EDIINT AS1 and AS2 TRANSPORT COMMUNICATION GUIDELINES

GS1

Blue Tower
Avenue Louise 326 – Bte 10
1050 Brussels - Belgium
Tel: 32(0)2-788 78 00

DISCLAIMER

GS1 is providing these voluntary guidelines as a service to interested industries. These voluntary guidelines were developed through a consensus process of interested parties.

Although efforts have been made to assure that the guidelines are correct, reliable, and technically accurate, GS1 makes no warranty or representation, express or implied, that these guidelines are correct, will not require modification as experience and technological advances dictate, or will be suitable for any purpose or workable in any application, or otherwise. Use of the guidelines is with the understanding that GS1 has no liability for any claim to the contrary, or for any damage or loss of any kind or nature. If a user perceives a need for a change to the standard, it should contact GS1.

Users are cautioned that these are voluntary industry guidelines. Should they conflict with government laws or regulations, the legal requirements supersede the guidelines.

Table of Contents

1 OVERVIEW

This document defines the EDIINT AS1 and AS2 Transport Communication Guidelines used by companies participating in e-Commerce using the GS1 published XML, EANCOM, I/C, UCS, and VICS data format standards. This document was developed by the Electronic Commerce Global Implementation Forum (ecGIF) group within GS1. Contact information for ecGIF co-chairs: John Duker, Procter & Gamble, duker.jp(at)pg.com; Jin Chun, Agentrics jchun(at)agentrics.com

All GS1 documents are maintained by the GS1 Global Standards Management Process, which operates under the GS1 auspices. All inquires concerning GS1 should be directed to your local GS1 Member Organisation – see: http://www.gs1.org/contact/worldwide.php   or

GS1
Avenue Louise 326 – Bte 10
1050 Brussels - Belgium
Tel: 32(0)2-788 78 00

This document defines the technical communication protocols used to transport EDI and XML data from one computer to another computer. A major objective of the Communication Guidelines is general accessibility to all sizes and type of companies, with security at least as high as today's conventional mail or telephone service. It is important to note, however, that each participant in these guidelines is responsible for taking whatever steps necessary to protect the confidentiality of its data. Further, the legality of transmitted electronic messages such as EDI and XML is left to the marketplace, and to the negotiation between individual buyers and sellers.

2 INTRODUCTION

The Communication Guidelines documented in the following pages have been designed to provide a practical and standard approach to the electronic exchange of data between participants. The objectives of the GS1 Global Standards Management Process in creating the document are to:

• Provide for the communication of EDI and XML data

• Identify alternative communication methods

• Specify the communication guidelines for industry use

• Provide operational guidelines for the use of the EDIINT-AS1and EDIINT-AS2 standards

2.1 SCOPE OF CHANGES FOR THESE GUIDELINES

A previous version of this document was published in the UCS Communications Standard as the "E-Commerce Transport Communication Guidelines" standard.

3 OBJECTIVES

One goal of the GS1 Global Standards Management Process is to provide communication methodologies to enable parties to exchange information between computers. The resulting Communication Guidelines specify the means of packaging EDI and XML data, and transferring it from a sender to a receiver.

The following objectives are considered in developing the Communication Guidelines:

• The use of proven technologies which are generally available.

• Enable participation by both large and small business entities.

• Provide for implementation at a reasonable cost.

• Provide communication guidelines, which include recommended operational requirements such as network availability for incoming connections and encryption characteristics. These guidelines are defined in light of current operating environments.

• Provide data integrity and security that is equal to or better than current methods of operation.

4 COMMUNICATION CONCEPT

Message standards allow users to convert business documents into a format that can be electronically exchanged. Such EDI or XML business documents are referred to as "transaction sets", "messages", or "documents", and their format is defined in the XML, EANCOM, I/C, UCS, and VICS data format message standards. The exchange of these business documents is a component of overall e-Commerce. The Communication Guidelines provide for the exchange of EDI interchanges and XML documents, transporting them from one company to another. Throughout this document, interchanges and documents will be referred to as EDI and XML data or as text.

As e-Commerce evolves and additional solutions become available, it is important for organisations to incorporate new services into their infrastructure, while continuing to support their existing trading partnerships. It is expected that multiple communication options will be used within organisations including Internet exchange, web services, direct connections, eMarketplaces (Exchanges), and Value Added Networks (VANs). These blended models will facilitate the growth of the global trading community to meet various business requirements.

4.1 EDI SYNTAX

EANCOM message standards refer to formatted business documents as "messages". I/C, UCS and VICS message standards refer to formatted business documents as "transaction sets". Both messages and transaction sets are made up of variable length data segments. Messages [transaction sets] are bounded by a message header segment (UNH) [transaction set header segment (ST)] and a message trailer segment (UNT) [transaction set trailer segment (SE)].

Groups of similar messages [transaction sets] are combined into functional groups. Functional groups can be [are] bounded by a functional group header segment (UNG) optional in EANCOM [(GS)] and a functional group trailer segment (UNE) optional in EANCOM [(GE)].

Finally, functional groups are combined into interchanges. An interchange is bounded by an interchange control header segment (UNB) and optionally a service string advice segment (UNA) [(ISA)] and an interchange control trailer segment interchange trailer segment (UNZ) [(IEA)]. For specific details on this syntax, refer to the appropriate data format message standard.

4.2 XML SYNTAX

XML message standards refer to formatted business documents as "documents". XML documents begin with the XML "declaration" in the first line of the document. This is followed by the "root element". Elements contain XML "tags" and content. Elements may also have "attributes" which contain information about the element and are delimited by quotation marks.

XML documents must be "well formed" and they may be "valid". Well-formed documents must contain at least one element. They must have properly nested tags, and the root element must be unique. XML documents may also be checked for validity, but it is not required that they be valid. XML documents are valid if they conform to a template containing rules such as a schema or a DTD. A document that does not have a schema or a DTD is not valid. A document that has a schema or a DTD but does not conform to it is invalid. For specific details on this syntax, refer to the appropriate data format message standard.

4.3 DATA DELIVERY

Delivery of EDI and XML data using this guideline occurs between a pair of participants utilizing the public Internet. Communication is always in a single direction, with the party sending data initiating the communication. Data is deposited at the recipient's location in what may be called an EDI or XML mailbox. After a connection is established, one or more EDI interchanges or XML documents may be sent. Both EDI interchange(s) and XML document(s) are sent as a continuous stream of data, with no physical record separator or line delimiter characters embedded in the data stream.

A participant may utilize the facilities of a third party service bureau known as a Value Added Network (VAN), Exchange or e-Marketplace in lieu of a total in-house implementation. The third party becomes either the sending or receiving partner in the two-party communication. Transfer of EDI or XML data between a company and a third party acting as their agent can occur in any format mutually arranged between the company and the third party.

5 INTERNET TRANSPORT USING EDIINT-AS1 AND EDIINT-AS2

These recommended implementation guidelines provide for the secure delivery of EDI or XML data using Internet transport. They define communications methods that may be used to transfer EDI or XML data between companies. Although they were developed primarily to support direct trading partner transmissions as illustrated in Figure 1 and Figure 2, they may also be used with VANs, e-Marketplaces or Exchanges. There is a third Internet transport approach based on FTP called EDIINT-AS3. AS3 is a draft standard which has not yet reached RFC status and does not yet have widespread adoption. The AS3 draft standard will not be discussed further in this document.

5.1   INTRODUCTION

The Internet Engineering Task Force (IETF) is the body that develops and maintains standards (Internet-Standards) and draft standards (Internet-Drafts) for the Internet. Internet documents are often referred to by their Request for Comment (RFC) number. RFCs can be found at http://www.ietf.org/rfc.html. For example, RFC 2821 is the document number for the "Simple Mail Transfer Protocol (SMTP)" and RFC 2616 is the document number for the "Hypertext Transfer Protocol (HTTP)" both used for Internet transport.

Internet-Drafts are working documents of the IETF and its working groups. They are valid for a maximum of six months and may be updated, replaced, or made obsolete by other documents at any time. Internet-Drafts are "works in progress". To obtain a copy of any of the EDIINT documents referenced in the following pages, the reader may access them at http://www.ietf.org/ID.html

5.2 SPECIFICATIONS

This document defines a minimum set of parameters and options to enable companies to use Internet transport securely for the exchange of EDI or XML data. EDIINT-AS1 is based upon SMTP and EDIINT-AS2 is based on HTTP. Both standards support the full range of required security - digital signature, encryption, and digitally signed return receipts. Figures 3 through 12 illustrate the process used to sign, encrypt and decrypt the data.

The nomenclature used in the normative sections of this document (sections 5.4 and 5.5) complies with ISO rules as specified in Annex H of the ISO/IEC Directives, Part 2, 2004, 5th edition [ISODir2]:
(http://isotc.iso.org/livelink/livelink.exe/4230517/ISO_IEC_Directives__Part_2__Rules_for_the_structure_and_drafting_of_International_Standards__2004__5th_edition___pdf_format_.pdf?func=doc.Fetch&nodeid=4230517)

The guidelines are based on work published by the EDI over the Internet Working Group (EDIINT) of the IETF, and the results of vendor conformance testing. The EDIINT Working Group developed RFC 1767 titled "MIME Encapsulation of EDI Objects" which allows EDI and XML data to be sent as an Internet Message as a special application type. RFC 1767 is on a standards track within the IETF.

The IETF has published four additional documents:

1. AS1 - "MIME-based Secure Peer-to-Peer Business Data Interchange Over the Internet"

   (http://www.ietf.org/rfc/rfc3335.txt)

2. AS2 - "MIME-based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)".

   (http://www.ietf.org/rfc/rfc4130.txt)

3. "Compressed Data for EDIINT"

   (http://www.ietf.org/internet-drafts/draft-ietf-ediint-compression-05.txt

4. "Certificate Exchange Message (CEM) for EDIINT"

   (https://datatracker.ietf.org/public/idindex.cgi?command=id_detail&id=12703)

These documents and successor documents (published with incremented version numbers) are the basis for these Guidelines. We shall refer to the current specification documents in the following pages as "AS1" and "AS2".

Currently, the Internet-Standards and Internet-Drafts referenced in AS1 and AS2 to achieve the minimum requirements of the AS1 and AS2 Standards are as follows:

RFC 1123	Requirements for Internet Hosts
RFC 1767	MIME Encapsulation of EDI Objects
RFC 1847	Security Multiparts for MIME

RFC 2045   MIME Format of Internet Message Bodies
RFC 2046   MIME Media Types
RFC 2049   MIME Conformance Criteria and Examples
RFC 2298   An Extensible Message Format for Message Disposition Notifications
RFC 2616   Hypertext Transfer Protocol -- HTTP/1.1
RFC 2821   Simple Mail Transfer Protocol (SMTP)
RFC 2822   Standard for the Format of Internet Text Messages
RFC 3370   Cryptographic Message Syntax (CMS) Algorithms
RFC 3798   Message Disposition Notification
RFC 3851   S/MIME Version 3.1 Message Specification
RFC 3852   Cryptographic Message Syntax

5.3   CONFORMANCE VALIDATION

To ensure that different software vendors' products meet the AS1 and AS2 standards, and that the products interoperate successfully with each other, GS1 has sponsored several vendor conformance validation tests. The Drummond Group Inc., an interoperability conformance consultancy, conducts the conformance testing. The results of these tests are documented as follows:

For AS1: http://www.drummondgroup.com/html-v2/as1-companies.html

For AS2: http://www.drummondgroup.com/html-v2/as2-companies.html

5.4   REQUIREMENTS

The following are minimum GS1 requirements for secure Internet transport. Business conditions may dictate higher levels of security for certain business documents or processes. Subsequent sections will list recommended practices. Requirements and recommendations apply equally to AS1 and AS2 unless otherwise noted.

Organisations that adopt these Guidelines may decide to use functionality beyond the minimum requirements as long as:

- The functionality is defined in AS1 and/or AS2, and
- both parties mutually agree to use the extended functionality

Encryption and Signature Requirements

Requirement 1

> Payload data SHALL be encrypted and digitally signed using the S/MIME specification (see RFC 3851).

Requirement 2

> The length of the one-time session (symmetric) key SHALL be 128 bits or greater.[1]

---

[1] Key lengths less than 128 bits are no longer considered secure. Triple DES, which uses 3 separate 56 bit keys to encrypt the data three times, is the recommended encryption algorithm. A newer algorithm called Advanced Encryption Standard (AES), while not currently used for EDIINT encryption, was developed under the National Institute of Standards and Technology leadership and supports key sizes of 128, 192, and 256 bits. AES is used by the US government and it is expected that it will be widely used by business applications in the future.

Requirement 3

The length of the Public/Private Encryption key SHALL be 1024 bits or greater.[2]

Requirement 4

The length of the Public/Private Signature key SHALL be 1024 bits or greater.

Requirement 5

The Signature Hash algorithm used SHALL be SHA1.[3]

Configuration Requirement

Requirement 6

Digitally signed receipts (Signed Message Disposition Notifications [MDNs][4]) SHALL be requested by the Sender of Message (see Glossary).

5.5 RECOMMENDATIONS

Recommendation 1 – MDN Request Option

Either Asynchronous or Synchronous MDNs MAY be used with EDIINT AS2[5]. There are potential issues with both synchronous and asynchronous MDNs, and Trading Partners need to jointly determine which option is best based on their operational environments and message characteristics. A discussion of both options follows these recommendations.

Recommendation 2 – MDN Delivery

Recipients SHOULD transmit the MDN as soon as technically possible to ensure that the message sender recognizes that the message has been received and processed by the receiving EDIINT software in a timely fashion. This applies equally to AS1 and AS2 as well as Asynchronous and Synchronous MDN requests.

Recommendation 3 – Delivery Resend with Asynchronous MDNs Requested

When a message has been successfully sent, but an asynchronous MDN has not been received in a timely manner, the Sender of Message SHOULD wait a configurable amount of time and then automatically resend the original message. A delivery resend of a message SHALL have the same content and the same Message-ID value as the initial message. The period of time to wait for a MDN and then automatically resend the original message is based on business and technical needs, but generally SHOULD not be less than one hour. There SHOULD be no more than two automatic resends of a message before personally contacting a technical support contact at the Receiver of Message site. This applies equally to AS1 and AS2.

There may be export or import restrictions affecting use of encryption technologies in a few countries. See http://www.bis.doc.gov/Encryption/Default.htm

[2] Key length options for public/private keys are: 512, 1024, or 2048 bits.

[3] SHA1 is considered a significantly stronger algorithm for creating document digests used for digital signatures than the MD5 algorithm.

[4] MDNs provide a guarantee to the sender that the message has been received and the recipient has signed an acknowledgment

[5] For EDIINT AS1, MDNs are always asynchronous, since SMTP (email) does not support bi-directional transmission.

Recommendation 4 – Delivery Retry for AS2

Delivery retry SHOULD take place when any HTTP response other than "200 OK" is received (for example, 401, 500, 502, 503, timeout, etc). This occurrence indicates that the actual transfer of data was not successful. A delivery retry of a message SHALL have the same content and the same Message-ID value as the initial message. Retries SHOULD occur on a configurable schedule. Retrying SHALL cease when a message is successfully sent (which is indicated by receiving a HTTP 200 range status code), or SHOULD cease when a retry limit is exceeded.

Recommendation 5 – Message Resubmission

If neither automated Delivery Retry nor automated Delivery Resend are successful, the Sender of Message MAY elect to resubmit the payload data in a new message at a later time. The Receiver of Message MAY also request message resubmission if a message was lost subsequent to a successful receive. If the message is resubmitted a new Message-ID MUST be used. Resubmission is normally a manual compensation.

Recommendation 6 – HTTP vs. HTTP/S (SSL)

For EDIINT AS2, the transport protocol HTTP SHOULD be used. However, if there is a need to secure the AS2-To and the AS2-From addresses and other AS2 header information, HTTPS[6] MAY be used in addition to the payload encryption provided by AS2. The encryption provided by HTTPS secures only the point to point communications channel directly between the client and the server.

Recommendation 7 – AS2 Header

For EDIINT AS2, the values used in the AS2-From and AS2-To fields in the header SHOULD be GS1 Global Location Numbers (GLNs)[7].

Recommendation 8 - SMTP

For EDIINT AS1, a dedicated SMTP server, separate from the normal email server SHOULD be used to ensure operational reliability.

Recommendation 9 - Compression

EDIINT compression MAY be used as an option, especially if message sizes are larger than 1MB. Although current versions of EDIINT software handle compression automatically, this SHOULD be bilaterally agreed between the sender and the receiver[8].

Recommendation 10 – Digital Certificate Characteristics

Digital certificates MAY either be from a trusted third party or self signed if bilaterally agreed between trading partners. If certificates from a third party are used, the trust level SHOULD be at a minimum what is termed 'Class 2' which ensures that validation of the individual and the organisation has been done.

---

[6] HTTPS might introduce operational complexities.

[7] The GLNs SHOULD be that of the sending server and receiving server respectively. When a hub or VAN is used, the GLN of the trading partner MAY be used when the AS2-To field is used for routing. Existing AS2 installations using values other than GLNs would need to reconfigure their software and coordinate with all of their trading partners prior to converting to the use of GLNs.

[8] If used, compression SHOULD comply with the IETF document "Compressed Data for EDIINT" http://www.ietf.org/internet-drafts/draft-ietf-ediint-compression-05.txt

<u>Recommendation 11 – Common Digital Certificate for Encryption & Signature</u>

A single digital certificate MAY be used for both encryption and signatures, however if business processes dictate, two separate certificates MAY be used. Although current versions of EDIINT software handle two certificates automatically, this SHOULD be bilaterally agreed between the sender and the receiver.

<u>Recommendation 12 – Digital Certificate Validity Period</u>

The minimum validity period for a certificate SHOULD be 1 year. The maximum validity period SHOULD be 5 years.

<u>Recommendation 13 – Digital Certificate – Automated Exchange</u>

The method for certificate exchange SHALL be bilaterally agreed upon. When the *Certificate Exchange Messaging for EDIINT* specification[9] is widely implemented by software vendors, its use will be strongly recommended. This IETF specification will enable automated certificate exchange once the initial trust relationship is established, and will significantly reduce the operational burden of manually exchanging certificates prior to their expiration.

<u>Recommendation 14 – HTTP and HTTP/S Port Numbers for AS2</u>

Receiving AS2 messages on a single port (for each protocol) significantly minimizes operational complexities such as firewall set-up and potential security exposures for both the sending and receiving partner. Ideally, all AS2 partners would receive messages using the same port number. However some AS2 partners have previously standardized to use a different port number than others and changing to a new port number would add costs without commensurate benefits.

Therefore AS2 partners MAY standardize on the use of port 4080 to receive HTTP messages and the use of port 5443 to receive HTTP/S (SSL) messages.

<u>Recommendation 15 – Duplicate AS2 Messages</u>

AS2 software implementations SHOULD use the 'AS2 Message-ID' value to detect duplicate messages and avoid sending the payload from the duplicate message to internal business applications. The Receiver of Message SHALL return an appropriate MDN even when a message is detected as a duplicate. Note: The Internet Engineering Task Force (IETF) is developing an *Operational Reliability for EDIINT AS2* specification[10] which defines procedures to avoid duplicates and ensure reliability.

<u>Recommendation 16 – Technical Support</u>

There SHOULD be a technical support contact for each Sender of Message and Receiver of Message. The contact information SHOULD include name, email address and phone number. For 24x7x365 operation, a pager or help desk information SHOULD be also provided.

5.6   SYNCHRONOUS vs. ASYNCHRONOUS MDNs

When requesting Message Disposition Notifications (MDNs), two different modes of AS2 behaviour are available. In asynchronous mode, the MDN is sent over a different TCP connection

---

[9] See IETF document https://datatracker.ietf.org/public/idindex.cgi?command=id_detail&id=12703

[10] See IETF document https://datatracker.ietf.org/public/idindex.cgi?command=id_detail&id=13578

than was used by the initial message. In synchronous mode, the MDN is sent using the HTTP(s) response over the existing TCP connection used by the initial message.

In principle, AS2 applications support either mode of operation, and it is a matter of agreement within the business relationship which mode of operation will be used. However, because usage characteristics and resource capacities can impact the modes of operation differently, the agreement should take into account a number of factors.

A chart of "Pros" and "Cons" pertaining to MDN mode for AS2 messages follows. This chart assumes that both partners (at different times) are initiating messages to be sent and will therefore also have infrastructure to receive messages.

Synchronous Mode MDN

Pro

- Fewer TCP connections are made in fewer directions.
- One partner can send data without having to listen on any port.
- Easier to track state of the protocol in that state does not have to be preserved between TCP connections. However, the protocol state must be persisted during application failure.

Con

- For large messages or heavily loaded servers, resources on both sides are tied up holding the connection open until the MDN is sent. Since significant processing may be needed to decrypt a message prior to the creation of a MDN, synchronous MDNs can result in transmission failures due to HTTP timeouts. High resource utilization levels tend to favour higher exception levels and overall higher system error rates.
- When the MDN response takes a long time to produce, an inactivity timer may close down the connection. [This timer may be in a network device or in the AS2 application.] Retries may just put the server under additional load, and not improve the delivery result.
- If the receiving AS2 application fails while waiting to send an MDN, and that protocol state is not persisted, the Sender of Message will not receive the MDN and may need to initiate a resend of the message.
- The use of proxy servers may preclude using synchronous MDNs.

Asynchronous Mode MDN

Pro

- Receiving the message is decoupled from processing the message and returning the MDN. As a result, HTTP sessions are freed as soon as the message is delivered (indicated by HTTP "200 OK" response code). This can alleviate connection time-out issues, especially for large messages or heavily loaded servers
- Potentially fewer concurrent TCP sessions due to shorter latency period, thus reducing memory and other requirements
- Message processing tasks (decryption and signature validation) and MDN generation can be undertaken after peak loads level off. [Asynchronous mode has a "checkpoint" between delivery and MDN creation.]

Con

- The state of the expected MDN must be tracked so that the arriving MDN is correlated correctly with previously sent AS2 message.
- More resources are required to create separate HTTP connections to return MDNs. For SSL, more SSL setup work will be required.
- Asynchronous mode may lead to duplicate messages being resent if MDN fails to arrive "quickly enough" and if application has resending logic active.

5.7   NETWORK AVAILABILITY

Except for scheduled maintenance, it is recommended that companies be capable of receiving EDI or XML data from their trading partners twenty-four hours a day, seven days a week. It is recognized that maintenance time can result in system outages, so maintenance time should be scheduled in advance, on a consistent basis, and communicated to trading partners. Notification to trading partners of planned outages should reduce the occurrence of alerts and errors when attempting to send to a system that is down.

5.8   IMPLEMENTATION CONSIDERATIONS

5.8.1   EDIINT-AS1 & EDIINT-AS2 FUNCTIONALITY COMPARED

Supported Functionality	EDIINT-AS1 [SMTP]	EDIINT-AS2 [HTTP(S)]
Privacy	X	X
Authentication	X	X
Integrity	X	X
Non-repudiation of Receipt	X	X
EDI Data Format	X	X
XML Data Format	X[11]	X
Transmit Large files without fragmenting (some SMTP servers automatically fragment large files into multiple partial messages)		X
Synchronous Transmission (no intermediate servers nor potential delays)		X
No special firewall rules needed	X	
Dial-up Internet connection	X[12]	

5.8.2   INTERNET FACILITIES

Companies are advised to ensure that their Internet Service Provider, as well as their internal infrastructure, strictly conform to all Internet-Standards and Internet-Drafts incorporated by reference into the AS1 and AS2 Standards.

In order to keep non-compliance issues to a minimum, it is recommended that companies implementing this Guideline initially test with companies already exchanging EDI or XML data using EDIINT transport as defined in these Guidelines.

Companies should evaluate their Internet Service Provider (ISP) in terms of availability, reliability, and responsiveness. Companies need to review or determine:

- The type of network redundancy the ISP maintains

- The physical connection of the ISP to the Internet Backbone

---

[11] While XML is not technically a part of the AS1 specification and has not yet been tested for interoperability, most AS1 software products support transporting the XML data format.

[12] It is expected that the receiving partner will create and send an MDN receipt immediately upon completion of processing of the inbound data by the EDIINT Server.

- If the ISP owns their own infrastructure
- The Service Level Agreements of the ISP
- Any size or volume restrictions imposed by the ISP

5.8.3 INTERNAL FACILITIES

When implementing these Guidelines, companies may also need to consider:

- What is the physical connection between the company and the ISP
- Is there single point of failure anywhere and will this impact "mission-critical" data
- Internal restrictions or non-standard behaviour with Firewall, SMTP server, Network Address Translation (NAT), Gateway, Tunnel, or Proxy server components
- Trading partners' restrictions or non-standard behaviour with Firewall, NAT, Gateway, Tunnel, or Proxy server components
- Production status of both SMTP Server (for AS1) and separate HTTP Server, if used, (for AS2). Support must be available 24x7x365 to ensure that e-Commerce transactions are not delayed.

5.8.4 SIGNED RECEIPTS

For both EDI and XML data, signed Message Disposition Notification (MDN) receipts at the communications level are required. The MDNs are created by the EDIINT Server. MDNs are different from, and do not replace, EDI Functional Acknowledgments (CONTRL messages and 997 transaction sets) which are created at the translator level. It is expected that the receiving partner will create and send an MDN receipt immediately upon completion of processing of the inbound data by the EDIINT Server.

5.8.5 CERTIFICATES

The specifications on which these Guidelines are based define a standard-based method to automatically exchange and synchronize certificates (public/private keys) – see Recommendation 13. However, until this standards-based method to exchange certificates is widely implemented by software vendors, Companies may need to manually exchange certificates (either self-signed or from a trusted Certificate Authority) with each of their trading partners.

In order to minimize the frequency with which certificates must be changed, companies may need to consider using the longest encryption key length that their partners can process beyond the minimum required by these Guidelines. Public/Private encryption and Signature key lengths can range from 512 to 2048 bits. One-time Symmetric encryption key lengths can range from 40 to 256 bits. (See Requirements 2-4.) Key length is directly related to the time that it takes to break a key and successfully decrypt a message. Other important factors for companies to consider are the monetary value of the EDI or XML transactions themselves, and their life span within the context of the industry.

5.8.6   SUPPORT SERVICES

Each company that implements these Guidelines must provide its own support services. These include setting up and testing with new partners, logging and reporting on communications activity, and the diagnosis, tracing, and resolution of end to end communications problems. Value-added networks may currently provide these support services.

The use of Internet transport for EDI or XML may complement existing Internet infrastructures. Each company must analyze the costs and benefits of this technology.

5.8.7   POINT TO POINT

These Guidelines use encryption facilities within the communications protocol for security. As a result, these Guidelines were developed under the assumption that EDI or XML data moves from point to point in such a manner that no intermediate party needs access to the contents of the EDI or XML data itself. If an intermediate party needs to view the data for rerouting to an ultimate recipient, or perform value added processing, that intermediate party will need to decrypt and potentially re-encrypt the data.

6 GLOSSARY

AS1	Applicability Statement 1 – An Internet Request For Comment (RFC) defining how applications can securely transport EDI and XML over the Internet using SMTP. It specifies how to transport data files.
AS2	Applicability Statement 2 – An Internet RFC defining how applications can securely transport EDI and XML over the Internet using HTTP. It specifies how to transport data files.
Authentication	Ensures the accurate identification of both the sender and the receiver. Is accomplished via digital signatures.
Ciphertext	Data that has been transformed from a 'plaintext' form into encrypted text (an unreadable form) via an encryption process.
Digital Certificate	A document that contains name, serial number, expiration dates & a copy of the owner's public key; used to encrypt data & validate signatures.
Digital Signature	An electronic signature that can be used to authenticate the identity of the sender of a message, and via the encrypted document digest, to ensure that the original content of the data that has been sent is unchanged.
Document Digest	A unique "fingerprint" summary (128 or 160 bits long) of an input file. It is used to create a digital signature and to ensure that the file has not been altered. It is also called a 'hash' and is produced by a checksum program that processes a file.
DTD	Data Type Definition – For an XML document, the DTD consists of mark-up code that indicates the grammar rules for the particular class of document. It specifies the valid syntax, structure, and format for defining the XML mark-up elements. GS1 recommends the use of schemas versus DTDs.
EANCOM	The EDI standard made available by GS1, which is an implementation guideline of the EDIFACT standard developed under the auspices of the United Nations.
EDI	Electronic Data Interchange – The exchange of structured business data computer to computer. EDI data format standards are developed by the EDIFACT Working Group of the United Nations and the Accredited Standards Committee (ASC) X12 of the American National Standards Institute.
EDIINT	EDI Over the Internet Working Group – A working group of the IETF that developed the AS1 and AS2 standards.
Encryption	A process that uses a mathematical algorithm and a key to transform data into an unreadable format (called ciphertext). A receiver can then use a key to restore the data to its original content.

GS1	GS1 is a leading global organisation dedicated to the design and implementation of global standards and solutions to improve the efficiency and visibility of supply and demand chains globally and across sectors.
GS1 US	The GS1 Member Organisation for the United States.
HTTP	Hypertext Transport Protocol - The HyperText Transfer Protocol (HTTP) is the de facto standard for transferring World Wide Web documents.
I/C	Industrial Commercial EDI - Denotes industry conventions and guidelines for companies dealing with Maintenance, Repair, Operations (MRO), Raw Materials and Packaging materials as issued by the GS1 US.
IETF	Internet Engineering Task Force - The Internet Engineering Task Force is a large, open, international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
Integrity	Ensures that data is not tampered with nor corrupted in transit. Is accomplished via document digests and digital signatures.
ISP	Internet Service Provider - A company that provides end users (individuals and companies) access to the Internet.
MDN	Message Disposition Notification – A document, typically digitally signed, acknowledging receipt of data from the sender.
Message	An Internet message consists of header fields (collectively called "the header of the message") followed by a body. The header is a sequence of lines of characters with special syntax. The body is a sequence of characters that follows the header and is separated from the header. See RFC 2822
Message-ID	Message Identifier - A globally unique identifier for a message. The sending implementation must guarantee that the Message-ID is unique. See RFC 2822.
MIME	Multipurpose Internet Mail Extension - MIME is a specification for enhancing the capabilities of standard Internet electronic mail. It offers a simple standardized way to represent and encode a wide variety of media types for transmission via the Internet.
Non-repudiation of Receipt	Confirms that the intended party received the data. Is accomplished via digital signatures and signed MDNs.
Payload	The body of the message that contains a business document(s) and is protected by encryption and a digital signature.
Privacy	Ensures that only the intended receiver can view the data. Is accomplished via a combination of encryption algorithms and message packaging.
Private Key	A value known only to the owner, used to create a signature and decrypt data encrypted by its corresponding public key.

Public Key	A value, known by everyone to whom the certificate has been distributed, used to encrypt data and validate a digital signature. Although mathematically related to the private key, it is astronomically difficult to derive from the public key.
Receiver of Message	The EDIINT application and/or site which receives the Message containing the business payload. The Receiver of Message sends a MDN back to the Sender of Message.
Retry	When attempting to send an AS2 message, the Sender of Message can encounter transient exceptions that result in a failure to obtain a HTTP status code or a transient HTTP error such as 503. "**Retry**" is the term used in this document to refer to an additional send attempt (HTTP POST) of the same message, with the same content and with the same Message-ID value. A Retry can occur whether the **Sender of Message** requests a Synchronous or Asynchronous MDN.
Resend	When a MDN response is not received in a timely manner, the Sender of Message may choose to resend the original message. **Resend** only applies when the **Sender of Message** requests an Asynchronous MDN. Because the message has already been sent, but has presumably not been processed according to expectation, the same message, with the same content and the same Message-ID value is sent again. This operation is referred to as a "**resend"** of the message. Resending ends when the MDN is received or the resend count is reached.
Resubmit	Neither Resending nor Retrying continue forever, but the data may still need to be exchanged at a later time, so a message may need to be resubmitted. When data that failed to be exchanged or was exchanged but later lost is resubmitted in a new message (with a new Message-ID value), it is called resubmission. Resubmission is normally a manual compensation.
Schema	A document definition, similar to a DTD but using special XML vocabulary named XML-Data. Schemas have significantly more functionality than DTDs.
Sender of Message	The EDIINT application and/or site which transmits the Message containing the business payload to the "Receiver of Message "
S/MIME	Secure MIME - S/MIME (Secure/Multipurpose Internet Mail Extensions) provides a consistent way to send and receive secure MIME data. Based on the popular Internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption).
SMTP	Simple Mail Transport Protocol - An Internet standard for transporting e-mail.
Symmetric Key	A single secret numerical key used to encrypt or decrypt a file, known only by the sender and receiver.
UCS	Uniform Communications Standard, as issued by GS1 US.

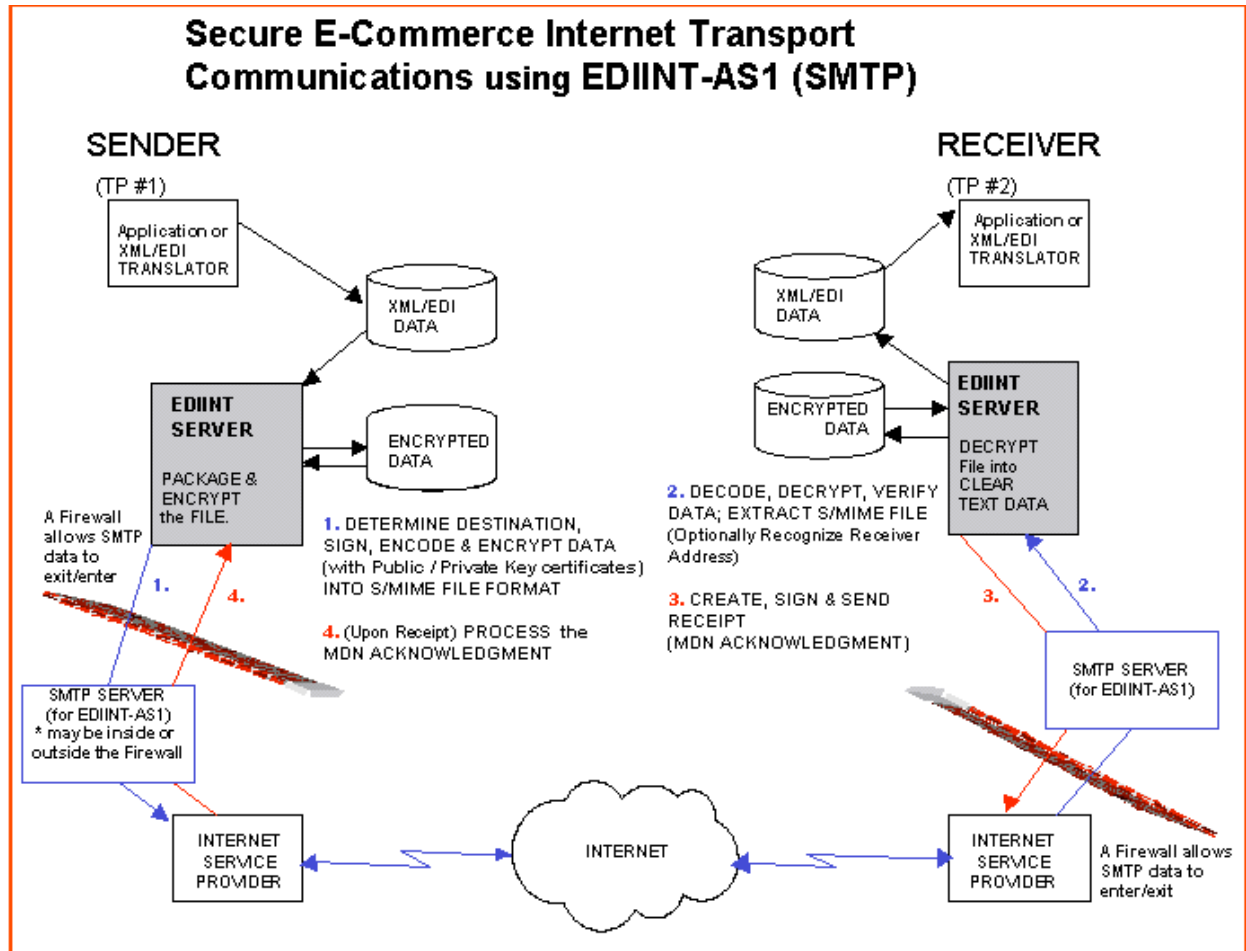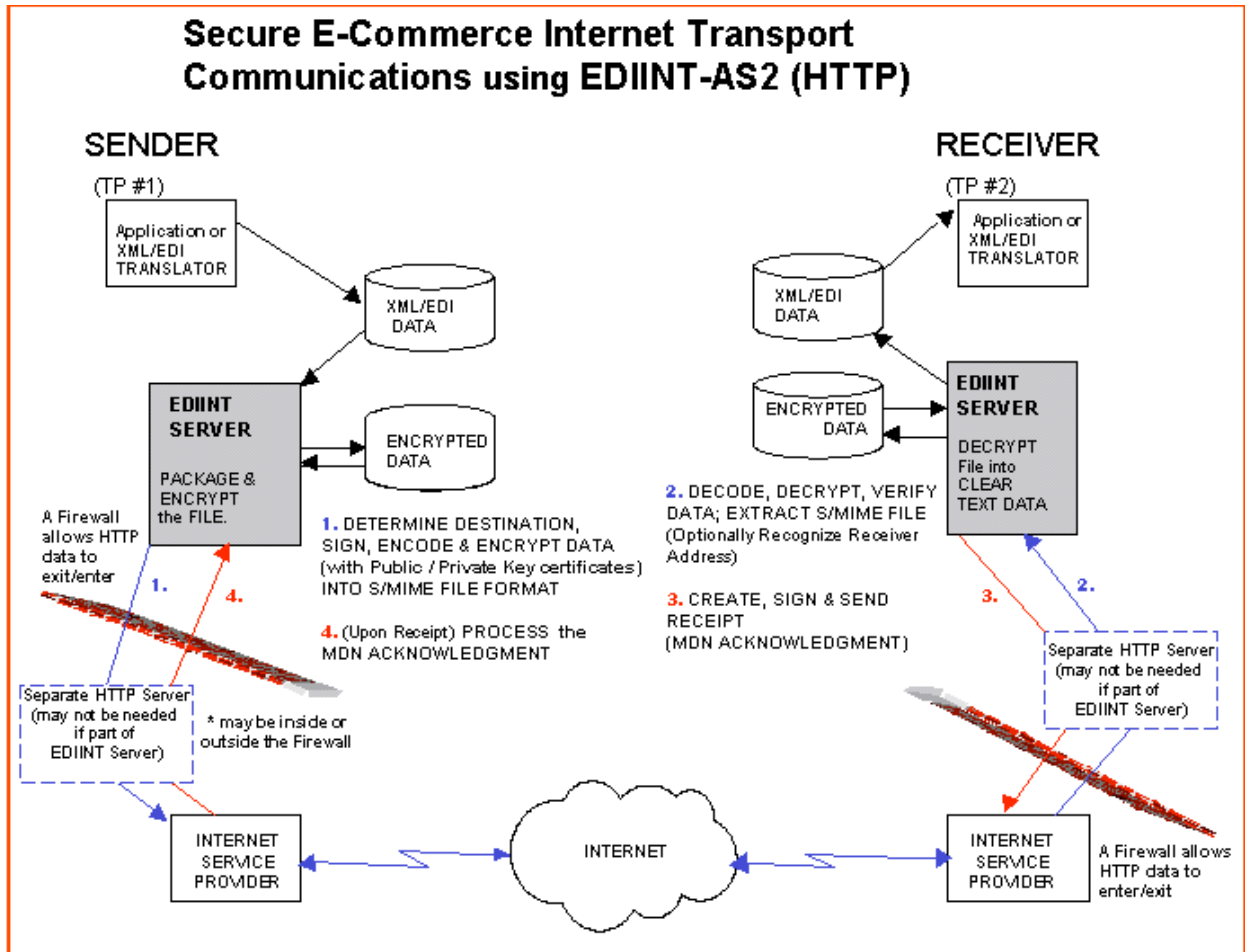| **UN/EDIFACT**	United Nations / Electronic Data Interchange for Administration, Commerce and Transport
VAN	Value Added Network
VICS	Voluntary Inter-Industry Commerce Standards – Denotes retail industry conventions and guidelines for Electronic Data Interchange as issued by the GS1 US.
XML	Extensible Mark-up Language

7 FIGURES

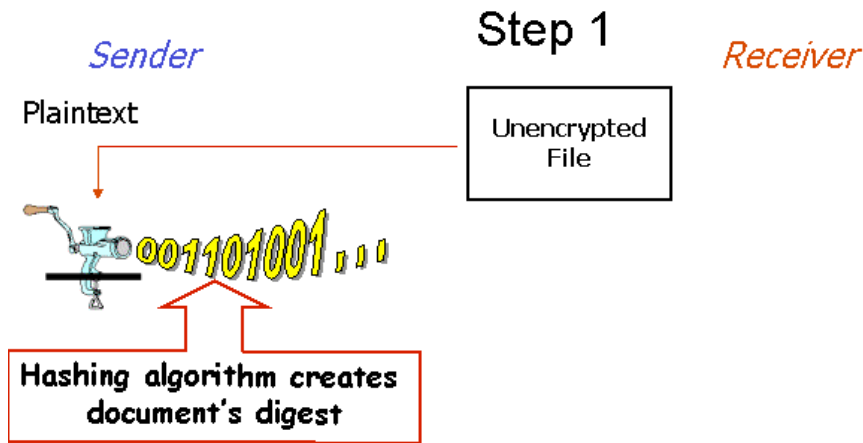Figure 1

Figure 2

EDIINT Public/Private Key Security Processing
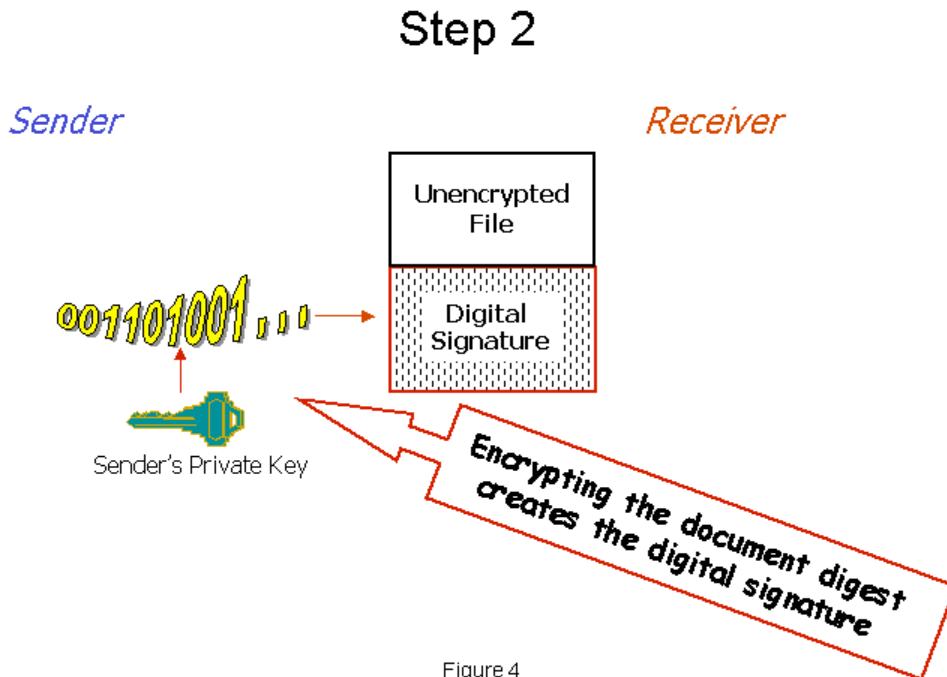## Step 1

Sender

Plaintext

Unencrypted File

00110100 1 , , ,

Hashing algorithm creates document's digest

Receiver

Figure 3

Step 2

Sender

Unencrypted File

00110100 1 , , ,

Sender's Private Key

Digital Signature

Encrypting the document digest creates the digital signature

Receiver

Figure 4

Step 3

Sender   Ciphertext   Receiver

One-time
Symmetric Key

Encrypted
File

Encrypted
Digital
Signature

Create a one-time use
symmetric key to encrypt the
file and the digital signature

Figure 5

Step 4

Sender   Digital Envelope   Receiver

One-time
Symmetric Key

Encrypt
the
one-time
symmetric
key

Receiver's Public Key

Encrypted
One-time Key

Encrypted
File

Encrypted
Digital
Signature

Encrypted
Document
Ready for
Transmission

Figure 6

Step 5

Sender

Digital Envelope

Receiver

Encrypted One-time Key

One-time Symmetric Key

Encrypted File

Encrypted Digital Signature

Decrypt the One-time Key

Receiver's Private Key

Figure 7

Step 6

Sender

Ciphertext

Receiver

Encrypted File

One-time Symmetric Key

Plaintext

Encrypted Digital Signature

Decrypt the file and the digital signature with the one-time symmetric key
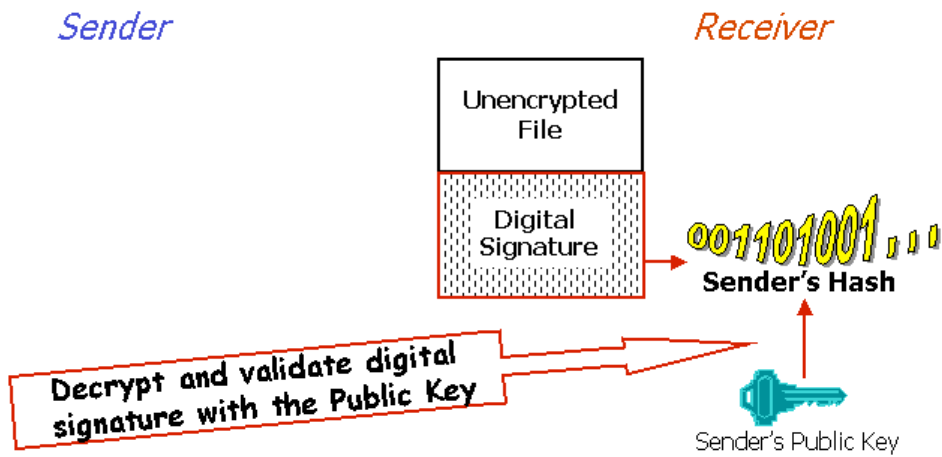
Figure 8

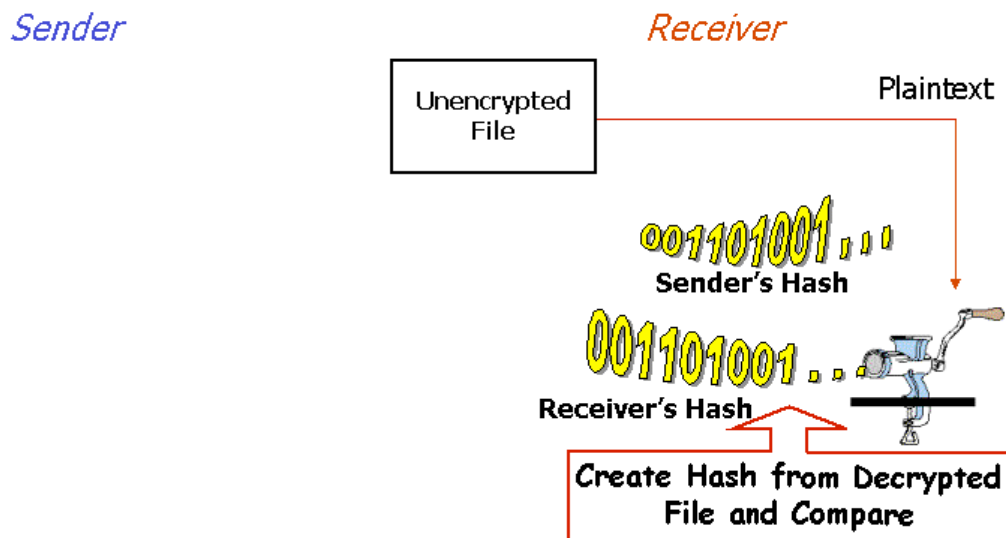## Step 7

Figure 9

Step 8

Figure 10

EDIINT Public/Private Key Security
Summary
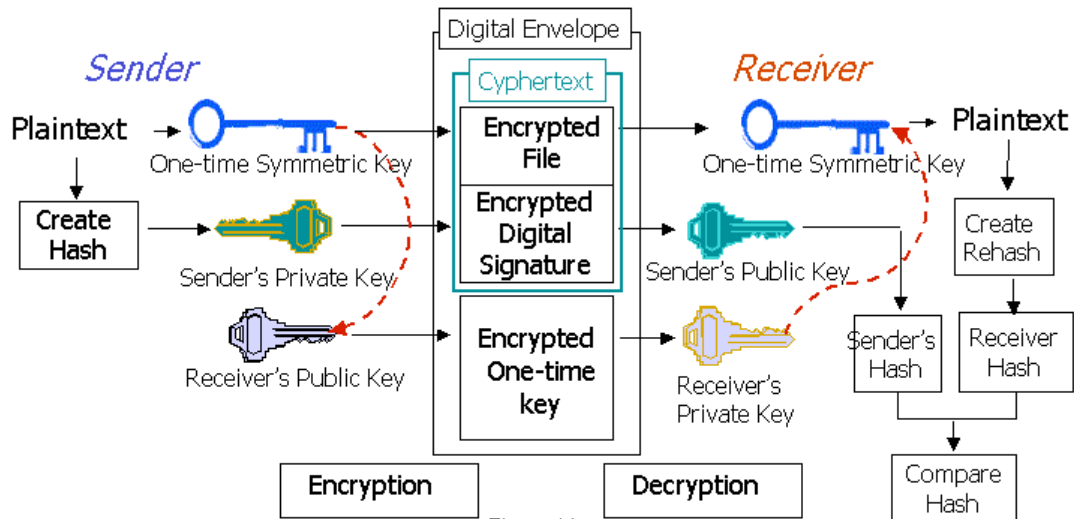
Figure 11

To Do This	Whose Key is used	What is Actually Encrypted/Decrypted with This Key
Create a signature to be sent	Sender's Private key	A Document Digest hash of the data
Encrypt the data to be sent	Sender's one-time use Symmetric key	The payload data file and the signature
Encrypt the Symmetric key (it is separately encrypted & sent with the data)	Receiver's Public key (accessed via receiver's certificate previously exchanged)	A one-time use Symmetric key
Receive & decrypt the Symmetric key sent with the data	Receiver's Private key	A one-time use Symmetric key
Decrypt the received data	Sender's one-time use Symmetric key	The payload data file and the signature
Decrypt & validate the signature (thus authenticating the sender)	Sender's Public key (accessed via sender's certificate previously exchanged)	A Document Digest hash

Figure 12