



**Telecommunications  
Industry Forum**

**Sponsored by the Alliance for  
Telecommunications Industry Solutions**

---

**Electronic Communications  
Interactive Agent  
Functional Specification**

---

TCIF-98-006  
Issue 3, Revision 2  
07/30/2002

---

## Electronic Communications Interactive Agent Functional Specification

Prepared for TCIF by the Electronic Communications Implementation Committee. For more information about TCIF, go to [www.atis.org](http://www.atis.org). To order this document, please visit the ATIS Document Store via [www.atis.org](http://www.atis.org). If you have questions or comments about this document, please contact the the document editor:

Stephen F. Reynolds, (314) 235-3449, [sr4140@momail.sbc.com](mailto:sr4140@momail.sbc.com) .

Copyright 2001 ATIS. All rights reserved.

This document is printed and distributed by the Alliance for Telecommunications Industry Solutions ("ATIS") on behalf of the Telecommunications Industry Forum ("TCIF"). Except as expressly permitted in the paragraph below, no part of this publication may be reproduced or distributed in any form, in an electronic system or otherwise, without the prior express written permission of ATIS. All requests to reproduce this document shall be in writing and sent to: TCIF Committee Administrator, c/o ATIS, 1200 G Street, NW, Suite 500, Washington, DC 20005.

Participants in the TCIF are hereby authorized to reproduce this document and distribute it within their own business organizations for TCIF-related business provided that this notice continues to appear in the reproduced document.

For ordering information, please contact:

ATIS  
1200 G Street, NW Suite 500  
Washington, DC 20005  
(202) 628-6380  
[tcif@atis.org](mailto:tcif@atis.org)

### Trademark Acknowledgments

RSA Security is a registered trademark of RSA Security Data Systems, Inc., a wholly-owned subsidiary of Security Dynamics Technologies, Inc., Bedford, Massachusetts.

### Notice of Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OF WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT TO CONFORMS OF ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR

THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

Currently in preview, click buy full version

---

## Revision History

12/07/2000 – Original Issue 3

06/13/2001 – Revision 1

1. To prevent an improper session close sequence, Sections 6.5, 7.8, and figure 4 are modified and Section 7.9 is added.
2. In Sections 9.3, 10.1, and 13, the reference to TCIF-98-009, Generic Implementation Guidelines for Connectivity has been changed to TCIF-99-016, Generic Guidelines for the use of TCP/IP in Electronic Bonding.

12/05/2001 – Revision 2

1. Removed HashedMessage (message integrity) message type. This was done to avoid redundant hashing for integrity purposes. TLS Protocol includes the hashing function to assure data integrity.
2. A recommendation is added that the IAs verify the authentication credentials and other relevant information regarding the trading partner.
3. A recommendation is added defining the minimum size and maximum numbers of TLS writes.
4. A recommendation is added regarding the implications of the Nagle factor on TCP/IP packets.
5. A recommendation for the implementation of a monitor in the socket manager is added. This monitor would issue an alarm if a configurable number of transactions is exceeded.
6. The object identifiers used in the production modules have been changed to conform to the values assigned in T1.274.2000. In order to uniquely specify the object identifiers the IA version (3) and release number (2) have been appended by the Technology Support editors.

## Table of Contents

<b>1</b>	<b>Introduction</b> .....	<b>7</b>
<b>2</b>	<b>Objectives</b> .....	<b>7</b>
<b>3</b>	<b>Architecture</b> .....	<b>8</b>
<b>4</b>	<b>Data Flow</b> .....	<b>10</b>
<b>5</b>	<b>Message Formatting</b> .....	<b>13</b>
5.1	Message Format Definitions .....	13
5.1.1	IA Status Message Detail Format.....	14
5.1.2	Optional Message Receipts.....	16
5.2	Message Syntax Definitions.....	16
5.2.1	ASN.1 Syntax for Basic Messages.....	17
5.2.2	ASN.1 Syntax for Message Integrity.....	17
5.2.3	ASN.1 Syntax for Non-Repudiation Messages.....	17
5.2.4	ASN.1 Syntax for IA Status .....	18
5.2.5	ASN.1 Syntax for Optional IA Receipts .....	18
<b>6</b>	<b>Client Specifications</b> .....	<b>19</b>
6.1	Determine IP Destination Address.....	20
6.2	Connect to Server.....	20
6.3	Send Data to Server .....	22
6.4	Transmission Logging.....	22
6.5	Client Disconnect.....	23
<b>7</b>	<b>Server Specifications</b> .....	<b>24</b>
7.1	Initialize Server .....	24
7.2	Accept Connection from Client .....	24
7.3	Message Read Setup .....	24
7.3.1	Create TLS Context (Memory Allocation).....	25
7.3.2	Initialize TLS Context.....	25
7.3.3	Read and Add Certificates from Local Library.....	25
7.3.4	Read and Add Private Key from Local Source.....	25
7.3.5	Set TLS Protocol Version.....	25
7.3.6	Set TLS Protocol Side.....	25
7.3.7	Set TLS I/O Preference .....	25
7.3.8	Set TLS Peer ID.....	25
7.3.9	TLS Handshake.....	25
7.4	TLS Read Processing.....	26
7.5	Route Data to Translator.....	26
7.6	Message Logging.....	27
7.7	Message Validation.....	27
7.7.1	Message Integrity .....	27
7.7.2	Non-Repudiation.....	27
7.8	Server Post Message Activities .....	27
7.9	Server Disconnect.....	27
<b>8</b>	<b>Interfaces</b> .....	<b>27</b>
8.1	Data Communications Protocol .....	28
8.2	Translators .....	28
<b>9</b>	<b>Design Considerations</b> .....	<b>28</b>
9.1	Multi-processing/Multi-threading .....	28
9.2	Persistent Connections .....	28

9.3	Connectivity .....	28
	Connectivity should be established in accordance with TCIF-99-016, which is incorporated herein by reference.....	28
9.4	IA Issue 2 message identification .....	28
<b>10</b>	<b>Operational Concerns .....</b>	<b>28</b>
10.1	Security .....	28
10.2	Data Sessions.....	29
10.3	Logging .....	29
10.3.1	Logging Levels .....	29
10.3.2	Log Files.....	29
10.4	Routing.....	30
10.5	Firewalls.....	30
10.6	Digital Certificates.....	30
<b>11</b>	<b>Error Handling/Recovery .....</b>	<b>30</b>
<b>12</b>	<b>Implementation Issues.....</b>	<b>30</b>
12.1	Interoperability .....	30
12.2	Port Assignments.....	31
12.3	Partner Responsibilities .....	31
<b>13</b>	<b>References .....</b>	<b>31</b>
<b>14</b>	<b>Contact Names &amp; Addresses .....</b>	<b>32</b>
	<b>Appendix A .....</b>	<b>32</b>
	<b>Appendix B .....</b>	<b>33</b>

**List of Figures**

Figure 1 - Dataflow.....	8
Figure 2 - IA Symmetrical Relationship.....	8
Figure 3 - IA Layered Architecture .....	9
Figure 4 - IA Message Flow .....	10
Figure 5 - Message Format Architecture.....	13

## 1 Introduction

The TCIF has recommended the use of Electronic Data Interchange (EDI), Transmission Control Protocol/Internet Protocol (TCP/IP) and Transport Layer Security (TLS) as a method of supporting interconnection between carriers. Traditionally, EDI transmissions have been exchanged between trading partners using a Value Added Network (VAN) or a direct connection, as outlined in Section 6, Communications, of the TCIF/EDI Guidelines. TCIF recognizes that for some business transactions, e.g., procurement of material using an 850 Purchase Order, a VAN or direct connect may still be used because the orders are normally stored and forwarded on a daily basis. The IA with TCP/IP using TLS is recommended for use with Local Service Orders, and can be used with all EDI transactions if a company so desires.

To functionally implement this recommendation the Interactive Agent (IA) has been developed. This document defines the technical specifications for the development, architecture, design, structure, and process-flow of the (IA).

The commercialization of TLS permits Issue 3 of the IA Specification to incorporate the more robust standard of TLS. This allows the Issue 3 IA to incorporate persistent sessions. While Issue 3 requires TLS, many toolkits allow for accepting an SSL3 handshake. The mechanism to identify messages from an IA using Issue 2 and SSL3 exists within this specification.

Extensions to the IA provide for the transport of non-EDI data such as Extensible Markup Language (XML) and plain text.

## 2 Objectives

This Interactive Agent specification embodies the following objectives:

- Open Architecture
- Public Standards
- Simplicity Of Design And Ease Of Implementation
- Wide Availability Of Development Tools
- Use Of Well Documented Technologies
- Provide For A Secure Transaction Environment:
  - Privacy
  - Authentication
  - Integrity
  - Non-Repudiation