple Center Key Management (Wholesale)
X9.30-1	Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 1: The Digital Signature Algorithm (DSA)
X9.30-2	Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 2: The Secure Hash Algorithm (SHA)
X9.30-3	Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 3: Certificate Management for DSA (Replaced by **X9.57**)
X9.31-1	Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry, Part 1: The RSA Signature Algorithm
X9.31-2	Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry, Part 2: The Hash Algorithm
X9.41	Security Services Management
X9.42	Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
X9.44	Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry: Management of Symmetric Keys Using RSA
X9.45	Enhanced Management Controls Using Attribute Certificates
X9.49	Remote Access for Financial Databases
X9.50	Certificate Management for Encryption Management.
X9.52	Triple Data Encryption Algorithm Modes of Operations

Reference Number	Title
X9.55	Certificate Extensions for Multi-Domain Operations
X9.57	Public Key Cryptography for the Financial Services Industry: Certificate Management
X9.59	Electronic Commerce Payments
X9.61	Financial Industry Cryptographic Module Service Calls and Audit Requirements
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
X9.65	Triple DEA Implementation Standard
X9.66	Security Requirements for Cryptographic Module
X9.68-1	Digital Certificates for Mobile/Wireless and High Transaction Volume Financial Systems: Domain Certificate Architecture
X9.68-2	Digital Certificates for Mobile/Wireless and High Transaction Volume Financial Systems:
X9.68-3	Digital Certificates for Mobile/Wireless and High Transaction Volume Financial Systems: Domain Certificate Syntax
X9.69	Framework for Key Management Extensions
X9.70	Management of Symmetric Keys Using Public Key Algorithms, Part 1: Requirements and Overview
X9.71	Keyed Hash Message Authentication Code (HMAC)
X9.72	Peer Entity Authentication Using Public Key
X9.73	Cryptographic Message Syntax
X9.74	Certificate Path Processing
X9.76	Partial Key Refreshing
X9.77	PKI Management Protocols
X9.78	Attribute Certificate Extensions
X9.79	Public Key Infrastructure – Practices and Policy Framework
X9.80	Prime Number Generator, Primality Testing, and Primality Certificates
X9.82	Random Number Generation
X9.84	Biometric Information Management and Security
X9.86	PIN Security in an Electronic-Commerce Environment
X9.87	PIN Security in a Hybrid Integrated-Circuit Magnetic Stripe Environment
X9.88	Long Term Non-Repudiation Using Digital Signatures
X9.89	Management Protocol for Short Certificates
TG-3	PIN Security Compliance
TG-4	Cryptographic Key Notation
TG-7	Initial DEA Key Distribution for PIN Entry and Transaction Originating Devices

Reference Number	Title
TG-9	ASN.1
TG-17	Mathematical Background for Elliptic Curve Cryptography
TG-19-0	Guideline for Validating Implementations According to ANSI Standards
TG-19-1	Part 1: Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures
TG-19-2	Validating X9 Cryptographic Technology Part 2: ECDSA
TG-19-3	Validating X9 Cryptographic Technology Part 3: rDSA Signature Algorithm
TG-19-4	Validating X9 Cryptographic Technology Part 4: Diffie-Hellman Key Agreement
TG-19-5	Validating X9 Cryptographic Technology Part 5: Triple DES Modes of Operation
TG-19-6	Conformance Testing for Certificate Path Processing (X9.74)
TG-19-7	EC Agreement and Key Management
TG-19-8	Management of Symmetric Algorithms Using Reversible Public Key Cryptography
TG-20	IP Security Guidelines
TG-24	Managing Risk and Migration Planning: Withdrawal of X9.9
TG-25	Managing Risk and Migration Planning: Withdrawal of X9.23
TG-26	Managing Risk and Migration Planning: Withdrawal of X9.17

3 DEFINITION(S)

Access Control **X9.49**
The collection of all controls used to assure that persons would have access only to information processing facilities for which they are authorized.

Accountability **X9.30:3, X9.57**
The property that ensures that the actions of an entity may be traced uniquely to the entity.

Accountability **X9.68**
The property that ensures that the actions of an entity may be traced uniquely to the entity. Accountability is obtained in public key systems by procedures designed to tie an entity to a public-private key pair and to insure that only this entity is able to obtain or use the private key of the pair.

Account Number **X9.86**
The assigned number that identifies the card issuer and cardholder. This account number is composed of an issuer identification number, an individual account Number Identification, and an accompanying check digit, as ISO 7812-1985: Identification Cards-Numbering system and registration procedure for issuer identifieers.

Acceptor **X9.24**
Same as card acceptor.

Acquirer **X9.8, X9.24, X9.86**
The institution (or its agent) which acquires from the card acceptor the financial data relating to the transaction and initiates that data into an interchange system.

Acquirer Gateway **X9.86**
An acquire-controlled facility that translates from the electronic-commerce public-key-cryptography infrastructure to the ATM/point-of-sale secret-key-cryptography infrastructure.

Activation data **X9.79**
Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, a biometric, or a manually held key share).

Active (Key State) ***X9.17-95(W)***
A key in the active state may be used to secure information from the originator and process received secure information.

Adaptation **X9.84**
The process of automatically update or refresh a reference template.

Addition Rule **X9.62**
An addition rule describes the addition of two elliptic curve points P1 and P2 to produce a third elliptic curve point P3. (See TG-17-199x, Sections 2.1 and 2.2.)

Address Certificate **X9.45**
A certificate issued by an entity, which administers or is knowledgeable of an address space, which binds an entity to an address.

ADF Allocation **X9.79**
The secure provision of space in the IC for subsequent use by an application supplier.

ADF Personalizer **X9.79**
The entity, which initially loads security and related operational parameters in the space, allocated in the IC for an ADF.

Agent *X9.28(W)*
See Multiple Center Agent

Agent Identity ***X9.17-95(W)***
The unique identity of an ANSI ***X9.28(W)*** agent.

Algorithm **X9.8, *X9.9(W)*, X9.19, X9.24, X9.86**
A clearly specified mathematical process for computation; a set of rules which, if followed, will give a prescribed result.

Algorithm Identifier X9.31:1
A unique identifier for a given encryption or hash algorithm, together with any required parameters. The unique identifier is an ASN.1 object identifier [6,7].

Alteration **X9.19**
The process of modifying one or more message elements of a message as a method of perpetrating a fraud.

Application Data File (ADF) **X9.79**
A file in the Integrated Circuit (IC) that supports one or more services.

Application Supplier **X9.79**
An entity which is responsible for an ADF after its allocation.

Asymmetric Cryptographic Algorithm **X9.30:1, X9.30:3, X9.31:1, X9.42, X9.57, X9.62, X9.68, X9.86**
A cryptographic algorithm that uses two related keys, a public key and a private key; the two keys have the property that, given the public key, it is computationally infeasible to derive the private key.

Attribute **X9.30:3, X9.57, X9.68**

Information, excluding the public key, key identities and algorithm identifier, which is provided by the entity or the CA and certified by the CA in an Attribute Certificate. Examples include the CA's liability limitations and binding information.

Attribute Authority (AA) **X9.30:3, X9.57, X9.68**

An entity trusted by one or more entities to create and assign attribute certificates.

Attribute Certificate **X9.30:3, X9.57, X9.68**

A set of attributes along with a public key certificate identifier. The attributes are bound to the public key certificate by the signature of the AA on the attribute certificate.

Audit Journal **X9.30:3, X9.57, X9.68**

A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to the output of the final results.

Audit Record Field ***X9.17-95(W)***

A field containing information about all entities involved in a transaction, as well as indicators of the types of processing that were performed by those entities.

Audit Trail **X9.30:3, X9.57, X9.68**

See Audit Journal.

Authentication ***X9.9(W)*, *X9.17-85(W)*, *X9.17-95(W)*, X9.19, *X9.23(W)*, X9.24, *X9.28(W),* X9.86**

The act of determining that a message has not been changed since leaving its point of origin. The identity of the originator is implicitly verified.

Authentication **X9.84**

The process of determining an individual's identity, either by verification or by identification

Authentication Algorithm ***X9.9(W)*, X9.19, X9.24, X9.86**

The application of a cryptographic process in which output text depends on all preceding input text.

Authentication data **X9.79**

Information used to verify the claimed identity of an entity, such as an individual, defined role, corporation, or institution.

Authentication Domain **X9.68**

See Domain

Authentication Element ***X9.9(W)*, X9.19, X9.24**

A contiguous group of bits or characters which are to be protected by being processed by the authentication algorithm.

Authentication Key ***X9.26(W)***
A DEA key used to authenticate data in accordance with ANSI *X9.9(W)*-1986.

Authentication Sequence Number ***X9.28(W)***
An incremental counter associated with the KDA used for the authentication of messages. The counter does not repeat before the expiration of the cryptoperiod of that KDA.

Authorization **X9.30:3, X9.57, X9.68**
The granting of rights.

Authorization Certificate **X9.45**
Any of a variety of attribute certificates used in the authorization process.

Authorization Procedure **X9.45**
Verification that a digitally signed transaction is acceptable according to the rules and limits of the parties involved.

Authorized Signatory **X9.45**
The top-level issuer of authorization certificates in an organization. Authorized signatories are designated in a signatory certificate, which is issued to an organization by an agreed signatory authority.

Base Key **X9.24**
A key which is used to derive (cryptographically compute) or decrypt transaction keys. Normally a single base key is used in a transaction- receiving (e.g., acquirer) TRSM to derive or decrypt the transaction keys used by a large number or originating (e.g., terminal) TRSMs.

Basis **X9.62**
A kind of representation for the elements of the finite field F2m. Two special kinds of bases are optimal normal bases and polynomial bases.

BAUDOT ***X9.23(W)***
A 5-bit per character information coding scheme (excluding optional start bits and stop bits); CCITT Alphabet Number 2.

Beneficiary Party(ies) ***X9.9(W)***
The ultimate party or parties to be credited or paid as a result of a transfer.

Biased **X9.19,** ***X9.17-85(W)***
With respect to generation of random or pseudo-random numbers, a process is biased if the occurrence of some numbers and/or patterns is more likely than others.

Binary String **X9.30:1, X9.42**
The binary string of a sequence of 0's and 1's. The leftmost bit is the most significant bit of the string. The right most bit is the least significant bit of the string.

Binary String to Integer Conversion **X9.30**
Let m be a binary string of length k. Let m1, m2, ..., mk be the bits of m from first (most significant) to last (least significant). Then m shall be converted to an integer x satisfying

$$X = \overset{k}{\underset{i=i}{S}} \quad 2(k-i)m1$$

Binary Vector **X3.106**
A sequence of bits.

Binning **X9.84**
Database partitioning based on information contained within (endogenous to) the biometric patterns.

Biometric **X9.84**
A measurable biological or behavioral characteristic, which reliably distinguishes one person from another, used to recognize the identity, or verify the claimed identity, of an enrollee.

Biometric Data **X9.84**
The extracted information taken from the biometric sample and used either to build a reference template or to compare against previously created reference template(s).

Biometric Sample **X9.84**
Initial (raw) biometric data which is captured and processed.

Biometric System **X9.84**
An automated system capable of capturing, extraction, matching and returning a decision (match/ non-match).

Birthday Phenomenon **X9.52, X9.65**
The ‘phenomenon’ states that for a category size of 365 (the days in a year), after only 23 people are gathered, the probability is greater than 0.5 that at least two people have a common birthday (month and day). That’s r = 32 from a category size of 365. In the DES world, where the category size is 2**64, this same probability of a repeat (match) occurs at approximately r = 2**32.

Bit String **X9.62**
A bit string is a sequence of 0's and 1's.

Bit String **X9.42**
A bit string is an ordered sequence of 0's and 1's. The left-most bit is the most-significant bit of the string. The right-most bit is the least-significant bit of the string.

Block **X3.106, X9.19, *X9.23(W)*, X9.52**
A data unit whose length is 64 bits.

Block Encryption **X9.19**
Under DEA, 64 bits of cleartext are encrypted to yield 64 bits of encrypted text.

Capturing **X9.84**
Taking a raw biometric sample.

CA-Certificate **X9.55**
A certificate for one CA issued by another CA.

Capturing **X9.84**
Taking a raw biometric sample.

Card Accepting Device (CAD) **X9.79**
A device used to interface with the ICC (smart card) during a session.

Card Acceptor **X9.8, X9.24**
The party accepting the card and presenting transaction data to an acquirer.

Cardholder **X9.79**
The person to whom the financial transaction ICC has been issued.

Card Issuer **X9.24**
The institution or its agent that issues the identification card to the cardholder.

Cascading Obsolete Flag ***X9.17-95(W)*, X9.57**
A character in the ST field of a DSM which indicates that all keys explicitly or implicitly identified in the IDD fields are to be placed in the Obsolete state.

Certificate **X9.30:1, X9.30:3, X9.31:1, X9.42, X9.57, X9.62, X9.68, X9.86**
The public key and identity of an entity together with some other information rendered unforgeable by signing the certificate with the private key of the certifying authority, which issued that certificate.

Certification Authority (CA) **X9.30:1, X9.30:3, X9.31:3, X9.42, X9.57, X.62, X9.68X9.86**
An entity trusted by one or more entities to create and assign certificates.

Certificate Information **X9.30:3, X9.57, X9.68**
The information in a certificate which is signed

Certificate Issuer **X9.79**
The issuer name in an X.509 certificate.

Certification Path **X9.30:3, X9.41, X9.55, X9.57, X9.68**
An ordered sequence of certificates of entities which, together with the public key of the initial entity in the path, can be processed to obtain the public key of the final entity in the path.

Certificate Policy (CP) **X9.79**
A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

Certification Policy Element **X9.55**
A named set of certificate policy rules relating to a class of activity across a community of distributed systems which has a common security requirement, e.g. electronic data exchange for the trading of goods within a given price range.

Certification Practice Statement (CPS) **X9.79**
A statement of the practices, that a certification authority employs in issuing, certificates. The Certification Practice Statement defines the equipment, policies and procedures the CA uses to satisfy the requirements specified in the certificate policies that are supported by it.

Certificate Rekey **X9.79**
The process whereby a subscriber with an existing key-pair and certificate receives a new certificate for a new public-key, following the generation of a new key pair.

Certificate Renewal **X9.79**
The process whereby a subscriber is issued a new instance of an existing certificate with a new validity period.

Certificate Request **X9.79**
Submission of a validated Registration Request by an RA to a CA to register an End Entity's public-key in a certificate.

Certificate Request Data **X9.30:3, X9.57, X9.68**
The "Certificate Request Data" (CertReqData) of an entity includes the entity's public key, entity identity, and other information included in the certificate or otherwise in the certificate management process.

Certificate Response **X9.79**
A message sent from a CA to an RA following Certificate Issuance.

Certificate Revocation List **X9.30:3, X9.57, X9.68, X9.86**
A list of revoked certificates.

Characteristic 2 Finite Field **X9.62**
A finite field containing 2m elements, where m ^{3} 1 is an integer.

Checkvalue **X9.24**
A computed value which is the result of passing a data value through a non-reversible algorithm.

Cipher Text **X3.92, X3.106, X9.8, *X9.17-85(W)*, *X9.17-95(W)*, X9.19, *X9.23(W)*, X9.24, *X9.26(W)*, *X9.28(W)*, X9.52, X9.86**
Data in its enciphered form.

Ciphertext ***X9.23(W)***
Encryption Element. An independently encrypted encryption element.

Ciphertext String ***X9.23(W)***
The ciphertext formed be encrypting concatenated encryption elements.

Ciphertext Substring ***X9.23(W)***
A segment of a ciphertext string.

Clain of Identity **X9.84**
The name or index of a claimed reference template or enrollee used by a biometric system for verification.

Claimant **X9.84**
A person submitting a biometric sample for verification claiming a legitimate or false identity.

Cleartext **X9.19, X9.24, X9.86**
Data in its original, unencrypted form.

Clocking **X9.52**
As used in this standard, the term “clocking” is used to connote the processing by one (or more if they operate concurrently) DEA functional block(s) of a 64-bit input block to produce a 64-bit output block.

Closed-Loop Response Integrity **X9.19**
The verification by the originator of the overall transaction integrity, i.e. of both the transaction request and its transaction response.

Common Data File (CDF) **X9.79**
A mandatory file that contains the common data elements stored in the ICC (smart card) and used to identify the card, the card issuer and the cardholder.

Communicating Pair ***X9.17-85(W)*, *X9.17-95(W)***
Two logical parties who have previously agreed to exchange data. A party and a center exchanging cryptographic service messages do not constitute a communicating pair.

Compromise **X9.8, X9.30:3, X9.57, X9.86**
A violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred.

Composite **X9.80**
An integer which has at least two prime factors.

Compromised Obsolete (Key State) ***X9.17-95(W)***
The integrity or secrecy of the key is suspect.

Compromised Obsolete Flag ***X9.17-95(W)***
A character in the ST field of a DSM which indicates that all keys explicitly implicitly identified in the IDD fields are to be placed in the Compromised Obsolete state.

Confidentiality **X9.30:3, X9.57**
The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Corresponding Key Field ***X9.17-95(W)***
Used in the context of a KSM, RFS or RTR, which is sent in response to an RSI which, contains a key field. A corresponding key field is a key field in the received/transmitted message, which is the same type and subtype as a key field in the transmitted/received message, or vice versa.

Credential **X9.69**
A set of access permissions

Credit Party ***X9.9(W)***
The party to be credited or paid by the receiving bank.

CRL Distribution Point **X9.55**
A directory entry whose certificateRevocationList and authorityRevocationList attributes contain partial CRL's covering a subset of the full set of certificates issued by one certificate authority.

Cross Certification **X9.30:3, X9.57, X9.68**
Cross certification is used by one CA to certify any CA other than a CA immediately adjacent (superior or subordinate) to it in a hierarchy.

Cryptography **X9.42, X9.49, X9.52**
The discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof.

Cryptographic Boundary **X9.52**
An explicitly defined contiguous perimeter that establishes the physical bounds around the set of hardware, software and firmware which is used to implement the TDEA and the associated cryptographic processes.

Cryptographic Equipment *X9.17-85(W), X9.28(W)*
A device wherein cryptographic functions (e.g., encryption, authentication, key generation) are performed.

Cryptographic Hash Function **X9.42**
A (mathematical) function that maps values from a large (possibly very large) domain into a smaller range. The function satisfies the following properties:

1. (one-way) It is computationally infeasible to find any input that maps to any per-specified output;

2. (Collision Free) It is computationally infeasible to find any two distinct inputs that maps to the same output.

Cryptographic Initialization **X9.52**
The process of entering the IV(s) into the TDEA to initialize the algorithm prior to the commencement of encryption or decryption.

Cryptographic Key (Key) **X3.106, X9.8, *X9.17-85(W)*, *X9.17-95(W)*, *X9.23(W)*, X9.24, *X9.28(W)*, X9.30:2, X9.30:3, X9.31:1, X9.42, X9.52, X9.57, X9.62, X9.86**
A parameter that determines the operation of a cryptographic function such as:
(a) the transformation from plain text to cipher text and vice versa,
(b) synchronized generation of keying material,
(c) digital signature computation or validation.

Cryptographic Keying Material ***X9.17-85(W)*, *X9.17-95(W)*, *X9.28(W)***
See Keying Material.

Cryptographic Material **X9.30:3, X9.57**
See Keying Material.

Cryptographic Module ***X9.17-95(W)*, X9.30:3, X9.57**
The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic, including cryptographic algorithms. A device wherein cryptographic functions (e.g., encryption, authentication, key generation) are performed.

Cryptographic Module Facility **X9.30:3, X9.57**
The physically protected enclosure (e.g., room or device) where a cryptographic module resides.

Cryptographic Service Message ***X9.17-85(W)*, *X9.17-95(W)*, *X9.28(W)***
A message for transporting keys or related information used to control a keying relationship.

Cryptographic Synchronization **X9.24**
The ability for two nodes, that cryptographically process a transaction, to determine the identical transaction key.

Cryptography **X9.30:1, X9.30:3,, X9.31:1, X9.31:2, X9.42, X9.44, X9.57, X9.62, X9.86**
The discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof.

Cryptoperiod ***X9.9(W)*, *X9.17-85(W)*, *X9.17-95(W)*, *X9.23(W)*, *X9.26(W)*, *X9.28(W)*, X9.30:1, X9.30:3, X9.31:1, X9.31:2, X9.31:3,, X9.57, X9.62**
The time span during which has specific key is authorized for use or in which the keys for a given system may remain in effect.

Customer **X9.8, X9.19**
The individual initiating the transaction.

Data Encryption Algorithm (DEA) ***X9.9(W)*, *X9.17-85(W)*, *X9.17-95(W)*, X9.19, *X9.23(W)*, X9.24, *X9.26(W)*, *X9.28(W)*, X9.52, X9.86**
The encryption algorithm specified by ANSI X3.92, Data Encryption Algorithm.

Data Integrity **X9.30:3, X9.57**
A property whereby data has not been altered or destroyed.

Data Key ***X9.17-85(W)*, *X9.17-95(W)*, *X9.28(W)***
A key used to encrypt and decrypt, or to authenticate data.

Data Separation **X9.69**
Using encryption as a means of access control.

Data Unit **X3.106, *X9.23(W)***
A binary vector of k bits numbered from the left denoted as (B1, B2, ..., Bk).

Date of Message Origination (Date) ***X9.9(W)***
The date on which the originator computed the MAC. This date may be used to synchronize the authentication process through selection of the proper key.

DEA Input Block **X3.106**
A block that is the final results of an encryption or decryption operation. The output block is designated (I1, I2, ..., I64), where I1, I2, ..., I64 represents bits.

DEA Output Block **X3.106**
A block that is the final results of an encryption or decryption operation. The output block is designated (O1, O2, ..., O64), where O1, O2, ..., O64 represents bits.

DEA Key (key) ***X9.9(W)*, *X9.26(W)***
A 64-bit quantity as defined by ANSI X3.92-1981.

DEA Device ***X9.17-85(W)***
The electronic hardware part or subassembly which implements only the DEA as specified in ANSI X3.92-1981, and which is validated by the National Institute of Standards and Technology (NIST).

Debit Party ***X9.9(W)***
The source of funds for a payment on the receiving bank's books.

Decipher **X3.106**
See Decrypt or Decryption.

Decipherment **X9.8**
The reversal of a previous reversible encipherment, rendering cipher text intelligible.

Decrypt **X3.106, X9.86**
To change ciphertext into plaintext.

Decrypt State **X3.106**
The state of the DEA executing the deciphering operation specified in ANSI X3.92-1981.

Decryption **X3.92, X3.106, *X9.17-85(W)*, *X9.17-95(W)*, *X9.23(W)*, X9.24, *X9.26(W)*, *X9.28(W)*, X9.52, X9.86**
A process of transforming ciphertext (unreadable) into plaintext (readable).

Degauss ***X9.17-85(W)*, *X9.17-95(W)***
To remove, erase or clear information from magnetic media.

Delegation **X9.45**
A certificate which delegates all or some of an entity's authority to another entity for some period of time.

Deletion **X9.19**
The process of preventing a message from being delivered to the intended recipient as a method of perpetrating a fraud.

Delimiter ***X9.9(W)***
A group of characters used to earmark the beginning and end of a data field or fields.

Delta CRL **X9.55**
A partial CRL indicating only changes since the last CRL issue.

Design Standard **X9.19**
Specific design criteria defining both results and method of performance per a standard.

Device Certificate **X9.45**
A certificate typically issued by a device manufacturer, which binds the identity of the device to its characteristics.

Diffie-Hellman Private Key **X9.42**
Given a set of domain parameters (*p, q, g*), a Diffie-Hellman private key *x* is an integer where $1 \leq x \leq q\text{-}1$. Note that it is acceptable to further restrict the interval to $1<x<q\text{-}1$, if desired. The private key of an entity's key pair is known only by the owner of that key. Note that the private key is denoted *x* for static private keys and *r* for ephemeral private keys. See private key.

Diffie-Hellman Public Key **X9.42**
Given a set of domain parameters (*p, q, g*), a Diffie-Hellman public key is an element of *GF(p)* that may be publicly known. For a given private key *x*, the corresponding public key *y* is defined as $g^x \bmod p$. Note that the public key is denoted *y* for static public keys and *t* for ephemeral public keys. See public key.

Digest Information **X9.31:1**
A message digest, proceeded by the algorithm identifier of the hash algorithm used to compute the digest.

Digital Signature **X9.30:1, X9.30:3,, X9.31:1, X9.31:2, X9.57, X9.62, X9.86**
A cryptographic transformation of data which, when associated with a data unit, provides the services of:

(a) Origin authentication,
(b) Data integrity, and
(c) Signer non-repudiation.

Digital Signature **X9.49**
A cryptographic transformation of data which, when associated with a data unit and accompanied by the corresponding public-key certificate, provides the services of:
(a) Origin authentication,
(b) Data integrity, and
(c) Signer non-repudiation

Discontinued Keys ***X9.17-95(W)***
Keys which have been deleted or marked so as not to be used to encrypt or authenticate Obsoleteeither data or other keys except for message reconstruction. States are used, the keys may be in either the Obsolete or Compromised state.

Discretionary Access Control **X9.79**
A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).

Distinguished Entity **X9.30**
A globally unique name for an entity.

Distinguished Name **X9.57, X9.68**
A globally unique name of an entity.

Domain **X9.68**
A logical construction consisting of all the domain-entities using a given cryptographic system and parameters set and having the same domain root CA.

Domain AA **X9.68**
An AA using the same parameters and algorithms as the DRCA and having its authority delegated from the DRCA (possibly through a hierarchy of other DCA's and/or DAA's).

Domain Root CA (DRCA) **X9.68**
The top level CA for a domain, identified uniquely by its public-private pair and associated cryptographic system parameters and algorithms.

Domain CA **X9.68**
A CA below a DRCA using the same parameters and algorithms as the DRCA and having its authority from the DRCA (possibly indirectly if multiple levels of hierarchies exist).

Domain-Entity **X9.68**
The Manifestation of an entity presented by a public-private key pair and its associated rights. For example an individual at a corporation may have a key pair (and the associated certificate) used for purchasing and one for approving employee transfer. Although both key pairs belong to the same entity, they map to two different domain-entities. The same individual may also have a key pair used for interacting with his bank and one for signing general e-mail massages. **Additional text requires review.**

Domain Parameters **X9.42**
The prime p that defines GF(p), a prime factor q of $p-1$, and an associated generator g of order in the multiplicative group GF(p)*

Dual Control **X9.8, *X9.17-85(W)*, *X9.17-95(W)*, X9.24, X9.30:3, X9.57, X9.68, X9.69**
A process of utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information whereby no single entity is able to access or utilize the materials, e.g. cryptographic key.

Duplication **X9.19**
Same as replay.

ECDSA **X9.62**
Elliptic Curve analog of the NIST Digital Signature Algorithm (DSA).

ECPP **X9.80**
Acronym for Elliptic Curve Primality Proving algorithm.

Effective Date ***X9.17-95(W)***
Used in the unique identification of a key. The date and time when a key is to be placed into use or activated (i.e., enters the Active state).

Effective Date of Key ***X9.28(W)***
The date and time when a key is to become active.

Electronic Distribution ***X9.17-95(W)***
Distribution of keying materials between entities by means of an electronic communication. Electronic distribution does not include electronic key loaders, such as smart cards.

Electronic Signature **X9.79**
A method of signing an electronic message that (a) authenticates and identifies a person as the source of an electronic message, and (b) indicates a person's approval of the information contained in the electronic message.

Elliptic Curve **X9.62**
An elliptic curve is a set of points specified by 2 parameters a and b, which are elements of a field F_q. The elliptic curve is said to be defined over F_q, and F_q is sometimes called the underlying field.

If q is a prime p (so the field is F_p), then the Weierstrass equation defining the curve is of the form $y^2 = x^3 + ax + b$, where $(4a^3 + 27b^2 \bmod p)$ ¹ 0. If q is a power of 2 (so the field is F_{2m}), then the Weierstrass equation defining the curve is of the form $y^2 + xy = x^3 + ax^2 + b$, where $b \neq 0$.

Elliptic Curve Key Pair **X9.62**
Given particular Elliptic Curve parameters, an *Elliptic Curve key pair* consists of an Elliptic Curve private key and the corresponding Elliptic Curve public key.

Elliptic Curve Parameters **X9.62**
These parameters specify an underlying field F_q, the type EC parameters of basis used to represent the elements of F_q, the equation of an elliptic curve over F_q, an elliptic point P of prime order, and the order n of P.

Elliptic Curve Point **X9.62**
If E is an elliptic curve defined over a field F_q, then an elliptic curve point is either a pair of field elements (x_P, y_P) (where x_P, y_P Î F_q) such that the values $x = x_P$ and $y = y_P$ satisfy the equation defining E, or a special point ∅ called the point at infinity.

Elliptic Curve Private Key **X9.62**
Given particular Elliptic Curve parameters, an Elliptic Curve private key consists of a random integer d in the interval [2,n-2].

Elliptic Curve Public Key **X9.62**
Given particular Elliptic Curve parameters, and an Elliptic Curve private key d, the corresponding *Elliptic Curve public key* consists of the elliptic curve point Q = dP.

Embedder **X9.79**
The entity which performs IC embedding.

Encipher **X3.106**
See Encrypt or Encryption.

Encipherment **X9.8**
The rendering of text unintelligible by means of an encoding mechanism.

Encrypt **X3.106, X9.86**
To change plaintext into ciphertext.

Encrypt State **X3.106**
The state of DEA executing the enciphering operation specified in ANSI X3.92-1981.

Encryption ***X9.9(W)*, X3.92, X3.106, *X9.17-85(W)*, *X9.17-95(W)*, X9.19, *X9.23(W)*, X9.24, *X9.26(W)*, *X9.28(W)*, X9.52, X9.84, X9.86**
A process of transforming plain text (readable) into cipher text (unreadable) for the purpose of security or privacy.

Encryption Algorithm **X3.92, X9.52, X9.86**
A set of mathematically expressed rules for rending information unintelligible by effecting a series of transformations to the normal representation of the information through the use of variable elements controlled by the application of a key.

Encryption Element ***X9.23(W)***
A contiguous group of characters which is to be encrypted.

Encryption Key ***X9.26(W)***
A DEA key used to encrypt or decrypt data in accordance with ANSI X3.92-1981.

End Entity **X9.55**
The subject of the final certificate in a certification path, i.e. that subject which is not a CA.

Enhanced Digital Signature **X9.88**
A digital signature with additional attributes that provide evidence of:

- Commitment by the signer;
  Identity and optionally role of the signer;
- Time of signature; and
- Signature policy under which the signature was applied.

Enhanced Signature **X9.88**
See: Enhanced Digital Signature

Enrollment **X9.84**
The process of collecting biometric samples from a person and the subsequent processing and storage of biometric reference templates representing that person's identity. See also *initial enrollment* and *re-enrollment*.

Entity **X9.30:3, X9.57**
A legal entity or an individual. Note that a Certification Authority is an entity.

Entity **X9.42**
A participant in any of the key agreement schemes in this standard. The words “entity” and “party” are used interchangably. This definition may admit many interpretations: it may or may not be limited to the necessary computational elements; it may or may not include or act on behalf of a legal entity. The particular interpretation chosen will not affect operation of the key agreement schemes.

Entity **X9.49, X9.68**
A legal entity, group, or an individual. An entity’s identity is authenticated before receiving financial services via remote access.

Entity **X9.79**
A legal entity, individual, or device. Note that an RA, CA, subject, relying party, application server, etc. are all entities.

Entity Authentication **X9.42, X9.49, X9.70**
The process of determining if a claimed identity matches an expected identity.

Ephemeral Data **X9.42**
Data is information (e.g. key material) that is relatively short-lived.

Ephemeral Key **X9.42**
A private or public key that is unique for each execution of a cryptographic scheme. An ephemeral private key is to be destroyed as soon as computational need for it is complete. An ephemeral public key may or may not be certified. In this standard, an ephemeral public key is represented by t, while an ephemeral private key is represented by r, with a subscript to represent the owner of the key.

Ephemeral-Key Domain Parameter **X9.42**
Domain parameters with which the ephemeral private/public keys are generated. These parameters are not necessarily short-lived. The same domain parameters may be used to generate multiple ephemeral private/public keys. In this standard, the parameters used exclusively to generate ephemeral keys are denoted by the subscript “e”. For example, (p_e, q_e, g_e) represents a set of ephemeral-key domain parameters.

Equal Error Rate **X9.84**

The probability or percentage of errors when the decision threshold of a system is set such that the false match rate is equal to the false non-match (historically crossover rate).

Error Service Message ***X9.28(W)***

ANSI **X9.17** message that is used to give a negative acknowledgment upon receipt of any ANSI **X9.17** cryptographic service message other than an ESM and to give the recipient data with which to recover.

Event Journal (Audit Journal or Audit Log) **X9.79**

A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to the output of the final results.

Exclusive-OR ***X9.9(W), X9.17-85(W), X9.17-95(W)*, X9.19, X9.24, *X9.26(W)*, X9.52**

A mathematical operation, symbol ⊕ , defined as:

$0 \oplus 0 = 0$,
$0 \oplus 1 = 1$,
$1 \oplus 0 = 1$, and
$1 \oplus 1 = 0$.

Equivalent to binary addition without carry.

Explicitly Identified ***X9.17-95(W)***

Used in the context of changing the state of a key to the Obsolete or Compromised Obsolete state by sending or receiving a DSM. A key is said to be explicitly identified if the name of the key is used in an IDD field.

Explicit Key Authentication **X9.42**

Explicit key authentication to Party U means that (1) U has assurance that V is the only other party possibly capable of computing the shared secret value used to derive the key, and (2) that U has evidence that V has actually derived the key. Combining implicit key authentication with key confirmation may provide explicit key authentication.

Extraction (Feature Extraction) **X9.84**

The process of converting raw biometric data into processed biometric for use in template comparison or reference template creation.

Eye Biometrics **X9.84**

Identification of a person by scanning either the iris or the retina of the eyeball.

Face Biometrics **X9.84**

The identification of a person by their facial image. This can include features in the visible spectrum, the infrared spectrum, or both.

Failure to Acquire **X9.84**
Failure of a biometric system to capture (and subsequently) extract biometric data.

False Acceptance Rate **X9.84**
Historical term. This standard uses the term *False Match Rate*.

False Match Rate **X9.84**
The probability that a biometric system will incorrectly identify an individual, or fail to reject an imposter. Historically also known as a Type II Error from hypothesis testing.

False Non-Match Rate **X9.84**
The probability that a biometric system will fail to verify the identity of a legitimate enrollee. Historically also known as a Type I Error from hypothesis testing.

False Rejection Rate **X9.84**
Historic term. This standard uses *False Non-Match Rate.*

Field Tag ***X9.9(W)*, *X9.17-85(W)*, *X9.17-95(W)*, *X9.28(W)***
A unique string of characters which identifies the meaning and location of the associated data field.

Filtering **X9.84**
Partitioning a database through the use of exogenous information about the user not discernable from the biometric patterns, such as sex, age or race.

Financial Institution **X9.19, X9.86**
An establishment responsible for facilitating customer-initiated transactions or transmission of funds for the extension of credit or the custody, loan, exchange, or issuance of money.

Financial Message ***X9.9(W)*, *X9.17-85(W)*, *X9.17-95(W)*, X9.19, *X9.23(W)*, X9.30:1, X9.30:3, X9.31:1, X9.57**
A communication containing information which has financial implications.

Finger Geometry **X9.84**
A physical biometric that analyses the shape and dimensions of one or more fingers.

Fingerprint **X9.84**
The pattern of friction ridges and valleys on an individual's fingertips that are considered unique to that individual.

Fixed Format Message ***X9.9(W)***
A message whose field characters and positions are predetermined.

Fixed Split **X9.69**
Secret key(s) used in all encryption/decryption operations, this split is unique to a particular organization or group.

Forgery **X9.30:1, X9.30:3, X9.31:1, X9.57**
The fabrication of information by one individual, entity or process and/or the claim that such information was received in a communication from another individual, entity, or process.

Forward Secrecy **X9.42**
The assurance provided to an entity that the session key established with another entity will not be compromised by the compromise of either entity's static private key in the future. Also known as perfect forward secrecy.

Forwarding ***X9.28(W)***
A process, normally performed by intermediate centers, whereby subscriber keys contained in an incoming CSM are decrypted, re-encrypted under a different transportation key and placed in an outgoing CSM.

Functional Testing **X9.79**
The portion of security testing in which the advertised features of a system are tested for correct operation.

Functionally Secure Device **X9.86**
A device with no inherent physical security characteristics (and which therefore relies totally upon 'device management' for its physical security), the functionality of which provides logical security so that the device can be compromised only by physical means (e.g. penetration of the device), which functionality cannot be subverted by unauthorized input into the device.

Global Name **X9.68**
A name that is unique to all systems. Global names are assured in compact certificates by the incorporation of a public hash in a local (non-unique) name.

Grantor *X9.26(W)*

The entity being asked to grant access privileges. The sign-on process begins when requesters attempt to sign-on to grantors. (Upon successful completion of all of the requirements for sign-on authentication as specified in ANSI ***X9.26(W)***, the identity of the requester is authenticated.)

Group ***X9.28(W)***
See Multiple Center Group

<Very Large SNIP>

Zeroized *X9.17-85(W)*, *X9.17-95(W)*, **X9.30:3, X9.57, X9.62**

The degaussing, erasing or overwriting of electronically stored data.

X-Coordinate **X9.62**

The x-coordinate of an elliptic curve point.

$P = (x_P, y_P)$ is x_P.

Y-Coordinate **X9.62**

The y-coordinate of an elliptic curve point.

$P = (x_P, y_P)$ is y_P.

SYMBOL AND ACRONYM ABBREVIATIONS

Acronym/Abbreviation **Meaning**

$\tilde{y}_p$

X9.62
The representation of the y-coordinate of a point P when point compression is used.

#E(F_q)

X9.62
If E is defined over F_q, then #E(F_q) denotes the number of points on the curve (including the point at infinity ○). #E(F_q) is called the order of the curve E.

#E(Fq)

X9.30:1
Number of points on the curve. #E(Fq) is called If E is defined Fq, then #E(Fq) denotes the order of E.

(*)KK

X9.17-85(W)
Key Encrypting Key or Key Pair.
(See KK and *KK.) An asterisk in parentheses is used to designate the use of either a single length key (KK) or a key pair (*KK).

(*)KKU

X9.17-95(W)
Key Encrypting Key or Key Pair, Notarized Ultimate Recipient.
(See KKU and *KKU.) An asterisk in parentheses is used to designate the use of either a single length key (KK) or a key pair for the (*KK).

*KK

X9.17-85(W)
Key Encrypting Key
Consists of two key encrypting keys used together to encrypt other keys. An asterisk is used to designate a key pair. Also used as a field tag for a key encrypting key pair.

*KK

X9.28(W)
Key Encrypting Key Pair
Also used as a field tag in a CSM.

Acronym/Abbreviation	Meaning
*KKU	***X9.17-85(W), X9.17-95(W), X9.28(W)*** **Key Encrypting Key Pair, Notarized Ultimate Recipient.** A field tag for a field which contains a key encrypting key for the pair intended for the ultimate recipient, encrypted under a notarizing key
a, b	**X9.62** Elements of Fq that define an elliptic curve E over Fq.
ABA	**X9.79** American Bankers Association
ABarA	**X9.79** American Bar Association
AES	**X9.69** Advanced Encryption Standard
AID	**X9.84** AID (Algorithm Identifier) is a unique identifier for a given encryption or hash algorithm, together with any required parameters. The unique identifier is an ASN.1 object identifier
ARL	**X9.88** Authority Revocation List
ARF	***X9.17-95(W), X9.28(W)*** Audit Record Field A field containing a record of who handled the messages in the transaction.
ASCII	***X9.23(W), X9.28(W)*** American Standard Code for Information Interchange A character set consisting of the ASCII (hexadecimal) characters A0-9" and AA-F@.
ASE	***X9.28(W)*** Expected ASN value field tag

Acronym/Abbreviation	Meaning
ANS	**X9.86** American National Standard
ANS	**X9.86** American National Standard Institute
ASN	***X9.28(W)*** Authentication Sequence Number field tag
ASN.1	**X9.41, X9.42, X9.70, X9.73, X9.84** Abstract Syntax Notation One
ATM	**X9.86** Automatic Teller Machine
B	**X9.62** MOV threshold. A positive integer B such that taking discrete logarithms over FqB is at least as difficult as taking elliptic curve logarithms over Fq. For this Standard, B shall be ≥20.
B=>	**X9.44** Binary string, e.g., B=01'
BER	**X9.30:3, X9.42, X9.55, X9.57, X9.68, X9.84** Basic Encoding Rules
BLOCK	**X9.30:2** A 512-bit string. A block (e.g., B) may be represented as a sequence of 16 words
C	**X9.69** Key Usage Control Vector
CA	**X9.55, X9.57** Certification Authority
CARAT	**X9.79** Certificate Authority Review and Accreditation Taskforce (NACHA)

Acronym/Abbreviation	**Meaning**
CBC	**X3.106, X9.19, *X9.23(W)*, X9.52, X9.69** Cipher Block Chaining The Cipher Block Chaining encryption mode of operation
CBCOFBM	**X9.52** Cipher Block Chaining with Output FeedBack Masking
CEK	**X9.73** Content Encryption Key
Cert(i)	**X9.42** A certificate containing user I's public key, y(i).
Cert_x	**X9.70** Certificate containing the public encryption key, (static) public key agreement key Y_x, or signature verification key of party *x*
CF	***X9.17-95(W)*** Confirmation Flag A field, which signals that a confirmation message is desired.
CFB	**X3.106, X9.19, *X9.23(W)*, X9.52** Cipher FeedBack The Cipher FeedBack encryption mode of operation
CFM	***X9.17-95(W)*** Disconnect Confirmation Message A message used to confirm that keys were discontinued.
CKD	***X9.17-85(W), X9.17-95(W), X9.28(W)*** Center for Key Distribution. Also known as Key Distribution Center A facility which generates and returns keys for distribution.

Acronym/Abbreviation	Meaning
CKM	**X9.69, X9.73** Constructive Key Management
CKT	**_X9.17-85(W)_,95, _X9.28(W)_** Center for Key Translation. Also known as a Key Translation Center A facility which transforms and returns keys for distribution.
CMS	**X9.73, X9.88** Cryptographic Message Syntax
CP	**X9.79** Certificate Policy
CPS	**X9.79** Certification Practice Statement
CRL	**X9.30:3, X9.55, X9.57, X9.68, X9.73** Certificate Revocation List
CRLF	***X9.17-95(W)*** Carriage Return/ Line Feed The pair of characters consisting of a carriage return and line feed.
CRT	**X9.80** Chinese Remainder Theorem
CSM	**_X9.17-85(W)_, _X9.17-95(W)_, _X9.26(W)_, _X9.28(W),_ X9.73** Cryptographic Service Message Tag for cryptographic service messages. It uses similar formats and notations as carriage return and described in ANSI X9.17-1985.

Acronym/Abbreviation **Meaning**

CTA

X9.17-85(W)*, *X9.17-95(W)*, *X9.28(W)
Count “A”
An incrementing binary counter used to control successive key distributions under a particular key encryption key. Used between a Key Distribution Center or a Key Translation Center and a party designated as “A”. Associated with a *KK used to encrypt either a (*)KK or KD(s) sent in a Cryptographic Service Message.

CTB

X9.17-85(W)*, *X9.17-95(W)*, *X9.28(W)
Count “B”
An incrementing binary counter used to control successive key distributions under a particular key encryption key. Used between a Key Distribution Center or a Key Translation Center and a party designated as “B”. Associated with a *KK used to encrypt either a (*)KK or KD(s) sent in a Cryptographic Service Message.

CTC

X9.28(W)
Count “C”
An incrementing binary counter used to control successive key distributions under a particular key encryption key. Used between a Key Distribution Center or a Key Translation Center and a party designated as “C”. Associated with a *KK used to encrypt either a (*)KK or KD(s) sent in a Cryptographic Service Message.

CTP

X9.17-85(W)*, *X9.17-95(W)
Count “P”
An incrementing binary counter used to control successive key distributions under a particular key encrypting key. Used in a point-to-point relationship. Associated with a (*)KK which is used to encrypt the highest level key(s) transported in a Cryptographic Service Message. Used between communicating pairs, but not between a CKD or a CKT and another party.

Acronym/Abbreviation	**Meaning**
CTR	***X9.17-85(W)**, **X9.17-95(W)**, **X9.28(W)*** Count "R" The count field of an error message which is equal to the received count and only when a count error occurs. . Sent only when a count value error occurs.
D	**X9.62** Elliptic curve private key.
D	**X9.44** Private (signature) exponent
DAM	**X9.79** Draft Amendment
DATA	***X9.26(W),*** **X9.71** The input of the Crypto Function. For example, the result of the Combine Function.
DEA	***X9.26(W)***, **X9.52** Data Encryption Algorithm The Data Encryption Algorithm specified in ISO 8227 and ANS X3.92.
DER	**X9.30:3, X9.42, X9.55, X9.57, X9.68, X9.84** Distinguished Encoding Rules
DES	**X3.106, X9.69** Data Encryption Standard (The Data Encryption Standard specified in FIPS Pub. 46)
D,H(X,Y)	**X9.70** Computation of shared secret using the Diffie-Hellman algorithm and the enclosed parameters; X is the private key and Y is a public key
DIT	**X9.55** **Directory information tree**
DIV	**X9.31:1** Integer Division

Acronym/Abbreviation	**Meaning**
DLP	**X9.42** Discrete Logarithm Problem
DN	**X9.30:3, X9.55, X9.57, X9.68** **Distinguished Name**
DNM	*X9.17-95(W)* **Disconnect Notify Message** Used by a center to notify the subscribers that keys should be discontinued.
DSA	**X9.30:3, X9.55, X9.57, X9.68** **Digital Signature Algorithm**
DSM	*X9.17-85(W)*, *X9.17-95(W)* **Disconnect Service Message** Optional message class used to discontinue one or more keys or to terminate a keying relationship.
DVCS	**X9.88** Data validation and certification server
e	**X9.62** Result of applying hash function to message M.
E	**X9.62** An elliptic curve over the field F_q defined by a and b.
e	**X9.44** Public (verification) exponent
e'	**X9.62** Result of applying hash function to message M'.
$E(F_q)$	**X9.30:1, X9.62** The set of all points on an elliptic curve E defined over F_q and including the point at infinity O.
EB	**X9.44** The encipherment block used as input to the encipherment process.

Acronym/Abbreviation	Meaning
ECB	***X9.26(W)*, X9.52, X9.69, X3.106** **Electronic Code Book** The Electronic Code Book encryption mode of operation
ECDSA	**X9.30:1** The Digital Signature Algorithm (DSA) using Elliptic Curve computation procedure.
ECPP	**X9.80** Elliptic Curve Primality Proving algorithm
ECSS	**X9.30:1** Elliptic Curve Signature Scheme.
ED	**X9.44** The encrypted data output by the encipherment process.
EDC	***X9.17-85(W)*, *X9.17-95(W)*** **Error Detection Code** An error detection code generated using the authentication algorithm and the fixed hexadecimal key, 0123456789ABCDEF.
EDK	***X9.17-85(W)*, *X9.17-95(W)*, *X9.28(W)*** **Effective Date of Key** A field or subfield which contains the date and Coordinated Universal Time when the key shall become active.
EDK1	***X9.17-95(W)*** Effective Date of Key The name for a subfield, which contains the effective date for the key in the key field containing the EDK1 subfield.

Acronym/Abbreviation	**Meaning**
EDK2	***X9.17-95(W)*** Effective Date of Key The name for a subfield, which contains the effective date for the key in the key field containing the EDK2 subfield.
$E_K(\bullet)$	**X9.70** Encryption of data under a symmetric key K
$\mathrm{Encr}_x(\bullet)$	**X9.70** Encryption of data under the public encryption key of party *x*.
ERF	***X9.17-85(W), X9.17-95(W), X9.26(W), X9.28(W)*** Error Field The field which identifies error conditions detected in a previous Cryptographic Service Message (CSM).
ERS	***X9.17-85(W), X9.17-95(W) X9.28(W)*** Error Recovery Key Key used to recover from count or other errors in a Service Message while in a Key Distribution Center or Key Translation Center environment.
ES	**X9.88** Enhanced Signature
ES-A	**X9.88** ES with archive validation data
ES-C	**X9.88** ES with complete validation data
ES-T	**X9.88** ES with timestamp
ES-X	**X9.88** ES with extended validation data

Acronym/Abbreviation **Meaning**

ESM

X9.17-85(W)**, 95,** ***X9.28(W)***
Error Service Message
Used to give a negative acknowledgment for the receipt of any Cryptographic Service Message other than an ESM, and to give the recipient data with which to recover.

ESS

X9.73
Extended Security Services

F_{2m}

X9.30:1, X9.62
The finite field containing $q = 2^m$ elements, where m is a positive integer. An optimal normal basis is a special kind or representation for the elements of the finite field F_{2m}.

FIPS

X9.41
Federal Information Processing Standard.

F_p

X9.62
The finite field containing q = p elements, where p is a prime.

F_q

X9.30:1, X9.62
The finite field containing q elements. For this Standard, q shall either be an odd prime number ($q = p$, $p > 3$) or a power of 2 ($q = 2^m$).

g

X9.42
A generator of the *q*-order cyclic subgroup of *GF(p)**, that is, an element of order *q* in the multiplicative group of *GF(p)*

G

X9.62
A distinguished point on an elliptic curve called the base point or generating point.

G

X9.42
A generator over the integers modulo p.

Acronym/Abbreviation	Meaning
G_x	**X9.70** For a key agreement algorithm, the group (domain) parameters associated with the public key of partyx.
GCD (a, b)	**X9.80** Greatest common divisor of integers a and b
GF(p*)*	**X9.42** The Galois Field defined by a prime *p*. The elements of *GF(p)* are typically represented by integers {0, 1, 2, …, *p*-1}. The two operations defined over *GF(p)* are addition and multiplication, which can be implemented by integer addition and multiplication modulo *p*, respectively. In this standard, an element of *GF(p)* is represented as an integer.
GP(p)*	**X9.42** Multiplicative group of GF(p), consisting of all the non-zero elements of GF(p).
GS1	***X9.26(W)*** Type 1 GSF GSF of type 1 authentication with a current PAI.
GS2	***X9.26(W)*** Type 2 GSF GSF of type 2 authentication with a current PAI.
GS3	***X9.26(W)*** Type 3 GSF GSF of type 3 authentication with a current PAI.
GSF	***X9.26(W)*** General Security Function It is used to protect the PAI and to authenticate the user or the node in the sign-on process.

Acronym/Abbreviation	Meaning
GSN	***X9.26(W)*** New GSF GSF of type 1 authentication with a new PAI.
GULS	**X9.41** Generic Upper Layers Security
H	**X9.62** $h = \#E(F_q)/n$, where n is the order of the base point G. h is called the cofactor.
H	**X9.31:1, X9.71** One-way hash function; the size of the output of H must be a multiple of 8 bits
H	**X9.31:1** Message digest (hash), output by the function H.
H	**X9.42** An ANSI approved hash function providing at least 160 bits of data output
H(m)	**X9.30:1** The hash of the bit string m computed using the SHA.
H(m)	**X9.30:2** The result of a hash computation (message digest) on the message, m.
H(•)	**X9.70** Hash of the enclosed data using an ANSI-approved hash algorithm
h	**X9.42** The hash value resulting from applying the hash function, H, to data
I&A	**X9.79** Identification and Authentication
IAD	**X9.86** Internet Access Device

Acronym/Abbreviation **Meaning**

IC
X9.86
Integrated Circuit

ICC
X9.86
Integrated Circuit Card

ID_x
X9.70
Identity of party *x*; in particular, *i* and *r* are initiator and responder

IDA
X9.17-85(W)*, *X9.17-95(W)
Identity of Key for Authentication
A field tag for a field, which contains the identity of the key to be used to authenticate a Disconnect Service Message. This key shall be discontinued.

IDA
X9.28(W)
Identity of the authenticated (MAC) Key field tag.

IDC
X9.17-85(W)*, *X9.17-95(W)
Identity of Key Distribution Center or Key Translation Center.

A field tag for a field which contains the identity of a center used Distribution Center or to be used in the transaction.

IDD
X9.17-85(W)*, *X9.17-95(W)
Identity of Key to be Discontinued
A field tag for a field, which contains the identity of a key to be discontinued.

IDD
X9.28(W)
Disconnect key ID field tag.

IDI
X9.28(W)
Initial recipient identification field tag.

IDK
X9.17-95(W)
Identity of Key. A name for a subfield containing the identity (name) of a key.

Acronym/Abbreviation Meaning

IDK1

X9.17-85(W), X9.17-95(W)
Key Identifier (Subfield). The name for a subfield which identifies (names) the key (subfield) being sent in a Cryptographic Service Message key field.

IDK1

X9.28(W)
The designator for the sub-field of a key field which is used to provide the name of the key transport in the key field

IDK2

X9.17-85(W), X9.17-95(W)
Key Encrypting Key Identifier (subfield). The name for a subfield which identifies (names) Identifier (subfield) the key encrypting key or key pair used to encrypt the key being sent in a Cryptographic Service Message key field.

IDK2

X9.28(W)
The designator for the sub-field of the key field which provides the name of the key encrypting key that was used to offset encrypt or notarize the key transport in the key.

IDU

X9.28(W)
Identity of Ultimate Recipient. This field is only used with in a Key Distribution Center or a Key Translation Center.

IDU

X9.17-85(W), X9.17-95(W), X9.28(W)
Identity of Ultimate Recipient
This field is only used with in a Key Distribution Center or a Key Translation Center environment.

IEC

X9.79
Internet Electrotechnical Commission

IETF

X9.73, X9.79
Internet Engineering Task Force

Acronym/Abbreviation	Meaning
INF	***X9.26(W)*** Information. Any user defined information as a parameter of the Combine Function.
IP	**X9.79** Internet Protocol
Ipad	**X9.71** The byte h’36’ repeats 64 times
INPUT	*X9.26(W)* Input. The input of the Section Function. For example, the result of a Crypto Function
IS	**X9.86** International Standard
ISAKMP	**X9.70** Internet Security Association and Key Management Protocol
ISO	**X9.86** International Organization for Standards
ITS	***X9.23(W)*** Initial Task Sequence Binary vector which may be prepended to a message.
ITU	**X9.55, X9.57** International Telecommunications Union
IUK	***X9.17-95(W)*** Intended Use of Key The name for a subfield, which identifies the intended use of a KD.
IUT	**TG-19-1** Implementation Under Test

Acronym/Abbreviation	Meaning
IV	***X9.17-85(W)***, ***X9.17-95(W)***, ***X9.23(W)***, ***X9.26(W)***, ***X9.28(W)***, **X9.52, TG-19-1** **Initialization Vector** Starting point for a DEA encryption/decryption process. Also used as a field tag in a CSM
j	**X9.42** A cofactor of p-1 along with q, i.e., ***p-1 = jq***
K	**X9.42** A shared symmetric key
K	**X9.62** Per-message secret value. For this Standard, k shall be a statistically unique and unpredictable integer in the interval [1, n-1].
K	***X9.26(W)***, **X9.69** Key A DEA key.
K	**X9.31:1** The length of the modulus n in bits
K	**X9.44, X9.71** The length of the modulus n in bits (after discarding any leading zero bits).
K	**X9.70** The symmetric key produced by the KMP exchange
KD	***X9.17-85(W)***, ***X9.17-95(W)***, ***X9.28(W)*** Data Key A data key. Also a field tag for a field in a CSM containing a data key.
KDA	***X9.28(W)*** Transportation data key used for authentication.
KDF	**X9.69** Key Usage Control Vector

Acronym/Abbreviation	Meaning
KDF(•)	**X9.70** Key derivation function applied to the enclosed data
KDU	***X9.17-85(W)*, *X9.17-95(W)*, *X9.28(W)*** Data Key, Notarized A field tag for a field which containing a data key for the Ultimate recipient encrypted under a notarized key.
KEK	**X9.41, X9.73** Key Encrypting Key
KKU	***X9.17-85(W)*, *X9.17-95(W)*, *X9.28(W)*** Key Encrypting Key, Notarized Key for Ultimate Recipient A field tag in a CSM for a field which contains a key encrypted for the ultimate recipient, encrypted under a notarizing key.
Kl	**X9.44** The length of the symmetric key, in bytes.
KMP	**X9.41** Key Management Protocol
KN	***X9.28(W)*** Notarization Key
KSM	***X9.17-85(W)*, *X9.17-95(W)*, *X9.28(W)*** Key Service Message Used to transfer keys between communicating pairs
L	**X9.42** The length of the parameter *p*. The value *L* shall always be greater than or equal to 1024
L	**X9.62** The length of a field element in octets; $l = \lceil t / 8 \rceil$.
L	**X9.31:1** The length of the prime factors p and q in bits

Acronym/Abbreviation	Meaning
L_{max}	**X9.62** Upper bound on the largest prime divisor of the cofactor h.
LCM (a, b)	**X9.80** Least common multiple of integers a and b
Log_2 x	**X9.30:1, X9.62** The logarithm of x to the base 2.
LRA	**X9.30:3, X9.55, X9.57, X9.68** Local Registration Agent
m, n, a	**X9.80** Any positive integers that may or may not be prime
M	**X9.62** The degree of the finite field F_{2^m}.
M	**X9.62** Message to be signed.
M	**X9.31:1** A message to be signed
M	**X9.44** The length of the data M to be encrypted.
M	**X9.44** Message to be encrypted
M	**X9.62** The degree of the finite field F_{2m}.
M'	**X9.62** Message as received.
m	**X9.42** The length of the parameter *q*. For this standard, the value *m* shall always be greater than or equal to 160. If *m* is not explicitly specified, it shall default to the value of 160.

Acronym/Abbreviation	Meaning
MAC	***X9.17-85(W)*, *X9.17-95(W)*, *X9.26(W)*, X9.41, X9.42, X9.49, X9.69, X9.70, X9.73** Message Authentication Code A Message Authentication Code computed in accordance with ANSI *X9.9(W)*. Also used as a field tag for a field, which contains a MAC.
MAC	**X9.84** **MAC (**Message Authentication Code) is a cryptographic value which is the result of passing information through the MAC algorithm using a symmetric key.
MB	**X9.44** Masked Block
MCL	***X9.17-85(W)*, *X9.17-95(W)*, *X9.26(W)*** Message Class The tag for the field that defines the type of Cryptographic Service Message (CSM).
MDNM	***X9.28(W)*** Multiple Center Disconnect Notify Message
MERR	***X9.28(W)*** Multiple Center Error Report
MESM	***X9.28(W)*** Multiple Center Error Service Message
MID	***X9.9(W)*:86, X9.30:1, X9.31:1, *X9.26(W)*, X9.62** Message Identifier
MIME	**X9.73** Multipurpose Internet Mail Extension
Mod	**X9.30:1, X9.30:2, X9.31:1, X9.44, X9.62, X9.80** Modulo

Acronym/Abbreviation	Meaning
Mod f(x)	**X9.62** Arithmetic modulo the polynomial f(x). If f(x) is a binary polynomial, then all coefficient arithmetic is performed modulo 2.
Mod n	**X9.30:1** arithmetic modulo n
Mod n	**X9.30:1, X9.30:2, X9.62** Arithmetic modulo n.
Mod p	**X9.42** The reduction modulo *p* on an integer value. If the context is clear, then "*mod p*" is sometimes omitted for brevity
Modulo	**X9.31:1, X9.44, X9.80** Arithmetic modulo n
MQV	**X9.42, X9.70, X9.73** Menezes-Qu-Vanstone Diffie-Hellman-based key agreement algorithm
MRFS	***X9.28(W)*** Multiple Center Request For Service
MRSI	***X9.28(W)*** Multiple Center Request Service Initiation
MRSM	***X9.28(W)*** Multiple Center Response Service Message
MRTR	***X9.28(W)*** Multiple Center Response To Request
MTCM	***X9.28(W)*** Multiple Center Transaction Confirm Message

Acronym/Abbreviation	Meaning
N	**X9.62** The order of the base point G. For this Standard, n shall be greater than 2^{160} and $4\sqrt{q}$, and shall be a prime number. n is the primary security parameter. The strength of ECDSA rests on two fundamental assumptions, the difficulty of finding a collision using the one-way hash function and the difficulty of solving the ECDLP. The difficulty of finding a collision using SHA-1 is thought to take 2^{80} steps. The difficulty of solving the ECDLP is related to the size of n – as n increases, the difficulty of the ECDLP increases. See Annex H for more information.
N	**X9.30:1** The order of the point P is n; this is the smallest positive integer such that nP=0 (infinity).
N	**X9.31:1, X9.44** RSA modulus; subscripting is used to identify a particular user "s" modulus.
N	**X9.62** The order of the point P. For this standard, n shall always be a prime number.
Nx	**X9.70** Nonce from party *x*
NACHA	**X9.79** National Automated Clearing House Association
NIST	**TG-19-1, X9.79** National Institute of Standards and Technology
NOS	***X9.17-85(W), X9.17-95(W)*** Notarization Indicator. A field tag that, when present, indicates that notarization was used.

Acronym/Abbreviation	**Meaning**
O	**X9.62** A special point on an elliptic curve called the point at infinity. This is the additive identity of the elliptic curve group.
OBD	***X9.17-95(W)*** Obsolete Date The name for a subfield containing an obsolete date for a key.
OCSP	**X9.88** Online Certificate Status Protocol
OFB	**X3.106, X9.52** Output FeedBack
OID	**X9.79** Object Identifier
Opad	**X9.71** The byte h'5c'repeats 64 times
ORG	***X9.17-85(W), X9.17-95(W), X9.26(W), X9.28(W)*** Originator. A field tag for a field, which contains the identity of the Cryptographic Service Message originator.
p, q	**X9.80** Prime numbers
P	**X9.62** An odd prime number.
P	***X9.17-85(W), X9.17-95(W)*** Key Parity (Subfield). The name for the subfield which indicates that the plaintext key conforms to the specification for odd parity. Also used as the contents of that subfield.

Acronym/Abbreviation **Meaning**

P

X9.30:1
P is a point (xp,yp) on an elliptic curve over a field Fq, where xp and yp are elements of Fq. The values x=xp and y=yp must satisfy the equation defining E. Xp is called the x-coordinator of P and yp is called the y-coordinator of P.

There is an addition rule, which allows the addition of two elliptic curve points P1 and P2 to produce a third elliptic curve point P3.

If k is a positive integer, then kP denotes the point obtained by adding together k copies of the point P. The process of computing kP from P and k is called exponentiation.

P

X9.42
Prime Modulus. A prime modulus, where 2L-1 < p < 2L for 512 < -L < - 10024, and L a multiple of 64.

P

X9.62
A point (xp, yp) on an elliptic curve. P is called the base point.

p, q

X9.31:1
Prime factors of n.

PAI

X9.26(W)
Personal Authenticating Information
Information used to authenticate a user's identity. The information can be derived from something the user knows (e.g., a secret password), something the user has (e.g., exclusive possession of a Badge), something the user is (e.g., fingerprint), or any combination of the three.

PCA

X9.30:3, X9.55, X9.57, X9.68
Policy Certification Authority

Acronym/Abbreviation	Meaning
PCM	*X9.26(W)* Grantor- generated. One of the four message classes used in the sign-On Change Message on authentication CSM.
PDU	**X9.41, X9.70** Protocol Data Unit
PER	**X9.84** Packed Encoding Rules
PED	**X9.86** PIN-entry devise
PIN	**X9.8, X9.69, X9.86** Personal Identification Number
PKI	**X9.79, IETF** Public-key Infrastructure
PKIX	**X9.79, IETF** Public-key Infrastructure (X.509) (IETF Working Group)
PM	**X9.41** Protection Mapping
POD	*X9.17-95(W)* Pending Obsolete Date The name for a subfield containing a pending obsoletedate for a key.
PS	**X9.30:1, X9.62** Padding string
Q	**X9.62** The number of elements in the field F_q.
Q	**X9.62** Elliptic Curve public key.

Acronym/Abbreviation	Meaning
r(i)	**X9.42** A random or pseudorandom integer with $0 < x < p$, selected by user i.
r_{min}	**X9.62** Lower bound on the desired (prime) order n of the base point G. For this Standard r_{min} shall be $>2^{160}$.
R_x	**X9.70** Ephemeral private key agreement for party *x*
RA	**X9.79** Registration Authority
RCV	***X9.28(W)*** A field tag for a field which contains the identity of the intended Cryptographic Service Message recipient.
RDN	**X9.30:3, X9.55, X9.57, X9.68** Relative Distinguished Name
RFC	**X9.79** Request For Comment
RFS	**_X9.17-85(W)_, 95, _X9.28(W)_** Request For Service message Used to request the translation of keys by a Key Translation Center for retransmission to another party.
RN	**X9.42** Random number used in constructing the encryption block.
RSA	**X9.41** Rivest-Shamir-Adelman (Public Key Cryptosystem)

Acronym/Abbreviation	Meaning
RSI	***X9.17-85(W)*, *X9.17-95(W)*, *X9.28(W)*** Request Service Optionally used to request keys from an request the other party Initiation Message or to generation of keys by a CKD
RSM	***X9.17-85(W)*, *X9.17-95(W)*, *X9.28(W)*** Response Service Message Used to provide an authenticated acknowledgment.
RTR	***X9.17-85(W)*, *X9.17-95(W)*, *X9.28(W)*** Response to Request Message Used to send keys from a Key Distribution Center or from a Key Translation Center.
S_x	**X9.70** Ephemeral public key agreement for party *x*
SA	**X9.41** Security Association
SAID	**X9.41** Security Association Identifier
SE	**X9.41** Security Exchange
SEI	**X9.41** Security Exchange Item
SHA	**X9.30:1, X9.30:2, X9.55, X9.57, X9.68** Secure Hash Algorithm as defined in ANSI X9.30-1993 Part 2, The Secure Hash Algorithm (SHA).
SHA-1	**X9.30:1, X9.30:2** as defined in ANSI X9.30-1995 Part 2, The Secure Hash Algorithm (SHA).

Acronym/Abbreviation	Meaning
SHA-1(m)	**X9.30:1** the result of a hash computation (message digest) on message m using the SHA-1 as defined in ANSI X9.30-1997, Part 2: The Secure Hash Algorithm (SHA-1) (Revised)
SIG$_x$(D)	**X9.70** Data D, concatenated with the signature on D by party *x*; shorthand for: D,SIG$_x$(D)
Signed$_x$(D)	**X9.70** Signature on data by party *x*
SMIB	**X9.69** Security Management Information Base
S/MIME	**X9.73** Secure MIME
SMTP	**X9.73** Simple Mail Transfer Protocol
SOE	***X9.26(W)*** Sign-on Error Request One of the four message-classes used in the sign- on authentication CSM.
SOM	***X9.26(W)*** Sign-on Message authentication CSM. One of the four message classes used in the sign-on.
ST	***X9.17-95(W)*** State. Used to indicate the state into which discontinued keys are to be placed.
ST	**X9.41** Security Transformation
SVR	***X9.17-85(W), X9.17-95(W), X9.28(W)*** **Service Request** A field tag for a field which specifies the type of service requested.

Acronym/Abbreviation	Meaning
T	**X9.62** The length of a field element in bits; $t = \lceil \log_2 q \rceil$. In particular, if $q = 2^m$, then a field element in F_{2^m} can be represented as a bit string of bit length $t = m$.
T	**X9.62** In the probabilistic primality test, the number of independent test rounds to execute. For this Standard T shall be ≥50.
T	**X9.30:1** A field element of Fq will be represented as a binary string of length t=j log2 qk. In particular, f q=2m, then a field element in F2m can be represented as a binary string of length t=m.
TCBC	**X9.52, TG-19-1** TDEA Cipher Block Chaining
TCBC-I	**TG-19-1** TDEA Cipher Block Chaining – Interleaved
TCFB	**X9.52, TG-19-1** TDEA Cipher FeedBack
TCFB-P	**TG-19-1** TDEA Cipher FeedBack – Pipelined
TDEA	**X9.52, TG-19-1** Triple Data Encryption Algorithm
TDES	**X9.52, TG-19-1** Triple DES
TECB	**X9.52, TG-19-1** TDEA Electronic CodeBook
TLS	**X9.70** Transport Layer Security
TMOVS	**TG-19-1** TDEA Modes of Operation Validation System

Acronym/Abbreviation	Meaning
TOFB	**X9.52, TG-19-1** TDEA Output FeedBack
TOFB-I	**TG-19-1** TDEA Output FeedBack Mode of Operation – Interleaved
Tr	**X9.62** Trace function. (See ANS X9.62, Annex.)
TRSM	**TG-19-1** Tamper Resistant Security Module
TSA	**X9.88** Timestamp Authority
TSP	**X9.88** Trusted Service Provider
TTM	***X9.26(W)*** TVP Transmission Message One of the four message classes used in the sign-on authentication CSM.
TVP	***X9.26(W)*** Time Variant Parameter
UDF	***X9.17-95(W)*** User Defined Field
UKM	**X9.73** User Keying Material
UKPT	**Tg-19-1** Unique-key-per-transaction
URL	**X9.79** Uniform Resource Locator
US	**X9.79** United States

Acronym/Abbreviation	Meaning
USR	***X9.26(W)*** User Identity of the user requesting access.
W	**X9.31:1** Length of the modulus n in bytes.
X	**X9.42** A random or pseudorandom integer with $0 < x < p$; this is the user "s" private key. Subscripting is used to indicate a particular user "s" key; e.g., xi is i=s private key.
XB	**X9.44** Expanded block created from M and used to construct EB.
x_p	**X9.62** The x-coordinate of a point P.
y_p	**X9.62** The y-coordinate of a point P.
Yp	**X9.30:1** Let P be a point (xp,yp) on an elliptic curve E defined over a field Fq. If point compression is not used, then yp is equal to yp. If point compression is used and q is a prime, then yp is equal to the last significant bit of yp. If point # compression is used and q is a power of 2, the yp is 0 if xp=0;if xp … 0, then is equal to the least significant bit of the field element yp C Xp-1. The point compression technique is described in Section 6.11 of the Standard.
Y_s	**X9.42** g(x) mod p; this is the user public key. Again, subscripting is used to indicate a particular user "s" public key.
Y_x	**X9.70** Static public key agreement for party *x*

Acronym/Abbreviation **Meaning**

Z

X9.70
Shared secret derived using DH(.) or MQV(.)

ZZ

X9.42
A shared secret value, represented by an octet string, that is obtained by implementing a key agreement scheme. Depending on which key agreement scheme is executed, *ZZ* may be oct(Z_e), oct(Z_s), oct(Z_e)||oct(Z_s), or oct(Z_{MQV})

Z_p

X9.62
The set of integers modulo p, where p is an odd prime number.

5 NOTATION

1, 2, …

X9.70
Integers denote tags used to distinguish between different messages of a protocol exchange; they may be of any type, as long as they are recognized and unique

$\bullet$

X9.30:2
multiplication

$\vee$

X9.30:1, X9.30:2, X9.31:1
bitwise logical "inclusive-or"

$\wedge$

X9.42

Multiplication operator of two elements *a* and *b*. Conventional algebraic positional notation is also used to denote multiplication where there is no chance of ambiguity. For example, *ab* and *a·b* are equivalent

$\oplus$

X9.30:1, X9.30:2, X9.31:1, X9.44, X9.71
bitwise logical "exclusive-or"

Example:

```
        01101100101110011101001001111011
⊕       01100101110000010110100110110111
=       00001001011110001011101111001100
```

$\lceil x \rceil$

X9.42, X9.62, X9.80
Ceiling: the smallest integer ≥ x. For example, $\lceil 5 \rceil = 5$ and $\lceil 5.3 \rceil = 6$.

$\lfloor x \rfloor$

X9.62, X9.80
Floor: the largest integer ≤ x. For example, $\lfloor 5 \rfloor = 5$ and $\lfloor 5.3 \rfloor = 5$.

[x, y]

X9.62
The interval of integers between and including x and y.

$|x|$

X9.31:1, X9.80
Absolute value of x; $|x|$ is -x if x > 0; otherwise it is simply x.

$\|\| x \|\|$	**X9.30:1, X9.42, X9.62** Length in bits of *x*, which may be an octet string or an integer
$\|G\|$	**X9.42** The number of elements in the group *G*. For the multiplicative group *GF*(*p*)*, *|GF(p)*|* = *p-1*
≡	Congruence. *A* ≡ *B* mod *C* means that (*A-B*) is divisible by *C*
||	**X9.30:1, X9.30:2**, **X9.31:1, X9.31:2**, **X9.44, X9.71** concatenation
[ ]	**X9.70** Optional protocol elements are enclosed in square brackets
~x	**X9.30:2, X9.31:1** bitwise logical "complement" of x.
+	**X9.31:1, X9.31:2, X9.44, X9.80** addition
*	**X9.80** Multiplication
√x	**X9.80** Square root of x
$\left(\frac{a}{n}\right)$	**X9.42, X9.80** Jacobi symbol of *a* with respect to *n*
[a,b]	**X9.42, X9.80** The set of real numbers from *a* to *b* inclusive
{a, b}	**X9.42** The set consisting of elements *a* and *b*
a\b	**X9.80** Evenly divides; e.g. a divides b evenly (with no remainder)
a^b	**X9.80** Exponentiation. *A* raised to the *b*'th power

a·b

X9.42

Multiplication operator of two elements *a* and *b*. Conventional algebraic positional notation is also used to denote multiplication where there is no chance of ambiguity. For example, *ab* and *a·b* are equivalent

b’01’

X9.80

Binary notation used to represent one or more bits

Gcd(x, y)

X9.62

The greatest common divisor of integers x and y.

oct(a)

X9.42

The octet representation of *a*

p

X9.42

A prime defining the Galois Field *GF(p)*, which is used as a modulus in the operations of *GF(p)*, where $2^{(L-1)} < p < 2^{L}$, for $L \geq 1024$, and *L* is a multiple of 256

pgenCounter

X9.42

A counter that is used to validate that a prime number was generated in accordance with this standard. *pgenCounter* is used to indicate the point at which a suitable prime number was determined. See Annex B.1.2

q

X9.42

A prime factor of *p*-1 such that $p = jq+1$ and $q > 2^{m-1}$. *GF(p)** has a cyclic subgroup of order *q*

$r_{\{U,V\}}$

X9.42

Party U or Party V’s ephemeral private key. $r_{\{U,V\}}$ is a random or pseudo-random integer with $1 \leq r_{\{U,V\}} \leq (q_e-1)$ when ephemeral-key domain parameters are used. For the case where only static-key domain parameters are being used, then $r_{\{U,V\}}$ should be chosen such that $1 \leq r_{\{U,V\}} \leq (q_s-1)$. Note that it is acceptable to further restrict the interval to $1 < r_{\{U,V\}} < (q_s-1)$, if desired

Seed

X9.42

Random value that is used as input to a pseudorandom number generator

$t_{\{U,V\}}$

X9.42

Party U or Party V's ephemeral public key. $t_{\{U,V\}}$ is an element of $GF(p_e)$, $t_{\{U,V\}} = (g_e \wedge r_{\{U,V\}}) \bmod p_e$ when ephemeral-key domain parameters are used. For the case where only static-key domain parameters are being used, $t_{\{U,V\}} = (g_s \wedge r_{\{U,V\}}) \bmod p_s$.

$t_{\{U,V\}}'$

X9.42

$t_{\{U,V\}}' = (t_{\{U,V\}} \ mod\ 2^w) + 2^w$, an integer such that $2^w \leq t_{\{U,V\}}' < 2^{w+1}$. It is used in the MQV algorithm

U

X9.42

The initiator in a key agreement protocol

V

X9.42

The responder in a key agreement protocol

W

X9.42

Specifies the ephemeral public key mask width in bits for use with the MQV shared secret element calculation methods; in this standard, $w = \lceil ||q||/2 \rceil$.

X_X

X9.70

Static key agreement key for party x.

$X \oplus Y$

X9.30:1, X9.62

Bitwise exclusive-or (also bitwise addition mod 2) of two bit strings X and Y of the same bit length.

$x \equiv y \pmod{n}$

X9.62

x is congruent to y modulo n. That is, (x mod n) = (y mod n).

x mod n

X9.62

The unique remainder r, $0 \leq r \leq n - 1$, when integer x is divided by n. For example, 23 mod 7 = 2.

$X||Y$

X9.30:1, X9.42, X9.62
Concatenation of two strings X and Y. X and Y are either both bit strings, or both octet strings

X=>

X9.31:2, **X9.44**
A string, with hexadecimal value enclosed in the quotes, e.g., X=01FF=

x-1

X9.31:1
Multiplicative inverse of x, mod some n; for a given x,xx-1 = 1 (mod n)

x^{-1} mod n

X9.62
If gcd (x, n) = 1, then x^{-1} mod n is the unique integer y, $1 \leq y \leq n - 1$, such that $xy \equiv 1 \pmod n$

$X \oplus Y$

X9.42

Bit-wise exclusive-or of two bit strings *X* and *Y* of the same bit length

$X \vee Y$

X9.42

Bit-wise inclusive-or of two bit strings *X* and *Y* of the same bit length

$X+Y$

X9.42

The addition of two numeric quantities *X* and *Y*. The operation may be followed by a reduction by the modulus

$x_{\{U,V\}}$

X9.42

Party U or Party V's static private key. $x_{\{U,V\}}$ is a random or pseudo-random integer with $1 \leq x_{\{U,V\}} \leq (q_s - 1)$. Note that it is acceptable to further restrict the interval to $1 < x_{\{U,V\}} < (q_s - 1)$, if desired

$y_{\{U,V\}}$

X9.42

Party U or Party V's static public key. $y_{\{U,V\}}$ is an element of $GF(p_s)$, $y_{\{U,V\}} = (g_s \wedge x_{\{U,V\}})\ mod\ p_s$

Z_s

X9.42

A shared secret element of $GF(p_s)$ that is computed from the static private/public keys by using the Diffie-Hellman algorithm

Z_e **X9.42**

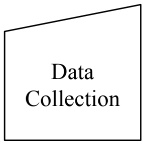
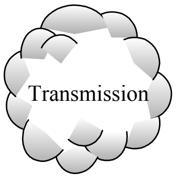
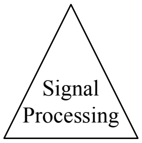
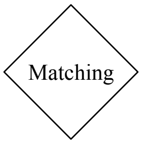
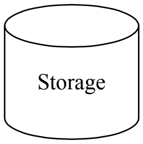
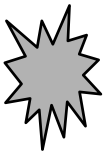
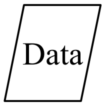
A shared secret element of $GF(p_e)$ that is computed from the ephemeral private/public keys by using the Diffie-Hellman algorithm

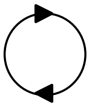
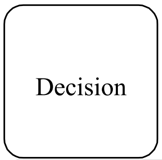
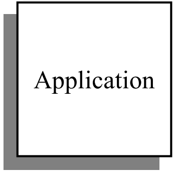
Z_{MQV} **X9.42**

A shared secret element of GF(p) that is computed from the static and ephemeral components by using the MQV algorithm

The notation used which are variants of the X.509 notations for certificates, certification paths, and related information and includes:

Notation	**Meaning**
P_1=>E_P	E*s public key verified using the CA*s primary private key.
P_2=>E_P	E*s public key verified using the CA*s secondary private key.
S_1<<E>>	E*s primary certificate signed using the CA*s primary private key.
S_2<<E>>	E*s secondary certificate signed using the CA*s secondary private key.
S_1S_2<<E>>	E*s multiply signed certificate signed using the CA*s primary and secondary private keys.
X{information}	The signing of 'information' by X.
X_p	X*s public key. E.g., X_{1p} is X_1*s public key.
X_{1s}	X_1*s private key.
X_l*X_2+	X_2*s certificate issued by the CA, X_1.
X_l*X_2+X_2*X_3+ X_{n-1}*X+	Certificate path. Each item in the path is the certificate for the CA, which produced the next item. This path is of arbitrary length and is functionally equivalent to X_l*X_n+. Possession of X_{1p} allows a user to extract the authenticated public key of $X_{n.}$
$X_{lp}{}^{l}X_1$*X_2	Unwrapping of a certificate or path. The public key of the leftmost CA (X_1) is used to extract the authenticated public key of the rightmost certificate (X_1*X_2+) by working through the path of intervening certificates. This example extracts X_{2p}.

Symbols	Meaning
	**X9.84** Symbol represents the data collection (or capture) component which includes the biometric reader hardware device and supporting software. See §**Error! Reference source not found.** ***Error! Reference source not found.*** for details. Inputs: physical world (finger, eye, etc.) Outputs: biometric data / objects
	**X9.84** Symbol represents the transmission component which may or may not be present in a biometric systems. See §**Error! Reference source not found.** ***Error! Reference source not found.*** for details. Inputs: biometric data / objects Outputs: biometric data / objects
	**X9.84** Symbol represents the signal processing component, also called feature extraction, which may be hardware, software, or firmware. See §**Error! Reference source not found.** ***Error! Reference source not found.*** for details. Inputs: biometric data / objects Outputs: biometric data / objects
	**X9.84** Symbol represents the matching component which may be hardware, software, or firmware. See §**Error! Reference source not found.** ***Error! Reference source not found.*** for details. Inputs: biometric data / objects Outputs: score
	**X9.84** Symbol represents the storage component, which includes a centralized data base, local storage on a work station, and removable media, such as a smart card. See §**Error! Reference source not found.** ***Error! Reference source not found.*** for details. Inputs: biometric data / objects Outputs: biometric data
	**X9.84** Symbol represents unprocessed "raw" biometric data.
	**X9.84** Symbol represents processed biometric data, inclusive of sample data, and biometric templates.

Symbols	Meaning
	**X9.84** Symbol representing a repeated function, such as a do-loop.
	**X9.84** Symbol representing the decision component which may be a stand alone process or located within the Matching or Application components. Inputs: score (see Matching) Outputs: yes / no
	**X9.84** Symbol representing an application component. Inputs: score / decision Outputs: application data

- End of File -