TR-45

Lawfully Authorized Electronic Surveillance

PN-4465 - RV1

©Copyright Telecommunications Industry Association 1997-2003~~2~~

All rights reserved.

This document is subject to change.

PN-4465-RV1

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-025A 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 Remand.

PN-4465-RV1

Document Revision History

Revision	Date	Remarks
0	November 1997	Initial
A	~~April 2000~~ 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.
B		

PN-4465-RV1

Contents

Abstract iii

Document Revision History iv

Contents v

List of Tables xi

List of Figures xiii

Foreword xv

1 Introduction 1
- 1.1 General 1
- 1.2 Purpose 1
- 1.3 Scope 2
- 1.4 Organization 2

2 References 3

3 Definitions and Acronyms 5

4 Stage 1 Description: User Perspective 16
- 4.1 Overview 16
- 4.2 Introduction 16
  - 4.2.1 Assumptions 16
  - 4.2.2 General Background 18
  - 4.2.3 Call Content Channels and Call Data Channels 19
- 4.3 Non-Call Associated Information Surveillance Service Description—Serving System IAP 21
- 4.4 Call Associated Information Surveillance Service Description—Call-Identifying Information IAP 21
  - 4.4.1 Introduction 21
  - 4.4.2 Basic Circuit Calls 22
  - 4.4.3 Conference Call Party Changes 22
- 4.5 Call Associated and Non-Call Associated Information Surveillance Service Description 23
  - 4.5.1 Introduction 23
  - 4.5.2 Intercept Subject Signaling IAP 23
    - 4.5.2.1 Subject-initiated Dialing and Signaling 23
    - 4.5.2.2 Dialed Digit Extraction 24
  - 4.5.3 Network Signaling IAP 24
    - 4.5.3.1 In-band and Out-of-band Signaling 24
- 4.6 Content Surveillance Service Description 24
  - 4.6.1 Circuit IAP 25
  - 4.6.2 Conference Circuit IAP - Content of Subject-initiated Conference Calls 29
  - 4.6.3 Packet Data IAP 30
- 4.7 Timing Information 34
- 4.8 Restrictions 35
  - 4.8.1 Lack of CDC and CCC Synchronization 35
  - 4.8.2 CDC Congestion 35
  - 4.8.3 CCC Exhaustion 35
  - 4.8.4 CCC Congestion 35

PN-4465-RV1

4.9 Packet Mode Technology 36
4.9.1 Introduction and Scope 36
4.9.2 cdma2000 Packet Data 37
4.9.2.1 cdma2000 Packet Data System Reference Model 37
4.9.2.2 General Principles 39
4.9.2.3 Applicability to Telecommunications Services 40
4.9.2.4 Normal Operation - Intercept Events for Lawful Interception 40
4.9.3 GPRS/UMTS 41
4.9.4 Voice over Packet Technologies in Wireline Telecommunications Networks 42

5 Stage 2 Description: Network Perspective 43
5.1 Introduction 43
5.2 Stage 2 Methodology 43
5.3 Network Reference Model 44
5.3.1 Functional Entities 44
5.3.1.1 Access Function (AF) 44
5.3.1.2 Delivery Function (DF) 45
5.3.1.3 Collection Function (CF) 46
5.3.1.4 Service Provider Administration Function (SPAF) 46
5.3.1.5 Law Enforcement Administration Function (LEAF) 46
5.3.2 Interface Reference Points 46
5.3.2.1 Reference Point *a* 46
5.3.2.2 Reference Point *b* 46
5.3.2.3 Reference Point *c* 47
5.3.2.4 Reference Point *d* 47
5.3.2.5 Reference Point *e* 47
5.4 Message Descriptions 47
5.4.1 Answer 47
5.4.2 CCClose 48
5.4.3 CCOpen 49
5.4.4 Change 50
5.4.5 ConferencePartyChange 51
5.4.6 Connection 53
5.4.7 ConnectionBreak 53
5.4.8 DialedDigitExtraction 54
5.4.9 NetworkSignal 55
5.4.10 Origination 58
5.4.11 PacketEnvelope 59
5.4.12 Redirection 60
5.4.13 Release 61
5.4.14 ServingSystem 62
5.4.15 SubjectSignal 63
5.4.16 TerminationAttempt 64
5.5 Message descriptions for cdma2000 packet data 65
5.5.1 cdma2000PacketDataSessionEstablishment 66
5.5.2 cdma2000PacketDataSessionTermination 67
5.5.3 cdma2000PacketDataInterceptStart 68
5.5.4 cdma2000PacketDataServingSystem 69
5.5.5 cdma2000PacketDataPacketFilter 70
5.5.6 cdma2000InterceptionofContent 71

6 Stage 3 Description: Implementation Perspective 73
6.1 Protocol Definition 73

PN-4465-RV1

6.2 CDC Protocol Definition 73
6.2.1 CDC Underlying Data Transmission 73
6.2.2 CDC Parameter Encoding Objectives 73
6.2.3 CDC Syntax Definitions 74
6.3 CDC Message Definitions 74
6.3.1 Answer Message 76
6.3.2 CCClose Message 76
6.3.3 CCOpen Message 77
6.3.4 Change Message 77
6.3.5 ConferencePartyChange Message 78
6.3.6 Connection Message 79
6.3.7 ConnectionBreak Message 79
6.3.8 DialedDigitExtraction Message 79
6.3.9 NetworkSignal Message 80
6.3.10 Origination Message 81
6.3.11 PacketEnvelope Message 81
6.3.12 Redirection Message 83
6.3.13 Release Message 83
6.3.14 ServingSystem Message 84
6.3.15 SubjectSignal Message 84
6.3.16 TerminationAttempt Message 85
6.4 CDC Parameter Definitions 86
6.4.1 AlertingSignal 86
6.4.2 AudibleSignal 86
6.4.3 BearerCapability 87
6.4.4 CallIdentity 87
6.4.5 CaseIdentity 87
6.4.6 CCCIdentity 88
6.4.7 IAPSystemIdentity 88
6.4.8 Location 88
6.4.9 PartyIdentity 89
6.4.10 PDUType 90
6.4.11 RedirectedFromInformation 90
6.4.12 TerminalDisplayInfo 91
6.4.13 TimeStamp 91
6.4.14 TransitCarrierIdentity 91
6.5 cdma2000 Abstract Syntax for Packet Data CII Delivery 91
6.6 CCC Protocols 95
6.6.1 CCC Encoding for Circuit-Mode Services 95
6.6.2 CCC Encoding for Packet-Mode Services 95
6.6.2.1 cdma2000 Abstract Syntax Notation for Packet Data CC Delivery 95
6.7 LAESP Compatibility Guidelines 96
6.7.1 Guidelines For Forward Compatibility 97
6.7.2 Guidelines For Backward Compatibility 97
6.7.2.1 Existing Messages 97
6.7.2.2 Parameters in Existing Messages 98
6.7.2.3 New Messages 98
6.7.2.4 New Parameters 98
6.7.2.5 New Parameter Fields 98
6.7.2.6 New Parameter Values 99

Annex A Deployment Examples 100
A.1 Possible Network Deployment of IAPs 100

PN-4465-RV1

A.2 Access and Delivery Function Equipment Configuration 102
A.3 Implementation of the *d*-interface 106
A.4 Implementation of the *e*-interface 108
A.5 Possible CDC Protocol Stacks 110
A.6 Possible CCC Protocol Stacks 111

Annex B CCC Delivery Methods 114
B.1 Circuit-Mode vs. Packet-Mode 114
B.2 Overview 115
B.3 Dedicated Circuit CCC Delivery 116
B.3.1 Obtain Network Address of Destination 117
B.3.2 Setup CCC to Destination 117
B.3.3 Destination Acceptance or Refusal of a CCC 118
B.3.4 CCC Continuity Verification 118
B.3.5 Associate Intercept Subject and Call Identity to the CCC 119
B.3.6 Call Content Transfer 119
B.3.7 Early CCC Release by the Destination 120
B.3.8 Disassociate CCC 120
B.3.9 Normal CCC Release by the Source. 120
B.4 Trunk Group CCC Delivery 121
B.4.1 Obtain Network Address of Destination 122
B.4.2 Setup CCC to Destination 122
B.4.3 Destination Acceptance or Refusal of a CCC 123
B.4.4 CCC Continuity Verification 126
B.4.5 Associate Intercept Subject and Call Identity to the CCC 126
B.4.6 Call Content Transfer 127
B.4.7 Early CCC Release by the Destination 127
B.4.8 Disassociate CCC 128
B.4.9 Normal CCC Release by the Source 128
B.5 Static Directory Number CCC Delivery 129
B.5.1 Obtain Network Address of Destination 130
B.5.2 Setup CCC to Destination 130
B.5.3 Destination Acceptance or Refusal of a CCC 131
B.5.4 CCC Continuity Verification 131
B.5.5 Associate Intercept Subject and Call Identity to the CCC 131
B.5.6 Call Content Transfer 131
B.5.7 Early CCC Release by the Destination. 131
B.5.8 Disassociate CCC 132
B.5.9 Normal CCC Release by the Source 132
B.6 Packet Data CCC Delivery 132
B.6.1 Obtain Network Address of Destination 133
B.6.2 Setup CCC to Destination 133
B.6.3 Destination Acceptance or Refusal of a CCC 133
B.6.4 CCC Continuity Verification 133
B.6.5 Associate Intercept Subject and Call Identity to the CCC 134
B.6.6 Call Content Transfer 134
B.6.7 Early CCC Release by the Destination 134
B.6.8 Disassociate CCC 134
B.6.9 Normal CCC Release by the Source 134
B.7 Delivery Bearer Service 134
B.8 Separated Content Delivery 135
B.9 Combined Content Delivery 135
B.10 Signaling for Switched Delivery 136

PN-4465-RV1

B.11 Call Content Delivery Delay 136
B.12 Call Content Distribution 137
B.13 DTMF C-Tone Signaling Procedures 137

Annex C CDC Delivery Methods 139
C.1 Dedicated Data Circuit CDC Delivery 139
C.2 Dedicated Data Link CDC Delivery 140
C.3 Call Data Distribution 140

Annex D Information Access Scenarios 141
D.1 Simple Abandoned Call Attempt 145
D.2 Partial Dial Abandon 145
D.3 Pre-Answer Abandon 146
D.4 Simple Outgoing Call 147
D.5 Re-Origination 148
D.6 Simple Incoming Call 149
D.7 Call Waiting and Recall 150
D.7.1 Call Waiting and Recall with a Single Call Identity 151
D.7.2 Call Waiting and Recall with Separate Leg Identities 152
D.7.3 Call Waiting and Recall with Separate Calls 153
D.8 Call Waiting with Talking Party Disconnect 154
D.8.1 Call Waiting with Talking Party Disconnect and a Single Call Identity 155
D.8.2 Call Waiting with Talking Party Disconnect and Separate Leg Identities 156
D.8.3 Call Waiting with Talking Party Disconnect and Separate Calls 157
D.9 Call Held and Retrieved 158
D.10 Three-Way Calling, Plus Call Turned Away 159
D.10.1 Three-Way Calling, Plus Call Turned Away with a Single Call Identity 159
D.10.2 Three-Way Calling, Plus Call Turned Away with Separate Leg Identities 161
D.10.3 Three-Way Calling, Plus Call Turned Away with Separate Calls 162
D.11 Call Forwarding—No Answer on a Single System 164
D.12 Call Forwarding—No Answer on Different Systems 165
D.13 Two Bearer Channels, Plus Call Transfer 166
D.14 Speed Calling 167
D.15 Multiple Translations on Single System 168
D.16 Multiple Call Scenario 169
D.17 Simple Call Delivery to a Mobile Station 170
D.18 Password Call Acceptance and Flexible Alerting 172
D.19 Password Call Acceptance and Call Forwarding 173
D.20 Completed Call To Busy Subscriber 174
D.21 Dialed Feature Code Digits 175
D.22 Call Release to Pivot 175
D.23 Intrasystem Handoff 177
D.24 Handoff to a Third System without Path Minimization 177
D.25 Connected Party Modification 179

Annex E Information Access Scenarios - J-STD-025A 180
E.1 Conference Call 180
E.1.1 Conference Call (ConferencePartyChange using PartyIdentities) 180
E.1.2 Conference Call (ConferencePartyChange using CallIdentities) 185
E.1.3 Conference Call (Connection/ConnectionBreak using PartyIdentities) 189
E.2 Call Waiting 192
E.2.1 Call Waiting with Recall (NetworkSignal and SubjectSignal) 193

PN-4465-RV1

E.3 Multi-stage Dialing (DialedDigitExtraction) 196

Annex F Optional Messages 198
F.1 ConnectionTest Message 198

Annex G LAES Administrative Interfaces 199

Annex H Possible e-Interface Delivery Methods for Packet Mode Telecommunications Services .. 200
H.1 Data Stream Framing Protocol Delivery Method 200
H.1.1 Introduction 200
H.1.2 Approach 200
H.1.2.1 Purpose 200
H.1.3 Format 200
H.1.4 Rules 201
H.1.5 Re-synchronization 202
H.1.6 Short Application Messages 202

Annex I J-STD-025 Abstract Syntax 203

PN-4465-RV1

List of Tables

Table 1: Definitions and Acronyms matrix 41
Table 2: Answer Message Parameters 48
Table 3: CCClose Message Parameters 49
Table 4: CCOpen Message Parameters 50
Table 5: Change Message Parameters 51
Table 6: ConferencePartyChange Message Parameters 52
Table 7: Connection Message Parameters 53
Table 8: ConnectionBreak Message Parameters 54
Table 9: DialedDigitExtraction Message Parameters 55
Table 10: NetworkSignal Message Parameters 58
Table 11: Origination Message Parameters 59
Table 12: PacketEnvelope Message Parameters 60
Table 13: Redirection Message Parameters 61
Table 14: Release Message Parameters 62
Table 15: ServingSystem Message Parameters 62
Table 16: SubjectSignal Message Parameters 64
Table 17: TerminationAttempt Message Parameters 65
Table 18: cdma2000PacketDataSessionEstablishment Message Parameters 67
Table 19: cdma2000PacketDataSessionTermination Message Parameters 68
Table 20: cdma2000PacketDataInterceptStart Message Parameters 69
Table 21: cdma2000PacketDataServingSystem Message Parameters 70
Table 22: cdma2000PacketDataPacketFilter Message Parameters 71
Table 23: cdma2000 CLICHeader Parameters 72
Table 24: IAP Primary Locations 100
Table 25: Simple Switch Connections 142
Table 26: Simple Abandoned Call Attempt Scenario 145
Table 27: Partial Dial Abandon Scenario 145
Table 28: Pre-Answer Abandon Scenario 146
Table 29: Simple Outgoing Call Scenario 147
Table 30: Alternate Steps for *en bloc* Sending 147
Table 31: Re-origination Call Scenario 148
Table 32: Alternate Re-origination Call Scenario Steps 149
Table 33: Simple Incoming Call Scenario 149
Table 34: Call Waiting with Recall Scenario with a Single Call Identity 151
Table 35: Call Waiting with Recall with Separate Leg Identities Scenario 152
Table 36: Call Waiting with Recall with Separate Calls Scenario 153
Table 37: Call Waiting with Talking Party Disconnect and a Single Call Identity Scenario . . 155
Table 38: Call Waiting with Talking Party Disconnect and Separate Leg IdentitiesScenario . . 156
Table 39: Call Waiting with Talking Party Disconnect and Separate Calls Scenario 157
Table 40: Call Held and Retrieved Scenario 158
Table 41: Three-Way Calling with a Single Call Identity Scenario 159
Table 42: Three-Way Calling Scenario with Separate Leg Identities 161
Table 43: Three-Way Calling with Separate Call Scenario 162
Table 44: Call Forwarding—No Answer on a Single System Scenario 164
Table 45: Call Forwarding—No Answer on Different Systems Scenario 165
Table 46: Two Bearer Channels, Plus Call Transfer Scenario 166
Table 47: Speed Calling Scenario 167
Table 48: Multiple Translations on a Single System Scenario 168
Table 49: Multiple Call Scenario 169
Table 50: Simple Call Delivery Scenario 170

PN-4465-RV1

Table 51: Password Call Acceptance and Flexible Alerting Scenario 172
Table 52: Password Call Acceptance and Call Forwarding Scenario 173
Table 53: Completed Call To Busy Subscriber 174
Table 54: Dialed Feature Code Digits Scenario 175
Table 55: Call Release to Pivot Scenario 175
Table 56: Intrasystem Handoff Scenario 177
Table 57: Handoff to a Third System without Path Minimization Scenario 177
Table 58: Connected Party Modification Scenario 179
Table 59: Conference Call (ConferencePartyChange using PartyIdentities) Scenario 181
Table 60: Conference Call (ConferencePartyChange using CallIdentities) Scenario 185
Table 61: Conference Call (Connection/ConnectionBreak using PartyIdentities) Scenario . . . 189
Table 62: Call Waiting with Recall Scenario 193
Table 63: Multi-stage Dialing (DialedDigitExtraction) Scenario 196
Table 64: ConnectionTest Message Parameters 198
Table 65: Format of DSFP 200

PN-4465-RV1

List of Figures

Figure 1: Electronic Surveillance Model 18
Figure 2: Call Content Channels and Call Data Channels 20
Figure 3: Circuit IAP for a Two-Way Communication 26
Figure 4: Circuit IAP for a Multi-Party Communication 27
Figure 5: Circuit IAP for an Incoming Call 28
Figure 6: Circuit IAP for a Redirected Call 29
Figure 7: Packet Data IAP to a Separated CCC (appropriate to all data services) 32
Figure 8: Packet Data IAP to a Combined CCC (connectionless data services only) 33
Figure 9: Packet Data IAP to a CDC (for selected packet types) 34
Figure 10: cdma2000 Wireless IP Network Access architecture 38
Figure 11: Network Reference Model 44
Figure 12: Land Line IAPs 100
Figure 13: Mobile Intercept Subject's Home System IAPs 101
Figure 14: Mobile Intercept Subject's Serving System IAPs 101
Figure 15: Mobile Intercept Subject's Redirecting System IAPs 102
Figure 16: External Delivery Function 102
Figure 17: Integrated Delivery Function with a Non-Distinct Administration Interface 103
Figure 18: Integrated Delivery Function with a Distinct Administration Interface 103
Figure 19: Mobile Telephone Systems with Two TSPs 104
Figure 20: Independently Administered External Pivoted Delivery 105
Figure 21: A possible functional model for CALEA in Voice over Packet scenario 106
Figure 22: Bridged Access 107
Figure 23: Looped Access 108
Figure 24: Possible Transmission Schemes for the *e*-Interface 109
Figure 25: Possible CDC Protocol Stacks 110
Figure 26: Possible Circuit-Mode CCC Protocol Stacks 112
Figure 27: Possible Packet-Mode CCC Protocol Stacks 113
Figure 28: Dedicated Circuit CCC Delivery 116
Figure 29: Setup CCC Using Dedicated Circuits 117
Figure 30: Associate CCC Using Dedicated Circuits 119
Figure 31: Transfer Call Content Using Dedicated Circuits 119
Figure 32: Disassociate CCC Using Dedicated Circuits 120
Figure 33: Dedicated Circuit CCC Release 121
Figure 34: Trunk Group CCC Delivery 121
Figure 35: Setup CCCs Using a Trunk from a Trunk Group 122
Figure 36: Acceptance of CCCs Using a Trunk of a Trunk Group 123
Figure 37: DF Timed Refusal of a CCC Using a Trunk of a Trunk Group 124
Figure 38: CF Timed Refusal of a CCC Using a Trunk of a Trunk Group 124
Figure 39: DF Refusal of a CCC Using a Trunk of a Trunk Group 125
Figure 40: CF Refusal of a CCC Using a Trunk of a Trunk Group 125
Figure 41: CCC Continuity Test 126
Figure 42: Transfer Call Content Using a Trunk in a Trunk Group 127
Figure 43: Early Release of CCC Using a Trunk in a Trunk Group 127
Figure 44: Release CCC Using a Trunk in a Trunk Group 128
Figure 45: Static Directory Number CCC Delivery 129
Figure 46: Setup Trunk to Destination 130
Figure 47: Packet Data CCC Delivery 133
Figure 48: Separated Content Delivery 135
Figure 49: Combined Content Delivery 135
Figure 50: Call Content Distribution 137

PN-4465-RV1

Figure 51: Pivoted Delivery with Distribution 137
Figure 52: Digit to DTMF Tone Mapping 138
Figure 53: DTMF C-tone Signaling 138
Figure 54: Dedicated Data Circuit CDC Delivery 139
Figure 55: Dedicated Data Link CDC Delivery 140
Figure 56: Switch Connection Diagram Conventions 142
Figure 57: LAES Object Tree 203

PN-4465-RV1

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 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 this Standard. All annexes are informative and are not considered part of this Standard

J-STD-025A 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 Remand.

<u>The enhancements to J-STD-025B are identified by underlined text.</u>

Information contained in Annexes A through D, F ~~and G~~ <u>through H</u> does not reflect additional terms, concepts, requirements, messages or parameters for capabilities added in J-STD-025A as mandated in FCC 99-230, CC Docket No. 97-213 and FCC 02-108, CC Docket No. 97-213, Order on Remand.

PN-4465-RV1

(This page intentionally left blank.)

PN-4465-RV1

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-025A 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 Remand.

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 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

PN-4465-RV1

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.

PN-4465-RV1

2 References

The documents that are referenced herein are for the sole purpose of identifying related normative reference sources and were used in the formulation of this standard. There are no direct or indirect claims regarding the property rights, legal or regulatory status of those documents listed.

103rd Congress

Communications Assistance for Law Enforcement Act, Public Law 103-414, 108 STAT. 4279 (Oct. 25, 1994).

International Telecommunications Union (ITU) standards:

[G.711] ITU-T Recommendation G.711, *Pulse Code Modulation (PCM) of Voice Frequencies.*

[X.208] ITU-T Recommendation X.208, *Specification of Abstract Syntax Notation One (ASN.1).*

[X.209] ITU-T Recommendation X.209, *Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

[Q.931] ITU-T Recommendation Q.931, *ISDN User-network Interface Layer 3 Specification for Basic Call Control.*

[X.25] ITU-T Recommendation X.25, *Interface Between Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit.*

American National Standards Institute (ANSI) T1 and TIA standards:

[T1.607] ANSI T1.607, *Integrated Services Digital Network (ISDN)—Layer 3 Signaling Specification for Circuit-Switched Bearer Service for Digital Subscriber Signaling System Number 1 (DSS1).*

[ANSI-41] ANSI/TIA/EIA-41-D, *Cellular Radiotelecommunictions Intersystem Operations, Telecommunications Industry Association*, 1997.

[T1.678] ANSI T1.678-2003, *American National Standard for Telecommunications - Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks.*

PN-4465-RV1

Federal Communications Commission (FCC):

[99-230] FCC 99-230, CC Docket 4/11/02.No. 97-213, Third Report and Order, Released 8/31/99.

[02-108] FCC 02-108, CC Docket No. 97-213, Order on Remand, Released 4/11/02.

Telcordia Publications:

[GR-506] GR-506-CORE, *LSSGR: Signaling for Analog Interfaces (A Module of the LATA Switching Systems Generic Requirements [LSSGR]*, FR-64, January 1, 1999), Issue 1, June 1996, Revision 1, November 1996.

[GR-268] GR-268-CORE, *ISDN Basic Rate Interface Call Control Switching and Signaling Generic Requirements*, Issue 1, July 1998.

[TR-444] TR-NWT-000444, *Switching System Requirements Supporting ISDN Access Using the ISDN User Part*, Issue 3, May 1993.

~~European Telecommunications Standards Institute (ETSI)~~:

3rd Generation Partnership Project (3GPP):

[GSM 02.40] GSM 02.40, *Digital cellular telecommunications system (Phase 2+); Procedure for call progress indications, Release 1998.*

[3G TS 33.106] 3rd Generation Partnership Project; *Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Requirements.*

[3G TS 33.107] 3rd Generation Partnership Project; *Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Architecture and Functions.*

[3G TS 33.108] 3rd Generation Partnership Project: *Technical Specification Group Services and System Aspects: 3G Security; Handover interface for Lawful Interception.*

Internet Engineering Task Force (IETF):

[IP] RFC791, *Internet Protocol*, 09-01-1981.

[PPP] RFC1661, *Point-to-Point Protocol*, 07-1994.

PN-4465-RV1

3 Definitions and Acronyms

abandoned: a call attempt that is released by the originating party before it is answered.

access: the technical capability to interface with a communications facility, such as a communications line or switch, so that intercepted call-identifying information and call content can be delivered to an LEA.

AF: Access Function.

agent: a network-based service or device that acts on behalf of a subscriber to send or receive communications (e.g., an interactive screening service, a reminder service, a delayed transmission service).

AMPS: Advanced Mobile Phone System, one of several wireless access methods.

ANSI: American National Standards Institute.

answering party: the party answering a call. This party may be different from the called party (e.g., a called number may alert a number of stations and the answering party may be any one of the alerting stations).

ASN.1: Abstract Syntax Notation One.

associate: a telecommunication user whose equipment, facilities, or services are communicating with a subject.

ATM: Asynchronous Transfer Mode.

B-channel: a 56- or 64-kbps ISDN Bearer channel.

BER: Basic Encoding Rules.

BRI: ISDN Basic Rate Interface consisting of two 64-kbps B-channels and one 16-kbps D-channel.

CALEA: Communications Assistance for Law Enforcement Act.

call: a sequence of events beginning with an initial connection or facility request and ending with the final release of all facilities used. A call may have one or more legs.

call appearance: an instance of a possible call with direct subscriber control. A party with three call appearances may be involved in and control three calls simultaneously. Some services, such as call forwarding, do not consume call appearances, because the subscriber cannot directly control the call.

call content: see content.

call content channel (CCC): the logical link between the device performing an electronic surveillance access function and the LEA that primarily carries the call content passed between an intercept subject and one or more associates.

PN-4465-RV1

call data channel (CDC): the logical link between the device performing an electronic surveillance access function and the LEA that primarily carries call-identifying information.

call deflection: allows the called party to interactively refuse an incoming call and send that call to another directory number, to voice mail, or to an announcement.

call delivery: redirects an incoming call to a mobile subscriber.

call diversion: is similar to call forwarding, except that the condition may be more complex and dynamic (e.g., its routing decisions may be based upon calling party number, calling party entry of a valid password, time-of-day, day-of-week, day-of-year, calling party location).

call forwarding: any of several features that redirect a call to another directory number (or voice mail), if a certain condition is met.

call-identifying information: defined in CALEA Section 102 (2) to be "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a [TSP]." Call-identifying information is "reasonably available" to a TSP if it is present at an intercept access point and can be made available without the carrier being unduly burdened with network modifications.

As defined in FCC 02-108, CC Docket 97-213: **destination** is a party or place [(e.g. network switch)] to which a call is being made (e.g., called party); **direction** is a party or place to which a call is re-directed or the party or place from which it came, either incoming or outgoing (e.g., re-directed-to party or redirected-from party); **origin** is a party initiating a call (e.g., calling party) or a place from which a call is initiated; and **termination** is a party or place at the end of the communication path (e.g., the called or call-receiving party, or the switch of a party that has placed another party on hold).

call management server (CMS): a core network functional entity whose function includes sending and receiving signaling and call control information (e.g., H.323 and SIP messages) for the management of a call to and from endpoints (e.g., Mobile Station.)

call transfer: allows a controlling subscriber to connect two other parties and then the controlling subscriber leaves the call.

called party: the destination party of a call.

calling party: the originating party of a call.

CCC: call content channel.

CCIR: International Telecommunications Union—Radio Sector.

CCITT: International Telecommunications Union—Telecommunications Standardization Sector.

CCT: Composite CDMA/TDMA, one of several wireless access methods.

PN-4465-RV1

CDMA: Code Division Multiple Access, one of several wireless access methods.

CDC: call data channel.

cell: in a wireless system, the sub-area to which a set of radio resources is allocated.

CF: Collection Function.

channel: an independent path for communicating between two points.

CIAP: Circuit Intercept Access Point.

circuit: a switchable bi-directional path between two locations. A circuit may be all or part of a channel. On an end-to-end circuit, separate physical facilities may be used for each segment of the circuit.

circuit-mode: a communication using bi-directional paths switched or connected when the communication is established. The entire communication uses the same path.

CMS: Call Management Server.

collection function: defined in FCC 99-230, CC Docket No. 97-213 to be "the location where lawfully authorized intercepted communications and call-identifying information is collected by a law enforcement agency (LEA)."

Commission: defined in CALEA Section 102 (3) to be "the Federal Communication Commission."

communication: in this Standard, communication refers to any wire or electronic communication, as defined in 18 USC 2510.

communication-identifying information: see call-identifying information.

communication intercept: see intercept.

communication session: a period of time over which the authorized intercept subject is allowed to use service provider network resources for the purpose of sending or receiving packets.

complete: a call attempt that is answered.

connection: a relationship between two or more parties of a call to allow communication between them.

content: defined in 18 USC 2510 (8) to be "when used with respect to any wire or electronic communications, includes any information concerning the substance, purport, or meaning of that communication."

content of subject-initiated conference calls: defined in FCC 99-230, CC Docket No. 97-213 to be the capability that permits an LEA to monitor the content of conversations by all parties connected via a conference call when the facilities under surveillance maintain a circuit connection to the call.

controlling party: the party invoking a feature.

PN-4465-RV1

core network: A portion of the delivery system composed of networks, system equipment, and infrastructures, connecting the service providers to the access network[1].

CSU: Channel Service Unit.

cut-through, full: completion of a connection in both directions.

cut-through, partial: completion of a connection in one direction, usually to allow the calling party to monitor call progress tones from the called end.

D-channel: a 16- or 64-kbps ISDN channel carrying control and signaling information and, optionally, packetized information and telemetry.

DC: direct current; a signaling method for representing the switchhook state of an instrument to the other end of a call using voltage or current on metallic interfaces or the "A" signaling bit on a DS-0 interface.

destination: see call-identifying information.

DF: Delivery Function.

dialed digit extraction: defined in FCC 99-230, CC Docket No. 97-213 to be the capability that permits an LEA to receive on the call data channel digits dialed by a subject when a call is connected to another TSP's service for processing and routing.

direction: see call-identifying information.

disconnect: a request from one of the parties of the call to release all or part of a connection.

DN: Directory Number

DSU: Data Service Unit.

DTMF: Dual-Tone Multi-Frequency.

electronic communications: defined in 18 USC 2510 (12) to be "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system."

electronic messaging services: defined in CALEA Section 102 (4) to be "software-based services that enable the sharing of data, images, sound, writing, or other information among computing devices controlled by the senders or recipients of the messages."

electronic storage: defined in 18 USC 2510 (17) to be "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

1. ITU-T Y.101 [2000, page 24].

PN-4465-RV1

electronic surveillance: the statutory-based legal authorization, process, and associated technical capabilities and activities of LEAs related to the interception of wire, oral, or electronic communications while in transmission. As used herein, also includes the acquisition of call-identifying information. As used in this Standard, *surveillance* refers to a single communication intercept, pen register, or trap and trace. Its usage in this Standard does not include administrative subpoenas for obtaining a subscriber's toll records and information about a subscriber's service that an LEA may employ before the start of a communication intercept, pen register, or trap and trace.

ESN: Electronic Serial Number.

feature code: the digits used to invoke or access a feature.

FG-D: Feature Group D

FQDN: Fully Qualified Domain Name

fully qualified domain name: the full name of a system, consisting of its local hostname and its domain name, including a top-level domain (tld). For example, "venera" is a hostname and "venera.isi.edu" is an FQDN. An FQDN should be sufficient to determine a unique Internet address for any host on the Internet.

functional entity: a system or subsystem capable of providing a defined service. A functional entity may be implemented as a separate physical entity or it may be incorporated with other functional entities in a common physical entity.

government: defined in CALEA Section 102 (5) to be "the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any State or political subdivision thereof authorized by law to conduct electronic surveillance."

GSM: Global System for Mobile Communications.

handoff: in a wireless system, the switching of the transmission means used by a call in progress without disruption of this call. Within this Standard handoff is synonymous with handover.

HDLC: High-level Data Link Control.

HLR: Home Location Register.

Home Location Register (HLR): the location register to which a user identity is associated with subscriber information (e.g. equipment identification, directory number, profile information, current Serving System, validation period). The HLR may serve more than one MSC. The HLR may be distributed over more than one physical entity.

Home System: the TSP system where a subscriber's subscription information is retained.

Hz: Hertz or cycles per second.

IAP: Intercept Access Point.

PN-4465-RV1

IDIAP: Call-Identifying Information Intercept Access Point.

idle state: a state in which there is no active communication path between a subscriber and the network (e.g., while on-hook).

IMEI: International Mobile Equipment Identifier.

IMSI: International Mobile Station Identifier.

IN: intelligent network.

in-band and out-of-band signaling: defined in FCC 99-230, CC Docket No. 97-213 to be the capability that permits an LEA to be informed when a network message that provides call-identifying information (e.g., ringing, busy, call waiting signal, message light) is generated or sent by the IAP switch to a subject using the facilities under surveillance. Excludes signals generated by customer premises equipment when no network signal is generated.

incomplete: a call attempt that cannot be routed to its destination (or answered).

information service: defined in CALEA Section 102 (6) to be "(A) the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunication; and (B) includes—(i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; (ii) electronic publishing; and (iii) electronic messaging services; but (C) does not include any capability for a [TSP's] internal management, control, or operation of its telecommunication network." see telecommunication service provider.

intercept: defined in 18 USC 2510 (4) to be "the aural or other acquisition of the content of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."

Intercept Access Point (IAP): a point within a telecommunication system where some of the communications or call-identifying information of an intercept subject's equipment, facilities and services are accessed.

intercept agent: see agent.

intercept subject: 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).

IP: Internet Protocol.

ISDN: Integrated Services Digital Network.

ISLP: Inter-System Link Protocol.

ISUP: ISDN User Part.

ITU-R: International Telecommunications Union - Radio Sector (formerly CCIR).

PN-4465-RV1

ITU-T: International Telecommunications Union - Telecommunications Standardization Sector (formerly CCITT).

kbps: kilobits (1000 bits) per second.

LAES: Lawfully Authorized Electronic Surveillance.

LAESP: LAES Protocol.

LAPB: Link Access Protocol—Balanced.

LAPD: Link Access Protocol—D-channel.

Law Enforcement Agency (LEA): a government entity with the legal authority to conduct electronic surveillance (e.g., the Federal Bureau of Investigation or a local police department).

LE: Law Enforcement.

LEA: Law Enforcement Agency.

LEAF: Law Enforcement Administration Function.

leg: a bi-directional call path associated with each network facility usage attempt and subsequent usage.

LPP: Lightweight Presentation Protocol.

MF: Multi-Frequency.

MIN: Mobile Identification Number.

mobile station (MS): The MS is a telephone set using a radio link with a public or non-public base station to access telephone network services.

Mobile Switching Center (MSC): The MSC is an automatic system which constitutes the interface for user traffic between the wireless (cellular or PCS) network and other public switched networks, or other MSCs in the same or other wireless networks.

MS: Mobile Station.

MSC: Mobile Switching Center.

MSISDN: Mobile Station International Subscriber Directory Number.

MTP: Message Transfer Part.

NAMPS: Narrow AMPS, one of several wireless access methods.

network address: an address appropriate to a particular network, e.g., a directory number for the PSTN, an X.121 address for an X.25 network, or an IP address for the Internet.

off-hook: the state of a telephone instrument indicating a readiness for service; the DC signaling of the readiness for service state.

on-hook: the state of a telephone instrument indicating a request for service disconnect, release, or service idleness; the DC signaling for service disconnect, release, or service idleness.

origin: see call-identifying information.

PN-4465-RV1

origination: an outgoing call attempt.

packet-mode: a communication where individual packets or virtual circuits of a communication within a physical circuit are switched or routed by the accessing telecommunication system. Each packet may take a different route through the intervening network(s).

PACS: Personal Access Communications System, one of several wireless access methods.

party hold, join, drop on conference calls: defined in FCC 99-230, CC Docket No. 97-213 to be the capability that permits an LEA to identify the parties to a conference call conversation at all times.

PCM: pulse code modulation.

PCS: Personal Communications Service.

PCS1900: one of several GSM-based wireless systems.

PDIAP: Packet Data Intercept Access Point.

PDU: Protocol Data Unit.

pen register: defined in 18 USC 3127 (3) to be "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business."

personal mobility: the ability of a user to access telecommunication services at any terminal on the basis of a personal identifier, and the capability of the network to provide those services according to the user's service profile. Personal mobility involves the network capability to locate the terminal associated with the user for the purposes of addressing, routing, and charging of the user's calls.

POTS: Plain Old Telephone Service. This usually refers to loop start lines with DTMF (tone) dialing or decadic (rotary) dialing.

PPP: Point-to-Point Protocol.

PRI: ISDN Primary Rate Interface consisting of twenty-three 64-kbps B-channels and one 64-kbps D-channel.

PSTN: Public Switched Telephone Network.

pulse code modulation (PCM): a method for communicating audio information using a 56 or 64 kbps digital bit stream. In the United States most PCM is encoded using the μlaw rules.

Redirecting System: the TSP system where incoming calls bound to a subscriber arrive for redirection instruction. This is called an Originating System in *TIA/EIA-41*, although the calls may be originated on another system.

PN-4465-RV1

recall: the alerting of a party in response to a previous call (e.g., *hold recall* alerts the controlling party after leaving a party on hold for a period of time, *transfer recall* alerts the controlling party when the transfer attempt has not been answered, *automatic recall* alerts the calling party of a previous call attempt).

registration: in wireless systems, the process that informs the Home System of the location and presence of a mobile station.

release: to place facilities used for a connection in the idle state where they can be used for other connections.

roaming: in a wireless system, the movement of a mobile station within or between wireless service areas where the mobile station can be located and can receive service.

Serving System: the TSP system currently providing telecommunication service to a subscriber, especially a roaming mobile subscriber.

short message service (SMS): a packet-mode data service, intended for transmission of small data messages, for wireless subscribers.

SLIP: Serial Link Internet Protocol.

SMS: short message service.

SPAF: Service Provider Administration Function.

SPID: Service Profile Identifier.

SSIAP: Serving System Identification Intercept Access Point.

subject: see intercept subject.

subject-initiated dialing and signaling information: defined in FCC 99-230, CC Docket No. 97-213 to be the capability that permits an LEA to be informed when a subject using the facilities under surveillance uses services that provide call-identifying information, such as call forwarding, call waiting, call hold, and three-way calling. Excludes signals generated by customer premises equipment when no network signal is generated [(i.e., when no subject-initiated signal is generated to the network)].

surveillance: within this Standard surveillance refers to electronic surveillance; see electronic surveillance.

SVC: Switched Virtual Circuit.

TCP: Transmission Control Protocol.

TDMA: Time Division Multiple Access, one of several wireless access methods.

TEI: Terminal Equipment Identity.

PN-4465-RV1

telecommunication service provider[1] **(TSP):** defined from CALEA Section 102 (8) to be, "a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire, and includes 1) a person or entity engaged in providing commercial mobile service, or 2) a person or entity engaged in providing wire or electronic communications switching or transmission service to the extent that the Commission finds such service is a replacement for a substantial portion of local telephone exchange service and that it is in the public interest to deem such a person or entity to be a [TSP] for purposes of this title. This does not include 1) persons or entities insofar as they are engaged in providing information services, and 2) any class or category of [TSPs] that the Commission exempts by rule after consultation with the U. S. Attorney General."

telecommunication support services: defined in CALEA Section 102 (7) to be "a product, software, or service used by a [TSP] for the internal signaling or switching functions of its telecommunication network."

terminal mobility: the ability of a terminal to access telecommunications services from different locations and while in motion, and the capability of the network to identify, locate, and communicate with that terminal. Terminal mobility while not on a call may involve *roaming*, or while on a call may involve *handoff*.

termination: an incoming call attempt. see also call-identifying information.

timing information: defined in FCC 99-230, CC Docket No. 97-213 to be the capability that permits an LEA to associate call-identifying information with the content of a call. A call-identifying message must be sent from the carrier's IAP to the LEA's Collection Function within eight seconds of receipt of that message by the IAP at least 95% of the time, and with the call event timestamped to an accuracy of at least 200 milliseconds.

transmission: the act of transferring communications from one location or another by a wire, radio, electromagnetic, photoelectronic, or photo-optical system.

transparent: end-to-end transmission without insertion or loss of information.

trap and trace device: defined in 18 USC 3127 (4) to be ~~"a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted."~~

"a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonable likely to identify the source of a wire of electronic communication, provided, however, that such information shall not include the contents of any communication".

1. This Standard uses the term *telecommunication service provider* instead of the CALEA term *telecommunication carrier*.

PN-4465-RV1

TSP: telecommunication service provider.

unobtrusive: not undesirably noticeable or blatant; inconspicuous; within normal call variances.

URL: Uniform Resource Locator.

USC: United States Code.

user-to-user signaling: a bi-directional packet-mode data service for wireline subscribers.

UTC: Coordinated Universal Time (as defined by the CCIR (ITU-R)).

virtual circuit: a packet-mode connection between two end-points. A virtual circuit may be *permanent* (with only a data transfer phase) or *switched* (with setup, data transfer, and release phases).

VoP: Voice over Packet.

WCDMA: Wideband Code Division Multiple Access, one of several wireless access methods.

wire communications: defined in 18, USC 2510 (1) to be "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication."

wireless: refers to cellular or personal communication service (PCS).

wireline: refers to traditional wire-based telephone service.

PN-4465-RV1

4 Stage 1 Description: User Perspective

This section describes the features and services of LAES from a user's perspective. In this case the user is the LEA and its monitoring equipment. The features and services are described with enough detail to let LEAs know what information can be collected and when it can be collected.

4.1 Overview

This Standard defines the means to access communications as an intercept access service. The services fall into four categories:

- non-call associated services to provide information about intercept subjects that is not necessarily related to a call (see 4.3);
- call associated services to provide call-identifying information about calls involving the intercept subjects (see 4.4);
- call associated and non-call associated services to provide subject and network signaling call-identifying information (see 4.5); and
- content surveillance services to provide access to an intercept subject's communications (see 4.6).

Timing information requirements are defined for call-identifying messages (see 4.7).

Restrictions are defined for exceptions (see 4.8).

4.2 Introduction

4.2.1 Assumptions

LAES capabilities allow a TSP to deliver the intercepted call content (e.g., voice, packet data, modem data) and call-identifying information to an authorized LEA.

Content: is defined in 18 USC 2510 (8) to be "when used with respect to any wire or electronic communications, includes any information concerning the substance, purport, or meaning of that communication."

Call-identifying information: is defined in CALEA Section 102 (2) to be "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a [TSP]."

As defined in FCC 02-108, CC Docket 97-213: **destination** is-a party or place [(e.g. network switch)] to which a call is being made (e.g., called party); **direction** is a party or place to which a call is re-directed or the party or place from which it came, either incoming or outgoing (e.g., redirected-to party or redirected-from party); **origin** is a party initiating a call (e.g., calling party) or a place from which a call is initiated; and **termination** is a party or place at

PN-4465-RV1

the end of the communication path (e.g., the called or call-receiving party, or the switch of a party that has placed another party on hold).

Call-identifying information is *reasonably available* if the information is present at an Intercept Access Point (IAP) for call processing purposes. With respect to the matters before the FCC in FCC 99-230, CC Docket No. 97-213, the commission has provided the following additional guidance: call-identifying information is "reasonably available" to a TSP if it is present at an intercept access point and can be made available without the TSP being unduly burdened with network modifications. Network protocols (except LAESP) do not need to be modified solely for the purpose of passing call-identifying information. The specific elements of call-identifying information that are reasonably available at an IAP may vary between different technologies and may change as technology evolves.

The terms *call content* and *call-identifying information* are used throughout this Standard. The term *call* in this Standard is intended to be used in a generic sense to denote a communication and is not limited to circuit-mode or connection-oriented communications.

Not all information delivered to law enforcement is call-identifying information or call content.

Call identities are used to correlate call-identifying information and call content.

For interception to occur at an IAP, each intercept subject under surveillance must be readily identifiable within the network by identifiers appropriate and available to that IAP for that technology (e.g., IP address, URLs). For interception of a communication involving an intercept subject, the communication must be reasonably available at the IAP. Therefore, a call involving an intercept subject can be intercepted at an Intercept Access Point if and only if that intercept subject is reasonably identifiable at that IAP.

Synchronization of network element time-of-day clocks is not required.

There is no requirement to provide message integrity to ensure that the message has not been altered in transmission.

There is no requirement to provide message sender authentication to ensure the integrity of message sender identification.

Reporting of network signaling applied toward the associate is not required.

Whenever a capability is described in this Standard, it is assumed that LEAs shall order and acquire adequate capacity in a timely manner for the capability to be performed.

It is recognized that the interception of packet data to meet CALEA requirements may require more or different physical and logical resources than are

PN-4465-RV1

required for circuit switched interception. The amount of resources required to meet LE capacity needs may not be the same as the circuit switched solution.

The call-identifying and call content information can only be delivered by a system for activities on that system (e.g., home system, serving system).

This document defines requirements and capabilities to support lawfully authorized electronic surveillance of packet-mode telecommunications services as required by CALEA in order to serve as a standardized method to meet CALEA obligations for such services. References in this document to a specific packet-mode data protocol or technology do not imply that any person or entity utilizing the referenced protocol or technology is or is not a Telecommunications Carrier nor do such references imply implicitly or explicitly the applicability of assistance capability requirements set forth in Section 103 of CALEA to such person or entity.

The requirements of the Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414, Section 103, Subsection a (Capability requirements) do not apply to information services.

4.2.2 General Background

The intercept function is viewed as five broad categories: access, delivery, collection, service provider administration, and law enforcement administration. These functions are discussed functionally without regard to their implementation. The relationships between these functional categories are shown in Figure 1.

Figure 1: **Electronic Surveillance Model**

The Access Function, consisting of one or more Intercept Access Points (IAPs), isolates an intercept subject's communications or call-identifying

PN-4465-RV1

information unobtrusively. The IAPs may vary between TSPs and may not be available on all systems.

To address the requirements in FCC 99-230, CC Docket No. 97-213, new IAPs have been defined (i.e., Intercept Subject Signaling, Network Signaling, Conference Circuit). In general, these IAPs indicate new, additional intercept functionality, and not specific implementations. Vendor and TSP implementations may satisfy these requirements by consolidating the various IAP functionalities.

The Delivery Function is responsible for delivering intercepted communications to one or more Collection Functions. The Delivery Function delivers information over two distinct types of channels: Call Content Channels (CCCs) and Call Data Channels (CDCs). The CCCs are generally used to transport call content, such as voice or data communications. The CDCs are generally used to transport messages which report call-identifying information, such as the calling party identities and called party identities.

The Collection Function is responsible for collecting and analyzing intercepted communications and call-identifying information. The Collection Function is the responsibility of the LEA. It is assumed that the LEA collection equipment maintains current state information concerning the associations between call identities and party identities and between call identities and CCC identities based on the messages delivered to the Collection Function. The collection equipment assumes that the last reported association remains in effect until a subsequent LAES message explicitly changes that association.

The Service Provider Administration Function is responsible for controlling the TSP Access and Delivery Functions.

The Law Enforcement Administration Function is responsible for controlling the LEA Collection Function. The Law Enforcement Administration Function is the responsibility of the LEA.

The lawful authorization, while neither a network entity nor an interface reference point, is an important part of LAES. No intercepts shall take place without specific lawful authorization.

4.2.3 Call Content Channels and Call Data Channels

A TSP is required to provide access to the communications and call-identifying information for particular intercept subjects.

A subject's call content is generally transported to the LEA over one or more CCCs. The actual number of CCCs will vary with each electronic surveillance according to the number of CCCs ordered by the LEA. Factors influencing this number are the subject's bearer capabilities, the subject's call capabilities, the type of communication being intercepted, the type and capacity of individual CCCs, the number of possible call appearances, and the subject's call-related activities. CCCs shall be provisioned as *combined* (i.e.,

PN-4465-RV1

carrying both the transmit and receive paths on one channel) or *separated* (i.e., using independent channels for the transmit and receive paths). Each CCC for an electronic surveillance must be capable of transporting one or more of the subject's intercepted bearer services. For some types of applications used by the subject (e.g., short message service), the call content may be transported over the CDC.

Additional CCCs shall be used (up to the number provisioned for a particular electronic surveillance) when the CCCs currently open are incompatible with the bearer services being intercepted. An example of this situation could be when a subject initiates a voice call, optionally places that call on hold, and initiates a second call using a different bearer service (e.g., fax or data).

The type of CCC delivered to an LEA may be influenced by the subject's bearer services, the manner in which the subject's call content is accessed, the preferences of the TSP, and the preferences of the LEA conducting the electronic surveillance. Communications that inherently use separate transmit and receive communications paths require separated CCCs. Other communications inherently combine the transmit and receive paths (or assume that the paths may be combined), so combined CCCs may be appropriate.

Call-identifying information is formatted into discrete messages using a specialized protocol called the Lawfully Authorized Electronic Surveillance Protocol (LAESP). The LAESP messages shall be transported to an LEA over a CDC. As defined in this Standard, a single CDC may support the delivery of LAESP messages for one or more electronic surveillances to a particular LEA collection facility.

The CDCs and CCCs shall use separate logical channels as shown in Figure 2. The CDC and CCC(s) may be transported to an LEA over separate or common physical facilities. The CDCs may be multiplexed onto one or more physical facilities.

Figure 2: **Call Content Channels and Call Data Channels**

Rare circumstances dictate that the call-identifying information, call content, or both, associated with a particular subject need to be delivered to more than one LEA Collection Function simultaneously. This will occur when different LEAs are conducting independent investigations on the same subject. The Delivery Function shall duplicate the call content, call-identifying information, or both, and deliver only authorized information. No more than five

PN-4465-RV1

Collection Functions are required to be supported for any single intercept subject. Separate circuits should be used to deliver the call content and call-identifying information to each LEA. The delivery options may be different for each path between an Access Function and a Collection Function.

Each CCC has a unique identity that is mutually agreed upon by the TSP and the LEA. The identity may be for a particular dedicated nailed up circuit, a dynamically allocated trunk member, or a directory number used for a switched connection. Each CCC may use a variety of physical implementations between the TSP and the LEA, but each CCC shall be uniquely identified.

4.3 Non-Call Associated Information Surveillance Service Description—Serving System IAP

Non-call associated information surveillance services access information within telecommunication systems. Information may be retrieved from existing messages and signaling or it may be derived from other information.

The Serving System Identification IAP (SSIAP) is the only non-call associated information IAP identified. The SSIAP shall report with a ServingSystem message the identification of the TSP providing service to a subject using a terminal or personal mobility service.

The serving system identification information includes the identity of the current system assigned to provide service for the mobile. Information regarding the occurrence of the event (e.g., identification of the system providing the intercept access, time, date) should be included. In some situations the Serving System may be identified with a directory number (e.g., when a mobile station registers to a personal base station).

In J-STD-025A, SSIAP is an identified non-call associated information IAP. See section 4.5 “Call Associated and Non-Call Associated Information Surveillance Service Description” on page 23.

4.4 Call Associated Information Surveillance Service Description—Call-Identifying Information IAP

4.4.1 Introduction

Call associated information surveillance services access information pertaining to call and service processing. This may span several functional entities.

The Call-Identifying Information IAP (IDIAP) is the only call associated information IAP identified. It provides expeditious access to the reasonably available call-identifying information for calls made by an intercept subject or for calls made to an intercept subject. This includes abandoned and incom-

PN-4465-RV1

plete call attempts and calls that are redirected (e.g., diverted, forwarded, or deflected) by the intercept subject's equipment, facilities, or services.

A call event is a user action or signal that may cause a call state change. These events are not intended to reflect a particular technology, but to describe the event in general.

The IAP shall access the call-identifying information for the intercept subject unobtrusively. Access to call-identifying information shall not deny the availability of any service to either the subject or associates.

In J-STD-025A, the IDIAP is an identified call-identifying IAP. See section 4.5 "Call Associated and Non-Call Associated Information Surveillance Service Description" on page 23.

4.4.2 Basic Circuit Calls

The following call events are defined for circuit-mode calls only:

Answer

A party has answered the call attempt.

Change

The identity(ies) of a call has been merged with the identity(ies) of other call(s) or split into multiple call identities.

Origination

The system has routed a call dialed by the subject or the system has translated a number for the subject.

Redirection

A call has been redirected (e.g., forwarded, diverted, or deflected).

Release

The facilities for the entire call have been released.

TerminationAttempt

A call attempt to an intercept subject has been detected.

4.4.3 Conference Call Party Changes

With respect to the matters before the FCC in FCC 99-230, CC Docket No. 97-213, the following has been added to this Standard:

PN-4465-RV1

The IDIAP provides conference call party change call-identifying information through the Party Hold, Join, Drop On Conference Calls service. This service permits an LEA to identify the parties to a subject-initiated conference call conversation at all times. The Party Hold, Join, Drop On Conference Calls capability is not required for two-party calls.

The IDIAP shall provide conference call party change call-identifying information of intercept subject calls to an On-demand Multi-Party (i.e., Meet Me) conference bridge, as it would be presented to the intercept subject (i.e., in a two-way communication) because no network signal would be generated to indicate intercept subject access and control of the conference feature.

4.5 Call Associated and Non-Call Associated Information Surveillance Service Description

4.5.1 Introduction

The Intercept Subject Signaling IAP (ISSIAP) and the Network Signaling IAP (NSIAP) provide access to call and non-call associated information surveillance services within a telecommunications system. They provide expeditious access to call and non-call associated signaling information. The ISSIAP provides access to intercept subject-initiated dialing and signaling information used to access features and services in a call or non-call associated form, including post cut-through digits dialed by the subject when a call is connected to another TSP's service for processing and routing. The NSIAP provides access to call-identifying network signaling information sent by the IAP to the subject to apply network signals (e.g., busy tone, reorder tone, call waiting tone).

The IAPs shall continue to access the signaling information for the intercept subject unobtrusively. Access to signaling information shall not deny the availability of any service to either the subject or associates.

4.5.2 Intercept Subject Signaling IAP

The following two subsections define call or non-call associated events for circuit-mode communications only.

4.5.2.1 Subject-initiated Dialing and Signaling

With respect to the matters before the FCC in FCC 99-230, CC Docket No. 97-213, the following has been added to this Standard:

This service permits an LEA to be informed when a subject using the facilities under surveillance uses services that provide call-identifying information, such as call forwarding, call waiting, call hold, and three-way calling. It excludes signals generated by customer premises equipment when no network signal is generated [(i.e., when no subject-initiated signal is generated to the network)].

PN-4465-RV1

4.5.2.2 Dialed Digit Extraction

With respect to the matters before the FCC in FCC 99-230, CC Docket No. 97-213, the following has been added to this Standard:

This service permits an LEA to receive, on the call data channel, digits dialed by a subject when a call is connected to another TSP's service for processing and routing. However, this service does not require a TSP to assure that a connection is with another TSP's service.

With respect to the matters before the FCC in FCC 02-108, CC Docket Number 97-213 (released 4/11/02), the following has been added to this Standard:

TSPs must have the equipment and software to support a dialed digit extraction capability with a toggle feature.

4.5.3 Network Signaling IAP

The following subsection defines call or non-call associated events for circuit-mode communications only.

4.5.3.1 In-band and Out-of-band Signaling

With respect to the matters before the FCC in FCC 99-230, CC Docket No. 97-213, the following has been added to this Standard:

This service permits an LEA to be informed when a network message that provides call-identifying information (e.g., busy, reorder, ringing, alerting, message waiting tone or visual indication, call waiting, calling or redirecting name/number information, displayed text) is generated or sent by the IAP switch to a subject using the facilities under surveillance. It excludes signals generated by customer premises equipment when no network signal is generated.

4.6 Content Surveillance Service Description

The IAPs for content surveillance are used to access the communications of an intercept subject. The content extracted by a content surveillance IAP shall be delivered over a CCC or CDC. The IAPs may be dynamically added or dropped as necessary to access the communications of the intercept subject.

The following categories of content IAPs have been defined (for a discussion of circuit-mode vs. packet-mode see Annex B.1):

- Circuit IAP;
- Conference Circuit IAP; and
- Packet Data IAP.

PN-4465-RV1

The IAPs for content surveillance shall access the transmissions to and from the intercept subject unobtrusively. Access to call content shall not deny the availability of any service to either the subject or associates.

Content surveillance services provide access to calls at the IAP. Abandoned or incomplete calls may also be accessed.

A TSP shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the TSP and the TSP possesses the information necessary to decrypt the communication.

The call-identifying information associated with the circuit-mode content surveillance is provided on the CDC by an IDIAP.

4.6.1 Circuit IAP

The Circuit IAP (CIAP) shall access the call content of circuit-mode communications to or from the equipment, facilities, or services of an intercept subject. This may include incoming calls to an intercept subject before they are answered and calls to an intercept subject that are redirected to another party. Loss of any portion (i.e., the beginning, middle, or end) of call content should not occur between call completion (answer) and call release. Call content may be delivered before answer and may include call progress tones or announcement.

Multiple CIAPs may be necessary for intercept subjects with multiple terminals or for terminals or services supporting multiple call appearances.

An idle CCC shall be selected from the CCCs available for this intercept subject and the selected destination. The selection criteria should use all CCCs on a regular basis.

PN-4465-RV1

Figure 3 shows the basic CIAP to access a two-way communication.[1]

Figure 3: **Circuit IAP for a Two-Way Communication**

1. The symbols used in Figure 3 represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

PN-4465-RV1

The Circuit IAP (CIAP) shall access a multi-party circuit-mode communication (e.g., Three-Way Calling, Conference Calling, or Meet Me Conferences) as it would be presented to the intercept subject. This is depicted in Figure 4.[1]

Figure 4: **Circuit IAP for a Multi-Party Communication**

In J-STD-025A, the Circuit IAP (CIAP) shall access the call content of On-demand Multi-Party (i.e., Meet Me Conference) circuit-mode communications as it would be presented to the intercept subject (i.e., two-way communication) because no network signal would be generated to indicate intercept subject access and control of the conference feature. Otherwise, Meet Me Conference calls are outside the scope of this standard. Figure 4 depicts how a CIAP may access the call content of multi-party circuit-mode communications.

1. The symbols used in Figure 4 represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

PN-4465-RV1

The CIAP may access a call to the intercept subject before the intercept subject answers, as shown in Figure 5.[1] This may provide access to call progress tones or announcements played toward the calling party. Normally the calling party is not cut-through and is not accessible until the call is answered. This access may be independent of the intercept subject, in that the intercept subject may be engaged in other services or communicating with other parties while the incoming call is accessed.

If the call is answered by the network for user interaction; (e.g., to request a personal identification number (PIN), password, or extension number), both the transmit and receive communication paths should be accessed.

Figure 5: **Circuit IAP for an Incoming Call**

1. The symbols used in Figure 5 represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

PN-4465-RV1

The CIAP shall access a call redirected by the intercept subject. Redirection includes any rerouting of a call, for example, call delivery, call forwarding, call deflection, or call diversion. This access is independent of the intercept subject, as the intercept subject may engage in another communication or service at any time while a redirected call is in progress as shown in Figure 6.[1]

Figure 6: **Circuit IAP for a Redirected Call**

4.6.2 Conference Circuit IAP - Content of Subject-initiated Conference Calls

With respect to the matters before the FCC in FCC 99-230, CC Docket No. 97-213, the following has been added to this Standard:

The Conference Circuit IAP (CCIAP) shall provide the Content of Subject-Initiated Conference Calls service (i.e., Three-Way Calling, Multi-Way Calling). This multi-party service permits an LEA to monitor the content of conversations by all parties connected to a subject-initiated conference call when the facilities under surveillance maintain a circuit connection to the call. Figure 4 depicts how a CCIAP may access the call content of multi-party circuit-mode communications.

The CCIAP shall continue to deliver content on subject-initiated multi-party conference calls when the subject has placed the conference call on hold. Call content for a single party on hold is not required to be delivered to law enforcement.

1. The symbols used in Figure 6 represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

PN-4465-RV1

4.6.3 Packet Data IAP

A Packet Data IAP (PDIAP) shall access data packets sent or received by the equipment, facilities, or services of an intercept subject when a packet-mode data service is provided. PDIAPs may be on the Serving System or on the Redirecting System. An IAP on the Redirecting System is only able to access some packets delivered to the intercept subject (and possibly none of the packets originated by the intercept subject).

If lawful interception is activated when a packet data service is already in use, interception should be initiated expeditiously. If lawful interception is deactivated during a packet data service, interception should be discontinued in an expeditious manner.

Packets shall be sent to the Collection Function when they are intercepted. The intercepted packets shall be delivered without interpretation or modification, except for possible re-framing, segmentation, or enveloping required to transport the information to the Collection Function or except to remove information that is not authorized.

A TSP shall not be responsible for interpreting the protocols beyond those protocols being processed by the TSP. A TSP shall not be responsible for decrypting or decompressing, or ensuring the government's ability to decrypt or decompress, any communication encrypted or compressed by a subscriber or customer, unless the encryption or compression was provided by the TSP and the TSP possesses the information necessary to decrypt or decompress the communication. A TSP that provides the government with information about how to decrypt or decompress a communication (e.g., identifying the type of compression software used to compress the communication, directing the government to the appropriate vendor that can provide decryption or decompression equipment, or providing the encryption key used to encrypt the communication) fully satisfies its obligation under the preceding sentence.

The access includes all packet-mode data transmissions regardless of their outcome. Interception of packet communications does not constitute a guarantee that the intercepted packets were also received by the terminating system (i.e., subject, associate). For example, when an SMS packet to a Mobile Station (MS) is intercepted, it is not known whether the packet was actually received by the MS.

When using the CCC delivery method (see Annex B "CCC Delivery Methods" on page 114) only the packets transmitted to, or received from the intercept subject under surveillance shall be delivered to the LEA.

PN-4465-RV1

A Packet Data IAP (PDIAP) provides access to one or more of the following packet-mode data services:

- ISDN user-to-user signaling;
- ISDN D-channel X.25 packet services;
- Short Message Services (SMS) for cellular and Personal Communication Services (e.g., NAMPS, *TIA/EIA-41*, PCS1900, or GSM-based technologies);
- wireless packet-mode data services (e.g., Cellular Digital Packet Data (CDPD), CDMA, TDMA, PCS1900, or GSM-based packet-mode data services);
- X.25 services;
- IP services;
- paging (one-way or two-way); and
- packet-mode data services using traffic channels.

PN-4465-RV1

Separated CCCs may be used to transport packet data to the Collection Function as shown in Figure 7.[1]

Figure 7: **Packet Data IAP to a Separated CCC (appropriate to all data services)**

1. The symbols used in Figure 7 represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

PN-4465-RV1

Connectionless data services may use separated delivery as shown above or they may use combined delivery as depicted in Figure 8.[1]

Figure 8: **Packet Data IAP to a Combined CCC (connectionless data services only)**

1. The symbols used in Figure 8 represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

PN-4465-RV1

Certain intercepted packets may be delivered over a CDC using PacketEnvelope messages as shown in Figure 9.[1]

Figure 9: **Packet Data IAP to a CDC (for selected packet types)**

4.7 Timing Information

With respect to the matters before the FCC in FCC 99-230, CC Docket No. 97-213, the following has been added to this Standard:

This capability permits an LEA to associate call-identifying information with the content of a call. A call-identifying message must be sent from the TSP's IAP to the LEA Collection Function within eight seconds of receipt of that message by the IAP at least 95% of the time, and with the call event time-stamped to an accuracy of at least 200 milliseconds.

This capability places timing requirements on call-identifying message generation after triggering events that shall be met for these messages. It also requires time stamp accuracy for call events.

1. The symbols used in Figure 9 represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

PN-4465-RV1

4.8 Restrictions

4.8.1 Lack of CDC and CCC Synchronization

The CDC and CCC information will not necessarily be synchronized when received by an LEA. The call content and call-identifying information are delivered to an LEA using the independent services of the CCCs and CDCs respectively, and these services can be provided on independent networks (e.g., dedicated circuits for the CCC and switched packet network delivery for the CDC).

4.8.2 CDC Congestion

When the call-identifying information intercept communication resources (e.g., CDCs) are limited, the communications are accessed on a first-in, first-out, non-queued basis. If a particular CDC is congested and the associated buffers (if any) are full, messages destined to that CDC may be discarded by the originating end. Unavailability or congestion of a CDC shall not affect other CCCs or CDCs.

4.8.3 CCC Exhaustion

When the call content intercept communication resources (e.g., CCCs) are limited, the communications are accessed on a first-come, first-served, non-queued basis. In other words, CCCs are assigned as they are needed. If a CCC is needed and none is available, that request is ignored, even if a CCC should subsequently become available during the communication pertaining to that request. The CCC may remain unused until the next request for a CCC for the subject is received. Unavailability of a CCC shall not affect other CCCs or CDCs.

Channels dedicated to a particular subject shall not be used for other subjects.

4.8.4 CCC Congestion

For CCCs used for packet-mode delivery, the bandwidth available depends upon the communication facilities and also upon concurrent traffic. If a packet-mode CCC toward the Collection Function becomes congested, intercepted packets may be discarded. Congestion of a CCC shall not affect other CCCs or CDCs.

PN-4465-RV1

4.9 Packet Mode Technology

Requirements specified in sections 1-4 of this document apply to packet based communications except where expressly stated otherwise.

4.9.1 Introduction and Scope

Packet Data LAES service shall provide the following interception functions:

- Call-identifying information only;
- Both call content and call-identifying information.

In cases where the TSP that provides an intercept subject's physical interface to the packet network is separated from the TSP that provides the packet-based communications service for which the intercept subject is under LAES, the capability to provide lawful access to communications content and communication-identifying information resides with the TSP that offers the packet-based communications service to the intercept subject *for that service*. This is based on the assumption that the TSP described here has been provided with lawful authorization and would have access to the appropriate identifiers for the intercept subject.

The material in this subsection is intended to provide a set of requirements covering packet-based telecommunications independent of technology or architecture. However, specific requirements might not apply to all of the technologies or services discussed in subsequent subsections of 4.9, depending on the characteristics of the technology or service and availability within the interception architecture.

The TSP shall provide LEAs with communication-identifying information for communications generated by or destined to the intercpet subject, regardless of whether or not those communications are successful.

When authorized, the TSP shall provide LEAs with communications content for communications generated by or destined to the intercept subject, including communications that have been redirected or have multiple communication recipients, when known by the TSP.

For interception to occur at an IAP, each intercept subject under surveillance must be readily identifiable within the network by identifiers appropriate and available to that IAP for that technology (e.g., IP address, URLs).

For interception of a communication involving an intercept subject, the communication must be reasonably available at the IAP.

Therefore, a call involving an intercept subject can be intercepted at an Intercept Access Point if and only if that intercept subject is reasonably identifiable at that IAP.

PN-4465-RV1

When the information is reasonably available at the IAP, the packet data LAESP shall indicate to the LEA the characteristics negotiated with the user (e.g.,codec, compression, bandwidth, type of session) for a call or session.

Packet data LAES service shall address packet mode services in which: (1) packet communication sessions are established by a Call Management Server (CMS), and (2) packet communication sessions established without a CMS.

The establishment, change, or release of a communication session across the accessing system or network from the subject's device to another network (not the endpoint) may be reported. Specific information describing these events may be reported on a technology specific basis.

4.9.2 cdma2000 Packet Data

This section describes the architecture and functional requirements for lawful interception of packet data within a third generation wireless system based on cdma2000 technology. An interception service is defined for a cdma2000 packet data system that provides support for the lawful interception of CII and CC for cdma2000 packet data services.

4.9.2.1 cdma2000 Packet Data System Reference Model

This section defines an interception service for a cdma2000 packet data system. The cdma2000 packet data system is described in TIA/EIA/IS-835, "cdma2000 Wireless IP Network Standard". The standard specifies three IP access services: Simple IPv4, Simple IPv6 and Mobile IPv4. The cdma2000 wireless IP architecture is shown in Figure 10 below. The Home Agent (HA) is not used for Simple IPv4 and Simple IPv6 access.

PN-4465-RV1

Figure 10: **cdma2000 Wireless IP Network Access architecture**

The LAES service, as provided by the standard LAES reference model (Section 4.2.2) is applicable to the cdma2000 packet data system. The following functional entities described by the LAES model may be applicable to the cdma2000 packet data system:

- Adf: The Service provider Administrative Function
- AF: The Access Function
- DF: The Delivery Function.

These functional entities are described in Section 5.3.1.1 “Access Function (AF)”, Section 5.3.1.2 “Delivery Function (DF)”, and Section 5.3.1.4 “Service Provider Administration Function (SPAF)” of this document and are shown in Figure 1.

4.9.2.1.1 Simple IP and Mobile IP

The three types of IP access services, namely Simple IPv4, Simple IPv6 and Mobile IPv4, can be described as follows:

Simple IPv4 access: the user establishes a Point-to-Point (PPP) link with the Packet Data Serving Node (PDSN) and uses a local IPv4 address provided by the PDSN to access the IPv4 network following successful authentication and authorization by the home network. The MS retains its assigned IPv4 address

PN-4465-RV1

for the lifetime of the PPP session. If the user moves to a new PDSN, the MS must initiate a new PPP connection with the new PDSN and the user will not be able to maintain the IPv4 address.

Simple IPv6 access: the user establishes a Point-to-Point (PPP) link with the Packet Data Serving Node (PDSN). Following successful authentication and authorization by the home network, the MS creates a link local IPv6 address from the interface identifier that was syuccesssfully negotiated with the PDSN. The MS also creates a global scope IPv6 address with the /64 globally unique prefix that the PDSN assigned for that PPP link. The MS retains its assigned /64 globally unique prefix for the lifetime of the prefix as indicated in the Router Advertisement from the PDSN. If the user moves to a new PDSN, the MS must initiate a new PPP connection with the new PDSN and the user may not be able to maintain the IPv6 address.

Mobile IPv4 access: The user establishes a PPP link with the PDSN and registers with the HA in the home network following successful user authentication and authorization by the home network. The user uses a home IPv4 address to access the IPv4 network. The HA maintains the Mobile IPv4 binding information for the MS and forwards data packets to the PDSN where the MS is currently registered.

The user uses either a static or dynamic IPv4 address belonging to its home IPv4 network. That is, the MS maintains a persistent IPv4 address even when handing off between radio networks connected to different PDSNs. This allows the users to sustain outgoing applications while roaming between IPv4 networks.

Based on the required CII, different network elements in the cdma2000 wireless IP network may be used as IAPs.

4.9.2.2 General Principles

The cdma2000 wireless network shall provide access to the intercepted CC and CII of the intercept subject on behalf of LEAs.

An intercept subject in a given cdma2000 network can be a subscriber of that cdma2000 network, or a user roaming from another cdma2000 network or from any other network capable of using that cdma2000 network. The intercepted CC and the CII can only be delivered for activities on that given cdma2000 network.

For interception, there needs to be a means of identifying the intercept subject. Subscriber identities used in the cdma2000 packet data system for interception of packet data shall be based on the intercept subject's identity (e.g., IMSI[1], Network Access Identifier (NAI), assigned IPv4 address, or assigned /64 globally unique prefix for IPv6 access).

1. IMSI is available for IX RTT access.

PN-4465-RV1

If the IAP is multicast aware, then the IAP reports multicast packets transmitted to or from an intercept subject if reasonably available at the IAP.

If the IAP is multicast aware, then the IAP reports multicase packets transmitted to or from an intercept subject i f reasonable available at the IAP.

4.9.2.3 Applicability to Telecommunications Services

The requirement for LAES service is that all telecommunications services using the CDMA2000 packet data standards should be capable of meeting the requirements within this section.

4.9.2.4 Normal Operation - Intercept Events for Lawful Interception

In general, the lawful interception service in a cdma2000 packet data system should be invoked when the IAP detects the following events that involves the intercept subject (e.g., the establishment of a packet data session, the transmission of CC).

The IAP shall report CII for the following cdma2000 packet data service events within a cdma2000 packet data system:

1. Successful or Unsuccessful (as defined in Table 18) packet data session establishment. If successful - reports the establishment of Simple IPv4 or Simple IPv6 or Mobile IPv4 packet data session. If unsuccessful - reports the reason for the failure of the packet data establishment attempt.
2. Packet data sessions are terminated - reports the end of a Simple IPv4 or Simple IPv6 or Mobile IPv4 packet data session.
3. Interception is started and at least one packet data session has previously been established - reports the start of interception for each established packet data session when at least one packet data session is already established, if the information is reasonably available at the IAP. There may be cases (e.g., handoff) where it may not be possible to report this event due to the lack of information at the IAP.
4. Serving system is changed - reports the identity of the system currently serving the intercept subject.
5. Packet filter event - reports the setup[1]/change/release of a particular packet filter.

The IAP shall report CC, when authorized, for the following cdma2000 packet data service events within a cdma2000 packet data system:

1. The Packet filter is a container that carries information to uniquely identify an IP flow. These fields are populated by extracting some of the parameters from IP/UDP headers of the packets for a particular flow. These parameters are used in the cdma2000 network to classify IP flows received from the Internet destined for a mobile station.

PN-4465-RV1

- User data packets are detected - reports data packets transmitted to or received from an intercept subject.

4.9.3 GPRS/UMTS

See 3rd Generation Partnership Project (3GPP) in the references section for information on lawful interception for GPRS/UMTS. Lawful intercept solutions for packet data and IP Multi-Media services, which includes VoP services, are defined in the specifications.

Table 1: **Definitions and Acronyms matrix**

J-STD-025B		3GPP specs.	
-	Call Content	CC	Content of Communication
CCC	Call Content Channel	-	Handover Interface port 3
CDC	Call Data Channel	-	Handover Interface port 2
CF	Collection Function	LEMF	Law Enforcement Monitoring Facility
-	Call-identifying Information	IRI	Intercepted Related Information
-	Call-identifying message	-	IRI record
DF	Delivery Function	-	Delivery Function/Mediation Function
-	a-interface	-	X1_1 interface
-	b-interface	-	HI1 interface
-	c-interface	-	X1_2 and X1_3 interfaces
-	d-interface	-	X2 and X3 interfaces
-	e-interface	HI	Handover Interface (HI2 and HI3)
IAP	Intercept Access Point	ICE+INE	Intercepting Control Element + Intercepting Network Element
-	Intercept Subject	-	Target
LAES	Lawfully Authorized Electronic Surveillance	LI	Lawful Intercept
-	CaseIdentity	LIID	Lawful Intercept IDentifier
LEAF	Law Enforcement Administration Function	ADMF	Administrative Function
SPAF	Service Provider Administrative Function	ADMF	Administration Function
-	SystemIdentity	NID	Network IDentifier
TSP	Telecommunication Service Provider	NVO/AP/ SvP	Network Operator/Access Provider/Service Provider

PN-4465-RV1

4.9.4 Voice over Packet Technologies in Wireline Telecommunications Networks

Editor's Note - Depending upon the reality that exists at the conclusion of the ballot, text option 1 **or** 2 will be included by the secretariat for publication. Option 1 text is to be included if the specification in preparation within T1S1 is complete and available for publication, while option 2 text is to be included if the specification is not yet ready for publication. Note 1

Option 1:

Specification of the unique aspects (i.e., those not common to all technologies, which is covered elsewhere in J-STD-025-B) of lawful interception for voice over packet technologies in wireline telecommunications networks is found in [T1.678].

Option 2:

Specification of the unique aspects (i.e., those not common to all technologies, which is covered elsewhere in J-STD-025-B) of lawful interception for Voice over Packet Technologies in Wireline Telecommunications Networks is under development by Technical Subcommittee T1S1 of the ATIS-sponsored Standards Committee T1-Telecommunications, accredited by ANSI.

PN-4465-RV1

5 Stage 2 Description: Network Perspective

5.1 Introduction

This section describes the information flows between the Access, Delivery, and Collection Functions to support LAES. The information flows are usually described as messages and information carried by a message.

5.2 Stage 2 Methodology

This section describes the methodology and organization for the development of the Stage 2 network perspective descriptions. A network reference model is developed and then information flows between functional entities over reference points are described.

Information is described in terms of a causing event and information associated with that event. Within each service description there is a set of events to support the particular service and a data dictionary to define a set of information elements to support the events.

Stage 2 for LAES CDCs deals with the movement of information between the Access, Delivery, and Collection Functions. The CDC Stage 2 description focuses on the information being transferred, rather than the transfer mechanism.

CCCs shall be delivered to LEAs using protocols as specified in Section 6.6.

PN-4465-RV1

5.3 Network Reference Model

The Network Reference model, as shown in Figure 11, consists of a set of functional entities and interface reference points between some of those functional entities. The functional entities provide the functions of the system, and an interface reference point allows information to be exchanged between the two functional entities connected by the interface reference point.

Figure 11: **Network Reference Model**

5.3.1 Functional Entities

5.3.1.1 Access Function (AF)

The Access Function, through its constituent Intercept Access Points (IAPs), is responsible for providing access to an intercept subject's communications, call-identifying information, or both.

PN-4465-RV1

The Access Function typically includes the ability:

- to access intercept subject's call-identifying information unobtrusively and make the information available to the Delivery Function;
- to access intercept subject call content unobtrusively and make the call content available to the Delivery Function; and
- to protect (e.g., prevent unauthorized access, manipulation, and disclosure) intercept controls, intercepted call content and call-identifying information consistent with TSP security policies and practices.

5.3.1.2 Delivery Function (DF)

The Delivery Function is responsible for delivering intercepted communications and call-identifying information to one or more Collection Functions.

The Delivery Function typically includes the ability:

- to accept call content for each intercept subject over one or more channels from the Access Function(s);
- to deliver call content for each intercept subject over one or more CCCs to a Collection Function;
- to accept call-identifying or packet-mode content information for each intercept subject over one or more channels and deliver that information to the Collection Function over one or more CDCs;
- to ensure that the call-identifying information and call content delivered to a Collection Function is authorized for a particular LEA;
- to duplicate and deliver authorized call-identifying information and content for the intercept subject to one or more Collection Functions (up to a total of five); and
- to protect (e.g., prevent unauthorized access, manipulation, and disclosure) intercept controls, intercepted call content and call-identifying information consistent with TSP security policies and practices.

PN-4465-RV1

5.3.1.3 Collection Function (CF)

The Collection Function is responsible for collecting lawfully authorized intercepted communications (i.e., call content) and call-identifying information for an LEA. The Collection Function is the responsibility of the LEA.

The Collection Function typically includes the ability:

- to receive and process call content information for each intercept subject; and
- to receive and process information regarding each intercept subject (e.g., call associated or non-call associated).

5.3.1.4 Service Provider Administration Function (SPAF)

The Service Provider Administration Function is responsible for controlling TSP electronic surveillance functions.

The functions of the SPAF are beyond the scope of this Standard.

5.3.1.5 Law Enforcement Administration Function (LEAF)

The Law Enforcement Administration Function is responsible for controlling LEA electronic surveillance functions. The Law Enforcement Administration Function is the responsibility of the LEA.

The functions of the LEAF are beyond the scope of this Standard.

5.3.2 Interface Reference Points

5.3.2.1 Reference Point *a*

Reference point *a*, or the *a*-interface, is the interface between the Service Provider Administration Function and the Access Function.

Reference point *a* is beyond the scope of this Standard.[1]

5.3.2.2 Reference Point *b*

Reference point *b*, or the *b*-interface, is the interface between the Law Enforcement Administration Function and the Collection Function.

Reference point *b* is beyond the scope of this Standard.

1. This reference point is required to protect (e.g., prevent unauthorized access, manipulation, and disclosure) 1) the privacy and security of communications and call-identifying information not authorized to be intercepted; and 2) information regarding the government's interception of communications and access to call-identifying information.

PN-4465-RV1

5.3.2.3 Reference Point *c*

Reference point *c*, or the *c*-interface, is the interface between the Service Provider Administration Function and the Delivery Function.

Reference point *c* is beyond the scope of this Standard.[1]

5.3.2.4 Reference Point *d*

Reference point *d*, or the *d*-interface, is the interface between the Access Function and the Delivery Function.

Reference point *d* is beyond the scope of this Standard.[1]

5.3.2.5 Reference Point *e*

Reference point *e*, or the *e*-interface, is the interface between the Delivery Function and the Collection Function.

Reference point *e* is defined by this Standard.[1]

5.4 Message Descriptions

The call events described in Stage 1 convey the basic information for reporting the disposition of a call. This section describes those events and supporting information.

Each message is described as consisting of a set of parameters. Each parameter is either:

- mandatory (M)—required for the message,
- conditional (C)—required in situations where a condition (defined in the usage column of the table where it occurs) is met, or
- optional (O)—provided at the discretion of the implementation.

The information to be carried by each parameter is identified. Please note that both optional and conditional parameters at Stage 2 are considered to be OPTIONAL syntactically in ASN.1 Stage 3 descriptions. The Stage 2 inclusion requirements take precedence over the Stage 3 syntax.

5.4.1 Answer

The Answer message reports when a circuit-mode call or call leg has been answered. Transmission is usually cut-through in both directions to the intercept subject or its agent.

1. This reference point is required to protect (e.g., prevent unauthorized access, manipulation, and disclosure) 1) the privacy and security of communications and call-identifying information not authorized to be intercepted; and 2) information regarding the government's interception of communications and access to call-identifying information.

PN-4465-RV1

The Answer message shall be triggered when:

- the intercept subject answers a call or call leg that has not been previously answered by the intercept subject;
- an agent of the intercept subject (e.g., by voice mail or for password screening) answers a call or call leg;
- an associate answers an outgoing call from the intercept subject as detected by the accessing functional entity;
- a call redirected by the intercept subject is answered as detected by the accessing functional entity; or
- the intercept subject or its agent answers a recalling associate (e.g., hold recall, transfer recall, or attendant recall).

The Answer message includes the following parameters:

Table 2: **Answer Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
Answering PartyIdentity	C	Include, when known, to identify the answering party or agent.
Location	C	Include, when a call terminating to the intercept subject's mobile terminal is answered, the location information is reasonably available at the IAP and delivery is authorized, to identify the location of an intercept subject's mobile terminal.
BearerCapability	C	Include, when known (or presumed), to indicate the granted bearer service.

See 6.3.1 "Answer Message" on page 76 for the Stage 3 description.

5.4.2 CCClose

The CCClose message reports the end of call content delivery.

The CCClose message shall be triggered when the CCC is released, such as when:

- the intercepted circuit-mode call is released;
- the intercepted circuit-mode call leg is released;
- the intercepted circuit-mode call is merged with another intercepted circuit-mode call; or
- the intercepted circuit-mode call leg is merged into another intercepted circuit-mode call.

PN-4465-RV1

The CCClose message may be triggered when:

- an early release of the circuit-mode or packet-mode CCC by the Collection Function or intervening network is detected (e.g., see B.4.7);
- a delivery channel for packet data is no longer required;
- the monitored packet-mode call is released; or
- a conference call is retrieved from a hold condition.

One CCClose message is required for each delivered combined CCC, separated CCC pair, or individual CCC.

The CCClose message includes the following parameters:

Table 3: **CCClose Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CCCIdentity	M	Identifies the CCC(s) used to deliver a particular call leg (e.g., a trunk identity, telephone number, or a data network address).

See 6.3.2 “CCClose Message” on page 76 for the Stage 3 description.

5.4.3 CCOpen

The CCOpen message associates a circuit-mode CCC with a particular call instance.

The CCOpen message shall be triggered when circuit-mode call content delivery begins. This should occur after a call is initiated (as an intercept subject origination or termination attempt), but prior to the cut-through of communications between the subject and associate (usually indicated with an answer).

The CCOpen message may be triggered when a conference call is placed on hold.

The CCOpen message may be triggered when a delivery CCC is required for packet-mode data. The CCOpen is required when intercepted packets are to be delivered over a circuit or over a packet switched data network. Packet-mode delivery uses a single packet data network service to deliver intercepted packets to a single address per Collection Function. Packet-mode delivery is differentiated from a circuit-mode intercept by including a PDUType parameter instead of a CallIdentity parameter. Circuit-mode delivery CCCs

PN-4465-RV1

may deliver packet-mode content as identified by the BearerCapability parameter or by an agreement between the TSP and LEA.

One CCOpen message is required for each delivered combined CCC, separated CCC pair, or individual CCC.

Delivery of call content is dependent upon appropriate provisioning of call content channels.

The CCOpen message includes the following parameters:

Table 4: **CCOpen Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
ContentType One of: CallIdentity PDUType	M	 Include for circuit-mode calls to identify a particular circuit-mode call for the CCC. A unique call identity may be generated for the CCOpen message which is used to correlate other messages with the delivered call content. Include for packet-mode calls to identify the type of packet data units being intercepted (e.g., IP, PPP, X.25 LAPB, ISDN D-channel).
CCCIdentity	M	Identifies the CCC(s) used to deliver a particular call leg (e.g., a trunk identity, telephone number, or a data network address).

See 6.3.3 “CCOpen Message” on page 77 for the Stage 3 description.

5.4.4 Change

The Change message reports a change in circuit-mode call identity(ies), especially when merging or splitting calls.

The Change message shall be triggered when:

- two or more call identities are merged into one call identity;
- an additional call identity is associated with an existing call,
- a call identity is split into two or more call identities; or
- a call identity is changed to another call identity.

PN-4465-RV1

The Change message includes the following parameters:

Table 5: **Change Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
Previous Calls	M	Identifies all of the existing calls to be affected. Any call identity that is mentioned as a previous call identity, but is not mentioned as a resulting call identity is released and may be reassigned to other calls.
Resulting Calls	M	Identifies the CallIdentity(ies) and CCCIdentity(ies) in each of the resulting calls. New unique call identities may be generated for the Change message which is used to correlate subsequent messages with the delivered call content.

See 6.3.4 “Change Message” on page 77 for the Stage 3 description.

5.4.5 ConferencePartyChange

The ConferencePartyChange message reports a change in circuit-mode call identity(ies), party identity(ies) or both when independently or in any combination reporting:

- a change in communicating parties;
- a previously communicating party(ies) is removed (e.g., hold service);
- a new party is joining the communicating parties; or
- a previously communicating party(ies) is dropped from the conference call.

The ConferencePartyChange message shall be triggered when there is a change in communicating parties, as:

- a new party joins the communicating parties;
- a previously communicating party(ies) is removed (e.g., hold service); or
- a previously communicating party(ies) or a removed party(ies) (e.g., hold service) is dropped from the conference call.

Whenever one or more CallIdentity(ies) are grouped together with one or more PartyIdentity(ies) and a CCCIdentity(ies), it means that all PartyIdentity(ies) are connected and communicating on the call represented by the group of CallIdentity(ies), and can be monitored (heard) on the CCCIdentity, with the exception of the removed or dropped groups.

PN-4465-RV1

In the RemovedIdentity(ies) or DroppedIdentity(ies) case, the grouping of PartyIdentity(ies) with a CallIdentity(ies) means that the identified PartyIdentity(ies) is disassociated with that CallIdentity(ies) and can not be monitored (heard) on the associated CCCIdentity.

Any CallIdentity(ies), PartyIdentity(ies), and CCCIdentity(ies) not connected to the same communications would be reported as separate groups within the CommunicatingIdentity(ies), RemovedIdentity(ies), or JoinedIdentity(ies).

This message shall not be used to open or close a CCC, to create a new call identity, or to release an existing call identity.

This message is not required when the information reported would be redundant with the information reported by other LAES call event messages.

The ConferencePartyChange message includes the following parameters:

Table 6: **ConferencePartyChange Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CommunicatingIdentity(ies)	C	Included when known, to identify all communicating call identity(ies), party identity(ies), or both on the identified conference call established by the intercept subject's service. This parameter may appear independently or in combination with other parameters.
DroppedIdentity(ies)	C	Included when known, to identify a previously communicating call identity(ies), party identity(ies), or both on the identified conference call established by the intercept subject's service; the dropped identity(ies) is no longer participating in the call. This parameter may appear independently or in combination with other parameters.
RemovedIdentity(ies)	C	Included when known, to identify a previously communicating call identity(ies), party identity(ies), or both on the identified conference call established by the intercept subject's service; the identity(ies) is removed (e.g., hold service) from a call. This parameter may appear independently or in combination with other parameters.
JoinedIdentity(ies)	C	Included when known, to identify a new communicating call identity(ies), party identity(ies), or both on the identified conference call established by the intercept subject's service; the joined identity(ies) has begun communicating on the call. This parameter may appear independently or in combination with other parameters.

PN-4465-RV1

See 6.3.5 “ConferencePartyChange Message” on page 78 for the Stage 3 description.

5.4.6 Connection

The Connection message reports the addition of one or more participants to an existing call (i.e., a leg is connected to the call so that communications can occur). The Connection message reports the participants to a subject-initiated conference call.

The Connection message shall be triggered when:

- the intercept subject’s service changes connections to allow participants to be added to a call under surveillance; or
- there are party hold, drop, join changes to a conference communication during a subject-initiated conference call.

This message, either alone or in combination with the ConnectionBreak message, can be used to satisfy the requirement to report the participants to a subject-initiated conference call. When the Connection message is used alone, it identifies all participants able to communicate with each other in a call.

This message is not required when the information reported would be redundant with the information reported by other LAES call event messages.

The Connection message includes the following parameters:

Table 7: **Connection Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
ConnectionInformation One or more of: ConnectedParties NewParties	M	 Identifies parties able to communicate to each other in a call. Identifies one or more parties added to a call.

See 6.3.6 “Connection Message” on page 79 for the Stage 3 description.

5.4.7 ConnectionBreak

The ConnectionBreak message reports when one or more participants are removed from an existing call (i.e., a leg is removed from a call so that communications can not occur). The ConnectionBreak message reports when

PN-4465-RV1

participants to a subject-initiated conference call are removed (e.g., temporarily or permanently).

The ConnectionBreak message shall be triggered when:

- the intercept subject's service changes connections to remove participants from a call under surveillance; or
- there are party hold or drop changes to a conference communication during a subject-initiated conference call.

This message, in combination with the Connection message, can be used to satisfy the requirement to report the participants to a subject-initiated conference call.

This message is not required when the information reported would be redundant with the information reported by other LAES call event messages.

The ConnectionBreak message includes the following parameters:

Table 8: **ConnectionBreak Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
ConnectionBreakInformation One or more of: RemovedParties RemainingParties DroppedParties	M	 Identifies parties removed (e.g., hold service) from a call. Identifies parties remaining in a call. Identifies parties permanently disconnected from a call.

See 6.3.7 "ConnectionBreak Message" on page 79 for the Stage 3 description.

5.4.8 DialedDigitExtraction

The DialedDigitExtraction message reports intercept subject-dialed digits when a call is connected to another TSP's service for processing and routing. The dialed digit extraction capability shall be provided with a toggle feature that can activate and deactivate this ccapability, as defined in FCC 02-108, CC Docket Number 97-213 (released 4/11/02). The post-cut through digits are digits dialed or signaled by the intercept subject after the initial call setup is completed and the call path is cut-through in both directions at the IAP switch. The digits may be reported on a digit-by digit basis, accumulated until

PN-4465-RV1

a buffer is filled, accumulated until a timer expires, or accumulated until the call is released.

A TSP may report dialed digits other than those that are call completing and has no obligation to determine which dialed digits actually complete a call.

The DialedDigitExtraction message shall be triggered only for circuit-mode calls when:

- digit-by-digit reporting is performed and a digit is detected; or
- digit accumulation is performed and the first of the following occurs:
  - i. a maximum of 32 digits have been accumulated in the buffer;
  - ii. 20 seconds have elapsed since detection of the first digit in the buffer; or
  - iii. the call is released.

The DialedDigitExtraction message includes the following parameters:

Table 9: **DialedDigitExtraction Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the triggering event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
Digits	M	Identifies the DTMF-tones transmitted by the intercept subject after the call is cut-through in both directions.

See 6.3.8 “DialedDigitExtraction Message” on page 79 for the Stage 3 description.

5.4.9 NetworkSignal

The NetworkSignal message reports signals generated or sent by the IAP switch to the intercept subject using the facilities under surveillance. The network signals reported by the NetworkSignal message are signals originated and applied by the accessing system IAP towards the intercept subject.

The NetworkSignal message is triggered when a network signal that provides call-identifying information is originated and applied by the IAP switch to an intercept subject.

The following triggering events are defined (referenced from LSSGR, ANSI-41 and GSM 02.40):

PN-4465-RV1

a. Dial tone is applied indicating an intercept subject has gone off-hook and the IAP is ready to accept address information from the intercept subject.

b. Recall dial tone is applied indicating that an IAP is ready to accept address information or other information from an intercept subject.

c. Expensive route warning tone is applied indicating an intercept subject has accessed the Automatic Flexible Routing (AFR) feature and the IAP switch selected outgoing route is designated as an expensive route.

d. Busy tone is applied indicating an intercept subject-originated incomplete call attempt.

e. Reorder tone or Congestion tone is applied indicating an intercept subject-originated incomplete call attempt.

f. Receiver Off-Hook (ROH) tone is applied indicating the intercept subject has left the phone receiver off hook and the line is receiving permanent signal treatment. This tone is also used in place of ringing when an operator system needs to alert an off-hook line.

g. Special Information Tone (SIT) is applied indicating an intercept subject-originated call has been routed to an announcement. SIT tones precede IAP switch generated announcements to permit the user and network equipment to detect the type of recorded announcement that follows the tone.

h. Ringback tone or Audible alerting is applied indicating an intercept subject-originated call attempt has progressed and the called party is being alerted.

i. Barge-in tone is applied indicating someone is about to barge-in on the intercept subject’s active call.

j. Call-associated out-of-band signal that is normally perceivable (seen or heard) by the intercept subject, such as tone commands (i.e., tones off) or visual call status indicator.

k. Alerting tone is applied indicating an incoming call attempt to the intercept subject.

l. Distinctive alerting tone is applied to allow classification of incoming calls to the intercept subject based on the called number or based on the calling number.

m. Reminder ring is applied to notify the intercept subject when a terminating call has been redirected.

n. Call waiting tone is applied indicating an incoming call to the intercept subject while the subject is in the communications state with another call.

o. Distinctive call waiting tone is applied to allow classification of incoming calls to the intercept subject, while the subject is in the communications state with another call, based on the called number or based on the calling number.

p. Confirmation tone is applied indicating the IAP has received information and has processed the request, such as the activation or deactivation of a feature or service.

q. Message waiting indicator tone is applied indicating message waiting services are available. This tone also indicates that the IAP is ready to accept address information or other information.

PN-4465-RV1

r. Denial tone (single 2.0 seconds burst of 480 Hz tone added to a 620 Hz tone) is applied towards the intercept subject indicating denial of a feature request.

s. Signaling information is delivered to the intercept subject identifying calling name and number and redirecting party name and number.

t. Alphanumeric information associated with a circuit-mode call is delivered to the intercept subject, such as text provided in the Q.931 display information element (e.g., calling name, redirecting name).

u. Intercept tone or Mobile Reorder tone (alternating 440Hz and 620 Hz tones each on for 250 ms.) is applied toward the intercept subject.

v. Answer tone is applied toward the intercept subject.

w. Tones off. All tones off.

x. Pip tone (four bursts (0.1 second on, 0.1 second off) of 480 Hz tone, and then off) is applied toward the intercept subject.

y. Abbreviated Intercept tone (4 seconds of Intercept tone) is applied toward the intercept subject.

z. Abbreviated Congestion tone (4 seconds of Congestion tone) is applied toward the intercept subject.

aa. Warning tone (a single 0.1 second burst of 480 Hz tone) is applied toward the intercept subject.

ab. Dial tone burst tone (a single 2.0 seconds burst of Dial tone) is applied toward the intercept subject.

ac. Standard announcement is applied toward the intercept subject as applicable per ANSI-41.

ad. Number Unobtainable tone is applied toward the intercept subject indicating that the dialed number is invalid or unobtainable.

ae. Authentication Failure tone is applied toward the intercept subject indicating that an authentication attempt has failed.

PN-4465-RV1

The NetworkSignal message includes the following parameters:

Table 10: **NetworkSignal Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	C	Included when the network signal is associated with a particular call.
Signal One or more of the following: AlertingSignal SubjectAudibleSignal TerminalDisplayInfo Other	M	Identifies the audio signals, visual signals, or displayed text applied by the accessing system that would normally be sensed by the intercept subject. Included when alerting is applied to the intercept subject's terminal to indicate its type. Included when audible signal is applied toward the intercept subject. Included when messages that may be displayed on the intercept subject's terminal are sent by the IAP including display messages, called number, calling party numbers, redirecting numbers, etc. Included as an alternative means of reporting the signaling information.

See 6.3.9 "NetworkSignal Message" on page 80 for the Stage 3 description.

5.4.10 Origination

The Origination message reports circuit-mode call origination attempts by the intercept subject, or number translations performed by the accessing system for the purpose of routing. More than one Origination message is possible for a single call attempt when numbers are expanded or translated.

The Origination message shall be triggered when:

- a call or call leg originated by the intercept subject is routed toward a destination within the accessing system;
- a call or call leg originated by the intercept subject is routed toward a destination on an external public or private network;
- the destination number for a call or call leg originated by the intercept subject is translated from one set of digits to another. For example, speed number expansion or 800-number translation;
- a call was attempted that was partially dialed, or that could not be completed by the accessing system; or
- a feature code was dialed or otherwise transmitted.

PN-4465-RV1

The Origination message includes the following parameters:

Table 11: **Origination Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system. A unique call identity may be generated for the Origination message which is used to correlate other messages. An exception is possible when such an attempt is considered part of an on-going call (e.g., three-way calling or conference calling for some systems).
Calling PartyIdentity	C	Include, when more specific than the intercept subject identity associated with the CaseIdentity, to identify the originating party.
Called PartyIdentity	C	Include, when known to identify the called party. This shall not be present for calls that were partially dialed or could not be completed by the accessing system.
Input	M	Identifies specific user or translation input including when a call is attempted without input (e.g., hot line).
Location	C	Include, when the location information is reasonably available at the IAP and delivery is authorized, to identify the location of an intercept subject's mobile terminal.
TransitCarrierIdentity	C	Include, when the transit network selection is known, to identify the transit carrier.
BearerCapability	C	Include, when known (or presumed), to indicate the requested bearer service for the origination.

See 6.3.10 "Origination Message" on page 81 for the Stage 3 description.

5.4.11 PacketEnvelope

The PacketEnvelope message is used to convey data packets over the CDC as they are intercepted. (Packet-mode communications delivered over CCCs or packet-mode communications using circuit-mode facilities do not use the PacketEnvelope.)

The PacketEnvelope message shall be triggered for the appropriate types of packet data services when:

- a packet-mode user communication intended for the intercept subject is detected; or
- a packet-mode user communication from the intercept subject is detected.

PN-4465-RV1

The PacketEnvelope message includes the following parameters:

Table 12: **PacketEnvelope Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	C	Include when the packet is associated with a particular call, call appearance, or call leg.
Location	C	Include, when the location information is reasonably available at the IAP and delivery is authorized, to identify the location of an intercept subject's mobile terminal.
Packet Information One of:	M	
ISDN- or ISUP-based user-to-user signaling information		Information pertaining to ISDN or ISUP user-to-user signaling messages.
TIA/EIA-41-based short message service		Information pertaining to *TIA/EIA-41* short message service messages.
GSM-based short message service		Information pertaining to GSM short message service messages.
Wireless IP-based service		Information pertaining to wireless IP-based service messages (e.g., CDPD). This parameter may also be used to information pertaining to non-wireless IP-based services.

See 6.3.11 "PacketEnvelope Message" on page 81 for the Stage 3 description.

5.4.12 Redirection

The Redirection message reports the redirection of a circuit-mode call.

The Redirection message shall be triggered when:

- an incoming call attempt to the intercept subject is forwarded (e.g., call forwarding or call diversion);
- an incoming call attempt to the intercept subject is deflected (e.g., call waiting deluxe or call deflection); or
- an incoming call attempt to an intercept subject with terminal or personal mobility is redirected to the intercept subject's current location (e.g., call delivery).

PN-4465-RV1

The Redirection message includes the following parameters:

Table 13: **Redirection Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call within a system.
Redirected-to PartyIdentity	M	Identifies the redirected-to party.
TransitCarrierIdentity	C	Included when the transit network selection is known to identify the transit carrier.
BearerCapability	C	Included when known (or presumed) to indicate the requested bearer service for the redirection.
System Identity	C	Included when a call to a wireless subscriber is redirected to another TSP and that identity is reasonably available.

See 6.3.12 “Redirection Message” on page 83 for the Stage 3 description.

5.4.13 Release

The Release message reports the release of the resources used for a circuit-mode call, call appearance, or call leg.

The Release message shall be triggered when:

- a circuit-mode call attempt is abandoned by the calling party; or
- a completed circuit-mode call is released.

The Release message may be triggered when a call leg or call appearance is released.

PN-4465-RV1

The Release message includes the following parameters:

Table 14: **Release Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system. The call identity is released.
Location	C	Include, when the location information is reasonably available at the IAP and delivery is authorized, to identify the location of an intercept subject's mobile terminal.
System Identity	C	Include, when a handed-off wireless call is released while being served by another TSP, to identify the last known TSP serving the subject.

See 6.3.13 "Release Message" on page 83 for the Stage 3 description.

5.4.14 ServingSystem

The ServingSystem message reports the TSP providing service to an intercept subject with terminal mobility, when the terminal is authorized for service.

A ServingSystem report shall be triggered when a mobile terminal is authorized for service with another TSP or in another service area.

The ServingSystem message includes the following parameters:

Table 15: **ServingSystem Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
SystemIdentity	C	Include, when authorizing service to a TSP, to identify the TSP.
NetworkAddress	C	Include, when available, to identify the redirect-to number of the base station (e.g., a personal or residential base station) providing service to the intercept subject.

See 6.3.14 "ServingSystem Message" on page 84 for the Stage 3 description.

PN-4465-RV1

5.4.15 SubjectSignal

The SubjectSignal message reports subject-initiated signals used to control a feature or service operation (e.g., call forwarding, call waiting, call hold and three-way calling). The user input may be uninterpretable and would result in no change in the control of a call, but a SubjectSignal message may still be generated.

The signal may be in-band or out-of-band and may be call-associated or non call-associated. However, digits dialed post cut-through as defined in section 5.4.8 “DialedDigitExtraction” are not detected by this function and are thus not provided in a SubjectSignal message.

The SubjectSignal message shall be triggered when:

- the intercept subject, using the facilities under surveillance, dials or signals to control services provided by the serving system;
- sufficient input has been received (e.g., the receiving IAP network element acts on the subject-initiated input); or
- the call attempt is abandoned with partial input (e.g., the interdigit timer expires or a subject abandons the call).

This message is not required when the information reported would be redundant with the information reported by other LAES call event messages.

PN-4465-RV1

The SubjectSignal message includes the following parameters:

Table 16: **SubjectSignal Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	C	Included when known to uniquely identify a call, call appearance, or call leg within a system.
Signal One or more of the following: SwitchhookFlash DialedDigits FeatureKey OtherSignalingInformation	M	Identifies the signal or dialing the IAP detects as originating from the intercept subject. Include to report specific subject-initiated input when detected at the IAP. Included when the user requests a switchhook flash. Included when digits are dialed. Included when a particular feature key was pressed. Included when other signaling information is initiated by the intercept subject.

See 6.3.15 “SubjectSignal Message” on page 84 for the Stage 3 description.

5.4.16 TerminationAttempt

The TerminationAttempt message reports an incoming circuit-mode call attempt to the intercept subject. This message shall be sent regardless of the disposition of the call (e.g., busy, answered, redirected).

The TerminationAttempt message shall be triggered when:

- an incoming call to an intercept subject is detected; or
- a recall attempt involving the intercept subject is detected (e.g., hold recall, transfer recall, or attendant recall).

PN-4465-RV1

The TerminationAttempt message includes the following parameters:

Table 17: **TerminationAttempt Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system. A unique call identity is generated for the TerminationAttempt message which is used to correlate other messages. An exception is possible when such an attempt is considered part of an on-going call (e.g., call waiting for some systems).
CallingPartyIdentity	M	Identifies the calling party to the extent known.
CalledPartyIdentity	C	Include, when more specific than the subject identity associated with the CaseIdentity, to identify the called party.
BearerCapability	C	Include, when known (or presumed), to identify the requested bearer service.
RedirectedFromInformation	C	Include when the incoming call has information about previous redirection.

See 6.3.16 “TerminationAttempt Message” on page 85 for the Stage 3 description.

5.5 Message descriptions for cdma2000 packet data

As in Section 5.4 the cdma2000 packet data session events described in the Stage 1 convey the basic information for reporting the disposition of a packet data session. This section describes those events and supporting information.

Each message is described as consisting of a set of parameters. Each parameter is either:

- mandatory (M) - required for the message;
- conditional (C) - required in situations where a condition (defined in the usage column of the table where it occurs) is met; or
- optional (O) - provided at the discretion of the implementation.

The information to be carried by each parameter is identified. Please note that both optional and conditional parameters at Stage 2 are considered to be OPTIONAL syntactically in ASN.1 Stage 3 descriptions. The Stage 2 inclusion requirements take precedence over the Stage 3 syntax.

The IPv4 Address and the NAI of the intercept subject shall be used to uniquely identify a packet data session of the intercept subject in the event of a successful packet data session establishment for Simple IPv4 or Mobile

PN-4465-RV1

IPv4. When the subject is using Simple IPv6 the first 64 bits (globally unique prefix) shall be used to uniquely identify the packet data session of the intercept subject.

5.5.1 cdma2000PacketDataSessionEstablishment

The cdmaPacketDataSessionEstablishment message reports the successful or unsuccessful establishment of a packet data session. The following information associated with the CII events is reported to the LEA.

The cdma2000PacketDataSessionEstablishment message shall be triggered upon the following events at an IAP:

- Successful PPP negotiation for Simple IPv4;
- Unsuccessful PPP negotiation for Simple IPv4, Simple IPv6, and Mobile IPv4;
- Successful or Unsuccessful registration for Mobile IPv4.
- Router Advertisement with the /64 globally unique prefix that is assigned to the subject after successful PPP negotiation for Simple IPv6.
- Router Advertisement with the /64 globally unique prefix that is assigned to the subject in response to a Router Solicitation from the subject for Simple IPv6.

The cdma2000PacketDataSessionEstablishment message includes the following parameters:

PN-4465-RV1

Table 18: **cdma2000PacketDataSessionEstablishment Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
SubjectIPAddress	M	Provide the IP address assigned for the session: - The IPv4 address allocated by the PDSN for Simple IPv4 access, or, -the /64 globally unique prefix assigned to the subject by the PDSN for Simple IPv6 access, or; - The Home IPv4 address assigned by the Home Agent. If establishment fails, a NULL value is provided.
SubjectIdentity	C	Observed identity or identities of the subject. Provide known identities.
IPAssignment	C	Provide when known to indicate a static or dynamic IP assignment: - Static or dynamic assignment for Simple IPv4. - Static or dynamic assignment of a /64 globally unique prefix for Simple IPv6, - Static or dynamic assignment for Mobile IPv4.
HaIPAddress	C	IPv4 address of the HA, only provided for Mobile IPv4 access.
FaCoA	C	Foreign Agent provided Care of Address, only provided for Mobile IPv4 access.
CorrelationNumber	C	Unique number for each established packet data session for correlating CC and CII when CII and CC are both reported.
LocationInformation	C	Provide for established packet data sessions, when authorized, to identify location information for the intercept subject's MS.
SessionEstablishmentFailure	C	Provide when session establishment fails and include the reason for failure when known. Examples include: - Mobile IPv4 rejected by the PDSN; - Mobile IPv4 rejected by the HA; - Access rejected by the home network; - PPP establishment unsuccessful.
CCAddress	C	Provide when content is being delivered, to identify the particular IP address and port number of the LEA used to deliver contents for a packet data session.

5.5.2 cdma2000PacketDataSessionTermination

The cdma2000PacketDataSessionTermination message reports the end of a Simple IPv4, Simple IPv6, or Mobile IPv4 packet data session.

PN-4465-RV1

The cdma2000PacketDataSessionTermination message shall be triggered upon the following events at an IAP:

- Release of PPP;
- Router advertisement lifetime expiry for Simple IPv6;
- MIP de-registration;
- MIP Registration-Revocation.; or
- MIP BInding Removal;

The cdma2000PacketDataSessionTermination message includes the following parameters:

Table 19: **cdma2000PacketDataSessionTermination Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Time and date that the event was detected.
SubjectIPAddress	M	Provide the IP address assigned for the session: - The IPv4 address allocated by the PDSN for Simple IPv4 access, or, -the /64 globally unique prefix assigned to the subject by the PDSN for Simple IPv6 access, or; - The Home IPv4 address assigned by the Home Agent.
HaIPAddress	C	IPv4 address of the HA, only provided for Mobile IPv4 access.
FaCoA	C	Foreign Agent provided Care of Address, only provided for Mobile IPv4 access.
CorrelationNumber	C	Unique number for each packet data session for correlating CC and CII when CII and CC are both reported.
LocationInformation	C	Provide, when authorized, to identify location information for the intercept subject's MS.
SessionTerminationReason	C	Provide the reason (e.g., release indicator or Acct-Term cause) for closing the packet data session, when known.

5.5.3 cdma2000PacketDataInterceptStart

The cdma2000PacketDataInterceptStart message reports the start of interception for each established packet data session when at least one packet data session is already established, if the information is reasonably available at the IAP. There may be cases (e.g., handoff) where it may not be possible to report this event due to the lack of information at the IAP.

The cdmaPacketDataInterceptStart message shall be triggered upon the following event at an IAP:

PN-4465-RV1

- A session is already established and an intercept is started.

The cdma2000PacketDataInterceptStart message includes the following parameters:

Table 20: **cdma2000PacketDataInterceptStart Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Time and date that the event was detected.
SubjectIPAddress	M	Provide the IP address assigned for the session: - The IPv4 address allocated by the PDSN for Simple IPv4 access; or -the /64 globally unique prefix assigned to the subject by the PDSN for Simple IPv6 access; or - The Home IPv4 address assigned by the Home Agent.
SubjectIdentity	C	Observed identity or identities of the subject. Provide known identities.
IPAssignment	C	Provide when known to indicate a static or dynamic IP assignment: - Static or dynamic assignment for Simple IPv4; - Static or dynamic assignment of a /64 globally unique prefix for Simple IPv6; - Static or dynamic assignment for Mobile IPv4.
HaIPAddress	C	IPv4 address of the HA, only provided for Mobile IPv4 access.
FaCoA	C	Foreign Agent provided Care of Address, only provided for Mobile IPv4 access.
CorrelationNumber	C	Unique number for each packet data session for correlating CC and CII when CII and CC are both reported.
LocationInformation	C	Provide, when authorized, to identify location information for the intercept subject's MS.
CCAddress	C	Provide when content is being delivered, to identify the particular IP address and port number of the LEA used to deliver contents for a packet data session.

5.5.4 cdma2000PacketDataServingSystem

The cdma2000PacketDataServingSystem message reports the identity of the system currently serving the intercept subject.

The cdma2000PacketDataServingSystem message shall be triggered upon the following events at an IAP:

PN-4465-RV1

- the reception of an Access Request or Accounting Request (start) at the Home AAA; or
- the reception of an MIP RRQ at the HA.

The cdma2000PacketDataServingSystem message includes the parameters in Table 21.

Either SubjectIPAddress or the SubjectIdentity must be included in the message.

Table 21: **cdma2000PacketDataServingSystem Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Time and date that the event was detected.
SubjectIPAddress	C	Provides the IPv4 address assigned for the session: -The Home IPv4 address used for the Mobile IPv4 session; - The Dynamic IPv4 address allocated by the PDSN for Simple IPv4 access, or; -The /64 globally unique prefix assigned to the subject by the PDSN for Simple IPv6 access.
SubjectIdentity	C	Observed identity or identities of the subject. Provide known identities.
ServingSystemIdentity	M	Identifies the entity that is currently serving the intercept subject.
HaIPAddress	C	IPv4 address of the HA, only provided for Mobile IPv4 access.
FaCoA	C	Foreign Agent provided Care of Address, only provided for Mobile IPv4 access.

5.5.5 cdma2000PacketDataPacketFilter

The cdma2000PacketDataPacketFilter message reports the setup/change/release of a particular packet filter.

The packet filters are used in the cdma2000 packet data network to identify specific IP flows. The cdma2000PacketDataPacketFilter message shall be triggered upon the following events at an IAP:

PN-4465-RV1

- signaling from the MS for a new packet filter;
- signaling from the MS for modification in packet filter;
- signaling from the MS for release or removal of a packet filter;
- the release of an auxiliary service instance with associated packet filters.

The cdma2000PacketDataPacketFilter message includes the following parameters:

Table 22: **cdma2000PacketDataPacketFilter Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Time and date that the event was detected.
SubjectIPAddress	M	Provide the IP address assigned for the session: - the IPv4 address allocated by the PDSN for Simple IPv4 access; -the /64 globally unique prefix assigned to the subject by the PDSN for Simple IPv6 access; or - the Home IPv4 address assigned by the Home Agent.
SubjectIdentity	C	Observed identity or identities of the subject. Provide known identities.
HaIPAddress	C	IPv4 address of the HA, only provided for Mobile IPv4 access.
FaCoA	C	Foreign Agent provided Care of Address, only provided for Mobile IPv4 access.
PacketFilterInformation	M	Provide packet filter information. TFT option for the subject IP address as signaled by the MS. See TIA-835 Rev. C standards.
CorrelationNumber	C	Unique number for each packet data session for correlating CC and CII when CII and CC are both reported.

5.5.6 cdma2000InterceptionofContent

The content of communications is delivered to the LEA using the cdma2000 lawful interception correlation (CLIC) header. The CLIC header is prepended to each intercepted packet before the intercepted packet is transported to the LEA. Examples of the transport mechanism include TCP and UDP.

The CLIC header is followed by the “payload” information element, which contains the intercepted packet. Only one payload[1] informaiton element is allowed per CLIC header (see section 6.6 on page 95).

1. CLIC parameters are per IP packet.

PN-4465-RV1

CLIC header is defined in ASN.1 ((see section 6.6 on page 95) and is encoded according to BER (X.209). It contains the following attributes:

Table 23: **cdma2000 CLICHeader *Parameters***

Parameter	MOC	Usage
cdma2000CCPSModuleID	M	Module identifier for cdma2000 communication content
CLICHeaderVersion	M	Identifies the version number of the CLIC header
CaseIdentity	M	Identifies the intercept subject
CorrelationNumber	C	Unique number for each established packet data session for correlating CC and CII when CII and CC are both reported. Required when intercepted sessions may be aggregated over the same CC Address (LEA IP Address and Port Number).
TimeStamp	M	Time and date that the event was detected.
SequenceNumber	C	Sequence Number is an increasing sequence number for the interception of IP packets. At a minimum, the sequence number should be unique per packet data session. Not required when TCP is the transport protocol.
IPPacketDirection	O	Indicated the direction of the IP packet (from the intercept subject or to the intercept subject).

PN-4465-RV1

6 Stage 3 Description: Implementation Perspective

6.1 Protocol Definition

A protocol is defined in three basic aspects:

a. Transfer Syntax,

b. Transfer Semantics, and

c. Procedures.

The transfer syntax defines the messages passed between two functional entities. This definition may include various structures, but eventually defines the entire message structure down to the bit level. The syntax specifies the ways in which bits of messages are encoded for exchanging information between two functional entities.

The transfer semantics assigns meanings to the bits, bytes and structures of the transfer syntax. The exchanges of meanings allows the functional entities to share information and to act upon that information.

Procedures define the behavior of the functional entities. Procedures define which functional entities are allowed to initiate a particular transaction. Procedures define the possible responses to a given stimulus especially when dependent upon prior exchanges.

6.2 CDC Protocol Definition

6.2.1 CDC Underlying Data Transmission

The CDC messages defined by this Standard are an Open System Interconnection (OSI) Layer 7 or Application Layer protocol. The protocol for the CDC messages is called the Lawfully Authorized Electronic Surveillance Protocol (LAESP). The LAESP messages shall be delivered over CDCs employing a Standard or widely used data communication protocol.

6.2.2 CDC Parameter Encoding Objectives

The following are the objectives of the parameter encoding:

a. Allow flexible usage of the LAESP to transport a variety of information.

b. Provide a consistent and complete syntax for transferring information.

c. Facilitate implementation of message encoding and decoding software by using standardized techniques.

d. Allow as much syntactical checking as practical to be performed by the message parsers rather than deferring to the application.

e. Allow for parameter extension and modification throughout the life of the protocol.

PN-4465-RV1

6.2.3 CDC Syntax Definitions

The transferred information and messages shall be encoded to be binary compatible with *X.208 Abstract Syntax Notation One* (ASN.1) and the *X.209 Basic Encoding Rules* (BER).

These recommendations use precise definitions of the words *type*, *class*, *value*, and *parameter*. Those definitions are paraphrased below for clarity.

A *type*; in the context of the abstract syntax or transfer syntax, is a set of all possible values. For example, an INTEGER is a type for all negative and positive integers.

A *class*, in the context of the abstract syntax or transfer syntax, is a one of four possible domains for uniquely defining a type. The classes defined by ASN.1 and BER are: UNIVERSAL, APPLICATION, CONTEXT, and PRIVATE. The UNIVERSAL class is reserved for international standards such as *X.208* and *X.209*. Most parameter type identifiers in the LAESP are encoded as CONTEXT specific class. Users of the LAESP may extend the protocol with PRIVATE class parameters without conflict with this Standard, but risk conflict with other users' extensions. APPLICATION class parameters are reserved by the LAESP Standard for future extensions.

A *value* is a particular instance of a type. For example, five (5) is a possible value of the type INTEGER.

A *parameter* in this Standard is a particular instance of the transfer syntax to transport a value consisting of a tag to identify the parameter type, a length to specify the number of octets in the value, and the value.

In the BER a *tag* (a particular type and class identifier) may either be a primitive or a constructor. A *primitive* is a pre-defined type (of class UNIVERSAL) and a *constructor* consists of other types (primitives or other constructors). A constructor type may either be *IMPLICIT* or *EXPLICIT*. An *IMPLICIT* type is encoded with the constructor identifier alone. Both ends of a communication must understand the underlying structure of the IMPLICIT types. *EXPLICIT* types are encoded with the identifiers of all the contained types. For example, an IMPLICIT Number of type INTEGER would be tagged only with the "Number" tag, where an EXPLICIT Number of type INTEGER would have the "INTEGER" tag within the "Number" tag. This Standard uses IMPLICIT tagging for more compact message encoding. Parameters of the CHOICE type are encoded EXPLICIT to ensure compatibility with various ASN.1 versions and compilers.

6.3 CDC Message Definitions

The LAESMessage parameter defines the LAES messages.

```
Laesp-j-std-025-b {iso(1) member-body(2) us(840) ti(113737) laes(2) tr45(0) j-std-
```

PN-4465-RV1

```
        025(0) j-std-025-b(2) version-1(0)}[1]

Laesp DEFINITIONS IMPLICIT TAGS ::=
BEGIN

LAESProtocol ::= CHOICE {
        lAESMessage           LAESMessage,
        lAESMessagePlus       LAESMessagePlus
                -- For J-STD-025-A solutions the LAESMessage choice should be
                -- selected .
                -- The LAESMessagePlus choice is recommended for solutions for
                -- revisions beyond J-STD-025-A.
}

LAESMessagePlus ::= SEQUENCE {
        protocolIdentifier OBJECT IDENTIFIER Laesp-j-std-025-b,
                -- assigned for each protocol syntax
        lAESMessage           LAESMessage
}

LAESMessage ::= CHOICE {
        answer         [1] Answer,
        ccClose        [2] CCClose,
        ccOpen         [3] CCOpen,
        change         [4] Change,
        origination    [5] Origination,
        packetEnvelope [6] PacketEnvelope,
        redirection    [7] Redirection,
        release        [8] Release,
        servingSystem  [9] ServingSystem,
        termAttempt    [10] TerminationAttempt,
--      connTest       [11] ConnectionTest,  - - see Annex F
        confPartyChange[12] ConferencePartyChange,
        connection     [13] Connection,
        connectBreak   [14] ConnectionBreak,
        dialedDgtExtrn [15] DialedDigitExtraction,
        networkSignal  [16] NetworkSignal,
        subjectSignal  [17] SubjectSignal
}
```

1. Annex I contains the LAES Object Tree.

PN-4465-RV1

6.3.1 Answer Message

The Answer message is used to report that a connection-oriented call or leg has been answered.

```
Answer ::= SEQUENCE {
               [0] CaseIdentity,
               [1] IAPSystemIdentity                OPTIONAL,
               -- include to identify the system containing the Intercept Access
               -- Function when the underlying data carriage does not imply that
               -- system.
               [2] TimeStamp,
               [3] CallIdentity,
answering      [4] PartyIdentity                    OPTIONAL,
               -- include, when known, to identify the answering party or agent
               [5] Location                         OPTIONAL,
               -- Include, when a terminating call is answered, the location
               -- information is reasonably available to the IAP and delivery is
               -- authorized, to identify the location of an intercept subject's
               -- mobile terminal.
               [6] EXPLICIT BearerCapability        OPTIONAL
               -- include, when known (or presumed), to indicate the granted bearer
               -- capability.
}
```

See 5.4.1 “Answer” on page 47 for the Stage 2 description.

6.3.2 CCClose Message

The CCClose message is used to report the end of call content delivery on the CCC.

```
CCClose ::= SEQUENCE {
               [0] CaseIdentity,
               [1] IAPSystemIdentity                OPTIONAL,
               -- include to identify the system containing the Intercept Access
               -- Function when the underlying data carriage does not imply that
       system.
               [2] TimeStamp,
               [3] EXPLICIT CCCIdentity
}
```

See 5.4.2 “CCClose” on page 48 for the Stage 2 description.

PN-4465-RV1

6.3.3 CCOpen Message

The CCOpen message is used to report the beginning of call content delivery on the CCC.

```
CCOpen ::= SEQUENCE {
               [0] CaseIdentity,
               [1] IAPSystemIdentity                OPTIONAL,
               -- include to identify the system containing the Intercept Access
               -- Function when the underlying data carriage does not imply that
               -- system.
               [2] TimeStamp,
               CHOICE {
                       [3] SEQUENCE OF CallIdentity, -- for circuit-mode intercepts
                       [4] PDUType                   -- for packet-mode intercepts
               },
               [5] EXPLICIT CCCIdentity
}
```

See 5.4.3 “CCOpen” on page 49 for the Stage 2 description.

6.3.4 Change Message

The Change message is used to report merging or splitting of connection-oriented call identities.

```
Change ::= SEQUENCE {
               [0] CaseIdentity,
               [1] IAPSystemIdentity                OPTIONAL,
               -- include to identify the system containing the Intercept Access
               -- Function when the underlying data carriage does not imply that
               -- system.
               [2] TimeStamp,
previous       [3] SEQUENCE OF -- previous call(s)
                       SEQUENCE OF CallIdentity, -- identity(ies) of a previous call
resulting      [4] SEQUENCE OF SEQUENCE { -- resulting call(s)
                       [0] SEQUENCE OF CallIdentity,
                       -- identity(ies) of resulting call
                       [1] EXPLICIT CCCIdentity     OPTIONAL
                       -- included when the content of the resulting call is
                       -- delivered to identify the CCC(s).
               }
}
```

See 5.4.4 “Change” on page 50 for the Stage 2 description.

PN-4465-RV1

6.3.5 ConferencePartyChange Message

The ConferencePartyChange message reports a change in the parties to a subject initiated conference call communication.

```
ConferencePartyChange ::= SEQUENCE {
                [0] CaseIdentity,
                [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                -- system.
                [2] TimeStamp,
communicating   [3] SEQUENCE OF SEQUENCE{
                -- include to identify parties participating in the communication.
                        [0] SEQUENCE OF CallIdentity  OPTIONAL,
                        -- identifies communicating call identities.
                        [1] SEQUENCE OF PartyIdentity OPTIONAL,
                        -- identifies communicating party identities.
                        [2] EXPLICIT CCCIdentity      OPTIONAL
                        -- included when the content of the resulting call is
                        -- delivered to identify the associated CCC(s).
                } OPTIONAL,
dropped         [4] SEQUENCE OF SEQUENCE{
                -- include to identify parties dropped from the communication.
                        [0] SEQUENCE OF CallIdentity  OPTIONAL,
                        -- identifies previously communicating, now dropped call
                        -- identity(ies).
                        [1] SEQUENCE OF PartyIdentity OPTIONAL,
                        -- identifies previously communicating, now dropped party
                        -- identity(ies).
                        [2] EXPLICIT CCCIdentity      OPTIONAL
                        -- included when a party(ies) to an existing communication
                        -- is dropped, to identify the associated CCC(s).
                } OPTIONAL,
removed         [5] SEQUENCE OF SEQUENCE{
                -- include to identify parties removed (e.g., hold service) from the
                -- communication.
                        [0] SEQUENCE OF CallIdentity  OPTIONAL,
                        -- identifies removed call identity(ies).
                        [1] SEQUENCE OF PartyIdentity OPTIONAL,
                        -- identifies removed party identity(ies).
                        [2] EXPLICIT CCCIdentity      OPTIONAL
                        -- included when a party(ies) to an existing communication
                        -- is removed, to identify the CCC(s).
                } OPTIONAL,
joined          [6] SEQUENCE OF SEQUENCE{
                -- include to identify parties newly added to the communication.
                        [0] SEQUENCE OF CallIdentity  OPTIONAL,
                        -- identifies newly added call identity(ies) to an existing
                        -- communication.
                        [1] SEQUENCE OF PartyIdentity OPTIONAL,
                        -- identifies newly added party identity(ies) to an existing
                        -- communication.
                        [2] EXPLICIT CCCIdentity      OPTIONAL
                        -- included when a party to an existing communication
                        -- is added, to identify the associated CCC(s).
                } OPTIONAL
}
```

See 5.4.5 “ConferencePartyChange” on page 51 for the Stage 2 description.

PN-4465-RV1

6.3.6 Connection Message

The Connection message reports parties to a call under surveillance.

```
Connection     ::= SEQUENCE   {
               [0] CaseIdentity,
               [1] IAPSystemIdentity                OPTIONAL,
               -- include to identify the system containing the Intercept Access
               -- Function when the underlying data carriage does not imply that
               -- system.
               [2] TimeStamp,
               [3] SEQUENCE OF CallIdentity,
               -- Connection Information
               -- The following two parameters are considered Connection
               -- Information.
               -- Include at least one of the following.

       connectedParties      [4]    SEQUENCE OF PartyIdentity            OPTIONAL,
       newParties            [5]    SEQUENCE OF PartyIdentity            OPTIONAL
}
```

See 5.4.6 “Connection” on page 53 for the Stage 2 description.

6.3.7 ConnectionBreak Message

The ConnectionBreak message reports parties removed from a call under surveillance.

```
ConnectionBreak::= SEQUENCE   {
               [0] CaseIdentity,
               [1] IAPSystemIdentity                OPTIONAL,
               -- include to identify the system containing the Intercept Access
               -- Function when the underlying data carriage does not imply that
               -- system.
               [2] TimeStamp,
               [3] SEQUENCE OF CallIdentity,
               -- ConnectionBreak Information
               -- The following three parameters are considered ConnectionBreak
               -- Information. Include at least one of the following.
       removedParties        [4]    SEQUENCE OF PartyIdentity            OPTIONAL,
       remainingParties      [5]    SEQUENCE OF PartyIdentity            OPTIONAL,
       droppedParties        [6]    SEQUENCE OF PartyIdentity            OPTIONAL
}
```

See 5.4.7 “ConnectionBreak” on page 53 for the Stage 2 description.

6.3.8 DialedDigitExtraction Message

The DialedDigitExtraction message reports post cut-through digits dialed by the intercept subject.

PN-4465-RV1

```
DialedDigitExtraction ::= SEQUENCE {
               [0] CaseIdentity,
               [1] IAPSystemIdentity                OPTIONAL,
               -- include to identify the system containing the Intercept Access
               -- Function when the underlying data carriage does not imply that
               -- system.
               [2] TimeStamp,
               [3] CallIdentity,
digits         [4] VisibleString (SIZE (1..32))
               -- e.g., “12345” or “*123” or “#345”
}
```

See 5.4.8 “DialedDigitExtraction” on page 54 for the Stage 2 description.

6.3.9 NetworkSignal Message

The NetworkSignal message reports network signals sent to the intercept subject.

```
NetworkSignal ::= SEQUENCE {
               [0] CaseIdentity,
               [1] IAPSystemIdentity                OPTIONAL,
               -- include to identify the system containing the Intercept Access
               -- Function when the underlying data carriage does not imply that
               -- system.
               [2] TimeStamp,
               [3] CallIdentity                     OPTIONAL,
               -- Signal
               -- The following four parameters are considered network-generated
               -- signals. Include at least one of the following four parameters to
               -- identify the signal being applied by the IAP.

alertingSignal        [4] AlertingSignal                  OPTIONAL,
subjectAudibleSignal  [5] AudibleSignal                   OPTIONAL,
terminalDisplayInfo   [6] TerminalDisplayInfo             OPTIONAL,
other                 [7] VisibleString (SIZE (1..128))   OPTIONAL
                      -- e.g., standard announcement or name of an announcement as
                      -- per ANSI-41.
}
```

See 5.4.9 “NetworkSignal” on page 55 for the Stage 2 description.

PN-4465-RV1

6.3.10 Origination Message

The Origination message reports authorized connection-oriented call origination attempts or number translations for the intercept subject performed by the Access Function.

```
Origination ::= SEQUENCE {
               [0] CaseIdentity,
               [1] IAPSystemIdentity                OPTIONAL,
               -- include to identify the system containing the Intercept Access
               -- Function when the underlying data carriage does not imply that
               -- system.
               [2] TimeStamp,
               [3] CallIdentity,
calling        [4] PartyIdentity                    OPTIONAL,
               -- include, when more specific than the subject identity associated
               -- with the CaseIdentity, to identify the calling party
called         [5] PartyIdentity                    OPTIONAL,
               -- include if known
input          CHOICE {
userInput              [6] VisibleString (SIZE (1..32)),
                       -- use if input is known to be from the user
                       -- e.g., “” (hot line), “12025551234” or “*123”
translationInput       [7] VisibleString (SIZE (1..32))
                       -- use for inputs to translation
                       -- e.g., “” (hot line), “12025551234” or “*123”
               },
               [8] Location                         OPTIONAL,
               -- Include, when the location information is reasonably available to
               -- the IAP and delivery is authorized, to identify the location of
               -- an intercept subject’s mobile terminal
               [9] TransitCarrierIdentity           OPTIONAL,
               -- include if known
               [10] EXPLICIT BearerCapability       OPTIONAL
               -- include if known (or presumed)
}
```

See 5.4.10 “Origination” on page 58 for the Stage 2 description.

6.3.11 PacketEnvelope Message

The PacketEnvelope message delivers intercepted packets to an LEA.

```
PacketEnvelope ::= SEQUENCE {
                       [0] CaseIdentity,
                       [1] IAPSystemIdentity                OPTIONAL,
                       -- include to identify the system containing the Intercept
       Access
                       -- Function when the underlying data carriage does not imply
                       -- that system.
                       [2] TimeStamp,
                       [3] CallIdentity                     OPTIONAL,
                       [4] Location                         OPTIONAL,
                       -- Include, when the location information is reasonably
```

PN-4465-RV1

```
        available
                        -- to the IAP and delivery is authorized, to identify the
                        -- location of an intercept subject's mobile terminal
packetInformation       CHOICE {
isdnUserToUserSignaling         [5] SEQUENCE {
callIdentity                            [0] CallIdentity,
sending                                 [1] PartyIdentity,
interceptedUUPacket                     [2] OCTET STRING (SIZE (1..128))     OPTIONAL
                                        -- Encoded according to T1.607 User-to-user
                                        -- information element starting with Octet 4.
                                },

tiaEia41ShortMessageService     [6] SEQUENCE {
originalOriginatingAddress              [0] PartyIdentity,
originalDestinationAddress              [1] PartyIdentity,
originatingAddress                      [2] PartyIdentity     OPTIONAL,
                                        -- include if known and different than the
                                        -- originalOriginatingAddress
destinationAddress                      [3] PartyIdentity     OPTIONAL,
                                        -- include if known and different than the
                                        -- original destinationAddress
smsTeleserviceIdentifier                [4] INTEGER (-32768.32767),--see TIA/EIA-41
interceptedISSMSPacket                  [5] OCTET STRING (SIZE (1.255))      OPTIONAL
                                },

gsmSMShortMessageService        [7] SEQUENCE {
senderAddress                           [0] PartyIdentity,
receiverAddress                         [1] PartyIdentity,
interceptedGSMSMSPacket                 [2] OCTET STRING (SIZE (1..255))     OPTIONAL
                                },

wirelessIPService               [8] SEQUENCE {
                                        -- This parameter may also be used for
                                        -- information pertaining to non-wireless
                                        -- IP-based services.
originatingAddress                      [0] PartyIdentity,
destinationAddress                      [1] PartyIdentity,
interceptedIPPacket                     [2] OCTET STRING (SIZE (1..70000))   OPTIONAL
                                }
                        }
}
```

See 5.4.11 “PacketEnvelope” on page 59 for the Stage 2 description.

PN-4465-RV1

6.3.12 Redirection Message

The Redirection message indicates that an incoming connection-oriented call attempt, originally directed toward a subject, has been redirected by the subject.

```
Redirection ::= SEQUENCE {
               [0] CaseIdentity,
               [1] IAPSystemIdentity                OPTIONAL,
               -- include to identify the system containing the Intercept Access
               -- Function when the underlying data carriage does not imply that
               -- system.
               [2] TimeStamp,
               [3] CallIdentity,
redirectedTo   [4] PartyIdentity,
               [5] TransitCarrierIdentity           OPTIONAL,
               -- include if known
               [6] EXPLICIT BearerCapability        OPTIONAL,
               -- include if known (or presumed)
systemIdentity [7] VisibleString (SIZE (1..15))     OPTIONAL
               -- include when a call to a wireless subscriber is redirected to
       another
               -- TSP and that identity is reasonably available.
               -- e.g., “MSCID-12345-123” or “2025551234”
}
```

See 5.4.12 “Redirection” on page 60 for the Stage 2 description.

6.3.13 Release Message

The Release message is used to report that a connection-oriented call has been released.

```
Release ::= SEQUENCE {
               [0] CaseIdentity,
               [1] IAPSystemIdentity                OPTIONAL,
               -- include to identify the system containing the Intercept Access
               -- Function when the underlying data carriage does not imply that
               -- system.
               [2] TimeStamp,
               [3] CallIdentity,
               [4] Location                         OPTIONAL,
               -- Include, when the location information is reasonably available to
               -- the IAP and delivery is authorized, to identify the location of
               -- an intercept subject’s mobile terminal
systemIdentity [5] VisibleString (SIZE (1..15))     OPTIONAL
               -- include, when a handed-off wireless call is released while being
               -- served by another TSP to identify the last known TSP serving the
               -- subject, e.g., “MSCID-12345-123” or “2025551234”
}
```

See 5.4.13 “Release” on page 61 for the Stage 2 description.

PN-4465-RV1

6.3.14 ServingSystem Message

The ServingSystem message is used to report a change in the current TSP or service area for terminal or personal mobility.

```
ServingSystem ::= SEQUENCE {
               [0] CaseIdentity,
               [1] IAPSystemIdentity                OPTIONAL,
               -- include to identify the system containing the Intercept Access
               -- Function when the underlying data carriage does not imply that
               -- system.
               [2] TimeStamp,
systemIdentity [3] VisibleString (SIZE (1..15))     OPTIONAL,
               -- include, when authorizing service to a TSP, to identify the TSP
               -- e.g., “MSCID-12345-123” or “2025551234”
networkAddress [4] VisibleString (SIZE (1..15))     OPTIONAL
               -- include if the serving TSP can only be identified by
               -- a redirect-to number e.g., a personal or residential base station
               -- directory number “2025551234”
}
```

See 5.4.14 “ServingSystem” on page 62 for the Stage 2 description.

6.3.15 SubjectSignal Message

The SubjectSignal message reports all signaling input by the intercept subject.

```
SubjectSignal ::= SEQUENCE {
               [0] CaseIdentity,
               [1] IAPSystemIdentity                OPTIONAL,
               -- include to identify the system containing the Intercept Access
               -- Function when the underlying data carriage does not imply that
               -- system.
               [2] TimeStamp,
               [3] CallIdentity                     OPTIONAL,
signal         [4] SEQUENCE {
               -- signal
               -- The following four parameters are considered subject-initiated
               -- signaling information. Include at least one of the following four
               -- parameters to identify the subject-signaling information being
               -- reported.
       switchhookFlash              [0] VisibleString (SIZE (1..128))    OPTIONAL,
                                    -- e.g, “FLASH”
       dialedDigits                 [1] VisibleString (SIZE (1..128))    OPTIONAL,
                                    -- e.g. “12013452367”, “*123”,
       featureKey                   [2] VisibleString (SIZE (1..128))    OPTIONAL,
                                    -- e.g.  “KEY1”, “HOLD”, “CONFERENCE” or any
       other
                                    -- function key.
       otherSignalingInformation    [3] VisibleString (SIZE (1..128))    OPTIONAL
                                    -- e.g., “HOME”
               }
}
```

See 5.4.15 “SubjectSignal” on page 63 for the Stage 2 description.

PN-4465-RV1

6.3.16 TerminationAttempt Message

The TerminationAttempt message is used to report a connection-oriented call termination attempt.

```
TerminationAttempt ::= SEQUENCE {
               [0] CaseIdentity,
               [1] IAPSystemIdentity                OPTIONAL,
               -- include to identify the system containing the Intercept Access
               -- Function when the underlying data carriage does not imply that
               -- system.
               [2] TimeStamp,
               [3] CallIdentity,
calling        [4] PartyIdentity,
called         [5] PartyIdentity                    OPTIONAL,
               -- include, when more specific than the subject identity associated
               -- with the CaseIdentity, to identify the called party.
               [6] EXPLICIT BearerCapability        OPTIONAL,
               -- included when known (or presumed)
               [7] RedirectedFromInformation        OPTIONAL
               -- include if this termination attempt is a result of a redirected
               -- call.
}
```

See 5.4.16 “TerminationAttempt” on page 64 for the Stage 2 description.

PN-4465-RV1

6.4 CDC Parameter Definitions

6.4.1 AlertingSignal

The AlertingSignal parameter defines the pitch and cadence of the alerting (ringing) signal. The AlertingSignal parameter shall be encoded as follows:

```
AlertingSignal ::= ENUMERATED {
        notUsed                (0),
        alertingPattern0       (1), -- normal alerting
        alertingPattern1       (2), -- distinctive alerting - Intergroup
        alertingPattern2       (3), -- distinctive alerting: Special/Priority
        alertingPattern3       (4), -- Electronic Key Telephone Service
        alertingPattern4       (5), -- reminder ring
        callWaitingPattern1    (6), -- basic call waiting tone
        callWaitingPattern2    (7), -- incoming additional call tone
        callWaitingPattern3    (8), -- priority additional call tone
        callWaitingPattern4    (9), -- distinctive call waiting tone
        bargeInTone            (10)
}
```

See “NetworkSignal Message” on page 80.

6.4.2 AudibleSignal

The AudibleSignal parameter is used to report the type of audible tone that is generated by the IAP switch and applied to the intercept subject. The AudibleSignal parameter shall be encoded as follows:

```
AudibleSignal ::= ENUMERATED {
        notUsed                (0),
        dialTone               (1),
        recallDialTone         (2),
        ringbackTone           (3),    -- RingbackTone or AudibleAlerting
        reorderTone            (4),    -- ReorderTone or CongestionTone
        busyTone               (5),
        confirmationTone       (6),
        expensiveRouteTone     (7),
        messageWaitingTone     (8),
        receiverOffHookTone    (9),
        specialInfoTone        (10),
        denialTone             (11),
        interceptTone          (12),   --InterceptTone or MobileReorder
        answerTone             (13),
        tonesOff               (14),
        pipTone                (15),
        abbreviatedIntercept   (16),
        abbreviatedCongestion  (17),
        warningTone            (18),
        dialToneBurst          (19),
        numberUnObtainableTone (20),
        authenticationFailTone (21)
}
```

See “NetworkSignal Message” on page 80.

PN-4465-RV1

6.4.3 BearerCapability

The BearerCapability parameter indicates a requested or granted bearer service.

```
BearerCapability ::= CHOICE {
        speech                [0] NULL,
        f3100HzAudio          [1] NULL,
        bearerCapInfoElement  [2] OCTET STRING (SIZE (1..64))
                -- encoded according to T1.607 Bearer Capability information
                -- element starting with octet 3
}
```

6.4.4 CallIdentity

The CallIdentity parameter is used to uniquely identify a particular call, call appearance, or call legs within the context of a single system. The CCOpen and Change messages can correlate the CallIdentity to one or more CCCs when content is delivered. A CallIdentity may be created with a CCOpen, Origination, TerminationAttempt, NetworkSignal or Change message. A CallIdentity may be released for other uses with a Release or Change message. CallIdentity shall not be immediately re-used. HLRs and similar systems that do not correlate messages with CallIdentity(ies) do not need to release the CallIdentity.

```
CallIdentity ::= SEQUENCE {
sequenceNumber        [0] VisibleString (SIZE (1..25)),
systemIdentity        [1] VisibleString (SIZE (1..15))     OPTIONAL
                      -- include when the system issuing the sequenceNumber is
                      -- different than the accessing system.
                      -- e.g., CLLI code, “MSCID-12345-123” or “2025551234” (E.164
                      -- address of node)
}
```

6.4.5 CaseIdentity

The CaseIdentity parameter contains a case identity assigned by the LEA for a particular electronic surveillance. The CaseIdentity will be designated by the LEA and provided to a TSP at the time of provisioning of an electronic surveillance.

```
CaseIdentity ::= VisibleString (SIZE (1..25))
                -- e.g., “FBI-12345” or “NYPD-12345”
```

PN-4465-RV1

6.4.6 CCCIdentity

The CCCIdentity parameter identifies the CCC or pair of CCCs used for conveying call content. Each CCC is identified with a VisibleString which may contain a directory number (e.g., “202-555-1111”), a trunk identity (e.g., “FBITG-001” or “LAES-999”), an IP network address (e.g., “IP: 101.012.103.104:100”) or an X.25 network address (e.g., “X121: 1234-5678901234”).

```
CCCIdentity ::= CHOICE {
combCCC        [0] VisibleString (SIZE (1..20)),    -- combined CCC
sepCCCpair     [1] SEQUENCE {                       -- separated CCC
sepXmitCCC            [0] VisibleString (SIZE (1..20)), -- transmit path
                      -- (from the intercept subject or redirected-to party)
sepRecvCCC            [1] VisibleString (SIZE (1..20)) -- receive path
                      -- (to the intercept subject or redirected-to party)
               },
indXmitCCC     [2] VisibleString (SIZE (1..20)), -- individual transmit path
               -- (from the intercept subject or redirected-to party)
indRecvCCC     [3] VisibleString (SIZE (1..20)), -- individual receive path
               -- (to the intercept subject or redirected-to party)
indCCC         [4] VisibleString (SIZE (1..20)) -- individual CCC without
               -- a specified direction. Use only in CCClose messages.
}
```

6.4.7 IAPSystemIdentity

The IAPSystemIdentity parameter identifies the system of the Intercept Access Point and should not imply the specific location of an intercept subject.

```
IAPSystemIdentity ::= VisibleString (SIZE (1..15))
        -- e.g., CLLI code, “MSCID-12345-123” or “2025551234” (E.164 address of
        node)
```

6.4.8 Location

The Location parameter identifies the cell of the subject’s mobile terminal. A toggle capability must be provided on a per surveillance basis.

```
Location ::= VisibleString (SIZE (1..32))    -- e.g., “WESTGATE” or “CELL017”
```

PN-4465-RV1

6.4.9 PartyIdentity

The PartyIdentity parameter identifies a party to a call or call attempt.

```
PartyIdentity ::= SEQUENCE {
                        -- include those identification elements necessary to
                        -- uniquely identify the party known at the point in call and
                        -- are authorized. At least one of the following parameters
                        -- is required.

esn                     [0] VisibleString (SIZE (8))                OPTIONAL,
                        -- AMPS-based Electronic Serial Number
                        -- a hexadecimal string e.g., “82ABCDEF”
imei                    [1] VisibleString (SIZE (1..15))            OPTIONAL,
                        -- GSM-based International Mobile Equipment Identity
tei                     [2] VisibleString (SIZE (1..15))            OPTIONAL,
                        -- ISDN-based Terminal Equipment Identity
spid                    [3] VisibleString (SIZE (3..20))            OPTIONAL,
                        -- ISDN-based Service Profile Identifier
imsi                    [4] VisibleString (SIZE (1..15))            OPTIONAL,
                        -- International Mobile Station Identity
                        -- E.212 number beginning with Mobile Country Code
min                     [5] VisibleString (SIZE (10))               OPTIONAL,
                        -- AMPS-based Mobile Identification Number
dn                      [6] VisibleString (SIZE (1..15))            OPTIONAL,
                        -- e.g., called directory number or network provided calling
                        -- number.
userProvided            [7] VisibleString (SIZE (1..15))            OPTIONAL,
                        -- user provided calling number as supplied
appearanceId            [8] VisibleString (SIZE (1..15))            OPTIONAL,
                        -- include for instruments or services with multiple line,
                        -- station, or call appearances
callingCardNum          [9] VisibleString (SIZE (1..20))            OPTIONAL,
ipAddress               [10] VisibleString (SIZE (1..32))           OPTIONAL,
                        -- IPv4 addressing with decimal quad notation e.g.,
                        -- “123.123.123.123” (not a URL)
x121                    [11] VisibleString (SIZE (1..15))           OPTIONAL,
                        -- begin with DNIC
trunkId                 [12] VisibleString (SIZE (1..32))           OPTIONAL,
                        -- indicate trunk group, trunk number or both
                        -- This is usually used to identify an associate when other
                        -- identifying information is not available.
                        -- This may also identify a subject’s agent (e.g., screening
                        -- service).
subaddress              [13] OCTET STRING (SIZE (2..21))            OPTIONAL,
                        -- encoded according to T1.607 Subaddress information element
                        -- starting with octet 3.

genericAddress          [14] SEQUENCE OF VisibleString (SIZE (1..32))OPTIONAL,
                        -- indicate use of the generic address
genericDigits           [15] SEQUENCE OF VisibleString (SIZE (1..32))OPTIONAL,
                        -- indicate use of the generic digits
genericName             [16] SEQUENCE OF VisibleString (SIZE (1..48))OPTIONAL,
                        -- indicate use of the generic name
port                    [17] VisibleString (SIZE (1..32))           OPTIONAL,
                        -- identify a particular equipment port.
                        -- This is used to identify an associate when other
                        -- identifying information is not available.
context                 [18] VisibleString (SIZE (1..64))           OPTIONAL,
                        -- when none of the other identities are known or to
                        -- identify the context and special considerations of the
                        -- supplied identifier(s), especially when the identifier(s)
                        -- is (are) abnormal (e.g., international, private,
```

PN-4465-RV1

```
        restricted,
                        -- operator, no address, hotel/motel, coin, etc.)
isdnHighLayer           [19] OCTET STRING (SIZE (2..14))            OPTIONAL,
                        -- include if known
                        -- encoded according to T1.607 High Layer Compatibility
                        -- information element starting with octet 3
isdnLowLayer            [20] OCTET STRING (SIZE (2..14))            OPTIONAL
                        -- include if known
                        -- encoded according to T1.607 Low Layer Compatibility
                        -- information element starting with octet 3
}
```

6.4.10 PDUType

The PDUType parameter indicates the intercepted packet type on a CCC (e.g., see Annex B.1). Negative values are reserved for bilateral agreement or protocol extension.

```
PDUType ::= ENUMERATED {
        isdnBchannel   (0),    -- see BearerCapability parameter
        isdnDchannel   (1),    -- intermixed Q.931, Q.932, and X.25
        ip             (2),    -- Internet protocol packets
        ppp            (3),    -- Internet point-to-point protocol packets
        x25            (4)     -- X.25 LAPB packets
}
```

See “CCOpen Message” on page 77.

6.4.11 RedirectedFromInformation

The RedirectedFromInformation parameter is used to report information about the last redirecting party and the original redirecting party on calls that are redirected to the subject.

```
RedirectedFromInformation ::= SEQUENCE {
lastRedirecting         [0] PartyIdentity                    OPTIONAL,
                        -- include if known
originalCalled          [1] PartyIdentity                    OPTIONAL,
                        -- include if known
numRedirections         [2] INTEGER (1..100)                 OPTIONAL
                        -- include if known
}
```

See “TerminationAttempt Message” on page 85.

PN-4465-RV1

6.4.12 TerminalDisplayInfo

The TerminalDisplayInfo parameter is used to report information that is displayed on the intercept subject's terminal. The TerminalDisplayInfo parameter shall be encoded as follows:

```
TerminalDisplayInfo   ::= SEQUENCE {
        generalDisplay        [0] VisibleString (SIZE(1..80))      OPTIONAL,
        calledNumber          [1] VisibleString (SIZE(1..40))      OPTIONAL,
        callingNumber         [2] VisibleString (SIZE(1..40))      OPTIONAL,
        callingName           [3] VisibleString (SIZE(1..40))      OPTIONAL,
        originalCalledNumber  [4] VisibleString (SIZE(1..40))      OPTIONAL,
        lastRedirectingNumber [5] VisibleString (SIZE(1..40))      OPTIONAL,
        redirectingName       [6] VisibleString (SIZE(1..40))      OPTIONAL,
        redirectingReason     [7] VisibleString (SIZE(1..40))      OPTIONAL,
        messageWaitingNotif   [8] VisibleString (SIZE(1..40))      OPTIONAL
}
```

See "NetworkSignal Message" on page 80.

6.4.13 TimeStamp

The TimeStamp parameter identifies the date and time of access.

```
TimeStamp ::= GeneralizedTime
```

6.4.14 TransitCarrierIdentity

The TransitCarrierIdentity parameter identifies an interexchange carrier.

```
TransitCarrierIdentity ::= VisibleString (SIZE (3..7))
                -- the carrier access code (if applicable) and carrier
        identification
                -- code e.g., "123" or "10123" or "1012345" or "9501234"
END
```

6.5 cdma2000 Abstract Syntax for Packet Data CII Delivery

```
CDMA2000CIIModule {iso(1) member-body(2) us(840) ti(113737) laes(2) tr45(0)
        cdma2000(1) cii(0) version-1(0)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS
        CaseIdentity, Timestamp

FROM Laesp-j-std-025-b{iso(1) member-body(2) us(840) ti(113737) laes(2) tr45(0) j-
        std-025(0) j-std-025-b(2) version-1(0)};
```

PN-4465-RV1

```
CDMA2000LAESMessage::= SEQUENCE
{
        cdma2000ModuleId       [0] CDMA2000CIIModule,
        cdma2000LAESMessageType[1] CDMA2000LAESMessageType
}

CDMA2000LAESMessageType::=CHOICE
{
        cdma2000PacketDataSessionEstablishment[0]
                                CDMA2000PacketDataSessionEstablishment,
        cdma2000PacketDataSessionTermination [1]
                                 CDMA2000PacketDataSessionTermination,
        cdma2000PacketDataInterceptStart     [2]
                                 CDMA2000PacketDataInterceptStart,
        cdma2000PacketDataServingSystem      [3]
                                 CDMA2000PacketDataServingSystem,
        cdma2000PacketDataPacketFilterInfo   [4]
                                 CDMA2000PacketDataPacketFilterInformation
}

-- message definitions

CDMA2000PacketDataSessionEstablishment ::= SEQUENCE
{
        caseIdentity           [0] CaseIdentity,
        iapSystemIdentity      [1] SystemIdentity            OPTIONAL,
        timeStamp              [2] TimeStamp,
        subjectIPAddress       [3] IpAddress,
        subjectIdentity        [4] SubjectId                 OPTIONAL,
        ipAssignment           [5] IpAssignment              OPTIONAL,
        haIPAddress            [6] IpAddress                 OPTIONAL,
        faCoA                  [7] IpAddress                 OPTIONAL,
        correlationNumber      [8] CorrelationNumber         OPTIONAL,
        locationInformation    [9] Location                  OPTIONAL,
        failureReason          [10] SessionEstablishmentFailureOPTIONAL,
        ccAddress              [11] CCAddress                OPTIONAL
}


CDMA2000PacketDataSessionTermination ::= SEQUENCE
{
        caseIdentity           [0] CaseIdentity,
        iapSystemIdentity      [1] SystemIdentity            OPTIONAL,
        timeStamp              [2] TimeStamp,
        subjectIPaddress       [3] IpAddress,
        haIPaddress            [4] IpAddress                 OPTIONAL,
        faCoA                  [5] IpAddress                 OPTIONAL,
        correlationNumber      [6] CorrelationNumber         OPTIONAL,
        locationInformation    [7] Location                  OPTIONAL,
        terminationReason      [8] SessionTerminationReason  OPTIONAL
}
```

PN-4465-RV1

```
CDMA2000PacketDataInterceptStart ::= SEQUENCE
{
        caseIdentity            [0] CaseIdentity,
        iapSystemIdentity       [1] SystemIdentity          OPTIONAL,
        timeStamp               [2] TimeStamp,
        subjectIPaddress        [3] IpAddress,
        subjectIdentity         [4] SubjectId               OPTIONAL,
        ipAssignment            [5] IpAssignment            OPTIONAL,
        haIPaddress             [6] IpAddress               OPTIONAL,
        faCoA                   [7] IpAddress               OPTIONAL,
        correlationNumber       [8] CorrelationNumber       OPTIONAL,
        locationInformation     [9] Location                OPTIONAL,
        ccAddress               [10] CCAddress              OPTIONAL

}

CDMA2000PacketDataServingSystem ::= SEQUENCE
{
        caseIdentity            [0] CaseIdentity,
        iapSystemIdentity       [1] SystemIdentity          OPTIONAL,
        timeStamp               [2] TimeStamp,
        subjectIPaddress        [3] IpAddress               OPTIONAL,
        subjectIdentity         [4] SubjectId               OPTIONAL,
        servingSystemIdentity   [5] SystemIdentity,
        haIPaddress             [6] IpAddress               OPTIONAL,
        faCoA                   [7] IpAddress               OPTIONAL
}

CDMA2000PacketDataPacketFilterInformation ::= SEQUENCE
{
        caseIdentity                [0] CaseIdentity,
        iapSystemIdentity           [1] SystemIdentity          OPTIONAL,
        timeStamp                   [2] TimeStamp,
        subjectIPaddress            [3] IpAddress,
        subjectIdentity             [4] SubjectId               OPTIONAL,
        haIPaddress                 [5] IpAddress               OPTIONAL,
        faCoA                       [6] IpAddress               OPTIONAL,
        packetFilterInformation     [7] SET OF PacketFilterInformation,
        correlationNumber           [8] CorrelationNumber       OPTIONAL
}
```

PN-4465-RV1

```
--parameter definitions

CCAddress ::=SEQUENCE
{
        leaIPAddress                    [0] IpAddress,
        leaPortNumber                   [1] PortNumber
}
        --The CCAddress (LEA IP Address and Port Number) for delivery of content
        --associated with the packet data communication session is pre-provisioned
        --based on mutual agreement between the LEA and the carrier for the
        --CaseIdentity.
        --A single CCAddress may be used to deliver content for all packet data
        --sessions (associated with a caseIdentity) or a unique CCAddress may be
        --used for each packet data session.


CorrelationNumber ::= OCTET STRING

IpAddress ::= CHOICE
{
        ipV4                            [1] IPvalue,
        ipV6                            [2] IPvalue,
        none                            [3] NULL
}

IpAssignment ::= ENUMERATED
{
        static                          (1),
        dynamic                         (2),
        unknown                         (3)
}

IPvalue ::= OCTET STRING (SIZE(4..16))
                        --this field will be coded in binary.

LocationInformation ::= OCTET STRING
                        -- The Location information shall be encoded with Cell
                        -- Identifier information as specified in TIA/IS-2001.

PacketFilterInformation ::= OCTET STRING
                        -- Formatted as defined by Packet Filter Content SubOption in
                        -- TIA-835-C.
PortNumber ::=INTEGER
                        --the value of the port number may be chosen from the
                        -- “ephemeral” range.

SessionFailureReason ::= VisibleString

SessionTerminationReason ::= VisibleString

SubjectId ::= SET
{
        nai                             [1] OCTET STRING,
        msid                            [2] OCTET STRING
                        --The MSID shall be encoded with an IMSI as specified in
                        -- TIA/IS-2001.
```

PN-4465-RV1

```
}

SystemIdentity ::= CHOICE
{
        ipV4                            [1] IPvalue,
        ipV6                            [2] IPvalue,
        fqdn                            [3] OCTET STRING
}

END                     --of CDMA2000CIIModule
```

6.6 CCC Protocols

The transferred information and messages shall be encoded to be binary compatible with *X.208 Abstract Syntax Notation One* (ASN.1) and the *X.209 Basic Encoding Rules* (BER). For information on these encoding rules please see section 6.2.3 on page 74.

6.6.1 CCC Encoding for Circuit-Mode Services

Call content shall be encoded on CCCs using a standard or widely used network bearer services. The intercepted content shall be delivered without modifying the content within the quality objectives for the intercepted network bearer service. Speech and 3.1 kHz audio bearer services intercepted and delivered over circuit-mode digital facilities shall use the μ-law encoding of ITU-T Recommendation *G.711*, *Pulse Code Modulation (PCM) of voice frequencies*.

Signaling on the CCC or out-of-band signaling may be used to inform the LEA when call content is being delivered.

6.6.2 CCC Encoding for Packet-Mode Services

Intercepted packet-mode data communications shall be delivered to an LEA when a CCC is used by forwarding the intercepted Protocol Data Units (PDUs) employing a standard or widely used protocol. The intercepted PDUs shall include sufficient addressing information to associate the PDU with the parties of the communication. The intercepted PDUs shall be delivered without modification, except for possible re-framing, segmentation, or enveloping required to transport the information to the Collection Function.

The choice of packet delivery protocol is determined at the time that the intercept is provisioned. This delivery method remains in effect until changed by subsequent provisioning.

6.6.2.1 cdma2000 Abstract Syntax Notation for Packet Data CC Delivery

```
CDMA2000CCModule {iso(1) member-body(2) us(840) ti(113737) laes(2) tr45(0)
```

PN-4465-RV1

```
        cdma2000(1) cc(1) version-1(0)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

        CaseIdentity, TimeStamp

FROM Laesp-j-std-025-b {iso(1) member-body(2) us(840) ti(113737) laes(2) tr45(0) j-
        std-025-b(2) version-1(0)}

        CorrelationNumber

FROM CDMA2000CIIModule {iso(1) member-body(2) us(840) ti(113737) laes(2) tr45(0)
        cdma2000(1) cii(0) version-1(0)};


CCIPPacketHeader::=SEQUENCE
{
        clicHeader              [1] CLICheader,
        payload                 [2] OCTET STRING
}

CLICheader ::= SEQUENCE
{
        cdma2000ccpsmoduleID    [0] OBJECT IDENTIFIER,
        version                 [1] Version,
        caseIdentity            [2] CaseIdentity,
        correlationNumber       [3] CorrelationNumber         OPTIONAL,
        timeStamp               [4] TimeStamp,
        sequenceNumber          [5] INTEGER (0..65535),
        iPPacketDirection       [6] IPPacketdirection         OPTIONAL,
        ...
}

Version ::= ENUMERATED
{
        version1(1)
}

IPPacketdirection ::= ENUMERATED
{
        fromSubject             [1],
        toSubject               [2],
        unknown                 [3]
}

END     --of CDMA2000CCModule
```

6.7 LAESP Compatibility Guidelines

The guidelines ensure that there is no long term impediment to the evolution of networks and the implementation of significant new functionality.

PN-4465-RV1

6.7.1 Guidelines For Forward Compatibility

When developing a new protocol or enhancing an existing protocol, it is important to remember that a node using one version of protocol may, in the future, need to communicate with nodes using the enhanced version of the basic protocol. Hence, the protocol should be easy to enhance (e.g., easy to add new optional parameters). In addition, procedures should be built into the existing protocol to handle the situations when new messages, known messages with unknown parameters, or known parameters with unknown codes are received.

All revisions of this Standard shall contain a mechanism for forward compatibility. The following list contains the basic requirements of the mechanism:

a. When the LAESP message is received and it contains all the required parameters, the additional parameters in the received message, known or unknown, may be ignored. The received message should not be rejected because of the unknown parameters in it. In cases that the received message should be relayed to another node, the additional parameters should be passed unchanged.

b. For existing protocols, state the action to be taken on receipt of spare or reserved values of defined parameters (e.g., treat as appropriate default values, transmit them unchanged at the intermediate nodes, and ignore them at the end nodes).

c. State that all new messages shall have the ability to add new optional fields.

d. Unallocated codes of defined fields should be examined and handled as either spare codes or a default code.

6.7.2 Guidelines For Backward Compatibility

When enhancing an existing protocol, it is important to keep in mind that a node using one version of a protocol may need to communicate with nodes using older versions of the same protocol. Hence, the protocol should not be changed abruptly into a form which the earlier protocol versions cannot even interpret. For example, one should not change a fixed length mandatory parameter to an optional parameter in an existing message.

All revisions of this Standard shall contain a mechanism for backward compatibility. The following list contains the basic guidelines to be included.

6.7.2.1 Existing Messages

a. The ability of receiving any existing messages shall be possible, since the removal of a message implies the removal of a function.

b. The effect of receiving any existing message, parameter, or function in a new version, must be the same as that in previous versions. The effects of new parameters or parameter values will thus be purely additive.

PN-4465-RV1

6.7.2.2 Parameters in Existing Messages

Message parameters in the Parameter Set consist of 2 basic types, mandatory and optional, and need not occur in a pre-defined order. All mandatory and optional parameters have variable length, although some parameters may have their length restricted.

The following guidelines shall apply:

a. Optional parameters shall not become mandatory.

b. Mandatory parameters shall not become optional.

c. Additional mandatory parameters shall not be added to an existing message.

d. Additional optional parameters can be added to an existing message.

e. Existing mandatory parameters shall not be removed from existing messages.

f. The range of any parameter for an existing message shall not be reduced.

g. The meaning of any defined parameter value shall not be changed on an existing message.

h. There are no restrictions on the parameters for new messages.

i. The sequence of parameters in an existing SEQUENCE type shall not be changed.

j. New parameters may be added to the end of an existing SEQUENCE type. (The value of the parameter identifiers used may be in any order to allow addition of existing parameters to an existing SEQUENCE type.)

k. New parameters may be added to an existing CHOICE type, unless the CHOICE is mandatory.

6.7.2.3 New Messages

New messages may be added after a Standard has been published; however, nodes that do not recognize these new messages will ignore them, internally indicating that the information was not recognized.

6.7.2.4 New Parameters

New optional parameters can be added to existing messages after a Standard has been published; however, nodes that do not recognize these new parameters may ignore them.

6.7.2.5 New Parameter Fields

New fields may be added to, or spare fields may be used in existing parameters; however, nodes that do not recognize these new fields may ignore these fields.

PN-4465-RV1

6.7.2.6 New Parameter Values

Previously spare, reserved, or unallocated parameter values can be used. These will be treated at the receiving node as defined in Item b of Section 6.7.1.

PN-4465-RV1

Annex A Deployment Examples

This Annex is informative and is not considered part of this Standard.

A.1 Possible Network Deployment of IAPs

IAPs may be implemented at a variety of points within a network, depending on the particular telecommunication equipment's architecture, the features and services that are being monitored, and the impact the monitoring at the selected point may have on normal call operation. Generally, it may be assumed that the primary location of the major IAPs are located in the network equipment shown in Table 24.

Table 24: **IAP Primary Locations**

IAP	Primary Equipment Location
CIAP	Circuit-mode switch
IDIAP	Circuit-mode or packet-mode switch
PDIAP	Packet-mode switch
SSIAP	Home Location Register

It is, however, possible to locate these IAPs within other types of equipment. It should be understood that an IAP placed in a node not corresponding to the primary type of equipment may provide reduced functionality.

For land line subscribers Figure 12 depicts a possible deployment where the access points are in several different pieces of equipment.

Figure 12: **Land Line IAPs**

Mobile telephony is more complex. The IAPs for a given intercept subject may be spread across several different clusters of equipment. There is a cluster of equipment at the intercept subject's home and there is another cluster of equipment around the system providing service to the intercept subject. These two clusters may be one and the same, but the more general

PN-4465-RV1

problem is when they are separate. Indeed for some TSPs, these clusters are always separated.

Figure 13 shows possible IAPs deployed in a mobile intercept subject's home equipment cluster.

Figure 13: **Mobile Intercept Subject's Home System IAPs**

Figure 14 shows possible IAPs deployed in a mobile intercept subject's Serving System equipment cluster.

Figure 14: **Mobile Intercept Subject's Serving System IAPs**

PN-4465-RV1

When the Redirecting System is a system other than the intercept subject's Home System, it may be desirable to access all of these Redirecting Systems to gain access to the call content of calls intended for the intercept subject. Figure 15 shows possible IAPs.

Figure 15: **Mobile Intercept Subject's Redirecting System IAPs**

A.2 Access and Delivery Function Equipment Configuration

There are several switching equipment configurations possible for intercept functions.

One method is to use an external Delivery Function as shown in Figure 16.

Figure 16: **External Delivery Function**

The Delivery Function may be integrated into the switch itself. There are two basic variations on this theme dealing with how separate and distinct the administration interfaces remain. These are shown in Figure 17 and Figure 18.

PN-4465-RV1

Figure 17: **Integrated Delivery Function with a Non-Distinct Administration Interface**

Figure 18: **Integrated Delivery Function with a Distinct Administration Interface**

PN-4465-RV1

Mobile telephone systems may involve separate home and serving TSPs. This situation is shown in Figure 19.

Figure 19: **Mobile Telephone Systems with Two TSPs**

Mobile telephony may elect to use pivoted delivery when a single TSP controls the Home and Serving Systems, where the CDCs and CCCs are centralized in a Delivery Function before interfacing the Collection Function. This allows a single point to control the information delivered to the Collection Function.

PN-4465-RV1

Figure 20 shows pivoted delivery where two totally independent systems are used. (Note: e_{bis} is an *e*-interface protocol used between two delivery boxes.)

Figure 20: **Independently Administered External Pivoted Delivery**

PN-4465-RV1

In the functional model shown in Figure 21, the Access and Delivery Functions are split into two separate functional blocks with interfaces between those functional blocks to communicate with each other.

Figure 21: **A possible functional model for CALEA in Voice over Packet scenario**

A.3 Implementation of the *d*-interface

The CDC should support all of the IAPs within the interfaced Access Functions. This means that if something is required for a particular Access Function, it should be provided on the corresponding *d*-interface. For example, if an Access Function supports a Call-Identifying Information IAP (IDIAP) for an HLR, only the incoming calls and originating calls known to the HLR need to be reported. Even though the IDIAP allows for the reporting of all user signaling, the HLR IDIAP need only report the signaling to which it has access.

Any given Delivery Function need only provide one CCC delivery method. The delivery method chosen depends upon local economic, policy, and technical factors. For example, using dedicated circuits is appropriate to installations already having them and for smaller systems in future installations. A trunk group offers some efficiencies which may reduce costs on larger systems. A static directory number, although it may have questionable complexity, may technically provide the interface.

The Delivery Function should not generate call-identifying data and call content on its own, so there is little difference in the call associated and non-call associated messages from the IAPs. All of the call content should come

PN-4465-RV1

across the *d*-interface. The Delivery Function may resolve interface differences between *d*- and *e*-interfaces, so it may need to handle different CCC delivery methods.

If the *d*-interface for the CCC is within the premises of a TSP, the need for transmission devices and intervening networks may be eliminated and simpler non-error handling protocols may be appropriate.

Accesses may be either bridged or looped. In a bridged access, the communication is accessed directly (e.g., in a time slot interchanger or with a bridging circuit) within the Access Function. Separate circuits are brought out for the transmit and receive paths of the accessed communication, as shown in Figure 22.

Figure 22: **Bridged Access**

In looped access the accessed communication is switched out of the Access Function as a circuit, looped through the Delivery Function and back into the Access Function, as shown in Figure 23. The Delivery Function is responsible for accessing the communication from the looped circuit and not disrupting the looped communication.

The bridged and looped access methods are considered to be logically equivalent, even though they have different physical implementations. They both access the intercept subject's transmit and receive communication paths.

If a subscriber's communications are combined, then combined delivery from the Access Function is sufficient. Even though some communications (e.g., speech and 3.1 kHz audio) are fully separated, combined delivery may still be appropriate since the communications must work even when communicating with an interface that supports only combined delivery. Even though combined delivery is sufficient, separated delivery is technically possible, but may not be economically viable.

Separated delivery on the *d*-interface allows the combining to take place in the Delivery Function. Combined delivery may be provided on the *d*-interface if all communications accessed by the IAP are by nature combined. There is some middle ground for the decision to be made on a per call basis using the negotiated bearer capability. The Combining can take place on

PN-4465-RV1

Figure 23: **Looped Access**

either the Access or Delivery Function, provided that the communications that require separated delivery are not combined.

The bottom line for the choices is that they are subject to implementation decisions based on economic and TSP policy. It is likely that large systems may have different implementations than small systems.

A.4 Implementation of the *e*-interface

Any given Delivery Function need only provide one CCC delivery method. The delivery method chosen depends upon local economic, policy, and technical factors. For example, using dedicated circuits is appropriate to installations already having them and for smaller systems in future installations. Static directory numbers allows for some savings in the number of trunks required on the Delivery Function and Collection Function. Trunk groups may offer some savings for some installations.

When the *e*-interface is implemented between the Delivery Function and the Collection Function, there may be a number of different protocols used in the interface. This is because there may be intervening networks and specialized transmission devices (e.g., modems, DSUs, CSUs). The intervening network allows the LEA to procure its communication services from a TSP other than the TSP providing the Access Function. Transmission devices allow carriage of information which may not otherwise be possible (e.g., using a modem to carry data over an analog facility).

PN-4465-RV1

Figure 24 shows a few possibilities of the use of different transmission schemes on the *e*-interface. In general, the interface protocol provided by a Delivery Function (at the *e*-interface) need not be the same as the interface at the Collection Function (at the e_4-interface). The interface protocol stack for each interface is chosen at the agreement of the two ends of the transmission line. Only when there is a direct physical connection between the Delivery Function and the Collection Function should the interface protocols be the same.

Figure 24: **Possible Transmission Schemes for the *e*-Interface**

PN-4465-RV1

A.5 Possible CDC Protocol Stacks

Figure 25 illustrates possible CDC Protocol Stacks. These are not meant to be definitive or exhaustive, but rather illustrative.

Figure 25: **Possible CDC Protocol Stacks** **(Sheet 1 of 2)**

PN-4465-RV1

Figure 25: **Possible CDC Protocol Stacks** **(Sheet 2 of 2)**

Dedicated data circuits should be used when delivery delay is of utmost importance.

Dedicated data links should be used where communication resources may be combined for a single destination.

Packet switched links should be used where communication services may be combined and packet switching services are available.

A.6 Possible CCC Protocol Stacks

Figure 26 illustrates possible CCC Protocol Stacks. This is not meant to be definitive or exhaustive, but rather illustrative.

Dedicated circuits are used when no call content delivery delay can be tolerated and in traditional intercept arrangements. Dedicated circuits may require a long lead time to establish a connection. Additional subscribers may not be added to a dedicated circuit, although dedicated circuits may be provisioned before they are needed.

Trunk groups may be used when some call content delivery delay can be tolerated and there is a high volume of call content deliveries between two points. A trunk group with excess capacity may be used by a new intercept subject without additional provisioning. Circuits may be added to a trunk group as necessary. Each intercept subject may be assigned a minimum number to reserve an intercept capacity for the intercept subject. The sum of the minimums should not exceed the capacity of the trunk group. Each intercept subject may also be assigned a maximum to limit the number of circuits that an intercept subject may use. This requires the trunk group to

PN-4465-RV1

Figure 26: **Possible Circuit-Mode CCC Protocol Stacks**

have some excess capacity. This engineering is the same on both sides of the trunk group.

Static directory numbers may be used when some call content delivery delay can be tolerated and a high flexibility for provisioning intercepts is desired. Static directory numbers on the source side use a common trunk group. Adding a trunk to a source is independent of adding a trunk to a destination. Trunks may be added at will. Intercepts may also be added provided there is enough excess capacity. Each intercept subject may be assigned a minimum number to reserve an intercept capacity for the intercept subject on the source side. This same number should be reserved on the destination side. The sum of the minimums should not exceed the capacity of the trunk group. Each intercept subject is assigned a maximum number of circuits. The number of circuits on the destination side should at least be equal to the sum of the minimums, and the maximum should allow for whatever excess capacity is desired to prevent blocking. The engineering is different on source and destination sides. Blocking may occur on other side.

Packet-mode content may be delivered over the CDC (for a small number of packet types). Other packet-mode content should be delivered using CCCs, possibly over a packet data network, as shown Figure 27. Dedicated facilities or subnetworks may be used between the PDIAP and the LEA to provide appropriate levels of security and throughput.

PN-4465-RV1

Figure 27: **Possible Packet-Mode CCC Protocol Stacks**

---

1. The packet delivery rate of IP encapsulated in X.25 and run over an X.25 network may not provide adequate throughput.

PN-4465-RV1

Annex B CCC Delivery Methods

This Annex is informative and is not considered part of this Standard.

B.1 Circuit-Mode vs. Packet-Mode

Circuit-mode communications move call content either as a metallic analog electrical signal or as a constant rate stream of bits. The stream of bits can be conveyed by various mechanisms including an ISDN B-channel, a DS-0, or an ATM circuit (even though ATM has the characteristics of packet-mode communication, it is essentially providing a circuit-mode communication when constant bandwidth is requested). Circuit-mode communications may carry a packetized data service, but that is transparent to the switching system. Digital circuit-mode switches route bit streams to their destination. Digital circuit-mode intercepts route intercepted bit streams to the authorized LEA.

Packet-mode communications move call content as a variable rate stream of bits conveyed by packets. Packet-mode switches route individual packets to their destination. Packet-mode intercepts route intercepted packets to the authorized LEA.

A circuit-mode communication can be intercepted and delivered only over circuit-mode delivery. This delivery may use dedicated channels (using a channel number) or it may use channels established on demand (using a directory number). Any directory number assigned by an LEA can only be used by one IAP to avoid conflicts and busy treatment.

A packet-mode communication can be delivered over a packet-mode delivery using the same or a different packet delivery protocol. This delivery can use a connectionless service, a permanently established connection-oriented service, or a connection-oriented service established on demand. All packet-mode delivery services require individual network addresses at the LEA to separate call content from various subjects and intercept access points.

A packet-mode communication can also be delivered using a circuit-mode delivery to convey packetized information. The circuit-mode connection may use dedicated channels or it may establish channels on demand. Once the circuit-mode channel is established, the packet-mode contents can be delivered using a packet protocol on top of the circuit-mode channel. This packet delivery protocol can be defined by mutual agreement between the LEA and the TSP or the protocol can be identified by the Bearer Capability in the SETUP message when ISDN is used end-to-end. The same delivery channel can be used for both circuit-mode and packet-mode delivery as indicated by the presence of CallIdentity or PDUType parameters in the CCOpen message.

In all cases of packet-mode intercepts, the type of packet-mode communication being intercepted is communicated by the PDUType parameter in the CCOpen message. Circuit-mode intercept of packet communications are identified by the BearerCapability parameter in various LAESP messages.

PN-4465-RV1

B.2 Overview

This annex describes the CCC delivery service as a set of mechanisms, characteristics, and options that may be considered when selecting a CCC delivery method:

a. A CCC delivery method defining the overall signaling protocol:

   - Dedicated Circuit (see B.3);
   - Trunk Group (see B.4);
   - Static Directory Number (see B.5); or
   - Packet Data (see B.6).

   The Access Function and the Collection Function shall support at least one delivery method. More than one technique may be supported for implementation richness or for failure backup and for handling of overloads of individual intercepts.

b. Bearer service for the call content itself (e.g., analog or digital) (see B.7).

c. Delivering an intercepted communication as separated channels (see B.8) or as a combined channel (see B.9).

d. Delivery signaling for the CCC (see B.10).

e. The amount of acceptable end-to-end delay for the particular intercept (see B.11).

f. Distributing the CCC to more than one Collection Function, each with its own delivery method and options (see B.12).

Intervening functional entities may convert the basic bearer service or the signaling method and may add additional delay.

Call content is delivered between the Access Function (or its IAPs) and the Delivery Function and between the Delivery Function and the Collection Function. The interface for both transfers is sufficiently similar to warrant only a single description. Within this section call content is described generically as being transferred from a *source* to a *destination*.

The delivery of intercepted call content information has several phases. These phases are as follows:

a. Obtain a network address of destination. Select the destination for the call content as either a destination directory number or a specific directly connected trunk.

b. Setup the CCC to destination. Establish a channel to the destination to be used for the delivery of call content.

c. Destination acceptance or refusal of a CCC. The destination is given the option, in some cases, to accept or refuse the CCC.

d. CCC continuity verification. Verify that the CCC has reached the destination and that it is capable of reliably transferring call content information.

PN-4465-RV1

e. Associate intercept subject and call identity to the CCC. Establish the association of the CCC with the intercept subject, an intercepted call, and an IAP. Recording of the call content by the destination should begin at this point.

f. Call content transfer. Transfer the intercepted call content. This phase lasts as long as necessary. Information identifying the call content is sent separately.

g. Early CCC release by the destination. Some delivery methods allow the destination to release the delivery CCC.

h. Disassociate CCC. Free up the association of the CCC to a particular call and intercept subject to allow it to be used for other purposes.

i. Normal CCC release by the source.

The information flows described in this section are written for a single CCC. These procedures should be repeated for each CCC used (e.g., for separated delivery).

B.3 Dedicated Circuit CCC Delivery

Dedicated circuit delivery uses one or more circuits to convey the call content for a single intercept subject as shown in Figure 28. Each circuit is dedicated to a particular intercept subject, so that circuit cannot be used for any other purpose. The circuit may be switched through the intervening network(s), but this switching is transparent to the usage of the circuit as the switching occurs when the circuit is provisioned. The intercept subject and the call content are identified with their association to a particular dedicated circuit.

Figure 28: **Dedicated Circuit CCC Delivery**

Dedicated circuits are circuits between two functions using dedicated equipment on both the source and destination. These circuits may be switched through an intervening network, although call setup procedures do not apply. Dedicated circuits are used in cases where no delivery delay is tolerable.

PN-4465-RV1

Dedicated circuits used for CCCs are assumed to have the following characteristics:

a. DC signaling is not available end-to-end as intervening switches may ignore and not pass along DC signaling. (DC signaling may be used for direct connections.)

b. DTMF C-tone may be used to convey DC signaling (i.e., off-hook, on-hook, decadic digits).

c. A particular dedicated circuit has only one intercept subject assigned to it.

d. An intercept subject may have one or more circuits available for delivering its call content.

e. Separate dedicated circuits are required for each intercept subject and destination pair.

f. The number of dedicated circuits to each Collection Function need not be equal.

B.3.1 Obtain Network Address of Destination

Select an idle circuit from the circuits available for this intercept subject and the selected destination. The selection criteria should use all circuits on a regular basis.

B.3.2 Setup CCC to Destination

No call setup is necessary.

Seize the selected dedicated circuit as shown in Figure 29.

Figure 29: **Setup CCC Using Dedicated Circuits**

a. The IAP is enabled and it detects that the intercept subject is communicating (e.g., an origination or termination attempt).

b. The dedicated circuit is seized to the Delivery Function. This may be indicated with a DC signaling off-hook (when directly connected), by dropping DTMF C-tone, or with a CCOpen message.

PN-4465-RV1

c. If applicable, the Delivery Function forwards the seizure indication to the dedicated circuit associated with the intercept subject to the Collection Function. The seizure may be indicated with a DC signaling off-hook (when directly connected), by dropping DTMF C-tone, or with a CCOpen message.

d. Optionally, the Delivery Function may seize dedicated circuits associated with the intercept subject to one or more additional authorized Collection Function.

B.3.3 Destination Acceptance or Refusal of a CCC

There is no mechanism defined for a destination to accept or refuse a dedicated circuit CCC.

B.3.4 CCC Continuity Verification

While dedicated circuits are idle, DTMF C-tone may be applied to them. The presence of DTMF C-tone may be used to indicate circuit continuity, although it does not verify the source of the circuit or its association with any intercept subject.

PN-4465-RV1

B.3.5 Associate Intercept Subject and Call Identity to the CCC

The intercept subject is associated with a dedicated circuit for the life of the intercept order, so all that is required is to select the particular dedicated circuit or trunk as shown in Figure 30. The CCOpen message may be used to associate a particular call with the dedicated circuit. The CCOpen is particularly required when multiple dedicated circuits for a given intercept subject are used.

Figure 30: **Associate CCC Using Dedicated Circuits**

B.3.6 Call Content Transfer

The TSP duplicates the intercepted call content and delivers it to the selected Collection Functions over the CCCs identified in the CCOpen message associated with the intercepted communications as shown in Figure 31.

Figure 31: **Transfer Call Content Using Dedicated Circuits**

a. The IAP is enabled and it detects that the intercept subject is communicating (e.g., an origination or termination attempt).

b. The intercept subject's communications are intercepted and duplicated, and sent to the Delivery Function.

PN-4465-RV1

c. If authorized, the Delivery Function passes the call content on to the Collection Function.

d. Optionally, the Delivery Function may duplicate the call content and deliver it to one or more additional authorized Collection Functions.

B.3.7 Early CCC Release by the Destination

Dedicated circuits may not be released early by the destination.

B.3.8 Disassociate CCC

The intercept subject is associated with a dedicated circuit for the life of the intercept, however the association for a particular call or intercept may be released with a CCClose message as shown Figure 32.

Figure 32: **Disassociate CCC Using Dedicated Circuits**

B.3.9 Normal CCC Release by the Source.

When a dedicated circuit is released, continuous DTMF C-tone may be applied. The circuit is free for subsequent intercepts of the same intercept subject.

The association of a dedicated circuit to a particular intercept subject and destination is only released when the intercept order is removed or expires as shown in Figure 33.

a. The IAP is enabled and it detects that the intercept subject has stopped communicating (e.g., the call was released or a party has been dropped).

b. The dedicated circuit is released to the Delivery Function. This may be indicated with a DC signaling on-hook (when directly connected), by applying DTMF C-tone, or with the CCClose message.

c. If applicable, the Delivery Function releases the dedicated circuit associated with the intercept subject to the Collection Function with a DC signaling on-hook (when directly connected), by applying DTMF C-tone, or with the CCClose message.

PN-4465-RV1

Figure 33: **Dedicated Circuit CCC Release**

d. Optionally, the Delivery Function may release the dedicated circuits associated with the intercept subject to one or more additional authorized Collection Functions.

B.4 Trunk Group CCC Delivery

Trunk group delivery uses a set of circuits between two functions to convey call content for a set of subscribers with a common destination as shown in Figure 34. These circuits may be switched on demand through an intervening network at the time of need. A given circuit in a trunk group may be used for any appropriate intercept subject. A line side interface may be part of a trunk group, although that is outside of the classical definition of a trunk group.

Figure 34: **Trunk Group CCC Delivery**

PN-4465-RV1

Circuits in a trunk group are assumed to have the following characteristics:

a. Seize, answer, disconnect and release signals are available using end-to-end (e.g., DC signaling possibly using the DS-0 A signaling bits, ISUP out-of-band signaling, ISDN PRI out-of-band signaling, BRI out-of-band signaling, loop start line signaling). The particular type of signaling used need not be end-to-end as long as it is interworked end-to-end.

b. There is a one-to-one correspondence between both ends of a trunk group to identify individual trunks within the trunk group.

c. DTMF C-tone may be used, but it is ignored for the purpose of signaling.

d. A particular trunk circuit is shared by several intercept subjects.

e. An intercept subject may use one or more trunk circuits for delivering its call content. The maximum number of circuits may be specified for a given intercept subject.

f. A trunk group goes to only one destination.

g. The number of trunk circuits to each Collection Function need not be equal.

B.4.1 Obtain Network Address of Destination

Select the trunk group based on the assigned destination. Select an idle trunk within the trunk group for the particular intercept. The selection criteria should use all trunks in the trunk group on a regular basis.

B.4.2 Setup CCC to Destination

Seize the trunk using appropriate trunk signaling (e.g., signal off-hook with the DS-0 A bits, off-hook on a loop start line, send a SETUP message for an ISDN PRI or BRI, send an Initial Address Message for an ISUP trunk) as shown in Figure 35.

Figure 35: **Setup CCCs Using a Trunk from a Trunk Group**

a. The IAP detects that the intercept subject is communicating.

PN-4465-RV1

b. The IAP sends a signal to seize the trunk to the Delivery Function.

c. If authorized, the Delivery Function sends a signal to seize the trunk to the Collection Function.

d. Optionally if authorized, the Delivery Function may send a trunk seizure signal to one or more additional Collection Functions.

B.4.3 Destination Acceptance or Refusal of a CCC

A trunk may be accepted by answering the trunk setup signaling (e.g., return an off-hook with the DS-0 A bits, go off-hook on a loop start line, send a Connect message for an ISDN PRI or BRI, send an Answer Message for an ISUP trunk) as shown in Figure 36.

Figure 36: **Acceptance of CCCs Using a Trunk of a Trunk Group**

a. When the trunk is seized at the Collection Function, it may accept the call by returning an answer indication.

b. Each additional Collection Function trunk seized may return an answer indication.

c. If the call is accepted by the Delivery Function, it may return an answer indication to the IAP.

A trunk may be refused by not answering the seize signal as shown in Figure 37 and Figure 38. If the expected answer signal does not arrive in time, the source assumes that the call was refused and proceeds to release the trunk circuit. A refusal by one Collection Function shall not prevent the delivery of call content to other Collection Functions.

a. When a trunk is seized by the IAP, an answer timer is started.

b. The answer timer expires, indicating that the call was refused, and…

c. …the IAP releases the trunk toward the Delivery Function.

a. When a trunk is seized by the Delivery Function, an answer timer is started.

b. The answer timer expires, indicating that the call was refused, and…

c. …the Delivery Function releases the trunk toward the Collection Function.

PN-4465-RV1

Figure 37: **DF Timed Refusal of a CCC Using a Trunk of a Trunk Group**

Figure 38: **CF Timed Refusal of a CCC Using a Trunk of a Trunk Group**

PN-4465-RV1

A trunk may be refused by some out-of-band signaling sending a release signal (e.g., ISDN or ISUP) as shown in Figure 39 and Figure 40. A refusal by one Collection Function shall not prevent the delivery of call content to another Collection Function that accepts the call content.

Figure 39: **DF Refusal of a CCC Using a Trunk of a Trunk Group**

a. A trunk is seized by the IAP.

b. The Delivery Function refuses the call by sending a release signal.

Figure 40: **CF Refusal of a CCC Using a Trunk of a Trunk Group**

a. A trunk is seized by the Delivery Function.

b. The Collection Function refuses the call by sending a release signal.

PN-4465-RV1

B.4.4 CCC Continuity Verification

Immediately upon acceptance of the seizure, the destination may loop around the CCC. The source may apply a test signal (or the call content itself) and verify that the signal returned is the same as the signal that was sent. This continuity test may have to account for various transmission and switching delays. Since a CCC could be looped around and delayed anywhere, this test does not confirm that the call content was actually delivered to its intended destination. CCC continuity verification is shown Figure 41.

Figure 41: **CCC Continuity Test**

c., e. When a CCC is seized; a tone, test pattern, or the call content is applied to the CCC by the source.

d., f. At the destination of the CCC, the received call content is looped around to the transmit path of the CCC. This loop around should remain in place for the duration of the call content delivery. The destination may detect a preamble tone or test pattern to verify that the CCC is valid from the source. The source shall verify continuity before delivering call content. the source should continuously or periodically verify that the looped around call content is as expected through the duration of call content delivery.

B.4.5 Associate Intercept Subject and Call Identity to the CCC

The CCOpen message associates the intercept subject and a particular call with a particular circuit in a trunk group.

The CCOpen message is communicated in the same manner as dedicated connections (see B.3.5).

PN-4465-RV1

B.4.6 Call Content Transfer

The TSP duplicates the intercepted call content and delivers it to the selected Collection Functions over the CCCs identified in the CCOpen message associated with the intercepted communications as shown Figure 42.

Figure 42: **Transfer Call Content Using a Trunk in a Trunk Group**

a. The IAP is enabled and it detects that the intercept subject is communicating.

b. The intercept subject's communications are intercepted and duplicated, and sent to the Delivery Function.

c. If authorized, the Delivery Function passes the call content on to the Collection Function.

d. Optionally, the Delivery Function may duplicate the call content and deliver it to one or more additional authorized Collection Functions.

B.4.7 Early CCC Release by the Destination

A trunk in a trunk group may be released early by the destination with the appropriate trunk release signaling (e.g., on-hook indication with the DS-0 A bits, on-hook on a loop start line, a DISCONNECT message for an ISDN PRI or BRI, a Release for an ISUP trunk) as shown Figure 43. The circuit is free for subsequent intercepts for any intercept subject. Once a CCC is released, the call content delivery may not be re-established.

Figure 43: **Early Release of CCC Using a Trunk in a Trunk Group**

PN-4465-RV1

a. The Collection Function determines that the call content is not of interest and it signals to release the trunk.

b. Additionally other Collection Functions may indicate that they are not interested in the call content and they independently signal to release the trunk.

c. When the Delivery Function determines that the call content is not of interest to any Collection Function, the Delivery Function may send a signal to release the trunk to the IAP.

If the destination is not provisioned for early release, the delivery of call content to the destination may be re-established by the source after an unintended early release.

B.4.8 Disassociate CCC

The CCClose message disassociates the intercept subject and a particular call with a particular trunk in a trunk group.

The CCClose message is used in the same manner as dedicated connections (see B.3.8).

B.4.9 Normal CCC Release by the Source

A trunk in a trunk group is normally released by the source with the appropriate trunk release signaling. (e.g., on-hook indication with the DS-0 A bits, on-hook on a loop start line, a DISCONNECT message for an ISDN PRI or BRI, a Release for an ISUP trunk) as shown in Figure 44. The circuit is free for subsequent intercepts for any intercept subject.

Figure 44: **Release CCC Using a Trunk in a Trunk Group**

a. The IAP detects that the intercept subject is no longer communicating.

b. The IAP sends a signal to release the trunk to the Delivery Function.

c. The Delivery Function sends a signal to release the trunk to the Collection Function.

PN-4465-RV1

d. Optionally if authorized, the Delivery Function may send a trunk release signal for each additional seized trunk to one or more Collection Functions.

B.5 Static Directory Number CCC Delivery

Static directory number delivery uses one or more switched connections to convey the call content for a particular intercept subject as shown in Figure 45. Each intercept subject is assigned one or more directory numbers with one number assigned for each CCC that may be delivered. The intercept subject is identified by its association with the directory number. The call content should be separately identified.

Figure 45: **Static Directory Number CCC Delivery**

A static directory number uses a circuit from a general set of circuits interfacing a telephone network. These circuits are switched through an intervening network. A given circuit may be used for any appropriate intercept subject. The circuit may be a line or a trunk and the type of circuit may change as the circuit is switched and interworked through the network from the source to the destination.

Only one call may be delivered to a static directory number at a time. No hunt groups may be used. This ensures that the call may be associated by using only the directory number for identification. One directory number should be assigned for the number of calls expected from each enabled IAP or Delivery Function.

Circuits used for static directory numbers are assumed to have the following characteristics:

a. Seize, setup, answer, disconnect and release signals are available using end-to-end (e.g., DC signaling possibly using the DS-0 A signaling bits and in-band tones, ISUP out-of-band signaling, ISDN PRI out-of-

PN-4465-RV1

band signaling, BRI out-of-band signaling, loop start line signaling). The particular type of signaling used need not be end-to-end as long as it is interworked end-to-end.

b. There is a one-to-one correspondence between a static directory number, an intercept subject and the CCC.

c. DTMF C-tone may be used, but it is ignored for the purpose of signaling.

d. A particular circuit is not dedicated to a particular intercept subject.

e. An intercept subject may use one or more circuits for delivering its call content. The maximum number of circuits may be specified for a given intercept subject for each destination.

f. Capacity for the CCCs may be reserved in each functional entity for each intercept subject.

g. Capacity for the CCCs may or may not be reserved in the network to reduce network blockage.

h. The number of circuits to each Collection Function need not be equal.

B.5.1 Obtain Network Address of Destination

Select an idle static directory number based on the intercept subject identity and destination. The selection criteria should use all directory numbers on a regular basis.

B.5.2 Setup CCC to Destination

Seize the trunk and setup the call to the destination as shown in Figure 46 using appropriate trunk signaling (e.g., signal off-hook with the DS-0 A bits followed by appropriate MF outpulsing, off-hook on a loop start line followed by appropriate DTMF outpulsing, send a SETUP message with the appropriate called number for an ISDN PRI or BRI, send an Initial Address Message with the appropriate called number for an ISUP trunk).

Figure 46: **Setup Trunk to Destination**

PN-4465-RV1

The CCC for a static directory number is established using normal call setup procedures (e.g., loop start line, ISDN, MF trunk or ISUP trunk).

a. IAP is enabled to the Delivery Function.

b. IAP sets up a CCC to Delivery Function.

c. Delivery Function sets up a CCC to an authorized Collection Function.

d. Additionally the Delivery Function may setup CCCs to other authorized Collection Functions.

B.5.3 Destination Acceptance or Refusal of a CCC

The CCC is accepted by answering the delivered call. The CCC may be refused by not answering the delivered call within a period of time (mutually agreed upon between the TSP and LEA) or by refusing the connection directly.

The acceptance or refusal is communicated in the same manner as trunked connections (see B.4.3).

B.5.4 CCC Continuity Verification

Circuit continuity should be verified upon call setup since the connection between the source and the destination is unknown without this test.

CCC continuity verification is done in the same manner as trunked connections (see B.4.4).

B.5.5 Associate Intercept Subject and Call Identity to the CCC

The intercept subject is associated with a static directory number for the life of the intercept. The CCOpen message associates a particular call with the static directory number.

The CCOpen message is communicated in the same manner as dedicated connections (see B.3.5).

B.5.6 Call Content Transfer

The TSP duplicates the intercepted call content and delivers it to the selected Collection Functions over the CCCs identified in the CCOpen message associated with the intercepted communications as shown Figure 42 (see B.4.6).

B.5.7 Early CCC Release by the Destination.

CCCs may be released early by the destination in the same manner as trunked connections (see B.4.7).

Releasing the CCC frees the static directory number for subsequent intercepts.

PN-4465-RV1

If the destination is not provisioned for early release, the delivery of call content to the destination may be re-established by the source after an unintended early release.

B.5.8 Disassociate CCC

The CCClose message disassociates the intercept subject and a particular call with the static directory number.

The CCClose message is used in the same manner as dedicated connections (see B.3.8).

B.5.9 Normal CCC Release by the Source

CCCs are released normally by the source in the same manner as trunked connections (see B.4.9).

Releasing the CCC frees the static directory number for subsequent intercepts.

B.6 Packet Data CCC Delivery

The text in this section may not apply to an IP network.

Packet data delivery uses one or more packet-switched connections to convey the call content for a particular intercept subject as shown in Figure 47. Either connection-oriented or connectionless packet data services may be used. Each intercept subject is assigned one or more data network addresses with one number assigned for each CCC that may be delivered. The intercept subject is identified by its association with the data network address. The call content is separately identified with the PDU Type parameter of the CCOpen message.

Only one communication may be delivered to a given data network address at a time. A unique address shall be used. This ensures that the communication may be associated by using only the data network address for identification. One data network address should be assigned for each of the number of communications expected from each enabled IAP or Delivery Function.

Channels used for packet data CCC delivery are assumed to have the following characteristics:

a. The relationship between the intercept subject, a particular IAP and the CCC is uniquely identified by the data network address.

b. A particular physical channel may be shared by several intercept subjects.

c. One or more channels may deliver the call content of any particular intercept subject. The maximum number of channels may be specified for a given intercept subject for each IAP and destination.

PN-4465-RV1

Figure 47: **Packet Data CCC Delivery**

d. Capacity for the CCCs may be reserved in each functional entity for each intercept subject.

e. Capacity for the CCCs may or may not be reserved in the network to reduce network blockage.

f. The number of channels to each Collection Function need not be equal.

B.6.1 Obtain Network Address of Destination

Select a data network address based on the intercept subject identity and destination.

B.6.2 Setup CCC to Destination

If necessary, setup a connection-oriented data call to the destination (e.g., an X.25 SETUP).

B.6.3 Destination Acceptance or Refusal of a CCC

The CCC is accepted by answering the delivered connection-oriented data call. The CCC may be refused by not answering the delivered call within a period of time (mutually agreed upon between the TSP and LEA) or by refusing the connection directly.

Connectionless CCC delivery channels cannot be refused.

B.6.4 CCC Continuity Verification

Data circuit continuity may be verified using normal link or end-to-end acknowledgments appropriate to the selected packet data service.

PN-4465-RV1

B.6.5 Associate Intercept Subject and Call Identity to the CCC

The intercept subject is associated with a network data address for the life of the intercept. The CCOpen message associates a particular call with the data network address in the same manner as dedicated connections.

The CCOpen message is communicated in the same manner as dedicated connections (see B.3.5).

B.6.6 Call Content Transfer

Call content is transferred using the data transfer appropriate to the selected packet data service.

B.6.7 Early CCC Release by the Destination

Connection-oriented CCCs may be released early by the destination.

Releasing the CCC frees the data network address for subsequent intercepts.

Connectionless CCCs are not released.

If the destination is not provisioned for early release, the delivery of call content to the destination may be re-established by the source after an unintended early release.

B.6.8 Disassociate CCC

The CCClose message disassociates the intercept subject and a particular call with the data network address.

The CCClose message is used in the same manner as dedicated connections (see B.3.8).

B.6.9 Normal CCC Release by the Source

A connection-oriented channel is released normally by the source.

Connectionless CCCs are not released.

Releasing the CCC frees the data network address for subsequent intercepts.

B.7 Delivery Bearer Service

Circuit-mode call content may be delivered with analog or digital circuits (DS-0 or ISDN B-channels) when voice (speech) or audio bearer services are delivered. Circuit-mode digital data bearer services require digital circuits.

PN-4465-RV1

Packet-mode communications may be delivered using circuit-mode CCCs, packet-mode CCCs, or a CDC (for certain packets).

B.8 Separated Content Delivery

The transmit and receive paths of the call content are kept separated. This type of delivery is appropriate for digital bearer services and some voice (speech) or audio services that take advantage of end-to-end separated communications. It may also be used to avoid the introduction of distortion in the delivery of the call content.

Call-identifying information is delivered over a separate data channel as shown in Figure 48.

Figure 48: **Separated Content Delivery**

B.9 Combined Content Delivery

The transmit and receive paths of the call content is combined and delivered over a single circuit for the communications of an intercept subject. This type of delivery is appropriate for voice (speech) and audio bearer service communications, especially when one of the parties is on a two-wire loop start line. Since the bridging device may cause signal distortion, this type of delivery may not be appropriate for digital bearer services.

Call-identifying information is delivered over a separate data channel as shown in Figure 49.

Figure 49: **Combined Content Delivery**

PN-4465-RV1

B.10 Signaling for Switched Delivery

Switched circuits may use any signaling method including the following:

- MF signaling (to access switching networks or to convey the directory number to the Collection Function upon network egress);
- ISUP signaling;
- ISDN signaling; or
- metallic signaling methods (e.g., analog facility signaling).

B.11 Call Content Delivery Delay

Call content may be delayed in some situations so that a channel can be setup and switched through a network and not lose any important call content (i.e., any call content after answer and before release).

The strategies for managing switched circuits is beyond the scope of this Standard. It is the responsibility of the Access or Delivery Function to ensure that a CCC is available or connected to the downstream Delivery or Collection Function for the timely delivery of the call content. Such strategies may include, but not be limited to, the following (in no particular order):

- delayed or
- anticipatory.

Delayed sets up a CCC delivery circuit connection to the downstream function upon demand. The call content is delayed by any time difference in the availability of call content and the acceptance by the downstream function(s).

Anticipatory sets up a circuit connection to the downstream function in anticipation of call content availability. Call content should not be lost or delayed. One or more circuits are set up when the intercept is provisioned. As circuits are used, additional circuit connections may be set up in anticipation of additional demand. The additional circuit connections may be dropped as the additional demand ceases.

PN-4465-RV1

B.12 Call Content Distribution

Call content may be distributed to more than one Collection Function as shown in Figure 50. The call content must be screened to ensure that only authorized content is delivered. The characteristics of each delivery may be different for each destination Collection Function.

Figure 50: **Call Content Distribution**

Call content may be delivered through an intervening Delivery Function, called a Pivoted Delivery Function, to allow a TSP to centralize its screening and distribution of intercepted information as shown in Figure 51.

Figure 51: **Pivoted Delivery with Distribution**

B.13 DTMF C-Tone Signaling Procedures

Some call events described in Stage 1 and Stage 2 can be signaled using tones. This method has been used for electronic surveillance circuits for years.

Tone signaling allows Plain Old Telephone Service (POTS) switchhook signaling of the intercepted communication to be sent over a CCC and yet allow the CCC to use its Direct Current (DC) loop signaling to communicate its switchhook signaling. While the intercept subject's telephone instrument is on-hook, a DTMF C-tone is sent. This allows for simple signaling for origination attempts, call controls (DTMF or decadic bursts for digits and switchhook flashes), answer, disconnect and release. The signals are differentiated by timing in the same manner as traditional DC signaling, that is:

a. C-tone off is off-hook or a seizure.

PN-4465-RV1

b. 10 ms C-tone on followed by 10 ms C-tone off (±10%) is a decadic dial pulse.

c. 100 ms C-tone off separates the individual decadic digits. A digit consists of 1 to 10 pulses (with 10 pulses representing the digit 0).

d. DTMF digits (0-9, * and #) are sent normally.

e. 200 to 1500 ms C-tone on followed by C-tone off is a switchhook flash.

f. 2000 ms C-tone on is a disconnect or on-hook.

Figure 52 shows the frequency pairs used for each DTMF digit.

Figure 52: **Digit to DTMF Tone Mapping**

Figure 53 shows an example of normal DC and DTMF signaling converted to DTMF C-tone signaling.

Figure 53: **DTMF C-tone Signaling**

Out-of-band signaling conveys additional information and is used for modern telephone services, such as ISDN and wireless.

PN-4465-RV1

Annex C CDC Delivery Methods

This Annex is informative and is not considered part of this Standard.

This Annex describes the CDC delivery services as a set of mechanisms, characteristics, and options that may be considered when selecting a delivery method.

CDCs may be delivered using one of the following delivery methods:

a. Dedicated data circuit, or

b. Dedicated data link.

Normally call-identifying information is sent as the events occur. Call-identifying information may be delayed to be synchronized with delayed call content.

C.1 Dedicated Data Circuit CDC Delivery

Call data is delivered over a data circuit that is dedicated to a particular intercept subject as shown in Figure 54.

Figure 54: **Dedicated Data Circuit CDC Delivery**

PN-4465-RV1

C.2 Dedicated Data Link CDC Delivery

Call data is delivered over a data circuit that is dedicated to a particular destination, but is shared with the intercept subjects monitored by the destination as shown in Figure 55.

Figure 55: **Dedicated Data Link CDC Delivery**

C.3 Call Data Distribution

Call data may be distributed to more than one Collection Function. The information delivered to each Collection Function must be duplicated and screened to ensure that only authorized information is delivered.

The delivery options may be different for each path between a Delivery and a Collection Function.

PN-4465-RV1

Annex D Information Access Scenarios

This Annex is informative and is not considered part of this Standard.

Several basic circuit-mode call scenarios are described in this section. The intent of this section is to provide representative examples of reported events over a CDC and changes in connections for the CCC. This section is not an exhaustive set of examples. Each specific scenario applies to a particular service and configuration, but should be considered to be applicable to other similar services and configurations. TSPs may provide access using configurations and accesses not shown and systems are not obligated to implement particular services or accesses in the way illustrated. There may also be implementation differences providing different numbers of CallIdentity per scenarios. (The scenarios assume that there is one CallIdentity used for each CCC, unless noted otherwise.)

The *Step* column provides a reference number for a scenario step.

The *Action* column describes a particular action by the intercept subject or by another party.

The *Reported Event* column describes the event messages sent over the CDC. The Interface Access Point (IAP) is depicted as “XXXIAP>.” Following the IAP is the party/channel involved in the event and then the event.

These scenarios show the CCOpen occurring at the earliest opportunity. The CCOpen is required before the call is answered. The CCOpen and CCClose may not occur at all in scenarios where the call is not answered. The CCOpen may be delayed until answer, such as step 5 in D.4 and step 3 in D.6.

In scenarios involving multiple systems, the IAPs for a system are subscripted to indicate a particular system. If all of the indicated intercepts are not activated, some information loss is possible. If all of the indicated intercepts are activated, some information may be duplicated.

The *Connection Diagram* column depicts the connections at the end of a particular action.

Figure 56 depicts the connection diagram convention used in this Standard to describe a switch connection for a single intercept call of a switching system.

The switch symbol represents a system which has been presented with the electronic surveillance court order.

The switch control symbol represents that part of the system that detects and processes any applicable signaling information.

The CCCs may use any content delivery service using one or more circuits (see Annex B).

PN-4465-RV1

Figure 56: **Switch Connection Diagram Conventions**

Call and telecommunication services are built from one or more of the following simple switch connections as shown in Table 25. Actual accesses may be accomplished with one or more of these simple switch connections.

Table 25: **Simple Switch Connections** **(Sheet 1 of 3)**

Switch Connection Name	Switch Connection Description	Diagram
Idle	The call connections for the IAP are idle.	
Intercept Subject Suspended	The intercept subject is suspended. No other party is connected. Announcements or tones may be applied toward the intercept subject.	
Intercept Subject Collect	The switch control is collecting digits from the intercept subject. No other party is connected to the intercept subject. Announcements or tones may be applied toward the intercept subject. The call content connection may be logical, rather than physical, provided that the information characterizes the system prompts to the subject and the responses from the subject.	
Intercept Subject Awaiting Answer	The intercept subject is waiting for the other party (A) to answer. The intercept subject may be able to hear call progress tones from the partially cut-through circuit.	

PN-4465-RV1

Table 25: **Simple Switch Connections** **(Sheet 2 of 3)**

Switch Connection Name	Switch Connection Description	Diagram
Intercept Subject Connected	The intercept subject is connected and fully cut-through to the other party (A) (at least from the switch perspective). If the intercept subject was previously cut-through, this may also be used to indicate a change in parties (i.e., a new party added, an existing party dropped, an existing party split off).	
Other Partial Cut-through	The other party (A) is partially cut-through to allow it to monitor call progress announcements or tones. The intercept subject may be alerting for party (A).	
Other Collect	The other party (A) is fully cut-through to allow it to monitor announcements and tones. Call control monitors in-band signaling tones from the other party (A).	
Other Suspended	The other party (A) is fully cut-through to allow it to monitor announcements or tones.	
Other Held	The other party (A) is placed on hold, but is not monitored.	
Redirection Alerting	A call between a party (A) and the intercept subject is redirected to one or more other parties (B). The call is only partially cut-through to allow party (A) to monitor call progress tones. One or more other parties (B) may be alerting, but none has answered.	
Redirection Await Answer	A call between a party (A) and the intercept subject is answered and redirected to one or more other parties (B). The call is only partially cut-through to the other parties (B) to allow party (A) to monitor call progress tones. One or more other parties (B) may be alerting, but none has answered. Monitored on the A leg, the call has been answered and cut-through.	 or
Redirection Connected	A call between a party (A) and the intercept subject is redirected to one or more parties (B). The call is fully cut-through to allow party (A) and the other parties (B) to communicate.	

PN-4465-RV1

Table 25: **Simple Switch Connections** **(Sheet 3 of 3)**

Switch Connection Name	Switch Connection Description	Diagram
Multi-Party Awaiting Answer	The intercept subject is attempting a call to party A and one or more other parties (B). The paths are only partially cut-through to allow the intercept subject to monitor call progress announcement and tones. Only the intercept subject leg is monitored.	
Multi-Party Connected and Awaiting Answer	The intercept subject has cut-through a call to party (A) and is attempting a call to one or more parties (B). The paths to the other parties (B) is only partially cut-through to allow the intercept subject to monitor call progress announcement and tones. Only the intercept subject leg is monitored.	
Multi-Party Connected	The intercept subject has cut-through a call to party (A) and one or more other parties (B). Only the intercept subject leg is monitored. The intercept subject with an existing multi-party connection has a change in parties (i.e., one or more parties joining, one or more parties dropped, one or more parties split off).	

PN-4465-RV1

D.1 Simple Abandoned Call Attempt

An intercept subject at (202) 555-0000 goes off-hook. Without dialing any digits, the intercept subject goes back on-hook.

Table 26: **Simple Abandoned Call Attempt Scenario**

Step	Action	Reported Event	Connection Diagram
1	An intercept subject at (202) 555-0000 goes off-hook.	CIAP> CCOpen (CCC1)	
2	Without dialing any digits, the intercept subject goes back on-hook.	IDIAP> Origination (User Input = “”) IDIAP> Release CIAP> CCClose (CCC1)	

D.2 Partial Dial Abandon

An intercept subject at (202) 555-0000 goes off-hook and dials a few digits (123). The intercept subject goes back on-hook.

Table 27: **Partial Dial Abandon Scenario**

Step	Action	Reported Event	Connection Diagram
1	An intercept subject at (202) 555-0000 goes off-hook and dials a few digits (123).	CIAP> CCOpen (CCC1)	
2	The intercept subject goes back on-hook.	IDIAP> Origination (User Input = “123”) IDIAP> Release CIAP> CCClose (CCC1)	

PN-4465-RV1

D.3 Pre-Answer Abandon

An intercept subject at (202) 555-0000 goes off-hook and dials Party A at (202) 555-1111. The call is extended to Party A. The intercept subject goes back on-hook before the call is answered.

Table 28: **Pre-Answer Abandon Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 goes off-hook to initiate a call.	CIAP> CCOpen (CCC1)	
3	The intercept subject dials Party A at (202) 555-1111.		No change.
4	The call is extended to Party A.	IDIAP> Origination (User Input="2025551111", Called Party=2025551111)	
5	The intercept subject abandons the call.	IDIAP> Release CIAP> CCClose (CCC1)	

PN-4465-RV1

D.4 Simple Outgoing Call

The intercept subject (S) at (202) 555-0000 goes off-hook to initiate a call and dials Party A at (202) 555-1111. After the call is completed, the intercept subject dials more digits. Later the intercept subject disconnects to release the call.

Table 29: **Simple Outgoing Call Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 goes off-hook to initiate a call.	CIAP> CCOpen (CCC1)	
3	The intercept subject dials Party A at (202) 555-1111.		No change.
4	The call is extended to Party A.	IDIAP> Origination (User Input="2025551111", Called Party=2025551111)	
5	Party A answers.	IDIAP> Answer ()	
6	The intercept subject dials more digits, 1234567.		No change.
7	The intercept subject releases.	IDIAP> Release CIAP> CCClose (CCC1)	

For system using *en bloc* sending (such as ISDN or wireless), steps 2, 3, and 4 may be combined into a single step.

Table 30: **Alternate Steps for *en bloc* Sending**

Step	Action	Reported Event	Connection Diagram
2 3 4	The intercept subject at (202) 555-0000 initiates a call to Party A at (202) 555-1111 using *en bloc* sending.	CIAP> CCOpen (CCC1) IDIAP> Origination (User Input="2025551111", Called Party=2025551111)	

PN-4465-RV1

D.5 Re-Origination

The intercept subject (S) at (202) 555-0000 goes off-hook to initiate a call and dials Party A at (202) 555-1111. After the call is completed, Party A hangs up. The intercept subject re-originates a call to Party B at (202) 555-2222. Later the intercept subject disconnects to release the call.

Table 31: **Re-origination Call Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 goes off-hook to initiate a call.	CIAP> CCOpen (CCC1)	
3	The intercept subject dials Party A at (202) 555-1111.		No change.
4	The call is extended to Party A.	IDIAP> Origination (User Input=“2025551111”, Called Party=2025551111)	
5	Party A answers.	IDIAP> Answer ()	
6	Party A disconnects.	IDIAP> Release CIAP> CCClose (CCC1)	
7	The intercept subject initiates another call with re-origination to Party B at (202) 555-2222.	CIAP> CCOpen (CCC1)	
8	The call is extended to Party B.	IDIAP> Origination (User Input=“2025552222”, Called Party=2025552222)	
9	Party B answers.	IDIAP> Answer ()	
10	The intercept subject releases.	IDIAP> Release CIAP> CCClose (CCC1)	

PN-4465-RV1

Alternatively steps 6 and 7 may be as follows for some switching systems:

Table 32: **Alternate Re-origination Call Scenario Steps**

Step	Action	Reported Event	Connection Diagram
6	Party A disconnects.	IDIAP> Release	
7	The intercept subject initiates another call with re-origination.		

D.6 Simple Incoming Call

The intercept subject (S) at (202) 555-0000 receives a voice call from Party A at (202) 555-1111. The intercept subject answers the call. The call is released.

Table 33: **Simple Incoming Call Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 receives a voice call from Party A at (202) 555-1111.	IDIAP> TerminationAttempt (2025551111) CIAP> CCOpen (CCC1)	
3	The intercept subject answers the call.	IDIAP> Answer (2025550000)	
4	The call is released.	IDIAP> Release CIAP> CCClose (CCC1)	

PN-4465-RV1

D.7 Call Waiting and Recall

The intercept subject (S) at (202) 555-0000 receives a voice call from Party A at (202) 555-1111. The intercept subject answers the call. Later, a second call arrives to alert the intercept subject from Party B at (202) 555-2222. The intercept subject answers the second call with Call Waiting. The intercept subject toggles back to the original call. The intercept subject ends that call by hanging up causing the held party to recall the intercept subject. The intercept subject answers the call. The second call is released.

This sequence is shown with three separate scenarios to show some variations of managing the CallIdentity parameter. It is shown with a single CallIdentity for the entire multiparty call, with a separate CallIdentity for each leg of a call merged into one CallIdentity, and with a CallIdentity for separate calls. The value of the CallIdentity is shown within square brackets, e.g., [1]. Separate calls are separated by commas, e.g., [1,2], and a call with multiple identities is shown with dots joining the constituent identities, e.g., [1•2].

PN-4465-RV1

D.7.1 Call Waiting and Recall with a Single Call Identity

Table 34: **Call Waiting with Recall Scenario with a Single Call Identity**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 receives a voice call from Party A at (202) 555-1111.	IDIAP> TerminationAttempt (2025551111 [1]) CIAP> CCOpen (CCC1 [1])	
3	The intercept subject answers the call.	IDIAP> Answer (2025550000 [1])	
4	Later, a second call arrives to alert the intercept subject from Party B at (202) 555-2222.	IDIAP> TerminationAttempt (2025552222 [2]) CIAP> CCOpen (CCC2 [2])	
5	The intercept subject answers the second call with Call Waiting.	IDIAP> Answer (2025550000 [2]) IDIAP> Change ([1,2 to 1]) CIAP> CCClose (CCC2)	
6	The intercept subject toggles back to the original call.		
7	The intercept subject ends that call by hanging up causing the held party to recall the intercept subject.	IDIAP> TerminationAttempt (2025552222 [1])	
8	The intercept subject answers the call.	IDIAP> Answer (2025550000 [1])	
9	The second call is released.	IDIAP> Release ([1]) CIAP> CCClose (CCC1)	

PN-4465-RV1

D.7.2 Call Waiting and Recall with Separate Leg Identities

Table 35: **Call Waiting with Recall with Separate Leg Identities Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 receives a voice call from Party A at (202) 555-1111.	IDIAP> TerminationAttempt (2025551111 [1]) CIAP> CCOpen (CCC1 [1])	
3	The intercept subject answers the call.	IDIAP> Answer (2025550000 [1])	
4	Later, a second call arrives to alert the intercept subject from Party B at (202) 555-2222.	IDIAP> TerminationAttempt (2025552222 [2]) CIAP> CCOpen (CCC2 [2])	
5	The intercept subject answers the second call with Call Waiting.	IDIAP> Answer (2025550000 [2]) IDIAP> Change ([1,2 to 1•2]) CIAP> CCClose (CCC2)	
6	The intercept subject toggles back to the original call.		
7	The intercept subject ends that call by hanging up causing the held party to recall the intercept subject.	IDIAP> Release ([1]) IDIAP> TerminationAttempt (2025552222 [2])	
8	The intercept subject answers the call.	IDIAP> Answer (2025550000 [2])	
9	The second call is released.	IDIAP> Release ([2]) CIAP> CCClose (CCC1)	

PN-4465-RV1

D.7.3 Call Waiting and Recall with Separate Calls

Table 36: **Call Waiting with Recall with Separate Calls Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 receives a voice call from Party A at (202) 555-1111.	IDIAP> TerminationAttempt (2025551111 [1]) CIAP> CCOpen (CCC1 [1])	
3	The intercept subject answers the call.	IDIAP> Answer (2025550000 [1])	
4	Later, a second call arrives to alert the intercept subject from Party B at (202) 555-2222.	IDIAP> TerminationAttempt (2025552222 [2]) CIAP> CCOpen (CCC2 [2])	
5	The intercept subject answers the second call with Call Waiting.	IDIAP> Answer (2025550000 [2])	
6	The intercept subject toggles back to the original call.		
7	The intercept subject ends that call by hanging up causing the held party to recall the intercept subject.	IDIAP> Release ([1]) CIAP> CCClose (CCC1) IDIAP> TerminationAttempt (2025552222 [2])	
8	The intercept subject answers the call.	IDIAP> Answer (2025550000 [2])	
9	The second call is released.	IDIAP> Release ([2]) CIAP> CCClose (CCC2)	

PN-4465-RV1

D.8 Call Waiting with Talking Party Disconnect

The intercept subject (S) at (202) 555-0000 receives a voice call from Party A at (202) 555-1111. The intercept subject answers the call. Later, a second call leg arrives to alert the intercept subject from Party B at (202) 555-2222. The intercept subject answers the second call leg with Call Waiting. The intercept subject toggles back to the original call. The original caller hangs up causing the held party to be connected to the intercept subject. The intercept subject answers the call. The second call leg is released.

This sequence is shown with three separate scenarios to show some variations of managing the CallIdentity parameter. It is shown with a single CallIdentity for the entire multiparty call, with a separate CallIdentity for each leg of a call merged into one CallIdentity, and with a CallIdentity for separate calls. The value of the CallIdentity is shown within square brackets, e.g., [1]. Separate calls are separated by commas, e.g., [1,2], and a call with multiple identities is shown with dots joining the constituent identities, e.g., [1•2].

PN-4465-RV1

D.8.1 Call Waiting with Talking Party Disconnect and a Single Call Identity

Table 37: **Call Waiting with Talking Party Disconnect and a Single Call Identity Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 receives a voice call from Party A at (202) 555-1111.	IDIAP> TerminationAttempt (2025551111 [1]) CIAP> CCOpen (CCC1 [1])	
3	The intercept subject answers the call.	IDIAP> Answer (2025550000 [1])	
4	Later, a second call leg arrives to alert the intercept subject from Party B at (202) 555-2222.	IDIAP> TerminationAttempt (2025552222 [2]) CIAP> CCOpen (CCC2 [2])	
5	The intercept subject answers the second call leg with Call Waiting.	IDIAP> Answer (2025550000 [2]) IDIAP> Change ([1,2 to 1]) CIAP> CCClose (CCC2)	
6	The intercept subject toggles back to the original call.		
7	The original caller hangs up causing the held party to be connected to the intercept subject.		
8	The second call leg is released.	IDIAP> Release ([1]) CIAP> CCClose (CCC1)	

PN-4465-RV1

D.8.2 Call Waiting with Talking Party Disconnect and Separate Leg Identities

Table 38: **Call Waiting with Talking Party Disconnect and Separate Leg IdentitiesScenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 receives a voice call from Party A at (202) 555-1111.	IDIAP> TerminationAttempt (2025551111 [1]) CIAP> CCOpen (CCC1 [1])	
3	The intercept subject answers the call.	IDIAP> Answer (2025550000 [1])	
4	Later, a second call leg arrives to alert the intercept subject from Party B at (202) 555-2222.	IDIAP> TerminationAttempt (2025552222 [2]) CIAP> CCOpen (CCC2 [2])	
5	The intercept subject answers the second call leg with Call Waiting.	IDIAP> Answer (2025550000 [2]) IDIAP> Change ([1,2 to 1•2]) CIAP> CCClose (CCC2)	
6	The intercept subject toggles back to the original call.		
7	The original caller hangs up causing the held party to be connected to the intercept subject.	IDIAP> Release ([1])	
8	The second call leg is released.	IDIAP> Release ([2]) CIAP> CCClose (CCC1)	

PN-4465-RV1

D.8.3 Call Waiting with Talking Party Disconnect and Separate Calls

Table 39: **Call Waiting with Talking Party Disconnect and Separate Calls Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 receives a voice call from Party A at (202) 555-1111.	IDIAP> TerminationAttempt (2025551111 [1]) CIAP> CCOpen (CCC1 [1])	
3	The intercept subject answers the call.	IDIAP> Answer (2025550000 [1])	
4	Later, a second call leg arrives to alert the intercept subject from Party B at (202) 555-2222.	IDIAP> TerminationAttempt (2025552222 [2]) CIAP> CCOpen (CCC2 [2])	
5	The intercept subject answers the second call leg with Call Waiting.	IDIAP> Answer (2025550000 [2])	
6	The intercept subject toggles back to the original call.		
7	The original caller hangs up causing the held party to be connected to the intercept subject.	IDIAP> Release ([1]) CIAP> CCClose (CCC1)	
8	The second call leg is released.	IDIAP> Release ([2]) CIAP> CCClose (CCC2)	

PN-4465-RV1

D.9 Call Held and Retrieved

The intercept subject (S) at (202) 555-0000 goes off-hook and calls Party A at 555-1111. The called party answers and they converse. The intercept subject puts the call on hold. The intercept subject retrieves the held call. The call is released.

Table 40: **Call Held and Retrieved Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 goes off-hook and…	CIAP> CCOpen (CCC1)	
3	…calls Party A at 555-1111.	IDIAP> Origination (User Input="5551111", Called Party=2025551111)	
4	The called party answers and they converse.	IDIAP> Answer ()	
5	The intercept subject puts the call on hold.		
6	The intercept subject retrieves the held call.		
7	The call is released.	IDIAP> Release CIAP> CCClose (CCC1)	

PN-4465-RV1

D.10 Three-Way Calling, Plus Call Turned Away

The intercept subject (S) at (202) 555-0000 goes off-hook and calls Party A at 555-1111. The called party answers and they converse. The intercept subject invokes Three-Way calling to call Party B at 555-2222. Party B answers. The three parties are joined into a conversation. Another call from Party C at 555-3333 is refused, because the intercept subject is busy. Party B at 555-2222 drops out of the call, but Party A at 555-1111 remains in the call. The call is released.

This sequence is shown with three separate scenarios to show some variations of managing the CallIdentity parameter. It is shown with a single CallIdentity for the entire multiparty call, with a separate CallIdentity for each leg of a call merged into one CallIdentity, and with a CallIdentity for separate calls. The value of the CallIdentity is shown within square brackets, e.g., [1]. Separate calls are separated by commas, e.g., [1,2], and a call with multiple identities is shown with dots joining the constituent identities, e.g., [1•2].

D.10.1 Three-Way Calling, Plus Call Turned Away with a Single Call Identity

Table 41: **Three-Way Calling with a Single Call Identity Scenario** **(Sheet 1 of 2)**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 goes off-hook and…	CIAP> CCOpen (CCC1 [1])	
3	…calls Party A at 555-1111.	IDIAP> Origination (User Input="5551111", Called Party=2025551111 [1])	
4	The called party answers and they converse.	IDIAP> Answer ([1])	
5	The intercept subject invokes Three-Way calling…		

PN-4465-RV1

Table 41: **Three-Way Calling with a Single Call Identity Scenario** **(Sheet 2 of 2)**

Step	Action	Reported Event	Connection Diagram
6	…to call Party B at 555-2222.	IDIAP> Origination (User Input="5552222", Called Party=2025552222 [1])	
7	Party B answers.	IDIAP> Answer ([1])	
8	The three parties are joined into a conversation.		
9	Another call from Party C 555-3333 is refused, because the intercept subject is busy.	IDIAP> TerminationAttempt (5553333 [2]) CIAP> CCOpen (CCC2 [2])	
10	Party C abandons its call attempt.	IDIAP> Release ([2]) CIAP> CCClose (CCC2)	
11	Party B 555-2222 drops out of the call, but Party A 555-1111 remains in the call.		
12	The call is released.	IDIAP> Release ([1]) CIAP> CCClose (CCC1)	

PN-4465-RV1

D.10.2 Three-Way Calling, Plus Call Turned Away with Separate Leg Identities

Table 42: **Three-Way Calling Scenario with Separate Leg Identities (Sheet 1 of 2)**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 goes off-hook and…	CIAP> CCOpen (CCC1 [1])	
3	…calls Party A at 555-1111.	IDIAP> Origination (User Input=“5551111”, Called Party=2025551111 [1])	
4	The called party answers and they converse.	IDIAP> Answer ([1])	
5	The intercept subject invokes Three-Way calling…	IDIAP> Change ([1 to 1•2])	
6	…to call Party B at 555-2222.	IDIAP> Origination (User Input=“5552222”, Called Party=2025552222 [2])	
7	Party B answers.	IDIAP> Answer ([2])	
8	The three parties are joined into a conversation.		
9	Another call from Party C 555-3333 is refused, because the intercept subject is busy.	IDIAP> TerminationAttempt (5553333 [3]) CIAP> CCOpen (CCC2 [3])	

PN-4465-RV1

Table 42: **Three-Way Calling Scenario with Separate Leg Identities** **(Sheet 2 of 2)**

Step	Action	Reported Event	Connection Diagram
10	Party C abandons its call attempt.	IDIAP> Release ([3]) CIAP> CCClose (CCC2)	
11	Party B 555-2222 drops out of the call, but Party A 555-1111 remains in the call.	IDIAP> Release ([2])	
12	The call is released.	IDIAP> Release ([1]) CIAP> CCClose (CCC1)	

D.10.3 Three-Way Calling, Plus Call Turned Away with Separate Calls

Table 43: **Three-Way Calling with Separate Call Scenario** **(Sheet 1 of 2)**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 goes off-hook and…	CIAP> CCOpen (CCC1 [1])	
3	…calls Party A at 555-1111.	IDIAP> Origination (User Input="5551111", Called Party=2025551111 [1])	
4	The called party answers and they converse.	IDIAP> Answer ([1])	
5	The intercept subject invokes Three-Way calling…	CIAP> CCOpen (CCC2 [2]) IDIAP> Change ([1,2 to 1•2])[a]	

PN-4465-RV1

Table 43: **Three-Way Calling with Separate Call Scenario** **(Sheet 2 of 2)**

Step	Action	Reported Event	Connection Diagram
6	…to call Party B at 555-2222.	IDIAP> Origination (User Input=“5552222”, Called Party=2025552222 [2])	
7	Party B answers.	IDIAP> Answer ([2])	
8	The three parties are joined into a conversation.		
9	Another call from Party C 555-3333 is refused, because the intercept subject is busy.	IDIAP> TerminationAttempt (5553333 [3]) CIAP> CCOpen (CCC3 [3])	
10	Party C abandons its call attempt.	IDIAP> Release ([3]) CIAP> CCClose (CCC3)	
11	Party B 555-2222 drops out of the call, but Party A 555-1111 remains in the call.	IDIAP> Release ([2]) CIAP> CCClose (CCC2)	
12	The call is released.	IDIAP> Release ([1]) CIAP> CCClose (CCC1)	

Table Notes

a. This Change message does not report the CCCs used because the call 1•2 is not delivered on a single CCC, but is rather delivered as separate and constituent calls 1 and 2.

PN-4465-RV1

D.11 Call Forwarding—No Answer on a Single System

An incoming call arrives for the intercept subject (S) at (202) 555-0000 from Party A at 555-1111. After ringing the intercept subject for a short time, the call is forwarded to Party B at 555-2222. The call is forwarded from that number to Party C at 555-3333. Party C answers the call. The call is released.

Table 44: **Call Forwarding—No Answer on a Single System Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	An incoming call arrives for the intercept subject at (202) 555-0000 from Party A at 555-1111.	IDIAP> TerminationAttempt (5551111) CIAP> CCOpen (CCC1)	
3	After ringing the intercept subject for a short time, the call is forwarded to Party B at 555-2222.	IDIAP> Redirection (5552222)	
4	The call is forwarded from that number to Party C at 555-3333. (Call forwarding is performed by Party B's service.)		
5	Party C answers the call.	IDIAP> Answer ()	
6	The call is released.	IDIAP> Release CIAP> CCClose (CCC1)	

The next scenario repeats this scenario, but shows it happening on different systems. Some system architectures may provide only the information shown in the next scenario, even when the call occurs in a single system.

PN-4465-RV1

D.12 Call Forwarding—No Answer on Different Systems

An incoming call arrives for the intercept subject (S) at (202) 555-0000 from Party A at 555-1111. After ringing the intercept subject for a short time, the call is forwarded to Party B at 555-2222. The call is forwarded from that number to Party C at 555-3333. Party C answers the call. The call is released.

Table 45: **Call Forwarding—No Answer on Different Systems Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	An incoming call arrives for the intercept subject at (202) 555-0000 from Party A at 555-1111.	IDIAP> TerminationAttempt (5551111) CIAP> CCOpen (CCC1)	
3	After ringing the intercept subject for a short time, the call is forwarded to Party B at 555-2222.	IDIAP> Redirection(5552222)	
4	The call is forwarded from that number to Party C at 555-3333. (Call forwarding is performed by Party B's service.)		
5	Party C answers the call.	IDIAP> Answer ()	
6	The call is released.	IDIAP> Release CIAP> CCClose (CCC1)	

PN-4465-RV1

D.13 Two Bearer Channels, Plus Call Transfer

The intercept subject (S) at (202) 555-0000, an ISDN subscriber calls Party A at 555-1111. Party A answers. Party B at 555-2222 calls the intercept subject. The intercept subject answers the call from Party B. The intercept subject transfers the call to Party C at 555-3333. Party C answers. Party A releases. Parties B and C release.

This sequence uses multiple call identities of managing the CallIdentity parameter. The value of the CallIdentity is shown within square brackets, e.g., [1].

Table 46: **Two Bearer Channels, Plus Call Transfer Scenario** **(Sheet 1 of 2)**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000, an ISDN subscriber calls Party A at 555-1111.	IDIAP> Origination (User Input="5551111", Called Party=2025551111 [1]) CIAP> CCOpen (CCC1 [1])	
3	Party A answers.	IDIAP> Answer ([1])	
4	Party B at 555-2222 calls the intercept subject.	IDIAP> TerminationAttempt (5552222 [2]) CIAP> CCOpen (CCC2 [2])	
5	The intercept subject answers the call from Party B.	IDIAP> Answer (Called [2])	
6	The intercept subject transfers the call to Party C at 555-3333.	IDIAP> Origination (User Input="5553333", Called Party=2025553333 [2])	
7	Party C answers	IDIAP> Answer ([2])	

PN-4465-RV1

Table 46: **Two Bearer Channels, Plus Call Transfer Scenario** **(Sheet 2 of 2)**

Step	Action	Reported Event	Connection Diagram
8	Party A releases.	IDIAP> Release ([1]) CIAP> CCClose (CCC1 [1])	
9	Parties B and C release.	IDIAP> Release ([2]) CIAP> CCClose (CCC2 [2])	

D.14 Speed Calling

The intercept subject (S) at (202) 555-0000 dials Party A using a speed number #12. The speed number is expanded to 555-1111. The call is abandoned.

Table 47: **Speed Calling Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 goes off-hook…	CIAP> CCOpen (CCC1)	
3	…and dials Party A using a speed number #12. The number is expanded to 555-1111.	IDIAP> Origination (User Input="#12", Called Party=2025551111)	
4	The call is abandoned.	IDIAP> Release CIAP> CCClose (CCC1)	

PN-4465-RV1

D.15 Multiple Translations on Single System

The intercept subject (S) at (202) 555-0000 dials Party A using a speed number, #12. The speed number is expanded to A' 800-555-1111. The 800 number is expanded by the switch to A" (202) 555-2222. The call is answered. The call is released.

Table 48: **Multiple Translations on a Single System Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 goes off-hook…	CIAP> CCOpen (CCC1)	
3	…and dials Party A using a speed number, #12. The number is expanded to A' 800-555-1111. This number is expanded to A" (202) 555-2222.	IDIAP> Origination (User Input="#12", Called Party=8005551111) IDIAP> Origination (Translation Input= "8005551111", Called Party=2025552222)	
4	The call is answered.	IDIAP> Answer ()	
5	The call is released.	IDIAP> Release CIAP> CCClose (CCC1)	

PN-4465-RV1

D.16 Multiple Call Scenario

A call from Party A at 555-1111 arrives and is forwarded to Party B at 555-2222. A call from Party C at 555-3333 arrives and is forwarded to Party B at 555-2222. The first call is released. The second call is released.

This sequence uses multiple call identities of managing the CallIdentity parameter. The value of the CallIdentity is shown within square brackets, e.g., [1].

Table 49: **Multiple Call Scenario**

Step	Action	Reported Event	Connection Diagram
1	A call from Party A at 555-1111 arrives and is forwarded to Party B at 555-2222.	IDIAP> TerminationAttempt (5551111 [1]) IDIAP> Redirection (5552222 [1]) CIAP> CCOpen (CCC1 [1])	
2	A call from Party C at 555-3333 arrives and is forwarded to Party B at 555-2222.	IDIAP> TerminationAttempt (5553333 [2]) IDIAP> Redirection (5552222 [2]) CIAP> CCOpen (CCC2 [2])	
3	The first call is answered.	IDIAP> Answer ([1])	
4	The second call is answered.	IDIAP> Answer ([2])	
5	The first call is released.	IDIAP> Release CIAP> CCClose (CCC1 [1])	
6	The second call is released.	IDIAP> Release CIAP> CCClose (CCC2 [2])	

PN-4465-RV1

D.17 Simple Call Delivery to a Mobile Station

A call to the intercept subject at (202) 555-0000 arrives at a roaming intercept subject's Home System (S') from Party A at (202) 555-1111. This call is redirected to the system serving the intercept subject (S) using a Temporary Local Directory Number of (202) 555-9999. The intercept subject answers the call. The call is released. (Note: this scenario assumes that the electronic surveillance order applies to both the Redirecting System (or as *TIA/EIA-41* calls it, the Originating System) and the current Serving System).

Table 50: **Simple Call Delivery Scenario** **(Sheet 1 of 2)**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle. The intercept subject is registered on a roaming system.		
2	A call to the intercept subject at (202) 555-0000 arrives at the intercept subject's Redirecting System from Party A at (202) 555-1111.	$IDIAP_1$> TerminationAttempt (2025551111) $CIAP_1$> CCOpen (CCC1)	
3	This call is redirected to the System Serving the intercept subject using a Temporary Local Directory Number of (202) 555-9999.	$IDIAP_{HLR}$> TerminationAttempt (2025551111)[a] $IDIAP_{HLR}$> Redirection (2025559999) $IDIAP_1$> Redirection (2025559999) $IDIAP_2$> TerminationAttempt (2025559999 redirected by 2025550000)[b] $CIAP_2$> CCOpen (CCC2)[c]	

PN-4465-RV1

Table 50: **Simple Call Delivery Scenario** **(Sheet 2 of 2)**

Step	Action	Reported Event	Connection Diagram
4	The intercept subject answers the call.	$IDIAP_1$> Answer () $IDIAP_2$> Answer (2025550000)	
5	The call is released.	$IDIAP_1$> Release $CIAP_1$> CCClose (CCC1) $IDIAP_2$> Release $CIAP_2$> CCClose (CCC2)	

Table Notes

a. The HLR-based IDIAP may be necessary for TSPs that allow call redirection without access to the call content.

b. Report the Temporary Local Directory Number (or equivalent) used to route the call rather than the terminal directory number.

c. If CCC1 and CCC2 pass through the same Delivery Function (e.g., pivoted content delivery), one of the CCCs should be eliminated. Before the subject answers, the CCC1 is the most appropriate channel. After the subject answers, CCC2 is the most appropriate channel.

PN-4465-RV1

D.18 Password Call Acceptance and Flexible Alerting

A call arrives at an intercept subject pilot number (202) 555-0000 from a party (A) at (202) 555-1111. The system prompts the calling party to enter a password. Party (A) enters a valid password, 123456. Flexible alerting alerts the intercept subject at 202-555-0000 and party (B) at 555-2222. The switch monitors their call progress tones. The intercept subject answers. The call attempt to B is automatically abandoned. The call is released.

Table 51: **Password Call Acceptance and Flexible Alerting Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	A call arrives at an intercept subject pilot number (202) 555-0000 from a party (A) at (202) 555-1111. The system prompts the calling party to enter a password.	IDIAP> TerminationAttempt (2025551111) IDIAP> Answer (TrunkId) CIAP> CCOpen (CCC1)	
3	Party (A) enters a valid password, 123456.		
4	Flexible alerting alerts the intercept subject at 202-555-0000 and party (B) at 555-2222. The switch monitors their call progress tones.	IDIAP> Redirection (2025550000) IDIAP> Redirection (5552222)	
5	The intercept subject answers. The call attempt to B is automatically abandoned.	IDIAP> Answer (2025550000)	
6	The call is released.	IDIAP> Release CIAP> CCClose (CCC1)	

PN-4465-RV1

D.19 Password Call Acceptance and Call Forwarding

A call arrives at an intercept subject number (202) 555-0000 from a party (A) at (202) 555-1111. The system answers the call and prompts the calling party to enter a password. Party (A) enters a valid password, 123456. The call is forwarded to Party (B). The call attempt is abandoned.

Table 52: **Password Call Acceptance and Call Forwarding Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	A call arrives at an intercept subject number (202) 555-0000 from a party (A) at (202) 555-1111. The system answers the call and prompts the calling party to enter a password.	IDIAP> TerminationAttempt (2025551111) IDIAP> Answer (TrunkId) CIAP> CCOpen (CCC1)	
3	Party (A) enters a valid password, 1233456.		
4	The call is forwarded to Party (B).	IDIAP> Redirection (5552222)	
5	The call is abandoned.	IDIAP> Release CIAP> CCClose (CCC1)	

PN-4465-RV1

D.20 Completed Call To Busy Subscriber

Previously the subject placed a call to busy subscriber A at 555-1111. The subject goes off-hook, enters a feature code *333 indicating that the call should be completed to the busy subscriber, and goes back on-hook. Later, subscriber A becomes available. The subject is alerted with distinctive alerting. The subject answers. The call is extended to subscriber A. The call is answered. Later both parties disconnect.

Table 53: **Completed Call To Busy Subscriber**

Step	Action	Reported Event	Connection Diagram
1	The call connections are idle. Previously the subject placed a call to busy subscriber A at 555-1111.		
2	The subject goes off-hook, enters a feature code *333 indicating that the call should be completed to the busy subscriber, and…	CIAP> CCOpen (CCC1) IDIAP> Origination (User Input="*333", Called Party=2025551111)	
3	…goes back on-hook.	IDIAP> Release CIAP> CCClose (CCC1)	
4	Later, subscriber A becomes available. The subject is alerted with distinctive alerting.	CIAP> CCOpen (CCC1) IDIAP> TerminationAttempt (TrunkID)	
5	The subject answers.	Answer (2025550000)	
6	The call is extended to Party A.	IDIAP> Origination (User Input="", Called Party=2025551111)	
7	The call is answered.	IDIAP> Answer ()	
8	Later both parties discon-nect.	IDIAP> Release CIAP> CCClose (CCC1)	

PN-4465-RV1

D.21 Dialed Feature Code Digits

The intercept subject at (202) 555-0000 invokes a feature code, *222, to deactivate Call Forwarding—Busy. The status of the change is provided audibly to the intercept subject. The call is released.

Table 54: **Dialed Feature Code Digits Scenario**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 invokes a feature code, *222. The status of the change is provided audibly to the intercept subject.	CIAP> CCOpen (CCC1) IDIAP> Origination (User Input = “*222”)	
3	The call is released.	IDIAP> Release CIAP> CCClose (CCC1)	

D.22 Call Release to Pivot

A call to intercept subject at (202) 555-0000 arrives at a roaming intercept subject’s Home System (S’) from Party A at (202) 555-1111. This call is redirected to the system serving the intercept subject (S) using a Temporary Local Directory Number of (202) 555-9999. The call is not answered and is redirected again by the redirecting system to Party B at 555-2222 (using release to pivot) to the forward-to number for an unanswered call.

Table 55: **Call Release to Pivot Scenario** **(Sheet 1 of 2)**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle. The intercept subject is registered on a Serving System.	$SSIAP_{HLR}$> ServingSystem	Redirecting (1) Serving (2)

PN-4465-RV1

Table 55: **Call Release to Pivot Scenario** **(Sheet 2 of 2)**

Step	Action	Reported Event	Connection Diagram
2	A call to intercept subject at (202) 555-0000 arrives at the intercept subject's Redirecting System from Party A at (202) 555-1111.	$IDIAP_1$> TerminationAttempt (2025551111) $CIAP_1$> CCOpen (CCC1)	
3	This call is redirected to the system serving the intercept subject using a Temporary Local Directory Number of (202) 555-9999.	$IDIAP_1$> Redirection (2025559999) $IDIAP_2$> TerminationAttempt (2025551111 redirected by 2025550000) $CIAP_2$> CCOpen (CCC2)	
4	After no answer, the call is forwarded to Party B at 555-2222 using release to pivot.	$IDIAP_1$> Redirection (5552222) $IDIAP_2$> Release $CIAP_2$> CCClose (CCC2)	
5	Party B answers the call.	$IDIAP_1$> Answer ()	
6	The call is released.	$IDIAP_1$> Release $CIAP_1$> CCClose (CCC1)	

PN-4465-RV1

D.23 Intrasystem Handoff

The intercept subject hands-off within a system.

Table 56: **Intrasystem Handoff Scenario**

Step	Action	Reported Event	Connection Diagram
1	The intercept subject is in the conversation mode on a system.	Previously: CIAP> CCOpen (CCC1)	
2	The MS is handed off to different cell within the same system.		

D.24 Handoff to a Third System without Path Minimization

The intercept subject is in the conversation mode on an Anchor System. The anchor MSC determines the call should be handed off to an adjacent system (without path minimization). After a time, the adjacent system determines that the call should be handed off to a third system. After a time the third system determines that the call should be handed to the Anchor System. The call is released.

Table 57: **Handoff to a Third System without Path Minimization Scenario (Sheet 1 of 2)**

Step	Action	Reported Event	Connection Diagram
1	The intercept subject is in the conversation mode on an Anchor System.	Previously: CIAP> CCOpen (CCC1)	
2	The anchor MSC determines the call should be handed off to an adjacent system.		

PN-4465-RV1

Table 57: **Handoff to a Third System without Path Minimization Scenario (Sheet 2 of 2)**

Step	Action	Reported Event	Connection Diagram
3	After a time, the adjacent system determines that the call should be handed off to a third system.		
4	After a time, the third system determines that the call should be handed back to the Anchor System.		
5	The call is released.	IDIAP> Release CIAP> CCClose (CCC1)	

PN-4465-RV1

D.25 Connected Party Modification

While the subject is in a stable call with another party A, the other party A transfers the call to another party B at 555-2222.

Table 58: **Connected Party Modification Scenario**

Step	Action	Reported Event	Connection Diagram
1	While the subject is in a stable call with another party A,…	Previously: CIAP> CCOpen (CCC1)	
2	…the other party A transfers the call to another party B at 555-2222.		

PN-4465-RV1

Annex E Information Access Scenarios - J-STD-025A

This Annex is informative and is not considered part of this Standard.

Several basic circuit-mode call scenarios are described in this section. The intent of this section is to provide representative examples of reported events over a CDC and changes in connections for the CCC. This section is not an exhaustive set of examples. Each specific scenario applies to a particular service and configuration, but may be considered to be applicable to other similar services and configurations. TSPs may provide access using configurations and accesses not shown and systems are not obligated to implement particular services or accesses in the way illustrated. There may also be implementation differences providing different numbers of CallIdentity per scenarios. (The scenarios assume that there is one CallIdentity used for each CCC, unless noted otherwise.)

For the switch connection diagram conventions see Annex D on page 141.

E.1 Conference Call

The intercept subject individually calls another party, then invokes multi-party service to place the newly called party in conversation with others previously placed in communication by the intercept subject (i.e., Conference Call).

E.1.1 Conference Call (ConferencePartyChange using PartyIdentities)

In this scenario, the ConferencePartyChange message is used. CCC1 monitors the multi-party conference communication. The Subject Signal and Network Signal messages have been omitted to focus the reader's attention to the ConferencePartyChange message usage.

Note: Pay close attention to the use of commas (,) and semicolons (;). Commas are used to separate identities (Call, Party, or CCC) within a single call. Semicolons are used to separate one call, with its associated identities (Call, Party, and CCC), from another call and its associated identities.

Note: Messages in italics are optional.

PN-4465-RV1

Table 59: **Conference Call (ConferencePartyChange using PartyIdentities) Scenario (Sheet 1 of 4)**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 goes off-hook and…	CIAP> CCOpen (CallIdentity=[1], CCCIdentity=CCC1)	
3	…calls Party A at 555-1111.	IDIAP> Origination (CallIdentity=[1], Called Party=2025551111, User Input="5551111")	
4	The called party answers and they converse.	IDIAP> Answer (CallIdentity=[1])	
5	The intercept subject invokes conference calling, Party A is placed on hold, and...	CIAP> CCOpen (CallIdentity=[2], CCCIdentity=CCC2) IDIAP>ConferenceParty–Change (Removed: CallIdentity=[1], PartyIdentity=2025550000, CCCIdentity= CCC1)	
6	… calls Party B at 555-2222.	IDIAP> Origination (CallIdentity=[2], Called Party=2025552222, User Input="5552222")	
7	Party B answers and communicates with the intercept subject.	IDIAP> Answer (CallIdentity=[2])	

PN-4465-RV1

Table 59: **Conference Call (ConferencePartyChange using PartyIdentities) Scenario (Sheet 2 of 4)**

Step	Action	Reported Event	Connection Diagram
8	The intercept subject requests all parties to be added to the conference. (Communicating parties are Parties [S, A, and B] on CCC1.)	IDIAP>Change (Previous: CallIdentity=[1]; CallIdentity=[2]; Resulting: CallIdentity=[1], CCCIdentity=CCC1) *IDIAP>ConferenceParty–Change* (Communicating: *CallIdentity=[1],* *PartyIdentity=2025550000,* *PartyIdentity=2025551111,* *PartyIdentity=2025552222,* *CCCIdentity=CCC1)* or (Joined: *CallIdentity=[1],* *PartyIdentity=2025550000,* *PartyIdentity=2025552222,* *CCCIdentity=CCC1)* CIAP>CCClose (CCCIdentity=CCC2)	
9	The intercept subject invokes conference calling, the conference is placed on hold, and... (Communicating parties are Parties [A and B] on CCC1.)	CIAP>CCOpen (CallIdentity=[3], CCCIdentity=CCC2) IDIAP>ConferenceParty-Change (Communicating: CallIdentity=[1], PartyIdentity=2025551111, PartyIdentity=2025552222, CCCIdentity=CCC1)	
10	...calls party X at 555-xxxx. (Communicating parties are Parties [A and B] on CCC1.)	IDIAP> Origination (CallIdentity=[3], Called Party=202555xxxx, User input=“555xxxx”)	

PN-4465-RV1

Table 59: **Conference Call (ConferencePartyChange using PartyIdentities) Scenario (Sheet 3 of 4)**

Step	Action	Reported Event	Connection Diagram
11	Party X answers and communicates with the subject. (Communicating parties are Parties [A and B] on CCC1 and Parties [S and X] on CCC2).	IDIAP> Answer (CallIdentity=[3])	
12	The intercept subject requests all parties to be added to the conference. (Communicating parties are [S, A, B, and X] on CCC1.)	IDIAP>Change (Previous: CallIdentity=[1]; CallIdentity=[3]; Resulting: CallIdentity=[1], CCCIdentity=CCC1) *IDIAP>ConferenceParty–Change* (Communicating: *CallIdentity=[1],* *PartyIdentity=2025550000,* *PartyIdentity=2025551111,* *PartyIdentity=2025552222,* *PartyIdentity=202555xxxx,* *CCCIdentity=CCC1)* or (Joined: *CallIdentity=[1],* *PartyIdentity=2025550000,* *PartyIdentity= 202555xxxx,* *CCCIdentity=CCC1)* CIAP>CCClose (CCCIdentity=CCC2)	
13	Party B hangs up from the call. (Communicating parties are [S,A, and X] on CCC1.)	IDIAP>ConferenceParty–Change (Communicating: CallIdentity=[1], PartyIdentity=2025550000, PartyIdentity=2025551111, PartyIdentity=202555xxxx, CCCIdentity=CCC1) or (Dropped: CallIdentity=[1], PartyIdentity=2025552222, CCCIdentity=CCC1)	

PN-4465-RV1

Table 59: **Conference Call (ConferencePartyChange using PartyIdentities) Scenario (Sheet 4 of 4)**

Step	Action	Reported Event	Connection Diagram
14	Later, the subject hangs up and the network releases all parties.	IDIAP>Release (CallIdentity=[1]) CIAP>CCClose (CCCIdentity=CCC1)	S

PN-4465-RV1

E.1.2 Conference Call (ConferencePartyChange using CallIdentities)

In this scenario the party identities are reported only on Origination messages, otherwise call identities are reported. The SubjectSignal and NetworkSignal messages have been omitted to focus the readers attention to the Conference-PartyChange message usage.

Note: Pay close attention to the use of commas (,) and semicolons (;). Commas are used to separate identities (Call, Party, or CCC) within a single call. Semicolons are used to separate one call, with its associated identities (Call, Party, and CCC), from another call and its associated identities.

Note: Messages in italics are optional.

Table 60: **Conference Call (ConferencePartyChange using CallIdentities) Scenario (Sheet 1 of 4)**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 goes off-hook and…	CIAP> CCOpen (CallIdentity=[1], CCCIdentity=CCC1)	
3	…calls Party A at 555-1111.	IDIAP> Origination (CallIdentity=[1], Called Party=2025551111, User Input="5551111")	
4	The called party answers and they converse.	IDIAP> Answer (CallIdentity=[1])	
5	The intercept subject invokes conference calling, Party A is placed on hold, and...	CIAP> CCOpen (CallIdentity=[2], CCCIdentity=CCC2) IDIAP>ConferenceParty–Change (Communicating: CallIdentity=[1], PartyIdentity=2025551111[a], CCCIdentity= CCC1)	
6	… calls Party B at 555-2222.	IDIAP> Origination (CallIdentity=[2], Called Party=2025552222, User Input="5552222")	

PN-4465-RV1

Table 60: **Conference Call (ConferencePartyChange using CallIdentities) Scenario (Sheet 2 of 4)**

Step	Action	Reported Event	Connection Diagram
7	Party B answers and communicates with the intercept subject.	IDIAP> Answer (CallIdentity=[2])	
8	The intercept subject requests all parties to be added to the conference. (Communicating parties are Parties [S, A, and B] on CCC1.)	IDIAP>Change (Previous: CallIdentity=[1]; CallIdentity=[2]; Resulting: CallIdentity=[1], CallIdentity=[2], CCCIdentity=CCC1) *IDIAP>ConferenceParty–Change* *(Communicating:* *CallIdentity=[1],* *CallIdentity=[2],* *PartyIdentity=2025550000,* *PartyIdentity=2025551111,* *PartyIdentity=2025552222,* *CCCIdentity=CCC1)* CIAP>CCClose (CCCIdentity=CCC2)	
9	The intercept subject invokes conference calling, the conference is placed on hold, and... (Communicating parties are Parties [A and B] on CCC1.)	CIAP>CCOpen (CallIdentity=[3], CCCIdentity=CCC2) IDIAP>ConferenceParty-Change (Communicating: CallIdentity=[1], CallIdentity=[2], PartyIdentity=2025551111[a], PartyIdentity=2025552222, CCCIdentity=CCC1)	
10	...calls party X at 555-xxxx. (Communicating parties are Parties [A and B] on CCC1.)	IDIAP>Origination (CallIdentity=[3], Called Party=202555xxxx, User input= “555xxxx”)	

PN-4465-RV1

Table 60: **Conference Call (ConferencePartyChange using CallIdentities) Scenario (Sheet 3 of 4)**

Step	Action	Reported Event	Connection Diagram
11	Party X answers and communicates with the subject. (Communicating parties are Parties [A and B] on CCC1 and Parties [S and X] on CCC2.)	IDIAP> Answer (CallIdentity=[3])	
12	The intercept subject requests all parties to be added to the conference. (Communicating parties are [S, A, B, and X] on CCC1.)	IDIAP>Change (Previous: CallIdentity=[1], CallIdentity=[2]; CallIdentity=[3]; Resulting: CallIdentity=[1], CallIdentity=[2], CallIdentity=[3], CCCIdentity=CCC1) *IDIAP>ConferenceParty–Change*[b] *(Communicating:* *CallIdentity=[1],* *CallIdentity=[2],* *CallIdentity=[3],* *PartyIdentity=2025550000,* *PartyIdentity=2025551111,* *PartyIdentity=2025552222,* *PartyIdentity=202555xxxx,* *CCCIdentity=CCC1)* CIAP>CCClose (CCCIdentity=CCC2)	
13	Party X hangs up from the call. (Communicating parties are [S,A, and B] on CCC1.)	IDIAP>ConferenceParty–Change (Communicating: CallIdentity=[1], CallIdentity=[2], PartyIdentity=2025550000[c], CCCIdentity=CCC1; Dropped: CallIdentity=[3][d], PartyIdentity=202555xxxx) IDIAP>Release (CallIdentity=[3])	

PN-4465-RV1

Table 60: **Conference Call (ConferencePartyChange using CallIdentities) Scenario (Sheet 4 of 4)**

Step	Action	Reported Event	Connection Diagram
14	Later, the subject hangs up and the network releases all parties.	IDIAP>Release (CallIdentity=[1]) IDIAP>Release (CallIdentity=[2]) CIAP>CCClose (CCCIdentity=CCC1)	S

Table Notes:

a. The PartyIdentities are needed to show which parties are on Hold.

b. Without PartyIdentities this message is redundant with the Change message.

c. This parameter would further clarify that the subject is not being Released with CallIdentity 3 but is remaining on the call.

d. This means that Party X dropped with CallIdentity 3 from the conversation. However, a Release message is needed to indicate CallIdentity 3 is no longer in use and will be available for reuse at a later time.

PN-4465-RV1

E.1.3 Conference Call (Connection/ConnectionBreak using PartyIdentities)

The SubjectSignal and NetworkSignal messages have been omitted to focus the readers attention to the Connection and ConnectionBreak messages.

Note: Pay close attention to the use of commas (,) and semicolons (;). Commas are used to separate identities (Call, Party, or CCC) within a single call. Semicolons are used to separate one call, with its associated identities (Call, Party, and CCC), from another call and its associated identities.

Note: Messages in italics are optional.

Table 61: **Conference Call (Connection/ConnectionBreak using PartyIdentities) Scenario (Sheet 1 of 3)**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 goes off-hook and…	CIAP> CCOpen (CallIdentity=[1], CCCIdentity=CCC1)	
3	…calls Party A at 555-1111.	IDIAP> Origination (CallIdentity=[1], Called Party=2025551111, User Input="5551111")	
4	The called party answers and they converse.	IDIAP> Answer (CallIdentity=[1])	
5	The intercept subject invokes conference calling, Party A is placed on hold, and...	CIAP> CCOpen (CallIdentity=[2], CCCIdentity=CCC2) IDIAP>ConnectionBreak[a] (CallIdentity=[1], RemovedParties: PartyIdentity=2025550000; RemainingParties: PartyIdentity=2025551111)	
6	… calls Party B at 555-2222.	IDIAP> Origination (CallIdentity=[2], Called Party=2025552222, User Input="5552222")	

PN-4465-RV1

Table 61: **Conference Call (Connection/ConnectionBreak using PartyIdentities) Scenario (Sheet 2 of 3)**

Step	Action	Reported Event	Connection Diagram
7	Party B answers and communicates with the intercept subject.	IDIAP> Answer CallIdentity=([2])	
8	The intercept subject requests all parties to be added to the conference. (Communicating parties are Parties [S, A, and B] on CCC1.)	IDIAP>Change (Previous: CallIdentity=[1]; CallIdentity=[2]; Resulting: CallIdentity=[1], CCCIdentity=CCC1) *IDIAP>Connection*[b] *CallIdentity=[1],* *ConnectedParties:* *PartyIdentity=2025550000,* *PartyIdentity=2025551111,* *PartyIdentity=2025552222)* CIAP>CCClose (CCCIdentity=CCC2)	
9	The intercept subject invokes conference calling, the conference is placed on hold, and... (Communicating parties are Parties [A and B] on CCC1.)	CIAP>CCOpen (CallIdentity=[3], CCCIdentity=CCC2) IDIAP>ConnectionBreak[a] (CallIdentity=[1], RemovedParties: PartyIdentity=2025550000; RemainingParties: PartyIdentity=2025551111, PartyIdentity=2025552222)	
10	...calls party X at 555-xxxx. (Communicating parties are Parties [A and B] on CCC1.)	IDIAP> Origination (CallIdentity=[3], Called Party=202555xxxx, User input= “555xxxx”)	
11	Party X answers and communicates with the subject. (Communicating parties are Parties [A and B] on CCC1 and Parties [S and X] on CCC2.)	IDIAP> Answer (CallIdentity=[3])	

PN-4465-RV1

Table 61: **Conference Call (Connection/ConnectionBreak using PartyIdentities) Scenario (Sheet 3 of 3)**

Step	Action	Reported Event	Connection Diagram
12	The intercept subject requests all parties to be added to the conference. (Communicating parties are [S, A, B, and X] on CCC1.)	IDIAP>Change (Previous: CallIdentity=[1]; CallIdentity=[3]; Resulting: CallIdentity=[1], CCCIdentity=CCC1) *IDIAP>Connection*[b] *(CallIdentity=[1],* *ConnectedParties:* *PartyIdentity=2025550000,* *PartyIdentity=2025551111,* *PartyIdentity=2025552222,* *PartyIdentity=202555xxxx)* *CIAP>CCClose* (CCCIdentity=CCC2)	
13	Party B hangs up from the call. (Communicating parties are [S,A, and X] on CCC1.)	IDIAP>ConnectionBreak[c] (CallIdentity=[1], RemainingParties: PartyIdentity=2025550000, PartyIdentity=2025551111, PartyIdentity=202555xxxx; DroppedParties: PartyIdentity=2025552222)	
14	Later, the subject hangs up and the network releases all parties.	IDIAP>Release (CallIdentity=[1]) CIAP>CCClose (CCCIdentity=CCC1)	

Table Notes:

a. This message can be constructed three ways: 1.) Report both Remaining and Removed parties. 2.) Report only Remaining parties. 3.) Report only Removed parties.

b. This message is redundant because all parties must follow their call identities when merged, which is reported by the Change message.

c. This message can be constructed three ways: 1.) Report both Remaining and Dropped parties. 2.) Report only Remaining parties. 3.) Report only Dropped parties.

PN-4465-RV1

E.2 Call Waiting

The intercept subject (S) at (202) 555-0000 originates a voice call to Party A at (202) 555-1111. Party A answers the call. Later, a second call arrives to alert the intercept subject from Party B at (202) 555-2222. The intercept subject answers the second call with Call Waiting. The intercept subject toggles back to the original call. The intercept subject ends that call by hanging up causing the held party to recall the intercept subject. The intercept subject answers the call. The second call is released.

This scenario shows each call with its own CallIdentity. This scenario contains no merging or splitting of CallIdentities and therefore the Change message is not required to be triggered. This scenario shows an example of the use of a single CCCIdentity. Therefore, CCClose and CCOpen messages are used to maintain the association between the CCCIdentity and two CallIdentities.

PN-4465-RV1

E.2.1 Call Waiting with Recall (NetworkSignal and SubjectSignal)

Table 62: **Call Waiting with Recall Scenario** **(Sheet 1 of 3)**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 goes off-hook and... ...hears dial-tone.	CIAP>CCOpen (CallIdentity=[1] CCCIdentity=CCC1) NSIAP>NetworkSignal (CallIdentity=[1] AudibleSignal=1)	
3	calls Party A at 555-1111 and ... ...hears ring-back tone.	IDIAP>Origination (CallIdentity=[1], CalledParty= 2025551111 User Input =”5551111”) NSIAP>NetworkSignal[a] (CallIdentity=[1] AudibleSignal=3)	
4	The called party answers the call and they converse.	IDIAP>Answer (CallIdentity=[1] PartyIdentity=2025551111)	
5	Later, a second call arrives from Party B at (202) 555-2222 and ... ...the intercept subject hears call waiting tone.	IDIAP>TerminationAttempt (CallIdentity=[2] PartyIdentity=2025552222) NSIAP>NetworkSignal (CallIdentity=[2] AlertingSignal=6)	

PN-4465-RV1

Table 62: **Call Waiting with Recall Scenario** **(Sheet 2 of 3)**

Step	Action	Reported Event	Connection Diagram
6	The intercept subject answers the second call with Call Waiting.	ISSIAP>SubjectSignal (CallIdentity=[1], Signal: (Switchhook Flash="Flash")) CIAP>CCClose (CCCIdentity=CCC1) CIAP>CCOpen (CallIdentity=[2] CCCIdentity=CCC1) IDIAP>Answer (CallIdentity=[2] PartyIdentity=2025550000)	
7	The intercept subject toggles back to the original call.	ISSIAP>SubjectSignal (CallIdentity=[2], Signal: (SwitchhookFlash="Flash")) CIAP>CCClose (CCCIdentity=CCC1) CIAP>CCOpen (CallIdentity=[1] CCCIdentity=CCC1)	
8	The intercept subject ends that call by hanging up ...	IDIAP>Release (CallIdentity=[1]) CIAP>CCClose (CCCIdentity=CCC1)	
9	... causing the held party to recall the intercept subject with alerting.	IDIAP>TerminationAttempt (CallIdentity=[2] PartyIdentity=2025552222) NSIAP>NetworkSignal (CallIdentity=[2] AlertingSignal=1) CIAP>CCOpen (CallIdentity=[2] CCCIdentity=CCC1)	
10	The intercept subject answers the call.	IDIAP>Answer (CallIdentity=[2] PartyIdentity=2025550000)	

PN-4465-RV1

Table 62: **Call Waiting with Recall Scenario** **(Sheet 3 of 3)**

Step	Action	Reported Event	Connection Diagram
11	Later, the second call is released.	IDIAP>Release (CallIdentity=[2]) CIAP> CCClose (CCCIdentity=CCC1)	S

Table Notes:

a. This message is used when the subject's switch receives a signal message and applies ring-back tone to the subject. If ring-back tone is applied in-band from the second TSP's switch then this message would not be generated by the subject's switch.

PN-4465-RV1

E.3 Multi-stage Dialing (DialedDigitExtraction)

The intercept subject originates a call through a secondary TSP. The secondary TSP answers the call and prompts the intercept subject to enter the destination number and calling card number. Party A answers, the two parties converse, then the call is ended.

Table 63: **Multi-stage Dialing (DialedDigitExtraction) Scenario** **(Sheet 1 of 2)**

Step	Action	Reported Event	Connection Diagram
1	The call connections for the IAP are idle.		
2	The intercept subject at (202) 555-0000 goes off-hook and… ...hears dial-tone	CIAP>CCOpen (CallIdentity=[1], CCCIdentity=CCC1) NSIAP>NetworkSignal (CallIdentity=[1], AudibleSignal=1)	
3	…calls a TSP switch at 1-800-555-1111.	IDIAP> Origination (CallIdentity=[1], Called Party=8005551111, User Input="18005551111") NSIAP>NetworkSignal[a] (CallIdentity=[1], AudibleSignal=3)	
4	The TSP switch answers and... ...prompts the intercept subject to enter the destination number followed by a # key, then a calling card number followed by a # key.	IDIAP>Answer (CallIdentity=[1]) (See footnote)[b]	
5	The intercept subject enters "404-555-1111#", then "1234-5678-9876#" within 20 seconds.	ISSIAP> DialedDigitExtraction[c] (CallIdentity=[1], Digits="4045551111#123456789876#')	
6	The call is routed to Party A.	(No reportable events)	
7	Party A answers and communicates with the intercept subject.	(No reportable events)	

PN-4465-RV1

Table 63: **Multi-stage Dialing (DialedDigitExtraction) Scenario** **(Sheet 2 of 2)**

Step	Action	Reported Event	Connection Diagram
8	The call is ended.	IDIAP>Release (CallIdentity=[1]) CIAP>CCClose (CCCIdentity=CCC1)	S

Table Notes:

a. This message is used when the subject's switch receives a signal message and applies ring-back tone to the subject. If the ring-back tone is applied in-band from the second TSP's switch then this message would not be generated by the subject's switch.

b. No messages are provided from the intercept subject's originating system because these events are occurring at the secondary TSP system, which is not performing surveillance.

c. If the intercept subject pauses more than twenty seconds or if the number of digits exceeds 32, then multiple DialedDigitExtraction messages would be sent.

PN-4465-RV1

Annex F Optional Messages

This Annex is informative and is not considered part of this Standard.

F.1 ConnectionTest Message

The ConnectionTest message is an optional message that may be used to verify the connectivity of the CDC. This message may be sent during the provisioning process or at any other time.

The ConnectionTest message may be triggered when:

a. manually invoked,

b. periodically at an implementation specific interval, or

c. automatically upon maintenance events.

The ConnectionTest message includes the following parameters:

Table 64: **ConnectionTest Message Parameters**

Parameter	MOC	Usage
CaseIdentity	O	Include to identify an associated Intercept Subject.
IAPSystemIdentity	O	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
Memo	O	Include any information that may be useful for the TSP to communicate to the LEA.

```
ConnectionTest ::= [11] SEQUENCE {
               [0] CaseIdentity                    OPTIONAL,
               [1] IAPSystemIdentity               OPTIONAL,
               -- include to identify the system containing the Intercept
               -- Access
               -- Function when the underlying data carriage does not imply
               -- that system.
               [2] TimeStamp,
memo           [3] VisibleString (SIZE (1..255))    OPTIONAL
}
```

PN-4465-RV1

Annex G LAES Administrative Interfaces

This Annex is informative and is not considered part of this Standard.

T1M1.5 has been working on a standard for the LAES administrative interfaces entitled *Operations, Administration, Maintenance and Provisioning (OAM&P)—Extension to Generic Network Information Model for Interfaces Between Service Provider Administrative System and Network Elements for Lawfully Authorized Electronic Surveillance.*

Refer to the following document or the latest version for information regarding the Reference Point *a* and Reference Point *c*:

ANSI T1.260-1998

This document is available from:

T1 Secretariat
1200 G St. NW Suite 500
Washington, DC 20005

PN-4465-RV1

Annex H Possible e-Interface Delivery Methods for Packet Mode Telecommunications Services

This Annex is informative and is not considered part of this Standard.

This Annex provides example Delivery Methods.

Note: This Annex is open to inclusion of or reference to other delivery methods.

H.1 Data Stream Framing Protocol Delivery Method

H.1.1 Introduction

This contribution proposes a method to use TCP/IP as a reliable delivery mechanism for application messages used for lawful intercept.

H.1.2 Approach

H.1.2.1 Purpose

This Data Stream Framing Protocol is designed to be used over a reliable data stream transport protocol (e.g. TCP) where discrete application messages are being sent and received. Since stream-based protocols such as TCP don't provide an inherent method to indicate the beginning and end of application messages, a generic "framing protocol" is defined here to met this need. This DSFP is a robust generic framing protocol that is self sufficient and provides its own validity checks. It allows for detecting errors in the synchronization of the data stream and provides a means to re-synchronize the data stream without requiring the underlying connection to be terminated.

H.1.3 Format

The format of the DSFP is shown below:

Table 65: **Format of DSFP**

Bit Number								Octet Number
8	7	6	5	4	3	2	1	
Prefix								1
								2
								3
								4
Version								5
Reserved								6
Length Indicator (LI)								7
								8

PN-4465-RV1

Table 65: **Format of DSFP**

Bit Number								Octet Number
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
Application Message								9
								...
								LI +8
Suffix								LI + 9
								LI + 10

The application message is framed with Prefix and Suffix character sequences. The inclusion of the Length Indicator enables the receiver to avoid searching for the Suffix within the data stream and enables efficient detection of synchronization problems by allowing the receiver to know where to expect the end of a message. The Prefix and Suffix characters are not escaped. In this sense, the DSFP is not a true framing protocol.

The Prefix is defined to be the ASCII string of 4 asterisks: “****”.

The Suffix is defined to be the ASCII string of 2 pluses: “++”.

The Version of the DSFP is set to zero.

The Reserved octet must be set to zero and must be ignored by the receiver.

H.1.4 Rules

As the data is read from the transport layer, the receiver performs the following steps:

1 Validate that each message begins with Prefix.

2 Validate that a Suffix exists exactly Length Indicator bytes after the Length Indicator.

If either Step 1 or Step 2 fails, then the receiver has lost synchronization with the sender. The receiver may either terminate the underlying transport layer connection or attempt to re-synchronize with the sender as described in Section H.1.5.

The following is an example of a more detailed set of steps that could be followed where the transport layer is TCP:

1 Read 8 bytes from the TCP socket.

2 Validate that the first 4 bytes is the ASCII string “****”.

3 The 7th and 8th bytes comprise the Length Indicator (LI). Read LI+2 bytes from the TCP socket.

4 Validate that the last two bytes (LI+1 and LI+2) is the ASCII string “++”.

If either Step 2 or Step 4 fails, then the receiver has lost synchronization with the sender. The receiver may either terminate the underlying reliable connection or attempt to re-synchronize with the sender as described in Section H.1.5.

PN-4465-RV1

H.1.5 Re-synchronization

A host that is trying to regain synchronization with the data stream will scan the data stream until the Prefix is detected and then use the Length Indicator and Suffix to verify that a complete Application Message has been extracted from the transport layer. Since the Prefix and the Suffix are not escaped, it is important that the receiver not only attempt to locate a Prefix, but also verify that a Suffix is where it is expected to be.

If the receiver has scanned 65,545 bytes (65,535 from Length Indicator + 10 overhead) from the data stream without successfully re-synchronizing with the sender, then the receiver should terminate the underlying transport layer connection. A particular interface with other hard constraints (e.g. network element buffer sizes), may terminate the underlying transport layer connection upon reaching that lower threshold.

Additionally, if the receiver has successfully re-synchronized with the sender, but then immediately loses synchronization again (when attempting to extract the next Application Message), then the receiver should terminate the underlying transport layer connection.

H.1.6 Short Application Messages

The error detection provided by the DSFP is not complete. Specifically, this protocol does not detect the case where there were no synchronization errors, but the application message was still too short to contain all of the mandatory data. This type of check is still required to be performed by the receiver in some fashion, but this type of error does not require the underlying transport layer connection to be terminated. The DSFP is not responsible for the detection of malformed application layer messages.

PN-4465-RV1

Annex I J-STD-025 Abstract Syntax

This Annex is informative and is composed of ASN.1 code ready to be compiled. The code is a reflection from the information in Chapter 5 and Chapter 6 with the exception of the material related to CDMA2000 in Section 6.5 “cdma2000 Abstract Syntax for Packet Data CII Delivery” and Section 6.6.2.1 “cdma2000 Abstract Syntax Notation for Packet Data CC Delivery”.

Note: This Annex does not include the expected convention of new text being underlined.

Figure 57: **LAES Object Tree**

PN-4465-RV1

```
Laesp-j-std-025-b {iso(1) member-body(2) us(840) ti(113737) laes(2) tr45(0) j-std-
        025(0) j-std-025-b(2) version-1(0)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

LAESProtocol ::= CHOICE {
        lAESMessage           LAESMessage,
        lAESMessagePlus       LAESMessagePlus
                -- For J-STD-025-A solutions the LAESMessage choice should be
                -- selected .
                -- The LAESMessagePlus choice is recommended for solutions for
                -- revisions beyond J-STD-025-A.
}

LAESMessagePlus ::= SEQUENCE {
        protocolIdentifier OBJECT IDENTIFIER Laesp-j-std-025-b,
                -- assigned for each protocol syntax
        lAESMessage           LAESMessage
}

-- The LAESMessage parameter defines the LAES messages.

LAESMessage ::= CHOICE {
        answer         [1] Answer,
        ccClose        [2] CCClose,
        ccOpen         [3] CCOpen,
        change         [4] Change,
        origination    [5] Origination,
        packetEnvelope [6] PacketEnvelope,
        redirection    [7] Redirection,
        release        [8] Release,
        servingSystem  [9] ServingSystem,
        termAttempt    [10] TerminationAttempt,
--      connTest       [11] ConnectionTest,  - - see Annex F
        confPartyChange[12] ConferencePartyChange,
        connection     [13] Connection,
        connectBreak   [14] ConnectionBreak,
        dialedDgtExtrn [15] DialedDigitExtraction,
        networkSignal  [16] NetworkSignal,
        subjectSignal  [17] SubjectSignal
}
```

PN-4465-RV1

```
-- Answer Message

-- The Answer message is used to report that a connection-oriented call or leg
-- has been answered.

Answer ::= SEQUENCE {
        caseIdentifier        [0] CaseIdentity,
        iapSystemIdentifier   [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                -- system.
        timeStamp             [2] TimeStamp,
        callIdentifier        [3] CallIdentity,
        answering             [4] PartyIdentity                    OPTIONAL,
                -- include, when known, to identify the answering party or agent

        location              [5] Location                         OPTIONAL,
                -- Include, when a terminating call is answered, the location
                -- information is reasonably available to the IAP and delivery is
                -- authorized, to identify the location of an intercept subject's
                -- mobile terminal
        bearerCapability      [6] EXPLICIT BearerCapability        OPTIONAL
                -- include, when known (or presumed), to indicate the granted bearer
                -- capability.
}


-- CCClose Message

-- The CCClose message is used to report the end of call content delivery on the
-- CCC.

CCClose ::= SEQUENCE {
        caseIdentifier        [0] CaseIdentity,
        iapSystemIdentifier   [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                -- system.
        timeStamp             [2] TimeStamp,
        cccIdentity           [3] EXPLICIT CCCIdentity
}
```

PN-4465-RV1

```
--CCOpen Message

-- The CCOpen message is used to report the beginning of call content delivery on
-- the CCC.

CCOpen ::= SEQUENCE {
        caseIdentifier          [0] CaseIdentity,
        iapSystemIdentifier     [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                -- system.
        timeStamp               [2] TimeStamp,
        circuitORpacket         CHOICE {
                callIdentities          [3] SEQUENCE OF CallIdentity,
                                                -- for circuit-mode intercepts
                pduType                 [4] PDUType
                                                -- for packet-mode intercepts
                },
        cccIdentity             [5] EXPLICIT CCCIdentity
}



-- Change Message

-- The Change message is used to report merging or splitting of connection-oriented
-- call identities.

Change ::= SEQUENCE {
        caseIdentifier          [0] CaseIdentity,
        iapSystemIdentifier     [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                -- system.
        timeStamp               [2] TimeStamp,
        previous                [3] SEQUENCE OF                -- previous call(s)
                callIdentities          SEQUENCE OF CallIdentity,
                                        -- identity(ies) of a previous call
        resulting               [4] SEQUENCE OF SEQUENCE {    -- resulting call(s)
                callIdentities          [0] SEQUENCE OF CallIdentity,
                                        -- identity(ies) of resulting call
                cccIdentity             [1] EXPLICIT CCCIdentity      OPTIONAL
                                                -- included when the content of the
                                                -- resulting call is delivered to
                                                -- identify the CCC(s).
                }
}
```

PN-4465-RV1

```
-- ConferencePartyChange Message

-- The ConferencePartyChange message reports a change in the parties to a subject initiated conference call
-- communication.

ConferencePartyChange ::= SEQUENCE {
        caseIdentifier          [0] CaseIdentity,
        iapSystemIdentifier     [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                -- system.
        timeStamp               [2] TimeStamp,
        communicating           [3] SEQUENCE OF SEQUENCE{
                -- include to identify parties participating in the communication.
                callIdentities          [0] SEQUENCE OF CallIdentity  OPTIONAL,
                        -- identifies communicating call identities.
                partyIdentities         [1] SEQUENCE OF PartyIdentity OPTIONAL,
                        -- identifies communicating party identities.
                cccIdentities           [2] EXPLICIT CCCIdentity      OPTIONAL
                        -- included when the content of the resulting call is
                        -- delivered to identify the associated CCC(s).
                } OPTIONAL,

        dropped                 [4] SEQUENCE OF SEQUENCE{
                -- include to identify parties dropped from the communication.
                callIdentities          [0] SEQUENCE OF CallIdentity  OPTIONAL,
                        -- identifies previously communicating, now dropped call
                        -- identity(ies).
                partyIdentities         [1] SEQUENCE OF PartyIdentity OPTIONAL,
                        -- identifies previously communicating, now dropped party
                        -- identity(ies).
                cccIdentities           [2] EXPLICIT CCCIdentity      OPTIONAL
                        -- included when a party(ies) to an existing communication
                        -- is dropped, to identify the associated CCC(s).
                } OPTIONAL,

        removed                 [5] SEQUENCE OF SEQUENCE{
                -- include to identify parties removed (e.g., hold service) from the
                -- communication.
                callIdentities          [0] SEQUENCE OF CallIdentity  OPTIONAL,
                        -- identifies removed call identity(ies).
                partyIdentities         [1] SEQUENCE OF PartyIdentity OPTIONAL,
                        -- identifies removed party identity(ies).
                cccIdentities           [2] EXPLICIT CCCIdentity      OPTIONAL
                        -- included when a party(ies) to an existing communication
                        -- is removed, to identify the CCC(s).
                } OPTIONAL,

        joined                  [6] SEQUENCE OF SEQUENCE{
                -- include to identify parties newly added to the communication.
                callIdentities          [0] SEQUENCE OF CallIdentity  OPTIONAL,
                        -- identifies newly added call identity(ies) to an existing
                        -- communication.
                partyIdentities         [1] SEQUENCE OF PartyIdentity OPTIONAL,
                        -- identifies newly added party identity(ies) to an existing
                        -- communication.
                cccIdentities           [2] EXPLICIT CCCIdentity      OPTIONAL
                        -- included when a party to an existing communication
                        -- is added, to identify the associated CCC(s).
                } OPTIONAL
}
```

PN-4465-RV1

-- **Connection Message**

-- The Connection message reports parties to a call under surveillance.

```
Connection     ::= SEQUENCE   {
        caseIdentifier        [0] CaseIdentity,
        iapSystemIdentifier   [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                -- system.
        timeStamp             [2] TimeStamp,
        callIdentities        [3] SEQUENCE OF CallIdentity,
                -- Connection Information
                -- The following two parameters are considered Connection
                -- Information.Include at least one of the following.
                connectedParties      [4]    SEQUENCE OF PartyIdentity     OPTIONAL,
                newParties            [5]    SEQUENCE OF PartyIdentity     OPTIONAL
}
```

-- **ConnectionBreak Message**

-- The ConnectionBreak message reports parties removed from a call under surveillance.

```
ConnectionBreak::= SEQUENCE   {
        caseIdentifier        [0] CaseIdentity,
        iapSystemIdentifier   [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                -- system.
        timeStamp             [2] TimeStamp,
        callIdentities        [3] SEQUENCE OF CallIdentity,
                -- ConnectionBreak Information
                -- The following three parameters are considered ConnectionBreak
                -- Information. Include at least one of the following.
                removedParties        [4]    SEQUENCE OF PartyIdentity     OPTIONAL,
                remainingParties      [5]    SEQUENCE OF PartyIdentity     OPTIONAL,
                droppedParties        [6]    SEQUENCE OF PartyIdentity     OPTIONAL
}
```

-- **DialedDigitExtraction Message**

-- The DialedDigitExtraction message reports post cut-through digits dialed by the intercept subject.

```
DialedDigitExtraction ::= SEQUENCE {
        caseIdentifier        [0] CaseIdentity,
        iapSystemIdentifier   [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                -- system.
        timeStamp             [2] TimeStamp,
        callIdentifier        [3] CallIdentity,
        digits                [4] VisibleString (SIZE (1..32))
                -- e.g., “12345” or “*123” or “#345”
}
```

PN-4465-RV1

```
-- NetworkSignal Message

--The NetworkSignal message reports network signals sent to the intercept subject.

NetworkSignal ::= SEQUENCE {
        caseIdentifier        [0] CaseIdentity,
        iapSystemIdentifier   [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                --system.
        timeStamp             [2] TimeStamp,
        callIdentifier        [3] CallIdentity                     OPTIONAL,
                -- Signal
                -- The following four parameters are considered network-generated
                -- signals. Include at least one of the following four parameters to
                -- identify the signal being applied by the IAP.

        alertingSignal        [4] AlertingSignal                   OPTIONAL,
        subjectAudibleSignal  [5] AudibleSignal                    OPTIONAL,
        terminalDisplayInfo   [6] TerminalDisplayInfo              OPTIONAL,
        other                 [7] VisibleString (SIZE (1..128))    OPTIONAL
                        -- e.g., standard announcement or name of an announcement as
                        -- per ANSI-41.
}
```

PN-4465-RV1

```
-- Origination Message

-- The Origination message reports authorized connection-oriented call origination
-- attempts or number translations for the intercept subject performed by the
-- Access Function.

Origination ::= SEQUENCE {
        caseIdentifier          [0] CaseIdentity,
        iapSystemIdentifier     [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                -- system.
        timeStamp               [2] TimeStamp,
        callIdentifier          [3] CallIdentity,
        calling                 [4] PartyIdentity                    OPTIONAL,
                -- include, when more specific than the subject identity associated
                -- with the CaseIdentity, to identify the calling number
        called                  [5] PartyIdentity                    OPTIONAL,
                -- include if known
        input   CHOICE {
                userInput               [6] VisibleString (SIZE (1..32)),
                        -- use if input is known to be from the user
                        -- e.g., “” (hot line), “12025551234” or “*123”
                translationInput        [7] VisibleString (SIZE (1..32))
                        -- use for inputs to translation
                        -- e.g., “” (hot line), “12025551234” or “*123”
                },
        location                [8] Location                         OPTIONAL,
                -- Include, when the location information is reasonably available to
                -- the IAP and delivery is authorized, to identify the location of
                -- an intercept subject’s mobile terminal
        transitCarrierId        [9] TransitCarrierIdentity           OPTIONAL,
                -- include if known
        bearerCapability        [10] EXPLICIT BearerCapability       OPTIONAL
                -- include if known (or presumed)
}



-- PacketEnvelope Message

-- The PacketEnvelope message delivers intercepted packets to an LEA.

PacketEnvelope ::= SEQUENCE {
        caseIdentifier          [0] CaseIdentity,
        iapSystemIdentifier     [1] IAPSystemIdentity                OPTIONAL,
                        -- include to identify the system containing the Intercept
                        -- Access Function when the underlying data carriage does not
                        -- imply that system.
        timeStamp               [2] TimeStamp,
        callIdentifier          [3] CallIdentity                     OPTIONAL,
        location                [4] Location                         OPTIONAL,
                        -- Include, when the location information is reasonably
                        -- available to the IAP and delivery is authorized,
                        -- to identify the location of an intercept subject’s mobile
                        -- terminal.
        packetInformation       CHOICE {
        isdnUserToUserSignaling[5] SEQUENCE {
                callIdentifier          [0] CallIdentity,
                sending                 [1] PartyIdentity,
                interceptedUUPacket     [2] OCTET STRING (SIZE (1..128))     OPTIONAL
                                        -- Encoded according to T1.607 User-to-user
                                        -- information element starting with Octet 4.
                                }, 
```

PN-4465-RV1

```
        tiaEia41ShortMessageService[6] SEQUENCE {
                originalOriginatingAddress    [0] PartyIdentity,
                originalDestinationAddress    [1] PartyIdentity,
                originatingAddress            [2] PartyIdentity     OPTIONAL,
                                        -- include if known and different than the
                                        -- originalOriginatingAddress
                destinationAddress            [3] PartyIdentity     OPTIONAL,
                                        -- include if known and different than the
                                        -- original destinationAddress
                smsTeleserviceIdentifier      [4] INTEGER (-32768..32767),
                                        --see TIA/EIA-41
                interceptedISSMSPacket        [5] OCTET STRING (SIZE (1..255))
        OPTIONAL
                                },

        gsmSMShortMessageService[7] SEQUENCE {
                senderAddress         [0] PartyIdentity,
                receiverAddress       [1] PartyIdentity,
                nterceptedGSMSMSPacket[2] OCTET STRING (SIZE (1..255))     OPTIONAL
                                },

        wirelessIPService     [8] SEQUENCE {
                                -- This parameter may also be used for
                                -- information pertaining to non-wireless
                                -- IP-based services.
                originatingAddress    [0] PartyIdentity,
                destinationAddress    [1] PartyIdentity,
                interceptedIPPacket   [2] OCTET STRING (SIZE (1..70000))   OPTIONAL
                                }
                        }
}



-- Redirection Message

-- The Redirection message indicates that an incoming connection-oriented call
-- attempt, originally directed toward a subject, has been redirected by the
-- subject.

Redirection ::= SEQUENCE {
        caseIdentifier        [0] CaseIdentity,
        iapSystemIdentifier   [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                -- system.
        timeStamp             [2] TimeStamp,
        callIdentifier        [3] CallIdentity,
        redirectedTo          [4] PartyIdentity,
        transitCarrierId      [5] TransitCarrierIdentity           OPTIONAL,
                -- include if known
        bearerCapability      [6] EXPLICIT BearerCapability        OPTIONAL,
                -- include if known (or presumed)
        systemIdentity        [7] VisibleString (SIZE (1..15))     OPTIONAL
                -- include when a call to a wireless subscriber is redirected to
                -- another TSP and that identity is reasonably available.
                -- e.g., “MSCID-12345-123” or “2025551234”
}
```

PN-4465-RV1

```
-- Release Message

-- The Release message is used to report that a connection-oriented call has been
-- released.

Release ::= SEQUENCE {
        caseIdentifier        [0] CaseIdentity,
        iapSystemIdentifier   [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                -- system.
        timeStamp             [2] TimeStamp,
        callIdentifier        [3] CallIdentity,
        location              [4] Location                         OPTIONAL,
                -- Include, when the location information is reasonably available to
                -- the IAP and delivery is authorized, to identify the location of
                -- an intercept subject's mobile terminal
        systemIdentity        [5] VisibleString (SIZE (1..15))     OPTIONAL
                -- include, when a handed-off wireless call is released while being
                -- served by another TSP to identify the last known TSP serving the
                -- subject, e.g., "MSCID-12345-123" or "2025551234"
}



-- ServingSystem Message

-- The ServingSystem message is used to report a change in the current TSP or
-- service area for terminal or personal mobility.

ServingSystem ::= SEQUENCE {
        caseIdentifier        [0] CaseIdentity,
        iapSystemIdentifier   [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                -- system.
        timeStamp             [2] TimeStamp,
        systemIdentity        [3] VisibleString (SIZE (1..15))     OPTIONAL,
                -- include, when authorizing service to a TSP, to identify the TSP
                -- e.g., "MSCID-12345-123" or "2025551234"
        networkAddress        [4] VisibleString (SIZE (1..15))     OPTIONAL
                -- include if the serving TSP can only be identified by
                -- a redirect-to number e.g., a personal or residential base station
                -- directory number "2025551234"
}
```

PN-4465-RV1

```
-- SubjectSignal Message

-- The SubjectSignal message reports all signaling input by the intercept subject.

SubjectSignal ::= SEQUENCE {
        caseIdentifier          [0] CaseIdentity,
        iapSystemIdentifier     [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                -- system.
        timeStamp               [2] TimeStamp,
        callIdentifier          [3] CallIdentity                     OPTIONAL,
        signal                  [4] SEQUENCE {
                -- signal
                -- The following four parameters are considered subject-initiated
                -- signaling information. Include at least one of the following four
                -- parameters to identify the subject-signaling information being
                -- reported.
                switchhookFlash       [0] VisibleString (SIZE (1..128))    OPTIONAL,
                                      -- e.g, "FLASH"
                dialedDigits          [1] VisibleString (SIZE (1..128))    OPTIONAL,
                                      -- e.g. "12013452367", "*123",
                featureKey            [2] VisibleString (SIZE (1..128))    OPTIONAL,
                                      -- e.g.  "KEY1", "HOLD", "CONFERENCE" or any
                                      -- other function key.
                otherSignalingInformation     [3] VisibleString (SIZE (1..128))
        OPTIONAL
                                      -- e.g., "HOME"
                }
}



-- TerminationAttempt Message

-- The TerminationAttempt message is used to report a connection-oriented call
-- termination attempt.

TerminationAttempt ::= SEQUENCE {
        caseIdentifier          [0] CaseIdentity,
        iapSystemIdentifier     [1] IAPSystemIdentity                OPTIONAL,
                -- include to identify the system containing the Intercept Access
                -- Function when the underlying data carriage does not imply that
                -- system.
        timeStamp               [2] TimeStamp,
        callIdentifier          [3] CallIdentity,
        calling                 [4] PartyIdentity,
        called                  [5] PartyIdentity                    OPTIONAL,
                -- include, when more specific than the subject identity associated
                -- with the CaseIdentity, to identify the called party.
        bearerCapability        [6] EXPLICIT BearerCapability        OPTIONAL,
                -- included when known (or presumed)
        redirectionFrom         [7] RedirectedFromInformation        OPTIONAL
                -- include if this termination attempt is a result of a redirected
                -- call
}



-- Parameter Definitions
```

PN-4465-RV1

```
-- AlertingSignal

-- The AlertingSignal parameter defines the pitch and cadence of the alerting
-- (ringing) signal. The AlertingSignal parameter shall be encoded as follows:

AlertingSignal ::= ENUMERATED {
        notUsed                (0),
        alertingPattern0       (1), -- normal alerting
        alertingPattern1       (2), -- distinctive alerting - Intergroup
        alertingPattern2       (3), -- distinctive alerting: Special/Priority
        alertingPattern3       (4), -- Electronic Key Telephone Service
        alertingPattern4       (5), -- reminder ring
        callWaitingPattern1    (6), -- basic call waiting tone
        callWaitingPattern2    (7), -- incoming additional call tone
        callWaitingPattern3    (8), -- priority additional call tone
        callWaitingPattern4    (9), -- distinctive call waiting tone
        bargeInTone            (10)
}


-- AudibleSignal

-- The AudibleSignal parameter is used to report the type of audible tone that is
-- generated by the IAP switch and applied to the intercept subject.
-- The AudibleSignal parameter shall be encoded as follows:

AudibleSignal ::= ENUMERATED {
        notUsed                (0),
        dialTone               (1),
        recallDialTone         (2),
        ringbackTone           (3),    -- RingbackTone or AudibleAlerting
        reorderTone            (4),    -- ReorderTone or CongestionTone
        busyTone               (5),
        confirmationTone       (6),
        expensiveRouteTone     (7),
        messageWaitingTone     (8),
        receiverOffHookTone    (9),
        specialInfoTone        (10),
        denialTone             (11),
        interceptTone          (12),   --InterceptTone or MobileReorder
        answerTone             (13),
        tonesOff               (14),
        pipTone                (15),
        abbreviatedIntercept   (16),
        abbreviatedCongestion  (17),
        warningTone            (18),
        dialToneBurst          (19),
        numberUnObtainableTone (20),
        authenticationFailTone (21)
}



-- BearerCapability

--The BearerCapability parameter indicates a requested or granted bearer service.

BearerCapability ::= CHOICE {
        speech                 [0] NULL,
        f3100HzAudio           [1] NULL,
        bearerCapInfoElement   [2] OCTET STRING (SIZE (1..64))
                -- encoded according to T1.607 Bearer Capability information
                -- element starting with octet 3
}
```

PN-4465-RV1

```
-- CallIdentity

--The CallIdentity parameter is used to uniquely identify a particular call, call
-- appearance, or call legs within the context of a single system. The CCOpen and
-- Change messages can correlate the CallIdentity to one or more CCCs when content
-- is delivered. A CallIdentity may be created with a CCOpen, Origination,
-- TerminationAttempt, NetworkSignal or Change message. A CallIdentity may be released
-- for other uses with a Release or Change message. CallIdentity shall not be
-- immediately re-used. HLRs and similar systems that do not correlate messages
-- with CallIdentity(ies) do not need to release the CallIdentity.

CallIdentity ::= SEQUENCE {
sequenceNumber        [0] VisibleString (SIZE (1..25)),
systemIdentity        [1] VisibleString (SIZE (1..15))     OPTIONAL
                      -- include when the system issuing the sequenceNumber is
                      -- different than the accessing system.
                      -- e.g., CLLI code, “MSCID-12345-123” or “2025551234” (E.164
                      -- address of node)
}

-- CaseIdentity

-- The CaseIdentity parameter contains a case identity assigned by the LEA for a
-- particular electronic surveillance. The CaseIdentity will be designated by the
-- LEA and provided to a TSP at the time of provisioning of an electronic
-- surveillance.

CaseIdentity ::= VisibleString (SIZE (1..25))
               -- e.g., “FBI-12345” or “NYPD-12345”

-- CCCIdentity

-- The CCCIdentity parameter identifies the CCC or pair of CCCs used for conveying
-- call content. Each CCC is identified with a VisibleString which may contain a
-- directory number (e.g., “202-555-1111”), a trunk identity (e.g., “FBITG-001” or
-- “LAES-999”), an IP network address (e.g., “IP: 101.012.103.104:100”) or an X.25
-- network address (e.g., “X121: 1234-5678901234”).

CCCIdentity ::= CHOICE {
combCCC       [0] VisibleString (SIZE (1..20)),    -- combined CCC
sepCCCpair    [1] SEQUENCE {                       -- separated CCC
       sepXmitCCC            [0] VisibleString (SIZE (1..20)), -- transmit path
                      -- (from the intercept subject or redirected-to party)
       sepRecvCCC            [1] VisibleString (SIZE (1..20)) -- receive path
                      -- (to the intercept subject or redirected-to party)
              },
indXmitCCC    [2] VisibleString (SIZE (1..20)), -- individual transmit path
              -- (from the intercept subject or redirected-to party)
indRecvCCC    [3] VisibleString (SIZE (1..20)), -- individual receive path
              -- (to the intercept subject or redirected-to party)
indCCC        [4] VisibleString (SIZE (1..20)) -- individual CCC without
              -- a specified direction. Use only in CCClose messages.
}


-- IAPSystemIdentity

--The IAPSystemIdentity parameter identifies the system of the Intercept Access
-- Point and should not imply the specific location of an intercept subject.

IAPSystemIdentity ::= VisibleString (SIZE (1..15))
       -- e.g., CLLI code, “MSCID-12345-123” or “2025551234” (E.164 address of
       -- node)
```

PN-4465-RV1

```
-- Location

--The Location parameter identifies the cell of the subject's mobile terminal.

Location ::= VisibleString (SIZE (1..32))    -- e.g., "WESTGATE" or "CELL017"

-- PartyIdentity

-- The PartyIdentity parameter identifies a party to a call or call attempt.

PartyIdentity ::= SEQUENCE {
               -- include those identification elements necessary to uniquely
               -- identify the party known at the point in call and are
               -- authorized. At least one of the following parameters is
               -- required.

esn                  [0] VisibleString (SIZE (8))                      OPTIONAL,
                     -- AMPS-based Electronic Serial Number
                     -- a hexadecimal string e.g., "82ABCDEF"
imei                 [1] VisibleString (SIZE (1..15))                  OPTIONAL,
                     -- GSM-based International Mobile Equipment Identity
tei                  [2] VisibleString (SIZE (1..15))                  OPTIONAL,
                     -- ISDN-based Terminal Equipment Identity
spid                 [3] VisibleString (SIZE (3..20))                  OPTIONAL,
                     -- ISDN-based Service Profile Identifier
imsi                 [4] VisibleString (SIZE (1..15))                  OPTIONAL,
                     -- International Mobile Station Identity
                     -- E.212 number beginning with Mobile Country Code
min                  [5] VisibleString (SIZE (10))                     OPTIONAL,
                     -- AMPS-based Mobile Identification Number
dn                   [6] VisibleString (SIZE (1..15))                  OPTIONAL,
                     -- e.g., called directory number or network provided calling
                     -- number.
userProvided         [7] VisibleString (SIZE (1..15))                  OPTIONAL,
                     -- user provided calling number as supplied
appearanceId         [8] VisibleString (SIZE (1..15))                  OPTIONAL,
                     -- include for instruments or services with multiple line,
                     -- station, or call appearances
callingCardNum       [9] VisibleString (SIZE (1..20))                  OPTIONAL,
ipAddress            [10] VisibleString (SIZE (1..32))                 OPTIONAL,
                     -- IPv4 addressing with decimal quad notation e.g.,
                     -- "123.123.123.123" (not a URL)
x121                 [11] VisibleString (SIZE (1..15))                 OPTIONAL,
                     -- begin with DNIC
trunkId              [12] VisibleString (SIZE (1..32))                 OPTIONAL,
                     -- indicate trunk group, trunk number or both
                     -- This is usually used to identify an associate when other
                     -- identifying information is not available.
                     -- This may also identify a subject's agent (e.g., screening
                     -- service).
subaddress           [13] OCTET STRING (SIZE (2..21))                  OPTIONAL,
                     -- encoded according to T1.607 Subaddress information element
                     -- starting with octet 3.

genericAddress       [14] SEQUENCE OF VisibleString (SIZE (1..32))     OPTIONAL,
                     -- indicate use of the generic address
genericDigits        [15] SEQUENCE OF VisibleString (SIZE (1..32))     OPTIONAL,
                     -- indicate use of the generic digits
genericName          [16] SEQUENCE OF VisibleString (SIZE (1..48))     OPTIONAL,
                     -- indicate use of the generic name
port                 [17] VisibleString (SIZE (1..32))                 OPTIONAL,
                     -- identify a particular equipment port.
                     -- This is used to identify an associate when other
                     -- identifying information is not available.
```

PN-4465-RV1

```
context                 [18] VisibleString (SIZE (1..64))                   OPTIONAL,
                        -- when none of the other identities are known or to
                        -- identify the context and special considerations of the
                        -- supplied identifier(s), especially when the identifier(s)
                        -- is (are) abnormal (e.g., international, private,
                        -- restricted, operator, no address, hotel/motel, coin, etc.)
isdnHighLayer           [19] OCTET STRING (SIZE (2..14))                    OPTIONAL,
                        -- include if known
                        -- encoded according to T1.607 High Layer Compatibility
                        -- information element starting with octet 3
isdnLowLayer            [20] OCTET STRING (SIZE (2..14))                    OPTIONAL
                        -- include if known
                        -- encoded according to T1.607 Low Layer Compatibility
                        -- information element starting with octet 3
}


-- PDUType

--The PDUType parameter indicates the intercepted packet type on a CCC (e.g., see
-- Annex B.1). Negative values are reserved for bilateral agreement or protocol
-- extension.

PDUType ::= ENUMERATED {
        isdnBchannel   (0),    -- see BearerCapability parameter
        isdnDchannel   (1),    -- intermixed Q.931, Q.932, and X.25
        ip             (2),    -- Internet protocol packets
        ppp            (3),    -- Internet point-to-point protocol packets
        x25            (4)     -- X.25 LAPB packets
}
```

PN-4465-RV1

```
-- RedirectedFromInformation

-- The RedirectedFromInformation parameter is used to report information about the
-- last redirecting party and the original redirecting party on calls that are
-- redirected to the subject.

RedirectedFromInformation ::= SEQUENCE {
lastRedirecting       [0] PartyIdentity                    OPTIONAL,
                      -- include if known
originalCalled        [1] PartyIdentity                    OPTIONAL,
                      -- include if known
numRedirections       [2] INTEGER (1..100)                 OPTIONAL
                      -- include if known
}


-- TerminalDisplayInfo

-- The TerminalDisplayInfo parameter is used to report information that is
-- displayed on the intercept subject's terminal. The TerminalDisplayInfo parameter
-- shall be encoded as follows:

TerminalDisplayInfo   ::= SEQUENCE {
       generalDisplay        [0] VisibleString (SIZE(1..80))      OPTIONAL,
       calledNumber          [1] VisibleString (SIZE(1..40))      OPTIONAL,
       callingNumber         [2] VisibleString (SIZE(1..40))      OPTIONAL,
       callingName           [3] VisibleString (SIZE(1..40))      OPTIONAL,
       originalCalledNumber  [4] VisibleString (SIZE(1..40))      OPTIONAL,
       lastRedirectingNumber [5] VisibleString (SIZE(1..40))      OPTIONAL,
       redirectingName       [6] VisibleString (SIZE(1..40))      OPTIONAL,
       redirectingReason     [7] VisibleString (SIZE(1..40))      OPTIONAL,
       messageWaitingNotif   [8] VisibleString (SIZE(1..40))      OPTIONAL
}



-- TimeStamp

-- The TimeStamp parameter identifies the date and time of access.

TimeStamp ::= GeneralizedTime


-- TransitCarrierIdentity

-- The TransitCarrierIdentity parameter identifies an interexchange carrier.

TransitCarrierIdentity ::= VisibleString (SIZE (3..7))
               -- the carrier access code (if applicable) and carrier
               -- identification code e.g., "123" or "10123" or "1012345" or
               -- "9501234"
END --of Laesp-j-std-025-b
```

PN-4465-RV1

Symbols
µ-law encoding 95
Numerics
3.1 kHz audio 95
    bearer service 87, 214
800-number translation 58
    scenario *168*
A
a-interface **46**
abandoned **5**, 25, 61
abbreviated dialing
    scenario *167*
Abstract Syntax Notation One 74, 95
access **5**
    bridged 107
    looped 107
Access Function 5, 18, 19, 21, 43, **44**, **45**, 45, 46, 47, 81, *106*, *107*, *108*, *115*, *136*, 210
AF **5**
agent **5**, 47, 48, 89, 216
    answering a call scenario *172*, *173*
    making a call scenario *174*
alerting
    multiple parties scenario *172*
AMPS **5**
AMPS-based 89, 216
analog facility *108*, *110*, *112*, *136*
Anchor System *177*, *178*
announcement 6, 28
ANSI **5**
ANSI T1.607 **3**
Answer 22, **47**, 75, **76**, *147*, *148*, *149*, *151*, *152*, *153*, *155*, *156*, *157*, *158*, *159*, *160*, *161*, *162*, *163*, *164*, *165*, *166*, *168*, *169*, *171*, *172*, *173*, *174*, *176*, *181*, *185*, *186*, *189*, *190*, *193*, *194*, *196*, 204, **205**
    ISUP *123*
answer
    (action) *5*, 7, 28, 64, *122*, *136*, *137*, *142*, *143*, *144*, *146*, *149*, *150*, *154*, *158*, *159*, *164*, *165*, *166*, *168*, *170*, *171*, *172*, *173*, *175*
    (signal) *123*, *129*
    indication *123*
    LAESMessage **75**, **204**
    timer *123*
answering *123*, *131*, *133*
    PartyIdentity
        Answer 48, 52, **76**, **205**
answering party **5**
Anticipatory ***136***

PN-4465-RV1

appearanceId **89**, **216**
appearances 89, 216
APPLICATION **74**, 74
ASN.1 **5**, 74, 95
associate **5**
asynchronous data 95
Asynchronous Transfer Mode 5
ATM **5**, *111*, *112*, *113*, *114*
attendant recall 48, 64
automatic callback
    scenario *174*
automatic recall 13
    scenario *174*
availability 22, 25
Awaiting Answer *142*
B
B-channel **5**
b-interface **46**
Basic Encoding Rules 74, 95
bearer channels
    scenario *166*
bearer service 95, *115*
    3.1 kHz audio 87, 214
    speech 87, 214
BearerCapability **87**, 90, **214**, 217
    Answer 48, 76, 205
    circuit-mode vs. packet-mode *114*
    Origination 59, 81, 210
    Redirection 61, 83, 211
    TerminationAttempt 65, 67, 68, 69, 71, 85, 213
bearerCapInfoElement 87, 214
BER **5**, 74, 95
BRI **5**
bridged access ***107***
busy 64
    scenario *159*
C
C-conditional **47**
c-interface **47**
CALEA iii, xv, 1, **5**, 6, 7, 8, 9, 10, 14, 16
call **5**
    busy scenario *159*
    simple incoming scenario *149*
    simple outgoing scenario *147*
call abandoned
    scenario *145*, *146*

PN-4465-RV1

call and service processing 21
call appeaances
    scenario *166*
call appearance **5**, 19, 25, 89, 216
call appearances
    scenario *166*, *169*
call associated and non-call associated services 16
call associated services 16
call attempt
    abandoned *146*
    access 28
    answered 7
    answered by network 28
    incomplete 10
    unanswered 5, 6, *146*
call completion to a busy suscriber scenario *174*
call content **5**
    channel **5**
    delivery delay *136*
    distribution ***137***
call data
    channel **6**
    distribution *140*
call deflection **6**, 22, 29, 60
call delivery **6**, 29, 60
    scenario *170*
call diversion **6**, 22, 29, 60
call forwarding **6**, 22, 29, 60
    activation scenario *175*
    scenario *169*, *173*
    scenario on different systems *165*
    single system scenario *164*
call fowarding
    chained scenario *169*
call hold
    scenario *158*
call progress tones 28
call releast to pivot scenario *175*
call retrieval
    scenario *158*
call screening
    scenario *172*, *173*
call transfer **6**
    scenario *166*
call waiting
    deluxe 60

PN-4465-RV1

recall scenario *150*
scenario *150*, *154*
called
directory number 89, 216
party **6**
PartyIdentity
Origination 59, **78**, **81**, **207**, **210**
TerminationAttempt 65, **85**, **213**
Called Party
Origination *146*, *147*, *148*, *158*, *159*, *160*, *161*, *162*, *163*, *166*, *167*, *168*, *174*, *181*, *185*, *189*, *196*
call-identifying information 1, 5, 6, **6**, 9, 10, 16, **16**, 19, 20, 21, 25, 35, 45
Intercept Access Point 10, 21
CallIdentity **87**, **215**
Answer 48, 52, 76, 205
CCOpen 50, 77, 206
Change **51**, **58**, 77, 206
circuit-mode vs. packet-mode *114*
correlation 17
multiple per call *141*, *180*
one per scenario assumption *141*, *180*
Origination 59, 78, 79, 80, 81, 207, 208, 209, 210
PacketEnvelope 60, 81, 82, 210
Redirection 61, 83, 211
Release 62, 83, 212
Resulting 51, 58
TerminationAttempt 65, 85, 213
callIdentity
PacketEnvelope **82**, **210**
calling
directory number 89, 216
party **6**
PartyIdentity
Origination 59, **78**, **80**, **81**, **207**, **208**, **209**, **210**
TerminationAttempt 65, **85**, **213**
callingCardNum **89**, **216**
carrier access code 91, 218
carrier identification code 91, 218
CaseIdentity **87**, **215**
Answer 48, 52, 76, 205
CCClose 49, 76, 205
CCOpen 50, 77, 206
Change 51, 53, 54, 55, 58, 64, 77, 206
ConnectionTest *198*
Origination 59, 78, 79, 80, 81, 207, 208, 209, 210
PacketEnvelope 60, 81, 210

PN-4465-RV1

Redirection 61, 83, 211
Release 62, 83, 212
ServingSystem 62, 84, 212, 213
TerminationAttempt 65, 67, 68, 69, 70, 71, 72, 85, 213
CCC 5, **6**
channel exhaustion 35
congestion 35
exhaustion **35**
lack of CDC synchronization 35
loss of content 25
synchronization with CDC 35
unique identity 21
CCCIdentity **88**, **215**
CCClose 49, 76, 205
CCOpen 50
Change 51, 77, 206
Resulting 51
CCClose **48**, 75, 76, *120*, *128*, *132*, *134*, *141*, *145*, *146*, *147*, *148*, *149*, *151*, *152*, *153*, *155*, *156*, *157*, *158*, *160*, *162*, *163*, *164*, *165*, *167*, *168*, *169*, *171*, *172*, *173*, *174*, *175*, *176*, *178*, *183*, *187*, *190*, *194*, *195*, 204, 205
ccClose **75**, **204**
CCIAP **29**
CCIR **6**, 10
CCITT **6**, 11
CCOpen **49**, 75, 77, *119*, *126*, *131*, *134*, *141*, 204, 206
(CCC1) *145*, *146*, *147*, *148*, *149*, *151*, *152*, *153*, *155*, *156*, *157*, *158*, *159*, *161*, *162*, *164*, *165*, *166*, *167*, *168*, *169*, *170*, *172*, *173*, *174*, *175*, *176*, *177*, *179*, *181*, *185*, *189*, *193*, *196*
(CCC2) *151*, *152*, *153*, *155*, *156*, *157*, *160*, *161*, *163*, *166*, *169*, *170*, *176*, *193*
circuit-mode vs. packet-mode *114*
ccOpen **75**, **204**
CCT **6**
CDC 6, **7**
congestion 35
lack of CCC synchronization 35
synchronization with CCC 35
CDMA **7**, 31
CDPD 31, 60
cell **7**
Cellular Digital Packet Data 31
CF **7**
Change 22, **50**, 75, 77, 204, 206
call waiting *151*, *152*, *155*, *156*
change **75**, **204**
channel **7**
channel exhaust

PN-4465-RV1

CCC 35
CDC (congestion) 35
CHOICE 74, 98
BearerCapability 87, 214
CCCIdentity 88, 215
CCOpen 77, 206
LAESMessage 75, 204
Origination 78, 81, 207, 210
PacketEnvelope 82, 210
CIAP **7**, 25, 26, 27, 28, 29, *100*
circuit **7**
Circuit IAP 24, **25**, 25, 27
Circuit Intercept Access Point 7
circuit-mode **7**, 25, 27, 48, 49, 50, 59, 61, 64, 77, *112*, *114*, 206
class **74**, 74
APPLICATION 74
CONTEXT 74
PRIVATE 74
UNIVERSAL 74
CLLI code 87, 215
coin 90, 217
Collection Function 7, 19, 20, 21, 30, 32, 35, 43, 45, **46**, 46, 47, 95, *104*, *108*, *109*, *115*, *117*, *120*, *122*, *123*, *125*, *127*, *128*, *129*, *130*, *131*, *133*, *136*, *137*, *140*
collection function **7**
combCCC **88**, **215**
combined **19**, 20, 88, *107*, *115*, ***135***, 215
Commission **7**
CommunicatingIdentity 52
communication **7**
communication intercept **7**
Communications Assistance for Law Enforcement Act iii, xv, 1, 5
compatibility guidelines 96
complete **7**
completed call To busy subscriber scenario *174*
conditional 47
conference calling 27
party hold, join, drop **12**
Conference Circuit IAP 24, 29
ConferencePartyChange 51
ConferencePartyChange message
CommunicatingIdentity 52
DroppedIdentity 52
HoldIdentity 52
JoinedIdentity 52
congestion
CCC 35

PN-4465-RV1

CDC 35
connected party modification scenario *179*
Connection 53
connection **7**
ConnectionBreakInformation 53, 54
DroppedParties 54
RemainingParties 54
RemovedIdentities 53, 54
RemovedParties 53, 54
connectionless service *114*
ConnectionTest ***198***
connnection-oriented service *114*
constructor 74
content **7**, **16**
subject-initiated conference calls 7
surveillance service 16, 24
ContentType
CCOpen 50
CONTEXT **74**, 74
context
PartyIdentity **89**, **217**
controlling party **7**
CSU **8**, *108*
C-tone *See also* DTMF C-tone
cut-through
full **8**
partial **8**
D
D-channel **8**
d-interface **47**, *106*
data network *113*
DC **8**
decadic dial pulse *138*
decimal quad notation 89, 216
decryption 25
dedicated circuit *115*
CCC delivery *116*
dedicated data circuit CDC delivery *139*
dedicated data link CDC delivery *140*
deflection*See also* call deflection
delayed delivery ***136***
delivery
bearer service *134*
delayed *136*
signaling for *136*
See also call delivery

PN-4465-RV1

Delivery Function 8, 19, 43, 45, **45**, 45, 47, *102*, *104*, *106*, *107*, *108*, *109*, *115*, *119*, *120*, *123*, *125*, *127*, *128*, *129*, *131*, *132*, *136*, *137*, *140*, *171*
destination **6**, 8, **16**
destinationAddress **82**, **211**
DF **8**
dialed digit extraction **8**
    message 54
dialed digit extraction message
    Digits 55
Dialed Feature Code Digits
    Scenario *175*
direction **6**, 8, **16**
directory number 89, *108*, *114*, 216
disconnect **8**, *138*
diversion *See also* call diversion
dn **89**, **216**
DNIC 89, 216
DroppedIdentity 52
DS-0 *110*, *111*, *112*, *113*, *114*
DSU **8**, *108*
DTMF **8**, *112*, *138*
    digits *138*
DTMF C-tone *117*, *118*, *120*, *122*, *130*, *137*, *138*
    frequency pairs *138*
    signaling procedures *137*
Dual-Tone Multi-Frequency 8
E
e-interface **47**, *105*, *107*, *108*
E.164 87, 215
E.164 address of node 88, 215
E.212 number 89, 216
electronic communications **8**
electronic messaging services **8**
Electronic Serial Number 89, 216
electronic storage **8**
electronic surveillance **1**, **9**
en bloc *147*
encoding
    objectives 73
    parameter identifier 74
encryption 25
equipment port 89, 216
esn **89**, **216**
existing messages 97
EXPLICIT **74**, 76, 77, 81, 83, 85, 205, 206, 210, 211, 213
extend the protocol 74

PN-4465-RV1

extension number 28
external network 58
F
f3100HzAudio 87, 214
facsimile 95
FCC 99-230, CC Docket No. 97-213 1, 7, 8, 10, 12, 13, 14, 19, 22, 23, 24, 29, 34
feature code **9**
    dialed digits 81, 210
    scenario *175*
feature code dialed 58
Feature Group D 9
FG-D **9**
FGD *112*
flash *138*
flexible alerting
    scenario *172*
forwarding *See also* call forwarding
frame relay *110*, *112*, *113*
functional entity **9**, 44
G
G.711 **3**, 95
GeneralizedTime 91, 218
genericAddress **89**, **216**
genericDigits **89**, **216**
genericName **89**, **216**
government **9**
Group 3 Fax 95
GSM-based **9**, 31, 60, 89, 216
gsmSMShortMessageService **82**, **211**
H
handoff **9**, 14
    into a system scenario *177*
    scenario *177*
handover *See also* handoff
HDLC **9**, *113*
hexadecimal string 89, 216
high layer compatibility 90, 217
HLR **9**, 9, *106*
hold
    scenario *158*
hold recall 13, 48, 64
HoldIdentity 52
Home Location Register **9**
Home System **9**, 13, *102*, *104*, *170*, *175*
    intercept access points *101*
hot line **59**, 81, 210

PN-4465-RV1

hotel/motel 90, 217
Hz **9**
I
IAP **9**, 10, 25, *100*, *115*, *116*, *122*, *123*, *125*, *127*, *128*, *129*, *131*, *132*, *142*, *146*, *147*, *148*, *149*, *151*, *152*, *153*, *155*, *156*, *157*, *158*, *159*, *161*, *162*, *164*, *165*, *166*, *167*, *168*, *170*, *172*, *173*, *175*, *181*, *185*, *189*, *193*, *196*
IAPs *101*
IAPSystemIdentity **88**, **215**
    Answer 48, 52, 76, 205
    CCClose 49, 76, 205
    CCOpen 50, 77, 206
    Change 51, 53, 54, 55, 58, 64, 77, 206
    ConnectionTest *198*
    Origination 59, 78, 79, 80, 81, 207, 208, 209, 210
    PacketEnvelope 60, 81, 210
    Redirection 61, 83, 211
    Release 62, 83, 212
    ServingSystem 62, 84, 212, 213
    TerminationAttempt 65, 67, 68, 69, 70, 71, 72, 85, 213
identifier encoding 74
IDIAP **10**, 21, 23, 25, *100*, *106*
idle state **10**
imei **89**, **216**
IMPLICIT **74**, 75, 204
imsi **89**, **216**
IN **10**
incoming calls *106*
incomplete **10**
    call attempts 25
    calls 58
indCCC **88**, **215**
indRecvCCC **88**, **215**
indXmitCCC **88**, **215**
information service **10**
input
    Origination 59, **78**, **81**, **207**, **210**
INTEGER 74
    PacketEnvelope 82, 211
    RedirectedFromInformation 90, 218
intercept **10**
Intercept Access Function 76, 77, 78, 79, 80, 81, 83, 84, 85, *198*, 205, 206, 207, 208, 209, 210, 211, 212, 213
Intercept Access Point 9, **10**, 88, 215
    Call-Identifying Information 21
    Circuit 24, **25**
    content surveillance 24, 25

PN-4465-RV1

Home System *101*
land line *100*
Packet Data 24, **30**
Redirecting System *102*
Serving System *101*
Serving System Identification 21
intercept agent **10**
intercept subject **1**, **10**
Intercept Subject Signaling 23
Dialed Digit Extraction 24
Subject-initiated Dialing and Signaling 23
interceptedGSMSMSPacket **82**, **211**
interceptedISSMSPacket **82**, **211**
interceptedUUPacket **82**, **210**
interface reference points 44, **46**
international 89, 217
International Mobile Equipment Identity 89, 216
International Mobile Station Identity 89, 216
Internet Protocol 10
Inter-System Link Protocol 10
intrasystem handoff *177*
IP **10**, *110*, *111*, *113*
network address 88, 215
ip **90**, **217**
ipAddress **89**, **216**
IP-based service 60
ISDN **10**
-based 60, 89, 216
B-channel *110*, *111*, *112*, *113*, *114*
Bearer Capability *114*
D-channel *110*, *111*
signaling *136*
User Part 10
isdnBchannel **90**, **217**
isdnDchannel **90**, **217**
isdnHighLayer **90**, **217**
isdnLowLayer **90**, **217**
isdnUserToUserSignaling
PacketEnvelope **82**, **210**
ISLP **10**, *113*
ISSIAP 23
ISUP **10**, *112*
Bearer Capability *114*
generic address 89, 216
generic digits 89, 216
generic name 89, 216

PN-4465-RV1

signaling *136*
ITU-R **10**
ITU-T **11**
J
JoinedIdentity 52
J-STD-025A 1, 21, 22, 27, 180
K
kbps **11**
L
lack of CDC and CCC synchronization **35**
LAES **11**
Protocol 11
LAESP **11**, 20, 73, *110*, *111*
encoding objectives 73
parameter identifier encoding 74
land line intercept access points *100*
LAPB **11**, 90, *110*, *111*, *113*, 217
LAPD **11**, *110*, *111*, *112*
lastRedirecting PartyIdentity **90**, **218**
Law Enforcement Administration Function 11, 19, **46**, 46
Law Enforcement Agency iii, xv, 1
law enforcement agency **11**
Lawfully Authorized Electronic Surveillance 11
Protocol 20
LEA 1, 2, 5, 6, 10, **11**, 16, 19, 45, 46, *108*
LEAF **11**
LEAs 112
leg **11**
Lightweight Presentation Protocol 11
line appearances 89, 216
scneario *166*
Link Access Protocol—Balanced 11
Link Access Protocol—D-channel 11
Location **88**, **216**
Answer 48, 52, 76, 205
Origination 59, 81, 210
PacketEnvelope 60, 81, 210
Release 62, 83, 212
looped access ***108***
loss of content 25
low layer compatibility 90, 217
LPP **11**, *110*, *111*
M
M-mandatory **47**
mandatory 47
meet me conference 27

PN-4465-RV1

memo
ConnectionTest *198*
message descriptions **47**
Message Transfer Part 11
metallic signaling *136*
MF **11**, *112*
MF signaling *136*
min **89**, **216**
Mobile Country Code 89, 216
mobile station **11**
Mobile Switching Center **11**
MOC
See also mandatory, optional, and conditional 47
modem *108*, *113*
more than one LEA 20
MS **11**
MSC **11**
MSCID 87, 215
MTP **11**, *112*
mu-law encoding 95
Multi-Frequency 11
multi-party 27
awaiting answer connection *144*
connected and awaiting answer connection *144*
Multiple CIAPs 25
multiplexed 20
N
NAMPS **11**, 31
network
answering call scenario *174*
network address **11**
network provided calling number 89, 216
network reference model 44
Network Signaling 24
In-band and Out-of-band Signaling 24
in-band and out-of-band signaling **10**
message 55
Signal 58
AlertingSignal 58
SubjectAudibleSignal 58
TerminalDisplayInfo 58
networkAddress
ServingSystem 62, **84**, **212**, **213**
new
messages 98
parameter fields 98

PN-4465-RV1

parameter values 99
parameters 98
no address 90, 217
no input 81, 210
Non-Call Associated Information Surveillance Service Description—Serving System IAP 21
non-call associated services 16
NSIAP 23
NULL 87, 214
number translation 58
input *81*, *210*
scenario *167*, *168*
single system scenario *168*
numRedirections **90**, **218**
O
O-optional **47**
OCTET STRING
BearerCapability 87, 214
ISDN high layer
PartyIdentity 90, 217
ISDN low layer
PartyIdentity 90, 217
Packet Envelope
GSM SMS packet 82, 211
TIA/EIA-41 SMS packet 82, 211
user-to-user packet 82, 210
PartyIdentity subaddress 89, 216
off-hook **11**, *137*
one-way paging 31
on-hook **11**, *138*
operator 90, 217
optional 47, 97, 98
origin **6**, 11, **16**
originalCalled PartyIdentity **90**, **218**
originalDestinationAddress **82**, **211**
originalOriginatingAddress **82**, **211**
originating calls *106*
Originating System 12, *170*
originatingAddress **82**, **211**
Origination 22, **58**, 75, **81**, *145*, *146*, *147*, *148*, *158*, *159*, *160*, *161*, *162*, *163*, *166*, *167*, *168*, *174*, *175*, *181*, *185*, *189*, *196*, 204, **210**
origination **12**, **75**, *148*, **204**
out-of-band signaling 95
P
Packet Data *115*
Packet Data CCC Delivery *132*
Packet Data IAP 24, **30**

PN-4465-RV1

Packet Data Intercept Access Point 12
PacketEnvelope 34, 75, **81**, 204, **210**
packetEnvelope **75**, **204**
packetInformation
    PacketEnvelope 58, 60, **82**, **210**
packet-mode **12**, 13, 15, 30, 30, 31, 49, 50, 59, 77, 95, *114*, 206
    CCC *113*
PACS **12**
paging 31
parameter **74**
    encoding objectives 73
    extension 73
    identifier encoding 74
    in existing messages 98
partial dial 58
    scenario *145*
PartyIdentity **89**, **216**
    Answer 76, 205
    Answering 48, 52
    called 59, 65
    calling 59, 65
    Origination 59, 78, 81, 90, 207, 210, 218
    PacketEnvelope 82, 210, 211
    RedirectedFromInformation 90, 218
    Redirected-to 61
    Redirection 61, 83, 211
    TerminationAttempt 65, 85, 85, 213, 213
password 28
    call acceptance scenario *172*, *173*
    screening 48
path minimization scenario *177*
PCM **12**, 95
PCS **12**
PCS1900 **12**, 31
PDIAP **12**, *100*
PDU **12**
PDUType **90**, **217**
    CCOpen 50, 77, 206
    circuit-mode vs. packet-mode *114*
pen register **12**
permanent **15**
personal base station 21
personal identification number 28
personal mobility **12**, 60, 84, 212
PIN 28
Pivoted Delivery Function *137*

PN-4465-RV1

Plain Old Telephone Service *137*
Point-to-Point Protocol 12
port **89**, **216**
port identity
    PartyIdentity 89, 216
POTS **12**, *137*
PPP **12**, *110*
ppp **90**, **217**
pre-answer abandon scenario *146*
previous calls
    Change 51, 53, 54, 55, 58, 64, **77**, **206**
PRI **12**
Primary Rate Interface 12
primitive **74**
PRIVATE **74**, 74
private network 58
private number 89, 217
Procedures 73
Protocol Data Unit 12
protocol extension 74
PSTN **12**, *113*
Public Switched Telephone Network 12
pulse code modulation **12**, 95
Q
Q.931 90, *112*, 217
Q.932 90, *110*, *111*, 217
R
reasonably available **17**
recall **13**
    answer 48
    scenario 150, *174*
    trigger 64
receive 20
receive path 20, 88, 215
receiverAddress PartyIdentity **82**, **211**
redirected 64
RedirectedFromInformation **90**, **218**
    scenario *176*
    TerminationAttempt 65, 67, 68, 69, 85, 213
redirectedTo PartyIdentity
    Redirection 61, **83**, **211**
Redirecting System **12**, 30, *102*, *170*, *175*, *176*
    intercept access points *102*
Redirection 22, **60**, 75, 83, *164*, *165*, *169*, *170*, *172*, *173*, *176*, 204, 211
redirection **75**, **204**
    action 29

PN-4465-RV1

alerting *143*
await answer symbol *143*
connected symbol *143*
to party 88, 215
reference point a **46**
reference point b **46**
reference point c **47**
reference point d **47**, *106*
reference point e **47**, *105*, *107*, *108*
registration **13**
Release 22, **61**, 75, 83, *145*, *146*, *147*, *148*, *149*, *151*, *152*, *153*, *155*, *156*, *157*, *158*, *160*, *162*, *163*, *164*, *165*, *167*, *168*, *169*, *171*, *172*, *173*, *174*, *175*, *176*, *178*, *195*, 204, 212
ISUP *127*, *128*
release **75**, **204**
(action) 5, 8, 11, **13**, 15, 48, 61, 83, *116*, *120*, *122*, *123*, *125*, *127*, *128*, *129*, *131*, *132*, *134*, *136*, *137*, 212
to pivot scenario *175*
re-origination scenario *148*
restricted 90, 217
resulting calls
Change 51, 55, **77**, **206**
roaming **13**, 14
routing 58
S
screening service 89, 216
seizure *137*
senderAddress PartyIdentity **82**, **211**
sending PartyIdentity
PacketEnvelope **82**, **210**
separate logical channels 20
separated **20**, 20, 88, *107*, *115*, ***135***, 215
sepCCCpair **88**, **215**
sepRecvCCC **88**, **215**
sepXmitCCC **88**, **215**
SEQUENCE 76, 77, 78, 80, 81, 82, 83, 84, 85, 87, 88, 89, 90, 98, *198*, 205, 206, 207, 208, 209, 210, 211, 212, 213, 215, 216, 218
SEQUENCE OF 77, 89, 206, 216
sequenceNumber **87**, **215**
Serial Link Internet Protocol 13
service area 1, 13, 62
ServingSystem 84, 212
Service Profile Identifier 89, 216
Service Provider Administration Function 13, 19, **46**, 46, 47
Serving System 9, **13**, 21, 30, *101*, *104*, *170*, *175*
intercept access points *101*
Serving System Identification Intercept Access Point 13, 21

PN-4465-RV1

ServingSystem 62, 75, **84**, 204, **212**
servingSystem **75**, **204**
short message service **13**, 20, 30, 31, 60, 82, 211
    PacketEnvelope 82, 211
Signal
    Subject Audible Signal 58
simple incoming call scenario *149*
simple outgoing call scenario *147*
SLIP **13**, *110*
SMS *See also* short message service **13**
smsTeleserviceIdentifier **82**, **211**
SPAF **13**
special considerations 89, 217
speech bearer service 87, 95, *107*, *134*, 214
speed calling
    scenario *167*
speed number expansion 58
    scenario 167
speed number translation
    168
spid **89**, **216**
SSIAP **13**, 21, 22, *100*
static directory number *106*, *115*
    CCC Delivery *129*
station appearances 89, 216
subaddress **89**, **216**
subject **1**, **13**
subject's agent 89, 216
subject-initiated dialing and signaling information **13**
SubjectSignal message 63
    Signal 64
        DialedDigits 64
        FeatureKey 64
        SwitchhookFlash 64
surveillance **9**, **13**
SVC **13**
switched **15**
switchhook flash *138*
synchronization of CDC and CCC 35
syntax definitions 74
System Identity
    Redirection 61
System Serving *170*
systemIdentity
    CallIdentity **87**, **215**
    Redirection **83**, **211**

PN-4465-RV1

Release 62, **83**, **212**
ServingSystem 62, **84**, **212**
T
T1.607
High Layer Compatibility 90, 217
Low Layer Compatibility 90, 217
Subaddress 89, 216
tag **74**
TCP **13**, *110*, *111*, *113*
TCP/IP services 31
TDMA **13**, 31
tei **89**, **216**
telecommunication carrier 14
telecommunication service provider iii, xv, 1, **14**, 14
telecommunication support services **14**
Temporary Local Directory Number *170*
termAttempt **75**, **204**
Terminal Equipment Identity 89, 216
terminal mobility **14**, 60, 62, 84, 212
termination **6**, **14**, **16**
TerminationAttempt 22, **64**, 75, **85**, *149*, *151*, *152*, *153*, *155*, *156*, *157*, *160*, *161*, *163*, *164*, *165*, *166*, *169*, *170*, *172*, *173*, *174*, *176*, *182*, *186*, *190*, *193*, *194*, 204, **213**
three-way calling 27
scenario *159*
TIA/EIA-41 12, 31, 60, 82, *170*, 211
tiaEia41ShortMessageService
PacketEnvelope **82**, **211**
TimeStamp **91**, **218**
Answer 48, 52, 76, 205
CCClose 49, 76, 205
CCOpen 50, 77, 206
Change 51, 53, 54, 55, 58, 64, 77, 206
ConnectionTest *198*
Origination 59, 78, 79, 80, 81, 207, 208, 209, 210
PacketEnvelope 60, 81, 210
Redirection 61, 83, 211
Release 62, 83, 212
ServingSystem 62, 84, 212, 213
TerminationAttempt 65, 67, 68, 69, 70, 71, 72, 85, 213
timing information **14**, 16
transfer recall 13, 48, 64
transfer semantics 73
transfer syntax 73
TransitCarrierIdentity **91**, **218**
Origination 59, 81, 210
Redirection 61, 83, 211

PN-4465-RV1

translation 58
    input 81, 210
    scenario *167*
    single system scenario *168*
translationInput
    Origination **81**, *168*, **210**
transmission **14**
Transmission Control Protocol 13
transmission devices *108*
transmit path 20, 88, 215
transparent **14**
trap and trace device **14**
trunk group 89, *106*, *115*, 216
    CCC delivery *121*
trunk identity 88, 215
trunk number 89, 216
trunkId **89**, **216**
    PartyIdentity
        Answer *172*, *173*
        TerminationAttempt *174*
TSP 6, 10, 14, 14, **15**, 16, 84, 87, *137*, 212, 215
two-way
    communication 26
    paging 31
type **74**
U
unique identity
    CCC 21
UNIVERSAL **74**, 74
unobtrusively **15**, 22, 25
URL **15**
USC **15**
user interaction 28
user provided calling number 89, 216
userInput
    Origination **78**, **81**, *145*, *146*, *147*, *148*, *158*, *159*, *160*, *161*, *162*, *163*, *166*, *167*, *168*, *174*, *175*, *181*, *185*, *189*, *196*, **207**, **210**
userProvided **89**, **216**
user-to-user signaling **15**, 60
UTC **15**
V
V.32 *110*
value **74**
virtual circuit **15**
VisibleString 89, 216
    appearance identity

PN-4465-RV1

PartyIdentity 89, 216
calling card number
PartyIdentity 89, 216
CaseIdentity 87, 215
CCCIdentity 88, 215
combined CCC
CCCIdentity 88, 215
context
PartyIdentity 89, 217
directory number
PartyIdentity 89, 216
ESN
PartyIdentity 89, 216
generic address
PartyIdentity 89, 216
generic digits
PartyIdentity 89, 216
generic name
PartyIdentity 89, 216
IAPSystemIdentity 88, 215
IMEI
PartyIdentity 89, 216
IMSI
PartyIdentity 89, 216
individual CCC
CCCIdentity 88, 215
individual receive path
CCCIdentity 88, 215
indiviual transmit path
CCCIdentity 88, 215
IP address
PartyIdentity 89, 216
Location 88, 216
memo
ConnectionTest *198*
MIN
PartyIdentity 89, 216
NetworkAddress
ServingSystem 84, 212, 213
separated receive path
CCCIdentity 88, 215
separated transmit path
CCCIdentity 88, 215
sequenceNumber
CallIdentity 87, 215
SPID

PN-4465-RV1

PartyIdentity 89, 216
SystemIdentity
CallIdentity 87, 215
Redirection 83, 211
Release 83, 212
ServingSystem 84, 212
TEI
PartyIdentity 89, 216
TransitCarrierIdentity 91, 218
translationInput
Origination 81, 210
trunk identity
PartyIdentity 89, 216
user provided number
PartyIdentity 89, 216
userInput
Origination 81, 210
X.121 address
PartyIdentity 89, 216
voice bearer service *134*
voice mail 6, 48
W
WCDMA **15**
wire communications **15**
wireless **15**
wireless IP-based service 60
wireline **15**
X
X.208 **3**, 74, 95
X.209 **3**, 74, 95
X.25 90, *110*, *111*, *113*, 217
network address 88, 215
services 31
x121 **89**, **216**
x25 **90**, **217**

PN-4465-RV1