

1

7/15/2005

2

3

EDIINT AS1 and AS2

4

COMMUNICATION

5

GUIDELINES

6

7

GS1



8

Blue Tower

9

Avenue Louise 326 – Bte 10

10

1050 Brussels - Belgium

11

Tel: 32(0)2-788 78 00

12 **DISCLAIMER**

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

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

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

27

28 Copyright © 2005 GS1.

29 All Rights Reserved.

30

30 Table of Contents

31	1 OVERVIEW.....	2
32	2 INTRODUCTION	2
33	2.1 SCOPE OF CHANGES FOR THESE GUIDELINES	2
34	3 OBJECTIVES.....	2
35	4 COMMUNICATION CONCEPT	3
36	4.1 EDI SYNTAX	3
37	4.2 XML SYNTAX.....	3
38	4.3 DATA DELIVERY	4
39	5 INTERNET TRANSPORT USING EDIINT-AS1 AND EDIINT-AS2.....	4
40	5.1 INTRODUCTION	4
41	5.2. SPECIFICATIONS.....	5
42	5.3. CONFORMANCE VALIDATION.....	6
43	5.4. REQUIREMENTS.....	6
44	5.5. RECOMMENDATIONS	7
45	5.6. NETWORK AVAILABILITY.....	8
46	5.7. IMPLEMENTATION CONSIDERATIONS	8
47	6 GLOSSARY	12
48	7 FIGURES	15
49	Figure 1. EDIINT-AS1.....	13
50	Figure 2. EDIINT-AS2	14
51	Figures 3 – 12 EDIINT Public/Private Key Security Processing	15
52		

53 1 OVERVIEW

54 This document defines the EDIINT AS1 and AS2 Transport Communication Guidelines used by
55 companies participating in e-Commerce using the GS1 published XML, EANCOM, I/C, UCS, and VICS
56 data format standards.

57 All GS1 documents are maintained by the GS1 Global Standards Management Process, which operates
58 under the GS1 auspices. All inquires concerning GS1 should be directed to your local GS1 Member
59 Organization – see: <http://www.gs1.org/index.php?http://www.gs1.org/members.html&2> or

60

61 GS1
62 Avenue Louise 326 – Bte 10
63 1050 Brussels - Belgium
64 **Tel:** 32(0)2-788 78 00

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

72 2 INTRODUCTION

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

- 76 • Provide for the communication of EDI and XML data
- 77 • Identify alternative communication methods
- 78 • Specify the communication guidelines for industry use
- 79 • Provide operational guidelines for the use of the EDIINT-AS1 and EDIINT-AS2 standards

80 2.1 SCOPE OF CHANGES FOR THESE GUIDELINES

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

83 3 OBJECTIVES

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

- 87 The following objectives are considered in developing the Communication Guidelines:
- 88 • The use of proven technologies which are generally available.
 - 89 • Enable participation by both large and small business entities.
 - 90 • Provide for implementation at a reasonable cost.
 - 91 • Provide communication guidelines, which include recommended operational requirements such as
92 network availability for incoming connections and encryption characteristics. These guidelines are
93 defined in light of current operating environments.
 - 94 • Provide data integrity and security that is equal to or better than current methods of operation.

95 **4 COMMUNICATION CONCEPT**

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

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

109 **4.1 EDI SYNTAX**

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

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

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

122 **4.2 XML SYNTAX**

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

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

133 **4.3 DATA DELIVERY**

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

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

145 **5 INTERNET TRANSPORT USING EDIINT-AS1 AND** 146 **EDIINT-AS2**

147

148 These recommended implementation guidelines provide for the secure delivery of EDI or XML data using
149 Internet transport. They define communications methods that may be used to transfer EDI or XML data
150 between companies. Although they were developed primarily to support direct trading partner
151 transmissions as illustrated in Figure 1 and Figure 2, they may also be used with VANs, e-Marketplaces
152 or Exchanges.

153 **5.1 INTRODUCTION**

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

160 Internet-Drafts are working documents of the IETF and its working groups. They are valid for a
161 maximum of six months and may be updated, replaced, or made obsolete by other documents at
162 any time. Internet-Drafts are “works in progress”. To obtain a copy of any of the EDIINT
163 documents referenced in the following pages, the reader may access them at
164 <http://www.ietf.org/html.charters/ediint-charter.html>

165 5.2. SPECIFICATIONS

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

171 The guidelines are based on work published by the EDI over the Internet Working Group
172 (EDIINT) of the IETF, and the results of vendor conformance testing. The EDIINT Working Group
173 (<http://www.ietf.org/html.charters/ediint-charter.html>) developed RFC 1767 titled "MIME
174 Encapsulation of EDI Objects" which allows EDI and XML data to be sent as an Internet Message
175 as a special application type. RFC 1767 is on a standards track within the IETF.

176 The IETF has published four additional documents:

177

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

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

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

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

183 3. "Compressed Data for EDIINT"

184 (<http://www.ietf.org/internet-drafts/draft-ietf-ediint-compression-04.txt>

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

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

187

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

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

193

194	RFC 1123	Requirements for Internet Hosts
195	RFC 2045	MIME Format of Internet Message Bodies
196	RFC 2046	MIME Media Types
197	RFC 2049	MIME Conformance Criteria and Examples
198	RFC 1767	MIME Encapsulation of EDI Objects
199	RFC 1847	Security Multiparts for MIME
200	RFC 2298	An Extensible Message Format for Message Disposition Notifications
201	RFC 2311	S/MIME Version 2 Message Specification
202	RFC 2312	S/MIME Version 2 Certificate Handling
203	RFC 2616	Hypertext Transfer Protocol -- HTTP/1.1
204	RFC 2630	Cryptographic Message Syntax
205	RFC 2821	Simple Mail Transfer Protocol (SMTP)
206	RFC 2822	Standard for the Format of Internet Text Messages

207 **5.3. CONFORMANCE VALIDATION**

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

213 For AS1: <http://ebusinessready.com/as1.html>

214 For AS2: <http://ebusinessready.com/as2.html>

215 **5.4. REQUIREMENTS**

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

220 **Digital Certificate Requirements**

221 Requirement 1

222 The length of the one-time session (symmetric) key must be 128 bits or greater.¹

223 Requirement 2

224 The length of the Public/Private Encryption key must be 1024 bits or greater.²

225 Requirement 3

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

227 Requirement 4

228 The Signature Hash algorithm used must be SHA1.³

230 **Configuration Requirement**

231 Requirement 5

232 Digitally signed receipts must be requested via Signed Message Disposition
233 Notifications (MDNs).⁴

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.

There may be export or import restrictions affecting use of encryption technologies in a few countries. See <http://www.bxa.doc.gov/encryption/> and <http://www.bxa.doc.gov/Encryption/docpr99.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

235

236

5.5. RECOMMENDATIONS

237

Recommendation 1

238

Asynchronous MDNs are recommended for EDIINT AS2.⁵

239

Recommendation 2

240

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.

241

242

243

244

Recommendation 3

245

When a message has been successfully sent, but a MDN has not been received in a timely manner, the initial sender should resend the original message with the same content and the same Message-ID value. The period of time to wait for a MDN is based on business and technical needs, but generally should not be less than one hour.

246

247

248

249

250

Recommendation 4

251

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 may be used.⁶

252

253

254

Recommendation 5

255

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.

256

257

Recommendation 6

258

For EDIINT AS1, a dedicated SMTP server, separate from the normal email server is recommended.

259

260

Recommendation 7

261

EDIINT compression may be used as an option, especially if message sizes are large. Although current versions of EDIINT software handle compression automatically, this should be bilaterally agreed between the sender and the receiver.⁸

262

263

⁵ Since significant processing is needed to decrypt a message prior to the creation of a MDN, requesting synchronous MDNs (which keeps the HTTP session open until the MDN is created) can result in transmission failures due to HTTP timeouts, especially with large messages and many messages being received. The use of proxy servers may preclude the use of synchronous MDNs. For EDIINT AS1, MDNs are always asynchronous, since SMTP (email) does not support bi-directional transmission.

⁶ HTTPS may introduce operational complexities, and should be carefully considered.

⁷ The GLNs should be that of the sending server and receiving server respectively. When a hub 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 will 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-04.txt>

264 Recommendation 8

265 Digital certificates can either be from a trusted third party or self signed if bilaterally
266 agreed between trading partners.

267 Recommendation 9

268 A single digital certificate may be used for both encryption and signatures, however if
269 business dictate separate certificates may be used. Although current versions of
270 EDIINT software handle two certificates automatically, this should be bilaterally
271 agreed between the sender and the receiver

272 Recommendation 10

273 The minimum validity period for a certificate should be 1 year. The maximum validity
274 period should be 5 years.

275 Recommendation 11

276 The method for certificate exchange must be bilaterally agreed upon. Note: The
277 Internet Engineering Task Force (IETF) is developing a *Certificate Exchange*
278 *Messaging for EDIINT* specification which will enable automated certificate exchange
279 once the initial trust relationship is established.⁹

280 Organizations that adopt these Guidelines may decide to use functionality beyond the minimum
281 requirements as long as:
282

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

285

286 5.6. NETWORK AVAILABILITY

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

293

294 5.7. IMPLEMENTATION CONSIDERATIONS

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

295

296

5.7.1 EDIINT-AS1 & EDIINT-AS2 FUNCTIONALITY COMPARED

297

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 ¹⁰	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 ¹¹	

298

¹⁰ 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.

¹¹ 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

299 **5.7.2 INTERNET FACILITIES**

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

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

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

- 308 • The type of network redundancy the ISP maintains
- 309 • The physical connection of the ISP to the Internet Backbone
- 310 • If the ISP owns their own infrastructure
- 311 • The Service Level Agreements of the ISP
- 312 • Any size or volume restrictions imposed by the ISP

313 **5.7.3 INTERNAL FACILITIES**

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

- 315 • What is the physical connection between the company and the ISP
- 316 • Is there single point of failure anywhere and will this impact "mission-critical" data
- 317 • Internal restrictions or non-standard behavior with Firewall, SMTP server, Network
318 Address Translation (NAT), Gateway, Tunnel, or Proxy server components
- 319 • Trading partners' restrictions or non-standard behavior with Firewall, NAT, Gateway,
320 Tunnel, or Proxy server components
- 321 • Production status of both SMTP Server (for AS1) and separate HTTP Server, if used,
322 (for AS2). Support must be available 24x7 to ensure that e-Commerce transactions
323 are not delayed.

324 **5.7.4 SIGNED RECEIPTS**

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

331 **5.7.5 CERTIFICATES**

332 The specifications on which these Guidelines are based do not define a standard-based
333 method to automatically exchange and synchronize certificates (public/private keys), nor
334 do they make provision for the use of inter-operable, standards-based certification
335 authorities to facilitate this process. When standards-based methods to exchange
336 certificates are developed, they will be incorporated into these guidelines.

337 Companies implementing these Guidelines must manually exchange certificates (either
338 self-signed or from a trusted Certificate Authority) with each of their trading partners. In
339 order to minimize the frequency that certificates must be changed, companies may need
340 to consider using the longest encryption key length that their partners can process
341 beyond the minimum required by these Guidelines. Public/Private encryption and
342 Signature key lengths can range from 512 to 2048 bits. One-time Symmetric encryption
343 key lengths can range from 40 to 256 bits. Key length is directly related to the time that it
344 takes to break a key and successfully decrypt a message. Other important factors for
345 companies to consider are the dollar value of the EDI or XML transactions themselves,
346 and their life span within the context of the industry.

347

348 **5.7.6 SUPPORT SERVICES**

349

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

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

357

358 **5.7.7 POINT TO POINT**

359

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

366

6 GLOSSARY

367

AS1	Applicability Statement 1 – An EDIINT draft standard 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 EDIINT draft standard 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 markup code that indicates the grammar rules for the particular class of document. It specifies the valid syntax, structure, and format for defining the XML markup elements.
EANCOM	The EDI standards manual made available by EAN International, which is an implementation guideline of the EDIFACT standard developed under the auspices of the United Nations.
EDI	Electronic Data Interchange – The exchange of business data computer to computer. Data format standards are developed by the Accredited Standards Committee (ASC) X12 of the American National Standards Institute and the EDIFACT Working Group of the United Nations.
EDIINT	EDI Over the Internet Working Group – A working group of the IETF that developed the AS1 and AS2 proposed 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.

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.
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 Internet mail.
Non-repudiation of Receipt	Confirms that the intended party received the data. Is accomplished via digital signatures and signed MDNs.
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.
Schema	A document definition, similar to a DTD but using special XML vocabulary named XML-Data. Schemas have significantly more functionality than DTDs.
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.
GS1 US	The GS1 Member Organization for the United States.
UN/EDIFACT	United Nations / Electronic Data Interchange for Administration, Commerce and Transport
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

368

7 FIGURES

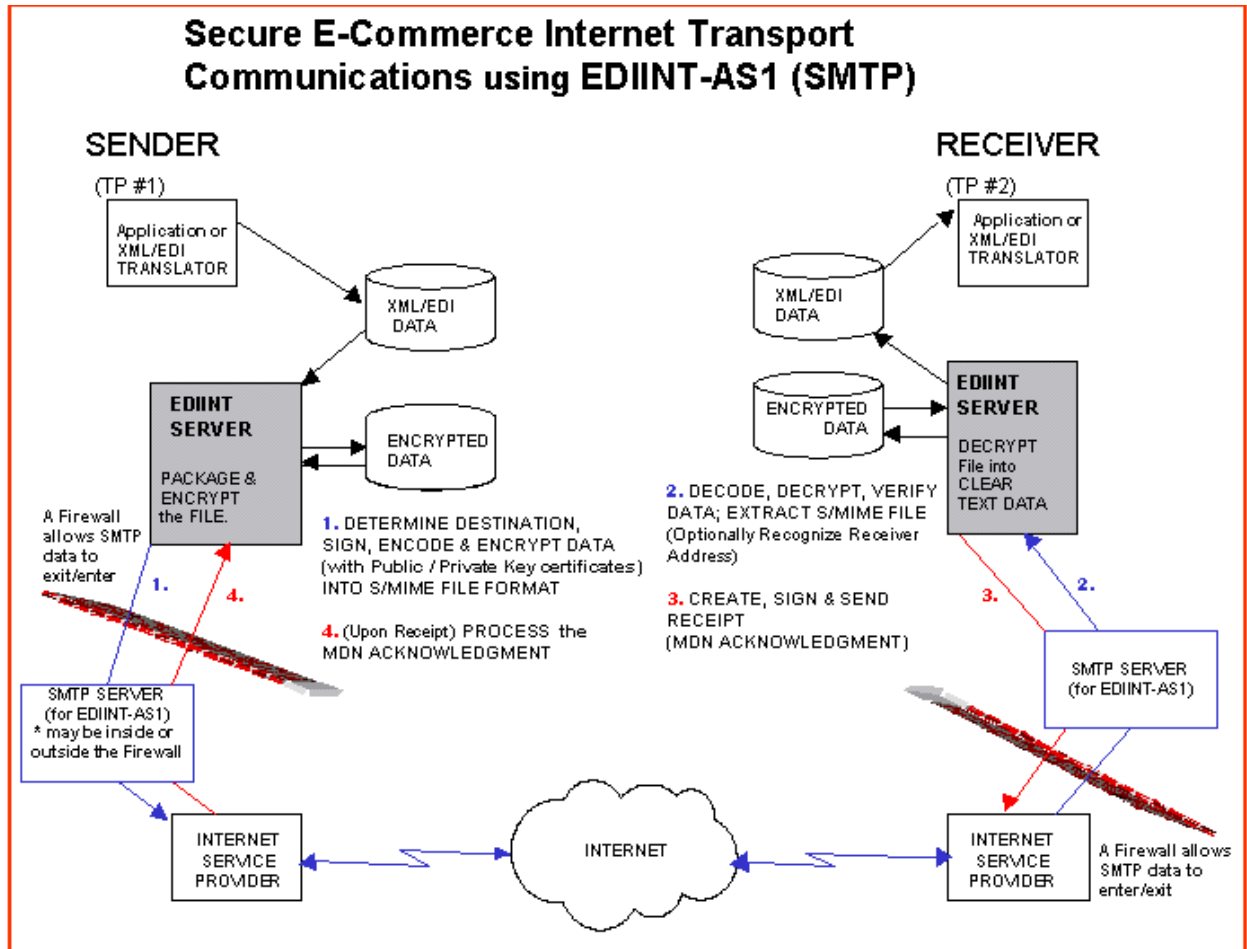


Figure 1

369

370

371

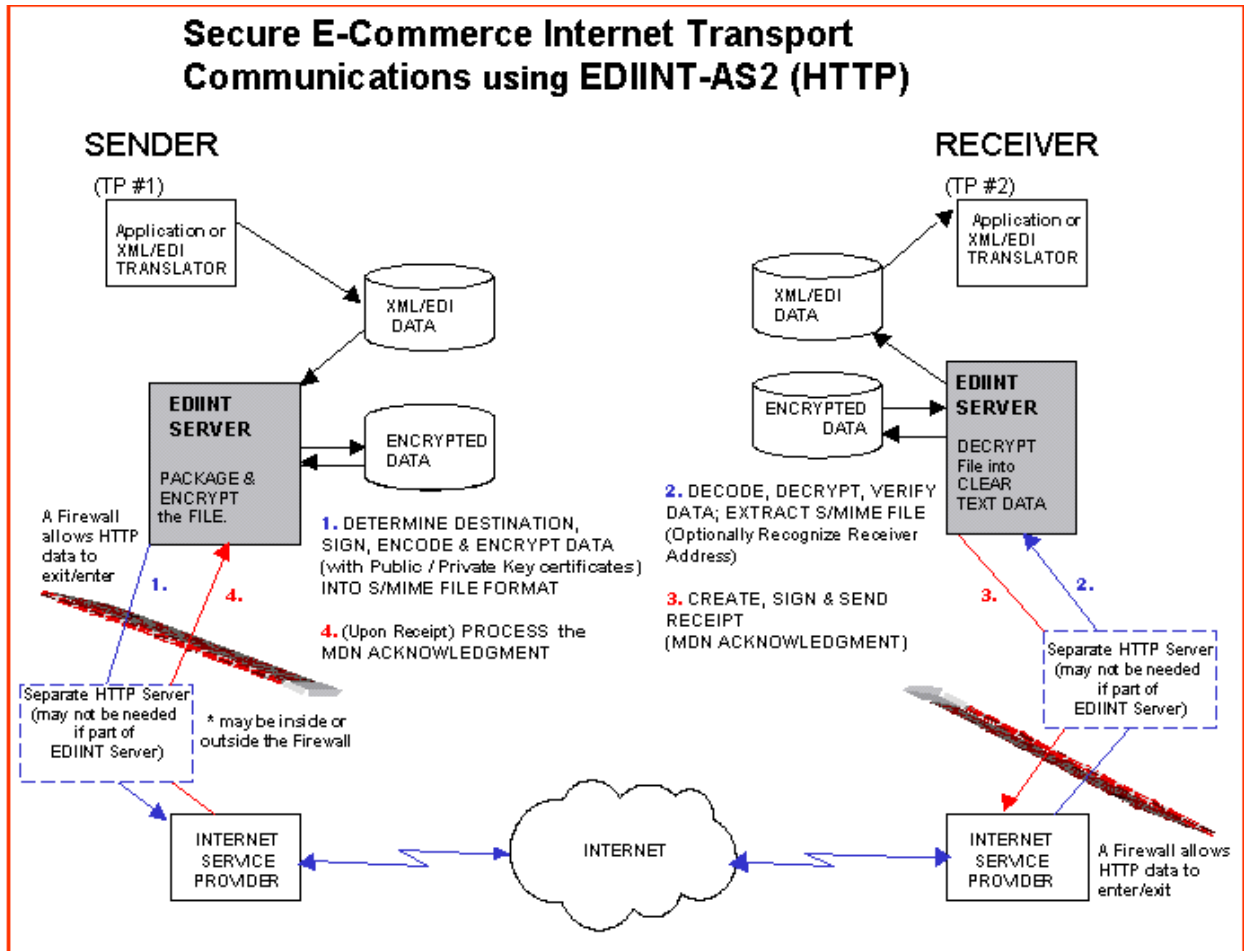


Figure 2

372

373

374

EDIINT Public/Private Key Security Processing

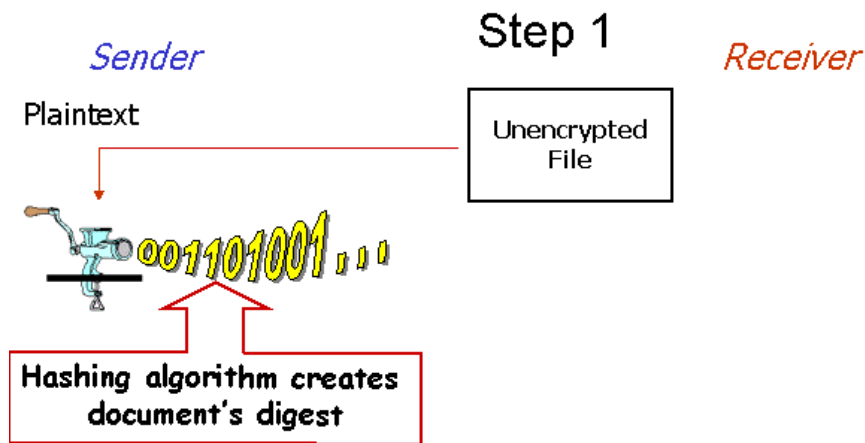


Figure 3

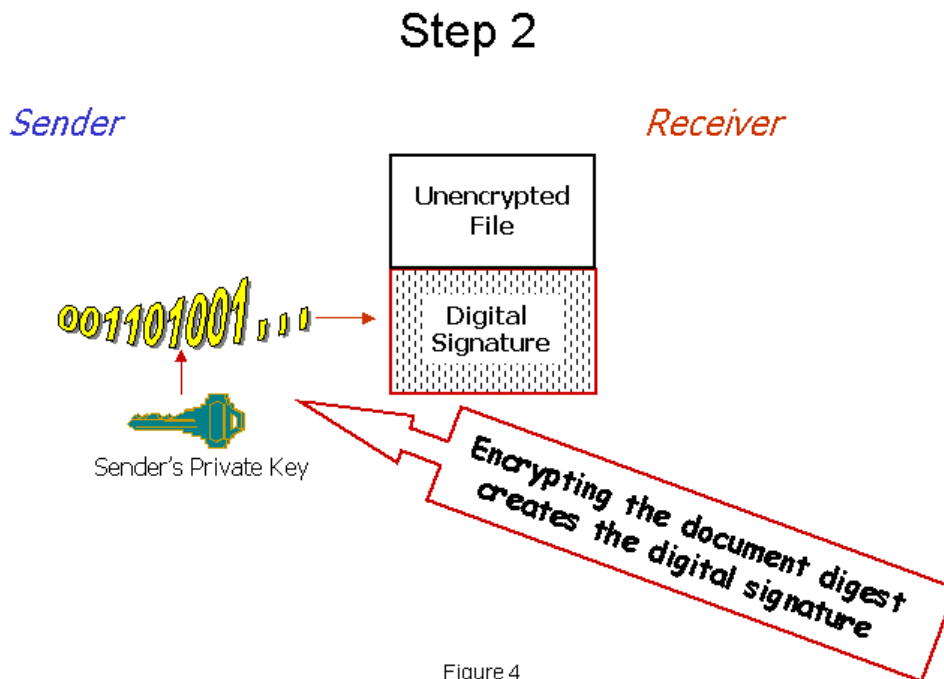


Figure 4

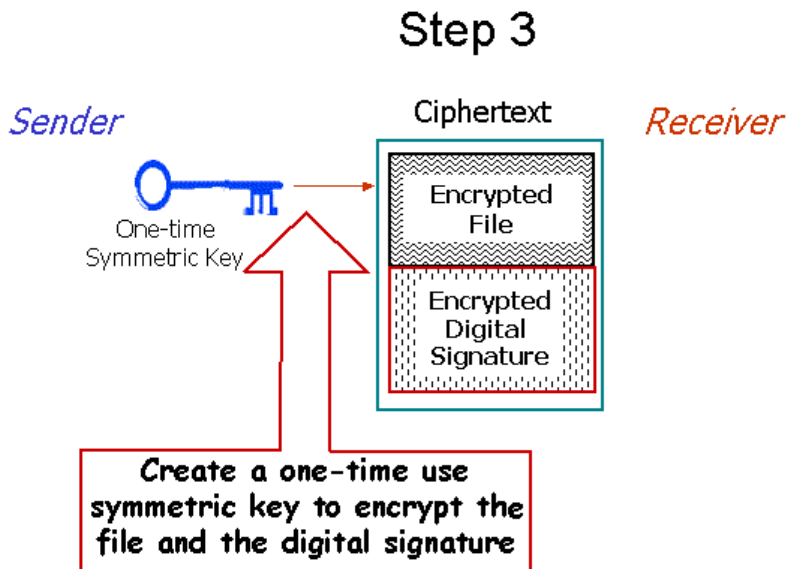


Figure 5

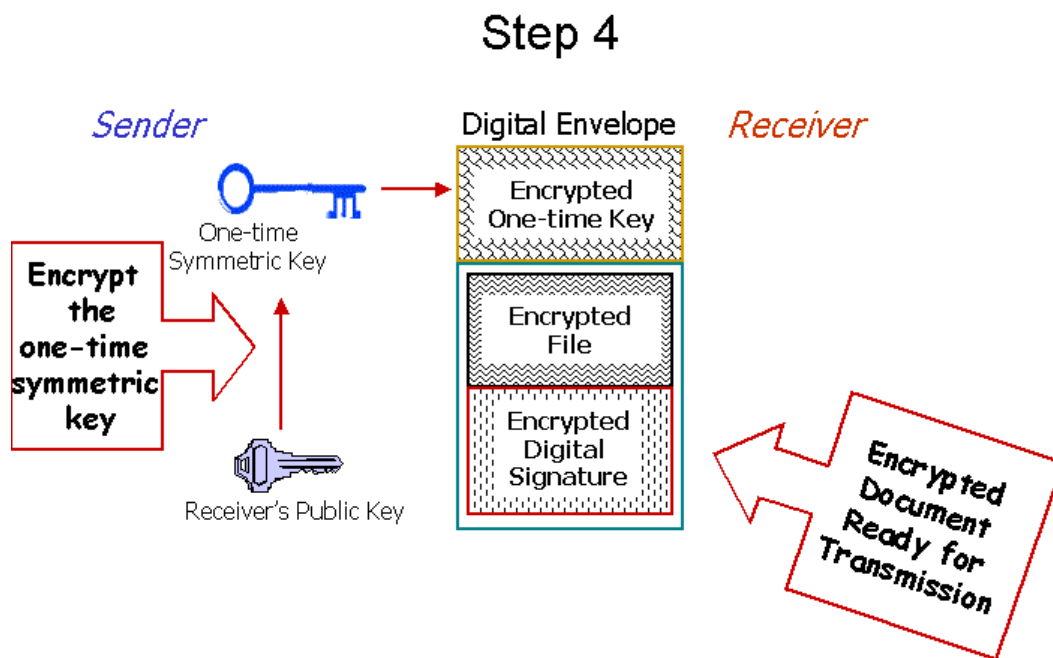


Figure 6

Step 5

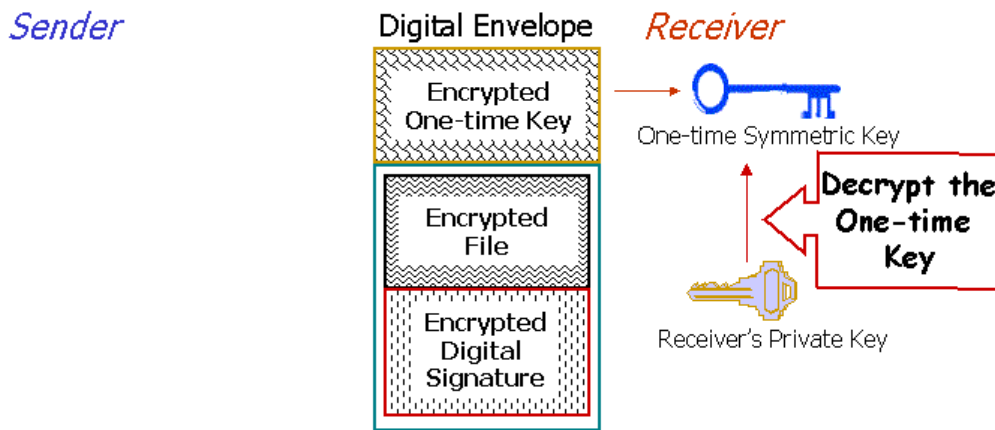


Figure 7

377

Step 6

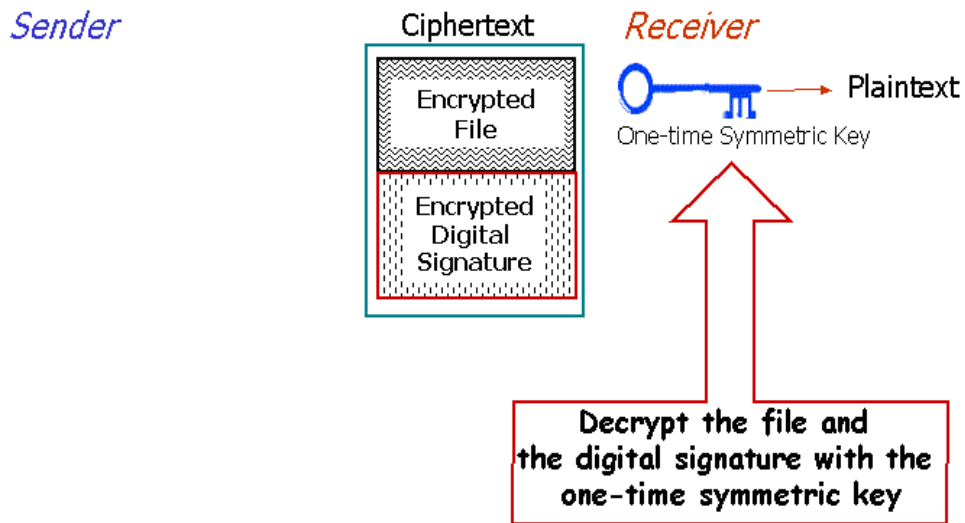


Figure 8

378

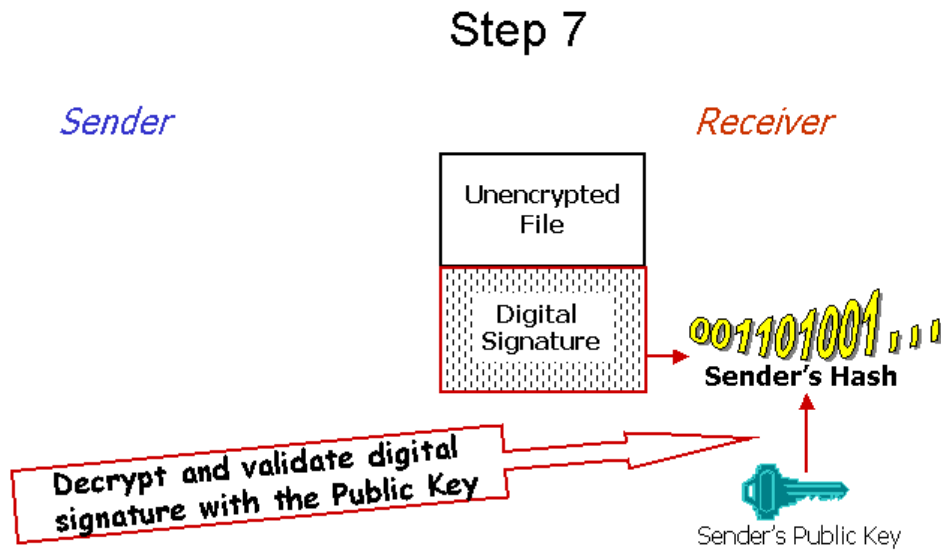


Figure 9

379

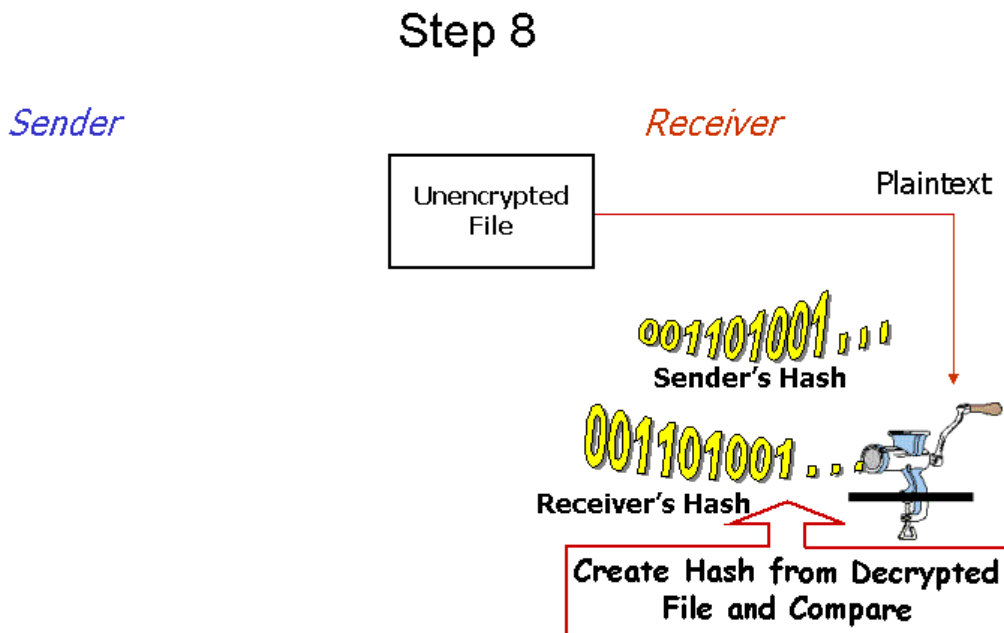


Figure 10

380

EDIINT Public/Private Key Security Summary

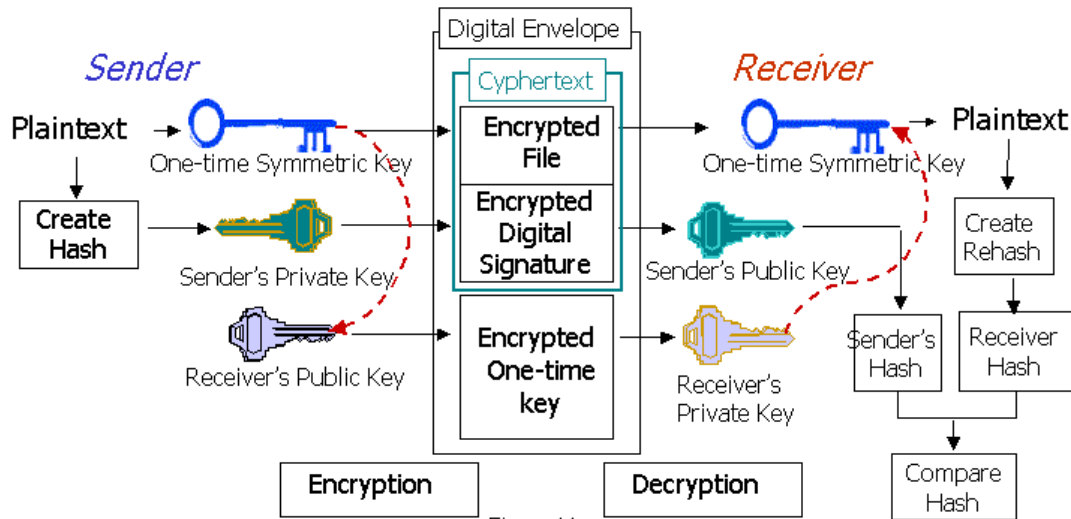


Figure 11

381

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

382