



ANSI/J-STD-025-B-2006
APPROVED: JULY 17, 2006
REAFFIRMATION: FEBRUARY 9, 2011
REAFFIRMATION: MAY 7, 2019

JOINT STANDARD

Lawfully Authorized Electronic Surveillance

J-STD-025-B

July 2006

Jointly developed by Telecommunications Industry Association
and Alliance for Telecommunications Industry Solutions



JOINT STANDARDS

Joint Standards and Publications are adopted in accordance with the American National Standards Institute (ANSI) patent policy. By such action, the Telecommunications Industry Association or the Alliance for Telecommunications Industry Solutions does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard or Publication.

This Standard does not purport to address all safety problems associated with its use or all applicable regulatory requirements. It is the responsibility of the user of this Standard to establish appropriate safety and health practices and to determine the applicability of regulatory limitations before its use.

This standard was developed under Project No. SP-3-4465-UGRV2-RF2-A, formulated under the cognizance of the TIA TR-45 Committee on Mobile & Personal Communications Systems and ATIS Wireless Technologies and Systems Committee and ATIS Packet Technologies and Systems Committee.

Published by

©TELECOMMUNICATIONS INDUSTRY ASSOCIATION 2019

Technology and Standards Department
1320 N. Courthouse Road, Suite 200
Arlington, VA 22201 U.S.A.

Or

©ALLIANCE FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS 2019

1200 G Street, NW
Suite 500
Washington, DC 20005
(202) 628-6380

All rights reserved
Printed in U.S.A

NOTICE FROM THE DEVELOPERS

This document has been approved by the Telecommunications Industry Association (TIA) Engineering Committee and the Alliance for Telecommunications Industry Solutions (ATIS).

Users may submit comments to the Standards Secretariat to TIA at the following address: 1320 N. Courthouse, Suite 200, Arlington, VA 22201-3438; Telephone (703)907-7700; Fax: (703)907-7727 or by email to standards@tiaonline.org.

This document was coordinated between ATIS and TIA.

A Word from TIA:

TIA Engineering Standards and Publications are designed to serve the public interest through eliminating misunderstanding between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for his/her particular need. Existence of such Standards and Publications shall not be in any respect preclude any member or nonmember of TIA from manufacturing or selling products not conforming to such Standards and Publications, nor shall the existence of such Standards and Publications preclude their voluntary use by those other than TIA members, whether the standard is to be used either domestically or internationally.

TIA Documents contain information deemed to be of technical value to the industry, and are published at the request of the originating Committee without necessarily following the rigorous public review and resolution of comments which is a procedural part of the development of an American National Standard (ANS). Further details of the development process are available in the TIA Procedures for American National Standards and TIA Engineering Committee Operating Procedures, located at [Standards Procedures and Guidelines](#)

A Word from ATIS:

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's business priorities. ATIS' member companies are currently working to address emergency services, 5G, robocall mitigation, Smart Cities, artificial intelligence-enabled networks, IoT, distributed ledger/blockchain technology, cybersecurity, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle – from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org. Follow ATIS on [Twitter](#) and on [LinkedIn](#).

NOTICE FROM PATENT HOLDERS

The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights.

By publication of this standard, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain a license. Details may be obtained from the Telecommunications Industry Association Alliance for Telecommunications Industry Solutions or the American National Standards Institute.

©Copyright Telecommunications Industry Association 2019

©Copyright Alliance for Telecommunications Industry Solutions 2019

All rights reserved

This document is subject to change.

NOTICE OF COPYRIGHT

This document is issued under a joint copyright by the Telecommunications Industry Association and the Alliance for Telecommunications Industry Solutions, and may not be reproduced without permission.

Reproduction of these documents either in hard copy or soft copy (including posting on the web) is prohibited without copyright permission. For copyright permission to reproduce portions of this document, please contact TIA Standards Department or go to the TIA website (www.tiaonline.org) for details on how to request permission. Details are located at: [Standards Procedures and Guidelines](#)

Organizations may obtain permission to reproduce a limited number of copies by entering into a license agreement. For information, contact:

IHS
15 Inverness Way East
Englewood, CO 80112-5794 or call
U.S.A. and Canada (1-800-525-7052)
International (303) 790-0600

OR
ATIS Document Center: <https://www.techstreet.com/atis/>
Alliance for Telecommunications Industry Solutions
1200 G Street, NW
Suite 500
Washington, DC 20005
(202) 628-6380

NOTICE OF DISCLAIMER AND LIABILITY

The document to which this Notice is affixed (the "Document") has been prepared by one or more Engineering Committees or Formulating Groups of the Telecommunications Industry Association ("TIA"). In addition, the Document was balloted by ATIS Wireless Technologies and Systems Committee and ATIS Packet Technologies and Systems Committee. TIA is not the author of the Document contents, but publishes and claims copyright to the Document pursuant to licenses and permission granted by the authors of the contents.

TIA Engineering Committees and Formulating Groups are expected to conduct their affairs in accordance with the TIA Procedures for American National Standards and TIA Engineering Committee Operating Procedures, the current and predecessor versions of which are available at [Standards Procedures and Guidelines](#). The ATIS Wireless Technologies and Systems Committee and ATIS Packet Technologies and Systems Committee is expected to conduct its affairs in accordance with the ATIS Operating Procedures which is available at <http://www.atis.org/legal/op.asp>.

TIA's function is to administer the process, but not the content, of document preparation in accordance with the Manual and, when appropriate, the policies and procedures of the American National Standards Institute ("ANSI"). Likewise, ATIS' function, and on behalf of its Committees and Forums, is to administer the process according to its Operating Procedures, but not develop the content of the document. TIA and ATIS do not evaluate, test, verify or investigate the information, accuracy, soundness, or credibility of the contents of the Document. In publishing the Document, TIA and ATIS disclaim any undertaking to perform any duty owed to or for anyone.

If the Document is identified or marked as a project number (PN) document, or as a standards proposal (SP) document, persons or parties reading or in any way interested in the Document are cautioned that: (a) the Document is a proposal; (b) there is no assurance that the Document will be approved by any Committee of TIA or any other body in its present or any other form; (c) the Document may be amended, modified or changed in the standards development or editing process.

The use or practice of contents of this Document may involve the use of intellectual property rights ("IPR"), including pending or issued patents, or copyrights, owned by one or more parties. Neither TIA nor ATIS makes any search or investigation for IPR. When IPR consisting of patents and published pending patent applications are claimed and called to TIA's attention, a statement from the holder thereof is requested, all in accordance with the Manual. When IPR consisting of patents are claimed and called to ATIS's attention, a statement from the holder thereof is requested, all in accordance with the ATIS's Operating Procedures. Neither TIA nor ATIS takes any position with reference to, and disclaims any obligation to investigate or inquire into, the scope or validity of any claims of IPR. Neither TIA or ATIS will neither be a party to discussions of any licensing terms or conditions, which are instead left to the parties involved, nor will TIA or ATIS opine or judge whether proposed licensing terms or conditions are reasonable or non-discriminatory. TIA does not warrant or represent that procedures or practices suggested or provided in the Manual have been complied with as respects the Document or its contents.

TIA and ATIS do not enforce or monitor compliance with the contents of the Document. TIA and ATIS do not certify, inspect, test or otherwise investigate products, designs or services or any claims of compliance with the contents of the Document.

ALL WARRANTIES, EXPRESS OR IMPLIED, ARE DISCLAIMED, INCLUDING WITHOUT LIMITATION, ANY AND ALL WARRANTIES CONCERNING THE ACCURACY OF THE CONTENTS, ITS FITNESS OR APPROPRIATENESS FOR A PARTICULAR PURPOSE OR USE, ITS MERCHANTABILITY AND ITS NON-INFRINGEMENT OF ANY THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS. TIA AND ATIS EXPRESSLY DISCLAIM ANY AND ALL RESPONSIBILITIES FOR THE ACCURACY OF THE CONTENTS AND MAKE NO REPRESENTATIONS OR WARRANTIES REGARDING THE CONTENT'S COMPLIANCE WITH ANY APPLICABLE STATUTE, RULE OR REGULATION, OR THE SAFETY OR HEALTH EFFECTS OF THE CONTENTS OR ANY PRODUCT OR SERVICE REFERRED TO IN THE DOCUMENT OR PRODUCED OR RENDERED TO COMPLY WITH THE CONTENTS.

NEITHER TIA NOR ATIS SHALL BE LIABLE FOR ANY AND ALL DAMAGES, DIRECT OR INDIRECT, ARISING FROM OR RELATING TO ANY USE OF THE CONTENTS CONTAINED HEREIN, INCLUDING WITHOUT LIMITATION ANY AND ALL INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, LITIGATION, OR THE LIKE), WHETHER BASED UPON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING NEGATION OF DAMAGES IS A FUNDAMENTAL ELEMENT OF THE USE OF THE CONTENTS HEREOF, AND THESE CONTENTS WOULD NOT BE PUBLISHED BY TIA WITHOUT SUCH LIMITATIONS.

Abstract

This Standard defines the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance. A TSP, manufacturer, or support service provider that is in compliance with this Standard will have a “safe harbor” under Section 107 of the Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414: “a [TSP] shall be found to be in compliance with the assistance capability requirements under [CALEA] Section 103, and a manufacturer of telecommunication transmission or switching equipment or a provider of telecommunication support services shall be found in compliance with [CALEA] Section 106.”

J-STD-025-A provides the enhancements necessary to support FCC 99-230, CC Docket No. 97-213, Third Report and Order and FCC 02-108, CC Docket No. 97-213, Order on Remand¹. J-STD-025-B provides enhancements to further support lawfully authorized electronic surveillance of packet data telecommunication services (e.g., cdma2000^{®2} packet data).

¹The FCC Third Report and Order [FCC 99-230, CC Docket No. 97-213] introductory paragraph states the following:

“Specifically, we require that all capabilities of J-STD-025 (interim standard) and six of nine “punch list” capabilities requested by the Department of Justice (DoJ)/Federal Bureau of Investigation (FBI) be implemented by wireline, cellular, and broadband PCS carriers. While we are requiring that a packet-mode capability be implemented by such carriers, we are not at this time adopting technical requirements for packet-mode communications, but will permit packet-mode data to be delivered to law enforcement under the interim standard, discussed below, pending further study of packet-mode communications by the telecommunications industry.”

²cdma2000 is a registered trademark of the Telecommunications Industry Association (TIA-USA).

Document Revision History

Revision	Date	Remarks
0	November 1997	Initial
A	February 2003	Revised to meet the requirements defined in FCC 99-230, CC Docket No. 97-213 and FCC 02-108, CC Docket No. 97-213.
<u>B</u>	<u>January 2004</u>	<u>Revised to include enhancements for packet based telecommunication technologies. J-STD-025-B is both a T1 Trial Use standard and a TIA standard.</u>
<u>B</u>	<u>June 2004</u>	<u>ANSI upgrade to include enhancements for packet based telecommunication technologies.</u>

Contents

1	Abstract	iii
2		
3		
4		
5	Document Revision History	iv
6		
7	Contents	v
8		
9		
10	List of Tables	xi
11		
12	List of Figures	xiii
13		
14	Foreword	xv
15		
16	1 Introduction	1
17	1.1 General	1
18	1.2 Purpose	2
19	1.3 Scope	2
20	1.4 Organization	2
21		
22	2 References	3
23		
24	3 Definitions and Acronyms	6
25		
26	4 Stage 1 Description: User Perspective	18
27	4.1 Overview	18
28	4.2 Introduction	18
29	4.2.1 Assumptions	18
30	4.2.2 General Background	21
31	4.2.3 Call Content Channels and Call Data Channels	22
32	4.3 Non-Call Associated Information Surveillance Service Description—Serving System IAP	23
33	4.4 Call Associated Information Surveillance Service Description—Call-Identifying Information IAP	24
34	4.4.1 Introduction	24
35	4.4.2 Basic Circuit Calls	25
36	4.4.3 Conference Call Party Changes	25
37	4.5 Call Associated and Non-Call Associated Information Surveillance Service Description	26
38	4.5.1 Introduction	26
39	4.5.2 Intercept Subject Signaling IAP	26
40	4.5.2.1 Subject-initiated Dialing and Signaling	26
41	4.5.2.2 Dialed Digit Extraction	26
42	4.5.3 Network Signaling IAP	27
43	4.5.3.1 In-band and Out-of-band Signaling	27
44	4.6 Content Surveillance Service Description	27
45	4.6.1 Circuit IAP	28
46	4.6.2 Conference Circuit IAP - Content of Subject-initiated Conference Calls	32
47	4.6.3 Packet Data IAP	33
48	4.7 Timing Information	37
49	4.8 Restrictions	38
50	4.8.1 Lack of CDC and CCC Synchronization	38
51	4.8.2 CDC Congestion	38
52	4.8.3 CCC Exhaustion	38
53		
54		
55		
56		
57		
58		
59		

4.8.4	CCC Congestion	38	1
4.9	Packet Mode Technology	39	2
4.9.1	Introduction and Scope	39	3
4.9.2	cdma2000® Packet Data	40	4
4.9.2.1	cdma2000® Packet Data System Reference Model	40	5
4.9.2.2	General Principles	42	6
4.9.2.3	Applicability to Telecommunications Services	43	7
4.9.2.4	Normal Operation - Intercept Events for Lawful Interception	43	8
4.9.3	GPRS/UMTS	44	9
4.9.4	Voice over Packet Technologies in Wireline Telecommunications Networks	45	10
5	Stage 2 Description: Network Perspective	46	11
5.1	Introduction	46	13
5.2	Stage 2 Methodology	46	14
5.3	Network Reference Model	47	15
5.3.1	Functional Entities	47	16
5.3.1.1	Access Function (AF)	47	17
5.3.1.2	Delivery Function (DF)	48	18
5.3.1.3	Collection Function (CF)	49	19
5.3.1.4	Service Provider Administration Function (SPAF)	49	20
5.3.1.5	Law Enforcement Administration Function (LEAF)	49	21
5.3.2	Interface Reference Points	49	22
5.3.2.1	Reference Point <i>a</i>	49	23
5.3.2.2	Reference Point <i>b</i>	49	24
5.3.2.3	Reference Point <i>c</i>	50	25
5.3.2.4	Reference Point <i>d</i>	50	26
5.3.2.5	Reference Point <i>e</i>	50	27
5.4	Message Descriptions	50	28
5.4.1	Answer	50	29
5.4.2	CCClose	51	30
5.4.3	CCOpen	52	31
5.4.4	Change	53	32
5.4.5	ConferencePartyChange	54	33
5.4.6	Connection	56	34
5.4.7	ConnectionBreak	56	35
5.4.8	DialingExtraction	57	36
5.4.9	NetworkSignal	58	37
5.4.10	Origination	61	38
5.4.11	PacketEnvelope	62	39
5.4.12	Redirection	63	40
5.4.13	Release	64	41
5.4.14	ServingSystem	65	42
5.4.15	SubjectSignal	66	43
5.4.16	TerminationAttempt	67	44
5.5	Message descriptions for cdma2000® packet data	68	45
5.5.1	cdma2000PacketDataSessionEstablishment	69	46
5.5.2	cdma2000PacketDataSessionTermination	70	47
5.5.3	cdma2000PacketDataInterceptStart	71	48
5.5.4	cdma2000PacketDataServingSystem	72	49
5.5.5	cdma2000PacketDataPacketFilter	73	50
5.5.6	cdma2000InterceptionofContent	74	51
6	Stage 3 Description: Implementation Perspective	76	52

1	6.1	Protocol Definition	76
2	6.2	CDC Protocol Definition	76
3	6.2.1	CDC Underlying Data Transmission	76
4	6.2.2	CDC Parameter Encoding Objectives	76
5	6.2.3	CDC Syntax Definitions	77
6	6.3	CDC Message Definitions	77
7	6.3.1	Answer Message	79
8	6.3.2	CCClose Message	79
9	6.3.3	CCOpen Message	80
10	6.3.4	Change Message	80
11	6.3.5	ConferencePartyChange Message	81
12	6.3.6	Connection Message	82
13	6.3.7	ConnectionBreak Message	82
14	6.3.8	DialedDigitExtraction Message	82
15	6.3.9	NetworkSignal Message	83
16	6.3.10	Origination Message	84
17	6.3.11	PacketEnvelope Message	84
18	6.3.12	Redirection Message	86
19	6.3.13	Release Message	86
20	6.3.14	ServingSystem Message	87
21	6.3.15	SubjectSignal Message	87
22	6.3.16	TerminationAttempt Message	88
23	6.4	CDC Parameter Definitions	89
24	6.4.1	AlertingSignal	89
25	6.4.2	AudibleSignal	89
26	6.4.3	BearerCapability	90
27	6.4.4	CallIdentity	90
28	6.4.5	CaseIdentity	90
29	6.4.6	CCIdentity	91
30	6.4.7	IAPSystemIdentity	91
31	6.4.8	Location	91
32	6.4.9	PartyIdentity	92
33	6.4.10	PDUType	93
34	6.4.11	RedirectedFromInformation	93
35	6.4.12	TerminalDisplayInfo	94
36	6.4.13	TimeStamp	94
37	6.4.14	TransitCarrierIdentity	94
38	6.5	cdma2000® Abstract Syntax for Packet Data CII Delivery	94
39	6.6	CCC Protocols	98
40	6.6.1	CCC Encoding for Circuit-Mode Services	98
41	6.6.2	CCC Encoding for Packet-Mode Services	98
42	6.6.2.1	cdma2000® Abstract Syntax Notation for Packet Data CC Delivery	98
43	6.7	LAESP Compatibility Guidelines	99
44	6.7.1	Guidelines For Forward Compatibility	100
45	6.7.2	Guidelines For Backward Compatibility	100
46	6.7.2.1	Existing Messages	100
47	6.7.2.2	Parameters in Existing Messages	101
48	6.7.2.3	New Messages	101
49	6.7.2.4	New Parameters	101
50	6.7.2.5	New Parameter Fields	101
51	6.7.2.6	New Parameter Values	102
52			
53			
54			
55			
56			
57			
58			
59			

Annex A	Deployment Examples	103	1
A.1	Possible Network Deployment of IAPs	103	2
A.2	Access and Delivery Function Equipment Configuration	105	3
A.3	Implementation of the <i>d</i> -interface	109	4
A.4	Implementation of the <i>e</i> -interface	111	5
A.5	Possible CDC Protocol Stacks	113	6
A.6	Possible CCC Protocol Stacks	114	7
			8
			9
Annex B	CCC Delivery Methods	117	10
B.1	Circuit-Mode vs. Packet-Mode	117	11
B.2	Overview	118	12
B.3	Dedicated Circuit CCC Delivery	119	13
B.3.1	Obtain Network Address of Destination	120	14
B.3.2	Setup CCC to Destination	120	15
B.3.3	Destination Acceptance or Refusal of a CCC	121	16
B.3.4	CCC Continuity Verification	121	17
B.3.5	Associate Intercept Subject and Call Identity to the CCC	122	18
B.3.6	Call Content Transfer	122	19
B.3.7	Early CCC Release by the Destination	123	20
B.3.8	Disassociate CCC	123	21
B.3.9	Normal CCC Release by the Source.	123	22
			23
			24
B.4	Trunk Group CCC Delivery	124	25
B.4.1	Obtain Network Address of Destination	125	26
B.4.2	Setup CCC to Destination	125	27
B.4.3	Destination Acceptance or Refusal of a CCC	126	28
B.4.4	CCC Continuity Verification	129	29
B.4.5	Associate Intercept Subject and Call Identity to the CCC	129	30
B.4.6	Call Content Transfer	130	31
B.4.7	Early CCC Release by the Destination	130	32
B.4.8	Disassociate CCC	131	33
B.4.9	Normal CCC Release by the Source	131	34
			35
B.5	Static Directory Number CCC Delivery	132	36
B.5.1	Obtain Network Address of Destination	133	37
B.5.2	Setup CCC to Destination	133	38
B.5.3	Destination Acceptance or Refusal of a CCC	134	39
B.5.4	CCC Continuity Verification	134	40
B.5.5	Associate Intercept Subject and Call Identity to the CCC	134	41
B.5.6	Call Content Transfer	134	42
B.5.7	Early CCC Release by the Destination.	134	43
B.5.8	Disassociate CCC	135	44
B.5.9	Normal CCC Release by the Source	135	45
			46
B.6	Packet Data CCC Delivery	135	47
B.6.1	Obtain Network Address of Destination	136	48
B.6.2	Setup CCC to Destination	136	49
B.6.3	Destination Acceptance or Refusal of a CCC	136	50
B.6.4	CCC Continuity Verification	136	51
B.6.5	Associate Intercept Subject and Call Identity to the CCC	137	52
B.6.6	Call Content Transfer	137	53
B.6.7	Early CCC Release by the Destination	137	54
B.6.8	Disassociate CCC	137	55
B.6.9	Normal CCC Release by the Source	137	56
			57
B.7	Delivery Bearer Service	137	58
B.8	Separated Content Delivery	138	59

1	B.9	Combined Content Delivery	138
2	B.10	Signaling for Switched Delivery	139
3	B.11	Call Content Delivery Delay	139
4	B.12	Call Content Distribution	140
5	B.13	DTMF C-Tone Signaling Procedures	140
6			
7			
8	Annex C	CDC Delivery Methods	142
9	C.1	Dedicated Data Circuit CDC Delivery	142
10	C.2	Dedicated Data Link CDC Delivery	143
11	C.3	Call Data Distribution	143
12			
13	Annex D	Information Access Scenarios	144
14	D.1	Simple Abandoned Call Attempt	148
15	D.2	Partial Dial Abandon	148
16	D.3	Pre-Answer Abandon	149
17	D.4	Simple Outgoing Call	150
18	D.5	Re-Origination	151
19	D.6	Simple Incoming Call	152
20	D.7	Call Waiting and Recall	153
21	D.7.1	Call Waiting and Recall with a Single Call Identity	154
22	D.7.2	Call Waiting and Recall with Separate Leg Identities	155
23	D.7.3	Call Waiting and Recall with Separate Calls	156
24	D.8	Call Waiting with Talking Party Disconnect	157
25	D.8.1	Call Waiting with Talking Party Disconnect and a Single Call Identity	158
26	D.8.2	Call Waiting with Talking Party Disconnect and Separate Leg Identities	159
27	D.8.3	Call Waiting with Talking Party Disconnect and Separate Calls	160
28	D.9	Call Held and Retrieved	161
29	D.10	Three-Way Calling, Plus Call Turned Away	162
30	D.10.1	Three-Way Calling, Plus Call Turned Away with a Single Call Identity	162
31	D.10.2	Three-Way Calling, Plus Call Turned Away with Separate Leg Identities	164
32	D.10.3	Three-Way Calling, Plus Call Turned Away with Separate Calls	165
33	D.11	Call Forwarding—No Answer on a Single System	167
34	D.12	Call Forwarding—No Answer on Different Systems	168
35	D.13	Two Bearer Channels, Plus Call Transfer	169
36	D.14	Speed Calling	170
37	D.15	Multiple Translations on Single System	171
38	D.16	Multiple Call Scenario	172
39	D.17	Simple Call Delivery to a Mobile Station	173
40	D.18	Password Call Acceptance and Flexible Alerting	175
41	D.19	Password Call Acceptance and Call Forwarding	176
42	D.20	Completed Call To Busy Subscriber	177
43	D.21	Dialed Feature Code Digits	178
44	D.22	Call Release to Pivot	178
45	D.23	Intrasystem Handoff	180
46	D.24	Handoff to a Third System without Path Minimization	180
47	D.25	Connected Party Modification	182
48			
49			
50			
51			
52			
53			
54	Annex E	Information Access Scenarios - J-STD-025-A	183
55	E.1	Conference Call	183
56	E.1.1	Conference Call (ConferencePartyChange using PartyIdentities)	183
57	E.1.2	Conference Call (ConferencePartyChange using CallIdentities)	188
58	E.1.3	Conference Call (Connection/ConnectionBreak using PartyIdentities)	192
59			

E.2	Call Waiting	195	1
E.2.1	Call Waiting with Recall (NetworkSignal and SubjectSignal)	196	2
E.3	Multi-stage Dialing (DialedDigitExtraction)	199	3
			4
Annex F	Optional Messages	201	5
F.1	ConnectionTest Message	201	6
			7
Annex G	LAES Administrative Interfaces	202	8
			9
Annex H	Possible e-Interface Delivery Methods for Packet Mode Telecommunications Services	203	10
			11
			12
H.1	Data Stream Framing Protocol Delivery Method	203	13
H.1.1	Introduction	203	14
H.1.2	Approach	203	15
H.1.2.1	Purpose	203	16
			17
H.1.3	Format	203	18
H.1.4	Rules	204	19
H.1.5	Re-synchronization	205	20
H.1.6	Short Application Messages	205	21
			22
Annex I	J-STD-025 Abstract Syntax	206	23
			24
Index	223	25
			26
			27
			28
			29
			30
			31
			32
			33
			34
			35
			36
			37
			38
			39
			40
			41
			42
			43
			44
			45
			46
			47
			48
			49
			50
			51
			52
			53
			54
			55
			56
			57
			58
			59

List of Tables

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59

Table 1:	Definitions and Acronyms matrix	44
Table 2:	Answer Message Parameters	51
Table 3:	CCClose Message Parameters	52
Table 4:	CCOpen Message Parameters	53
Table 5:	Change Message Parameters	54
Table 6:	ConferencePartyChange Message Parameters	55
Table 7:	Connection Message Parameters	56
Table 8:	ConnectionBreak Message Parameters	57
Table 9:	DialedDigitExtraction Message Parameters	58
Table 10:	NetworkSignal Message Parameters	61
Table 11:	Origination Message Parameters	62
Table 12:	PacketEnvelope Message Parameters	63
Table 13:	Redirection Message Parameters	64
Table 14:	Release Message Parameters	65
Table 15:	ServingSystem Message Parameters	65
Table 16:	SubjectSignal Message Parameters	67
Table 17:	TerminationAttempt Message Parameters	68
Table 18:	cdma2000PacketDataSessionEstablishment Message Parameters	70
Table 19:	cdma2000PacketDataSessionTermination Message Parameters	71
Table 20:	cdma2000PacketDataInterceptStart Message Parameters	72
Table 21:	cdma2000PacketDataServingSystem Message Parameters	73
Table 22:	cdma2000PacketDataPacketFilter Message Parameters	74
Table 23:	cdma2000® CLICHeader Parameters	75
Table 24:	IAP Primary Locations	103
Table 25:	Simple Switch Connections	145
Table 26:	Simple Abandoned Call Attempt Scenario	148
Table 27:	Partial Dial Abandon Scenario	148
Table 28:	Pre-Answer Abandon Scenario	149
Table 29:	Simple Outgoing Call Scenario	150
Table 30:	Alternate Steps for <i>en bloc</i> Sending	150
Table 31:	Re-origination Call Scenario	151
Table 32:	Alternate Re-origination Call Scenario Steps	152
Table 33:	Simple Incoming Call Scenario	152
Table 34:	Call Waiting with Recall Scenario with a Single Call Identity	154
Table 35:	Call Waiting with Recall with Separate Leg Identities Scenario	155
Table 36:	Call Waiting with Recall with Separate Calls Scenario	156
Table 37:	Call Waiting with Talking Party Disconnect and a Single Call Identity Scenario	158
Table 38:	Call Waiting with Talking Party Disconnect and Separate Leg Identities Scenario	159
Table 39:	Call Waiting with Talking Party Disconnect and Separate Calls Scenario	160
Table 40:	Call Held and Retrieved Scenario	161
Table 41:	Three-Way Calling with a Single Call Identity Scenario	162
Table 42:	Three-Way Calling Scenario with Separate Leg Identities	164
Table 43:	Three-Way Calling with Separate Call Scenario	165
Table 44:	Call Forwarding—No Answer on a Single System Scenario	167
Table 45:	Call Forwarding—No Answer on Different Systems Scenario	168
Table 46:	Two Bearer Channels, Plus Call Transfer Scenario	169
Table 47:	Speed Calling Scenario	170
Table 48:	Multiple Translations on a Single System Scenario	171
Table 49:	Multiple Call Scenario	172
Table 50:	Simple Call Delivery Scenario	173

<i>Table 51:</i>	Password Call Acceptance and Flexible Alerting Scenario	175	1
<i>Table 52:</i>	Password Call Acceptance and Call Forwarding Scenario	176	2
<i>Table 53:</i>	Completed Call To Busy Subscriber	177	3
<i>Table 54:</i>	Dialed Feature Code Digits Scenario	178	4
<i>Table 55:</i>	Call Release to Pivot Scenario	178	5
<i>Table 56:</i>	Intrasystem Handoff Scenario	180	6
<i>Table 57:</i>	Handoff to a Third System without Path Minimization Scenario	180	7
<i>Table 58:</i>	Connected Party Modification Scenario	182	8
<i>Table 59:</i>	Conference Call (ConferencePartyChange using PartyIdentities) Scenario	184	9
<i>Table 60:</i>	Conference Call (ConferencePartyChange using CallIdentities) Scenario	188	10
<i>Table 61:</i>	Conference Call (Connection/ConnectionBreak using PartyIdentities) Scenario . . .	192	11
<i>Table 62:</i>	Call Waiting with Recall Scenario	196	12
<i>Table 63:</i>	Multi-stage Dialing (DialedDigitExtraction) Scenario	199	13
<i>Table 64:</i>	ConnectionTest Message Parameters	201	14
<i>Table 65:</i>	Format of DSFP	203	15
			16
			17
			18
			19
			20
			21
			22
			23
			24
			25
			26
			27
			28
			29
			30
			31
			32
			33
			34
			35
			36
			37
			38
			39
			40
			41
			42
			43
			44
			45
			46
			47
			48
			49
			50
			51
			52
			53
			54
			55
			56
			57
			58
			59

List of Figures

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59

<i>Figure 1:</i>	Electronic Surveillance Model	21
<i>Figure 2:</i>	Call Content Channels and Call Data Channels	23
<i>Figure 3:</i>	Circuit IAP for a Two-Way Communication	29
<i>Figure 4:</i>	Circuit IAP for a Multi-Party Communication	30
<i>Figure 5:</i>	Circuit IAP for an Incoming Call	31
<i>Figure 6:</i>	Circuit IAP for a Redirected Call	32
<i>Figure 7:</i>	Packet Data IAP to a Separated CCC (appropriate to all data services)	35
<i>Figure 8:</i>	Packet Data IAP to a Combined CCC (connectionless data services only)	36
<i>Figure 9:</i>	Packet Data IAP to a CDC (for selected packet types)	37
<i>Figure 10:</i>	cdma2000® Wireless IP Network Access architecture	41
<i>Figure 11:</i>	Network Reference Model	47
<i>Figure 12:</i>	Land Line IAPs	103
<i>Figure 13:</i>	Mobile Intercept Subject's Home System IAPs	104
<i>Figure 14:</i>	Mobile Intercept Subject's Serving System IAPs	104
<i>Figure 15:</i>	Mobile Intercept Subject's Redirecting System IAPs	105
<i>Figure 16:</i>	External Delivery Function	105
<i>Figure 17:</i>	Integrated Delivery Function with a Non-Distinct Administration Interface	106
<i>Figure 18:</i>	Integrated Delivery Function with a Distinct Administration Interface	106
<i>Figure 19:</i>	Mobile Telephone Systems with Two TSPs	107
<i>Figure 20:</i>	Independently Administered External Pivoted Delivery	108
<i>Figure 21:</i>	A possible functional model for CALEA in Voice over Packet scenario	109
<i>Figure 22:</i>	Bridged Access	110
<i>Figure 23:</i>	Looped Access	111
<i>Figure 24:</i>	Possible Transmission Schemes for the e-Interface	112
<i>Figure 25:</i>	Possible CDC Protocol Stacks	113
<i>Figure 26:</i>	Possible Circuit-Mode CCC Protocol Stacks	115
<i>Figure 27:</i>	Possible Packet-Mode CCC Protocol Stacks	116
<i>Figure 28:</i>	Dedicated Circuit CCC Delivery	119
<i>Figure 29:</i>	Setup CCC Using Dedicated Circuits	120
<i>Figure 30:</i>	Associate CCC Using Dedicated Circuits	122
<i>Figure 31:</i>	Transfer Call Content Using Dedicated Circuits	122
<i>Figure 32:</i>	Disassociate CCC Using Dedicated Circuits	123
<i>Figure 33:</i>	Dedicated Circuit CCC Release	124
<i>Figure 34:</i>	Trunk Group CCC Delivery	124
<i>Figure 35:</i>	Setup CCCs Using a Trunk from a Trunk Group	125
<i>Figure 36:</i>	Acceptance of CCCs Using a Trunk of a Trunk Group	126
<i>Figure 37:</i>	DF Timed Refusal of a CCC Using a Trunk of a Trunk Group	127
<i>Figure 38:</i>	CF Timed Refusal of a CCC Using a Trunk of a Trunk Group	127
<i>Figure 39:</i>	DF Refusal of a CCC Using a Trunk of a Trunk Group	128
<i>Figure 40:</i>	CF Refusal of a CCC Using a Trunk of a Trunk Group	128
<i>Figure 41:</i>	CCC Continuity Test	129
<i>Figure 42:</i>	Transfer Call Content Using a Trunk in a Trunk Group	130
<i>Figure 43:</i>	Early Release of CCC Using a Trunk in a Trunk Group	130
<i>Figure 44:</i>	Release CCC Using a Trunk in a Trunk Group	131
<i>Figure 45:</i>	Static Directory Number CCC Delivery	132
<i>Figure 46:</i>	Setup Trunk to Destination	133
<i>Figure 47:</i>	Packet Data CCC Delivery	136
<i>Figure 48:</i>	Separated Content Delivery	138
<i>Figure 49:</i>	Combined Content Delivery	138
<i>Figure 50:</i>	Call Content Distribution	140

<i>Figure 51:</i> Pivoted Delivery with Distribution	140	1
<i>Figure 52:</i> Digit to DTMF Tone Mapping.	141	2
<i>Figure 53:</i> DTMF C-tone Signaling.	141	3
<i>Figure 54:</i> Dedicated Data Circuit CDC Delivery.	142	4
<i>Figure 55:</i> Dedicated Data Link CDC Delivery.	143	5
<i>Figure 56:</i> Switch Connection Diagram Conventions	145	6
<i>Figure 57:</i> LAES Object Tree	206	7
		8
		9
		10
		11
		12
		13
		14
		15
		16
		17
		18
		19
		20
		21
		22
		23
		24
		25
		26
		27
		28
		29
		30
		31
		32
		33
		34
		35
		36
		37
		38
		39
		40
		41
		42
		43
		44
		45
		46
		47
		48
		49
		50
		51
		52
		53
		54
		55
		56
		57
		58
		59

Foreword

This foreword is not part of this Standard.

The specification of interface compatibility requirements between telecommunication service providers (TSPs) and law enforcement agencies (LEAs) was developed as a Joint Standards Project between ANSI-Accredited Telecommunications Industry Association, Engineering Committee TR-45, and ANSI-Accredited Committee T1–Telecommunications.

This Standard defines the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance. A TSP, manufacturer, or support service provider that is in compliance with this Standard will have a “safe harbor” under Section 107 of the Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414: “a [TSP] shall be found to be in compliance with the assistance capability requirements under [CALEA] Section 103, and a manufacturer of telecommunication transmission or switching equipment or a provider of telecommunication support services shall be found in compliance with [CALEA] Section 106.”

There are ~~eight~~^{seven} annexes ~~in~~ to this Standard. All annexes are informative and are not considered part of this Standard.

J-STD-025-A provides the enhancements necessary to support FCC 99-230, CC Docket No. 97-213, Third Report and Order and FCC 02-108, CC Docket No. 97-213, Order on Remand¹. J-STD-025-B provides enhancements to further support lawfully authorized electronic surveillance of packet data telecommunication services (e.g., cdma2000® packet data).

The enhancements for J-STD-025-B are identified by underlined text. Strike-through text indicates deleted J-STD-025-A text.

All annexes are informative. Information contained in Annexes A through D, and F ~~and G~~ through H does not reflect additional terms, concepts, requirements, messages or parameters for capabilities added in J-STD-025-A as mandated in FCC 99-230, CC Docket No. 97-213 and FCC 02-108, CC Docket No. 97-213, Order on Remand. Annex E, Informative Access Scenarios - J-STD-025-A, is exclusively dedicated to J-STD-025-A scenarios. Annex I contains compilable ASN.1 code.

¹ The FCC Third Report and Order [FCC 99-230, CC Docket No. 97-213] introductory paragraph states the following:

“Specifically, we require that all capabilities of J-STD-025 (interim standard) and six of nine “punch list” capabilities requested by the Department of Justice (DoJ)/Federal Bureau of Investigation (FBI) be implemented by wireline, cellular, and broadband PCS carriers. While we are requiring that a packet-mode capability be implemented by such carriers, we are not at this time adopting technical requirements for packet-mode communications, but will permit packet-mode data to be delivered to law enforcement under the interim standard, discussed below, pending further study of packet-mode communications by the telecommunications industry.”

1 Introduction

1.1 General

This Standard defines the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance. A TSP, manufacturer, or support service provider that is in compliance with this Standard will have a “safe harbor” under Section 107 of the Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414: “a [TSP] shall be found to be in compliance with the assistance capability requirements under [CALEA] Section 103, and a manufacturer of telecommunication transmission or switching equipment or a provider of telecommunication support services shall be found in compliance with [CALEA] Section 106.”

J-STD-025-A provides the enhancements necessary to support FCC 99-230, CC Docket No. 97-213, Third Report and Order and FCC 02-108, CC Docket No. 97-213, Order on Remand¹. J-STD-025-B provides enhancements to further support lawfully authorized electronic surveillance of packet data telecommunication services (e.g., cdma2000® packet data).

As used in this Standard, electronic surveillance refers to the interception and monitoring of communications (i.e., call content), call-identifying information, or both, for a particular telecommunication subscriber as lawfully authorized. In this Standard intercept subject, or more simply a subject, is a telecommunication service subscriber whose communications, call-identifying information, or both, have been authorized by a court to be intercepted and delivered to an LEA. The identification of the subject is limited to identifiers used to access the particular equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity).

As a precondition for a TSP’s assistance with Lawfully Authorized Electronic Surveillance (LAES), an LEA must serve a TSP with the necessary legal authorization identifying the intercept subject, the communications and information to be accessed, and service areas where the communications and information can be accessed. Once this authorization is obtained, the TSP shall perform the access and delivery for transmission to the government’s procured equipment, facilities, or services.

LEAs recognize that in many instances the telecommunication services subscribed to by certain intercept subjects may permit a TSP to access and

1. The FCC Third Report and Order [FCC 99-230, CC Docket No. 97-213] introductory paragraph states the following:

“Specifically, we require that all capabilities of J-STD-025 (interim standard) and six of nine “punch list” capabilities requested by the Department of Justice (DoJ)/Federal Bureau of Investigation (FBI) be implemented by wireline, cellular, and broadband PCS carriers. While we are requiring that a packet-mode capability be implemented by such carriers, we are not at this time adopting technical requirements for packet-mode communications, but will permit packet-mode data to be delivered to law enforcement under the interim standard, discussed below, pending further study of packet-mode communications by the telecommunications industry.”

deliver communications and call-identifying information without the TSP having to modify its networks or systems. In these instances, the TSP may be fully compliant with the assistance capability requirements set forth in CALEA. For example, a TSP could effect a central office- or local loop-based interception using conventional methods of access and delivery and fully meet an LEA's electronic surveillance needs.

1.2 Purpose

The purpose of this Standard is to facilitate a TSP's compliance with the assistance capability requirements defined in Section 103 of CALEA. This Standard defines services and features to support LAES and the interfaces to deliver intercepted communications and call-identifying information to an LEA when authorized. This Standard also defines a protocol for delivering specific information elements to LEAs. Compliance with this Standard satisfies the "safe harbor" provisions of Section 107 of CALEA and helps ensure efficient and industry-wide implementation of the assistance capability requirements.

1.3 Scope

The scope of this Standard is to define the services to support LAES and the interface between a TSP and an LEA.

1.4 Organization

[Section 2 "References"](#) is a list of references used in the preparation of this Standard.

[Section 3 "Definitions and Acronyms"](#) defines words and acronyms that are used in this Standard.

[Section 4 "Stage 1 Description: User Perspective"](#) defines the LAES services from the user point of view. The user in this case is the LEA.

[Section 5 "Stage 2 Description: Network Perspective"](#) defines the network entities and information flows to implement LAES services from a network point of view.

[Section 6 "Stage 3 Description: Implementation Perspective"](#) defines the messages and information elements to implement LAES services from an implementation point of view.