



A more extensive and update-to-date glossary is maintained on the bTrade website at http://www.btrade.com/resource_center/glossary/G0.asp

Algorithm (cryptographic)

A clearly specified mathematical computation process; A set of rules, which gives a prescribed result.

Alias

Another name for an object that is more easily remembered for a network or software object. Example: Your PC client name or a server directory folder.

Alphanumeric

A character set that contains both letters and digits.

ANSI

American National Standards Institute. ANSI is a private, non-profit organization responsible for the development and approval of voluntary consensus standards in the United States. ANSI approves standards developed primarily by trade, technical, professional, consumer, and labor organizations.

ANSI X12.58

An ANSI X12 security structures standard that defines data formats required for authentication and encryption to provide integrity, confidentiality, and verification of the security originator to the security recipient for the exchange of Electronic Data Interchange (EDI) data defined by Accredited Standards Committee (ASC) X12. See ANSI ASC X12.

ANSI X.509

Public key cryptography; it is the ITU-T (International Telecommunications Union-T) standard for certificates. X.509 v3 refers to certificates containing or capable of containing extensions.

AS1

(Applicability Statement 1) is the draft specification standard by which vendor applications communicate EDI data. AS2/AS1 is a specification about how to transport data, not how to validate or process data. AS2/AS1 only specifies the means to connect, deliver, validate and reply to (receipt) data in a secure, reliable, non-reputable way. The data is then dispatched to the appropriate processor based upon its content-type. AS2/AS1 makes no specification about how that dispatch or subsequent processing is accomplished. Vendors who sell AS2/AS1 compliant software will also provide the correct processing packages to support these functions. AS2/AS1 is designed to be only the means by which these processes connect and transport data



AS2

Applicability Statement 2 is the draft specification standard by which vendor applications communicate EDI (or other data such as XML) over the Internet using HTTP.

Authentication

The process of identifying an individual, usually based on a [username](#) and [password](#). In [security systems](#), authentication is distinct from [authorization](#), which is the process of giving individuals [access](#) to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

CA

Certifying Authority or Certification Authority. Secure server that signs end-user certificates and publishes revocation data. Before issuing a certificate, the CA follows published policies to verify the identity of the trading partner that submitted the certificate request. Once issued, other trading partners can trust the certificate based upon the trust placed in the CA and its published verification policy. TDManager is the CA product used with TDAccess. See certificate and TDManager.

Certificate

A public key certificate, certificates are issued by a certification authority (CA), which includes adding the CA's distinguished name, a serial number and 7 starting and ending validity dates to the original request. The CA then adds its digital signature to complete the certificate. See CA and digital signature.

Certificate request

An uncertified public key created by a trading partner as part of the Rivest Shamir Adleman (RSA) key-pair generation. The certificate request must be approved by a certification authority (CA), which issues as a certificate, before it can be used to secure data. See CA, public key, RSA, trading partner, and uncertified public key.

Cipher-text

Another name for encrypted data.

TDCommPress

bTrade, inc.'s underlying core utilities that allow you to compress, encrypt, authenticate, and assure data files for cross-platform file transfers over public and private networks.

Decryption

The process of transforming cipher-text into plaintext.

DES

Digital Encryption Standard. A standard, U.S. Government symmetric encryption algorithm, which endorsed by the U.S. military for encrypting "unclassified, yet sensitive" information. The Data Encryption Standard is a block cipher, symmetrical



algorithm (extremely fast) that uses the same private 64-bit key for encryption and decrypting. This is a 56-bit DES-CBC with an Explicit Initialization Vector (IV). Cipher Block Chaining (CBC) requires an initialization vector to start encryption. The IV is explicitly given in the IPsec packet. See block cipher, triple DES, and symmetric algorithm. digital signature. An electronic signature can be applied to any electronic document. An asymmetric encryption algorithm, such as the Rivest Shamir Adleman (RSA) algorithm, is required to produce a digital signature. The signature involves hashing the document and then encrypting the result with the sender's private key. Any trading partner can verify the signature by decrypting it with the sender's public key, re-computing the hash of the document, and comparing the two hash values for equality. See hash function, private key, public key, and RSA.

Digital Signature

A [digital](#) code that can be attached to an electronically transmitted message that uniquely identifies the sender. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be. Digital signatures are especially important for [electronic commerce](#) and are a key component of most [authentication](#) schemes. To be effective, digital signatures must be unforeseeable. There are a number of different [encryption](#) techniques to guarantee this level of security.

DISA

Data Interchange Standards Association: Secretariat for ASC X.12.

Distinguished name

A set of data that identifies a real-world entity, such as a person in a computer-based context.

ebXML

(electronic business Extensible Markup Language)

A modular suite of specifications for standardizing [XML](#) globally in order to facilitate trade between organizations regardless of size. The specification gives businesses a standard method to exchange XML-based business messages, conduct trading relationships, communicate data in common terms and define and register business processes.

EDI

Electronic Data Interchange: The inter-organizational, computer-to-computer exchange of business documentation in a standard, machine-processed format; using national or international standards. See also ANSI X12 and EDIFACT.

EDIFACT

United Nations Electronic Data Interchange for Administration, Commerce, and Transport. International standard set by the UN and administered in the U.S. by DISA. This standard has been widely implemented in western Europe.

**EDI name**

A unique identifier used by the Comm-Press2000 software and public networks for addressing and routing EDI files.

Encryption

The process of transforming plaintext into an unintelligible form (ciphertext) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decrypting process (two-way encryption).

FTP

File Transfer Protocol. A TCP-based, application-layer, Internet Standard protocol for moving data files from one computer to another.

Hub

A large company with a highly-developed EDI program that actively encourages EDI implementation and development among its vendors and other business partners.

Key (cryptographic)

A parameter that determines the transformation from plaintext to ciphertext or vice versa. For example, a Digital Encryption Standard (DES) key is a 64-bit parameter consisting of 56 key bits and 8 bits, which may be used for odd parity. See DES and odd parity.

Key generation

The trustworthy process of creating a private key/public key pair. The public key is supplied to an issuing authority during the certificate application process.

Key interval

The time period for which a cryptographic key will be active.

Key pair

A private key and its corresponding public key. The public key can verify a digital signature created by using the corresponding private key. See private key and public key.

MAC

Message Authentication Code. A cryptographically computed value that is the result of passing text or numeric data through the authentication algorithm using a specific cryptographic key. [Specific] Refers to an ANSI standard for a checksum that is computed with a keyed hash that is based on DES. The ANSI standard MAC algorithm is equivalent to cipher block chaining (CBC) with an initialization vector (IV) equal to zero.

MDN

Message Disposition Notification. Messages sent asynchronously or synchronously notifying the sender the outcome of the message whether it was processed successfully. Usually used in AS1 or AS2 communications.



Non-repudiation

Provides proof of the origin or delivery of data in order to protect the sender against a false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent.

ODBC

Open Database Connectivity is a standard or open application programming interface (API) for accessing a database. Using ODBC statements in a program, you can access files in a number of different databases, including Access, dBase, DB2, Excel, and text. In the newer distributed object architecture called Common Object Request Broker Architecture (CORBA), the Persistent Object Service (POS) is a superset of both the Call-Level Interface and ODBC.

Participant

Reference to a trading partner in the TDManager application. See trading partner.

Participant name

A program field that identifies the trading partner; normally the most commonly used name recognized for the trading partner, such as a surname, a system identification, etc.

Passphrase

A string of 64 characters used to encrypt private keys. Passphrases (passwords) are randomly generated during the key generation process. They may be stored with the private key or written to a separate file when the TDManager™ run-time files are imported.

PKI

(public key infrastructure)

A system of [digital certificates](#), [Certificate Authorities](#), and other registration authorities that verify and authenticate the validity of each party involved in an [Internet](#) transaction. PKIs are currently evolving and there is no single PKI nor even a single agreed-upon standard for setting up a PKI. However, nearly everyone agrees that reliable PKIs are necessary before [electronic commerce](#) can become widespread.

A PKI is also called a *trust hierarchy*.

Plaintext

Unencrypted data; intelligible data that can be directly acted upon without decryption.

Private key

The mathematical value of an asymmetric key pair that is not shared with trading partners. The private key works in conjunction with the public key to encrypt and decrypt data. For example, when the private key is used to encrypt data, only the public key can successfully decrypt that data. See secret-key.

**Public key**

The mathematical value of an asymmetric key pair that is shared with trading partners. The public key works in conjunction with the private key to encrypt and decrypt data. For example, when the public key is used to encrypt data, only the private key can successfully decrypt that data.

Public key encryption

Encryption that uses a key pair of mathematically related encryption keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature. This permits users to verify each other's messages without having to securely exchange secret keys.

RC2

A variable key size block cipher, designed to be a replacement for DES.

RC4

A variable-key-size stream cipher that is ten times faster than DES, according to RSA Data Security, Inc.

Receiver

The receiving trading partner, system or process that is the destination of transmitted data.

Repudiation

The denial or attempted denial by an entity involved in a communication of having participated in all or part of the communication.

RSA Public Key Cryptography

Rivest Shamir Adleman. An RSA public key (asymmetric) cryptosystem used for encryption and transmitting digital signatures. The RSA algorithm is the most commonly used encryption and authentication algorithm and is part of the Netscape and Microsoft Internet browsers.

SECFILE

An optional Comm□Press2000 program table that defines how to interpret a customer's proprietary header information in order to identify the sender, the receiver, and the data classification.

SECOFR

The primary security administrator (Security Officer) that is responsible for setting Global Security Options for the TDManager application,. See security administrators.

**Secret key**

The value used in a symmetric encryption algorithm to encrypt and decrypt data. Only the trading partners authorized to access the encrypted data must know secret keys.

Security administrators

The secondary security managers (created by the primary administrator, SECOFR) defined in the TDManager application. These users define trading partners (called participants), define trading partner relationships, and approve certificate requests. See participants, SECOFR, and trading partners.

Self-signed certificate

A Certifying Authority's (CA) certificate is signed by itself, indicating the CA is at the root of its signing chain.

Sender

The sending trading partner, system or process that is the originator of transmitted data.

Session key

A random, one-time secret key used in one session.

SSL

Secure Sockets Layer. A program layer created by Netscape for managing the security of message transmissions in a network. Netscape's idea is that the programming for keeping your messages confidential ought to be contained in a program layer between an application (such as your Web browser or HTTP) and the Internet's TCP/IP layers. The SSL upper layer provides asymmetric cryptography for server authentication (verifying the server's identity to the client) and optional client authentication (verifying the client's identity to the server), and enables them to negotiate a symmetric encryption algorithm and secret session key (to use for data confidentiality) before the application protocol transmits or receives data. A keyed hash provides data integrity service for encapsulated data.

TDAccess

TDAccess is a secure data communications bTrade, inc. product that links customer business applications and processes to different IP gateways, portals, and servers used by e-Business trading communities. TDAccess software (1) displays critical audit information on a real-time basis, (2) is distributed from bTrade, inc.'s Internet, (3) employs high-performance data transmissions, and (4) uses state-of-the-art data compression to secure session transactions via the Internet.

TDManager

A bTrade, inc. product that manages key critical functions of a business-to-business electronic commerce network for customers. These include registering trading partners, classifying data, defining security relationships among partners, and distributing client software, TDManager is used to exchange and validate certificates or generate



public/private keys for all trading partner participants. TDManager interoperates with public certificate authorities such as Entrust Technologies and Verisign, Inc.

TLS

Transport Layer Security. BTrade, inc. supports version 3 of this Netscape protocol. Secure Socket Layer Version 3.0 standard developed to provide security for web server and web browser applications. SSL has been endorsed and included in the Transport Layer Security protocol promoted with the Internet Engineering Task Force (IETF) by several major data communications technology corporations, such as IBM.

Trading community

Organizations who agree to send and receive specific EDI messages between each other.

Trading partner

A supplier, customer, service provider, or other party with whom business documents are routinely exchanged. Referred to as a participant in the TDManager application.

Transaction ID

Classification code for the data contained in an associated file. The classification is based on the X12 classifications for Transactions and Groups of Transactions.

Triple DES

A security enhancement to Digital Encryption; Standard (DES) encryption that employs three-successive single-DES block operations using two or three unique DES keys, this increases resistance to known cryptographic attacks by increasing the effective key length. See DES.

VAN

Value Added Network. The source or service that resolves the issues resulting from communicating with a number of different trading partners. They provide EDI communication skills, expertise, and equipment necessary to communicate electronically.

X12

An international standard for EDI messages, developed by the Accredited Standards Committee (ASC) for the American National Standards Institute (ANSI).

X12.58

An ANSI security structures standard that defines data formats required for authentication and encryption to provide integrity, confidentiality, and verification of the security originator to the security recipient for the exchange of Electronic Data Interchange (EDI) data defined by Accredited Standards Committee (ASC)

X12 See ANSI ASC X12.

X.509

The most widely used [standard](#) for defining [digital certificates](#). X.509 is actually an [ITU Recommendation](#), which means that has not yet been officially defined or approved. As a result, companies have implemented the standard in different ways. For example, both [Netscape](#) and [Microsoft](#) use X.509 certificates to implement [SSL](#) in their Web servers and browsers. But an X.509 Certificate generated by Netscape may not be readable by Microsoft products, and vice versa.

XML

(eXtensible Markup Language)

A specification developed by the [W3C](#). XML is a pared-down version of [SGML](#), designed especially for [Web](#) documents. It allows designers to create their own customized [tags](#), enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.