
**Information technology —
Telecommunications and information
exchange between systems — Private
Integrated Services Network —
Inter-exchange signalling protocol — Call
intrusion supplementary service**

*Technologies de l'information — Télécommunications et échange
d'information entre systèmes — Réseau privé à intégration de services —
Protocole de signalisation d'interéchange — Service supplémentaire
d'intrusion d'appel*



Contents

Foreword	iv
Introduction	v
1 Scope	1
2 Conformance	1
3 Normative references	1
4 Definitions	2
4.1 External definitions	2
4.2 Other definitions	3
5 List of acronyms	3
6 Signalling protocol for the support of SS-CI	4
6.1 SS-CI description	4
6.2 SS-CI operational requirements	4
6.2.1 Requirements on an Originating PINX	4
6.2.2 Requirements on a Terminating PINX	4
6.2.3 Requirements on a Transit PINX	4
6.2.4 Requirements on an Unwanted User PINX	4
6.3 SS-CI coding requirements	5
6.3.1 Operations	5
6.3.2 Notifications	8
6.3.3 Information elements	8
6.3.4 Messages	9
6.4 SS-CI state definitions	9
6.4.1 States at the Originating PINX	9
6.4.2 States at the Terminating PINX	10
6.5 SS-CI signalling procedures for activation, deactivation and registration	10
6.6 SS-CI signalling procedures for invocation and operation	10
6.6.1 Actions at the Originating PINX	10
6.6.2 Actions at the Terminating PINX	12
6.6.3 Actions at the Unwanted User PINX	16
6.6.4 Actions at a Transit PINX	16
6.7 SS-CI impact of interworking with public ISDNs	16
6.8 SS-CI impact of interworking with non-ISDNs	16
6.9 Protocol interactions between SS-CI and other supplementary services and ANFs	16

© ISO/IEC 1996

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

ISO/IEC Copyright Office * Case Postale 56 * CH-1211 Genève 20 * Switzerland
Printed in Switzerland

6.9.1	Interaction with Calling Name Identification Presentation (SS-CNIP)	16
6.9.2	Interaction with Connected Name Identification Presentation (SS-CONP)	17
6.9.3	Interaction with Call Completion to Busy Subscriber (SS-CCBS)	17
6.9.4	Interaction with Call Completion on No Reply (SS-CCNR)	17
6.9.5	Interaction with Call Transfer (SS-CT)	17
6.9.6	Interaction with Call Forwarding Unconditional (SS-CFU)	17
6.9.7	Interaction with Call Forwarding Busy (SS-CFB)	17
6.9.8	Interaction with Call Forwarding No Reply (SS-CFNR)	18
6.9.9	Interaction with Call Deflection (SS-CD)	18
6.9.10	Interaction with Path Replacement (ANF-PR)	18
6.9.11	Interaction with Call Offer (SS-CO)	19
6.9.12	Interaction with Do Not Disturb (SS-DND)	19
6.9.13	Interaction with Do Not Disturb Override (SS-DNDO)	19
6.10	SS-CI parameter values (timers)	19
6.10.1	Timer T1	19
6.10.2	Timer T2	20
6.10.3	Timer T3	20
6.10.4	Timer T4	20
6.10.5	Timer T5	20
6.10.6	Timer T6	20
Annex A	Signalling protocol for the support of Path Retention	21
Annex B	Protocol Implementation Conformance Statement (PICS) proforma	30
Annex C	Examples of message sequences	40
Annex D	Specification and Description Language (SDL) representation of procedures	48
Annex E	Imported ASN.1 definitions	61

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote.

International Standard ISO/IEC 14846 was prepared by ECMA (as Standard ECMA-203) and was adopted, under a special “fast-track procedure”, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

Annexes A and B form an integral part of this International Standard. Annexes C, D and E are for information only.

Introduction

This International Standard is one of a series of International Standards defining services and signalling protocols applicable to Private Integrated Services Networks (PISNs). The series uses ISDN concepts as developed by ITU-T and conforms to the framework of International Standards for Open Systems Interconnection as defined by ISO/IEC.

This particular International Standard specifies the signalling protocol for use at the Q reference point in support of the Call Intrusion (CI) supplementary service.

This page intentionally left blank

Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Inter-exchange signalling protocol - Call intrusion supplementary service

1 Scope

This International Standard specifies the signalling protocol for the support of the Call Intrusion supplementary service (SS-CI) at the Q reference point between Private Integrated Services Network Exchanges (PINXs) connected together within a Private Integrated Services Network (PISN).

SS-CI is a supplementary service which, on request from the calling user, enables the calling user to establish communication with a busy called user by breaking into an established call between the called user and a third user (unwanted user).

The Q reference point is defined in ISO/IEC 11579-1.

Service specifications are produced in three stages and according to the method specified in CCITT Recommendation I.130. This International Standard contains the stage 3 specification for the Q reference point and satisfies the requirements identified by the stage 1 and stage 2 specifications in ISO/IEC 14845.

The signalling protocol for SS-CI operates on top of the signalling protocol for basic circuit switched call control, as specified in ISO/IEC 11572, and uses certain aspects of the generic procedures for the control of supplementary services specified in ISO/IEC 11582.

This International Standard also specifies additional signalling protocol requirements for the support of interactions at the Q reference point between SS-CI and other supplementary services and ANFs.

Note 1 - Additional interactions that have no impact on the signalling protocol at the Q reference point can be found in the relevant stage 1 specifications.

This International Standard is applicable to PINXs which can interconnect to form a PISN.

2 Conformance

In order to conform to this International Standard, a PINX shall satisfy the requirements identified in the Protocol Implementation Conformance Statement (PICS) proforma in annex B.

3 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 11572:1996,	<i>Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Circuit-mode bearer services - Inter-exchange signalling procedures and protocol.</i>
ISO/IEC 11574:1994,	<i>Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Circuit-mode 64 kbit/s bearer services - Service description, functional capabilities and information flows.</i>
ISO/IEC 11579-1:1994,	<i>Information technology - Telecommunications and information exchange between systems - Private integrated services network - Part 1: Reference configuration for PISN Exchanges (PINX).</i>
ISO/IEC 11582:1995,	<i>Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Generic functional protocol for the support of supplementary services - Inter-exchange signalling procedures and protocol.</i>
ISO/IEC 13869:1995,	<i>Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Inter-exchange signalling protocol - Call transfer supplementary service.</i>

ISO/IEC 13873:1995,	<i>Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Inter-exchange signalling protocol - Call diversion supplementary services.</i>
ISO/IEC 13874:1995,	<i>Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Inter-exchange signalling protocol - Path replacement additional network feature.</i>
ISO/IEC 14843:1996,	<i>Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Inter-exchange signalling protocol - Call offer supplementary service</i>
ISO/IEC 14844:1996,	<i>Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Inter-exchange signalling protocol - Do not disturb and do not disturb override supplementary services</i>
ISO/IEC 14845:1996,	<i>Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Specification, functional model and information flows - Call intrusion supplementary service</i>
CCITT Rec. I.112:1988,	<i>Vocabulary of terms for ISDNs (Blue Book).</i>
CCITT Rec. I.210:1988,	<i>Principles of telecommunication services supported by an ISDN and the means to describe them (Blue Book).</i>
CCITT Rec. Z.100:1988,	<i>Specification and Description Language (Blue Book).</i>
CCITT Rec. Q.950:1994	<i>Digital Subscriber Signalling System No. 1 (DSS1) supplementary services protocols; Structure and general principles.</i>

4 Definitions

For the purposes of this International Standard, the following definitions apply.

4.1 External definitions

This International Standard uses the following terms defined in other documents:

– Application Protocol Data Unit (APDU)	(ISO/IEC 11582)
– Basic Service	(CCITT Rec. I.210)
– Call, Basic Call	(ISO/IEC 11582)
– Coordination Function	(ISO/IEC 11582)
– Connection	(ISO/IEC 13863)
– Cooperating PINX	(ISO/IEC 13874)
– Established call	(ISO/IEC 14845)
– Forced release	(ISO/IEC 14845)
– Incoming Gateway PINX	(ISO/IEC 11572)
– Inter-PINX link	(ISO/IEC 11572)
– Interpretation APDU	(ISO/IEC 11582)
– Intruding call	(ISO/IEC 14845)
– Network Facility Extension (NFE)	(ISO/IEC 11582)
– Notification	(ISO/IEC 11582)
– Originating PINX	(ISO/IEC 11572)
– Outgoing Gateway PINX	(ISO/IEC 11572)

– Private Integrated Services Network (PISN)	(ISO/IEC 11579-1)
– Private Integrated Services Network Exchange (PINX)	(ISO/IEC 11579-1)
– Rerouteing PINX	(ISO/IEC 11573)
– Served user	(ISO/IEC 14845)
– Signalling	(CCITT Rec. I.112)
– Supplementary Service	(CCITT Rec. I.210)
– Supplementary Services Control Entity	(ISO/IEC 11582)
– Terminating PINX	(ISO/IEC 11572)
– Transit PINX	(ISO/IEC 11572)
– User	(ISO/IEC 11574)

4.2 Other definitions

busy : A property of a user for whom either a Network Determined User Busy or User Determined User Busy condition exists.

conference type connection : A connection between the served user, the wanted user and the unwanted user, where all users have user information connection with each other.

impending intrusion warning notification : A notification provided before communication is established between the served user and the wanted user.

isolation : The breaking of the user information connection to and from the unwanted user during intrusion.

path retention : The retaining of the network connection between the Originating PINX and the Terminating PINX so that a supplementary service (such as SS-CI) can be invoked without establishing a new connection.

Served User PINX : The PINX serving the served user.

wanted user : The called user in the intruding call.

Note 2 - This user is known as user B in ISO/IEC 14845.

unwanted user : The user other than the wanted user in the established call.

Note 3 - This user is known as user C in ISO/IEC 14845.

Unwanted User PINX : The PINX of the unwanted user.

wait on busy : A condition in which the intruding call is disconnected from the wanted user and is waiting for the wanted user to become not busy.

5 List of acronyms

ANF	Additional Network Feature
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation no. 1
CICL	Call Intrusion Capability Level
CIPL	Call Intrusion Protection Level
ISDN	Integrated Services Digital Network
NFE	Network Facility Extension
PICS	Protocol Implementation Conformance Statement
PINX	Private Integrated Services Network Exchange
PISN	Private Integrated Services Network

SDL	Specification and Description Language
SS-CI	Call Intrusion supplementary service
WOB	Wait On Busy

6 Signalling protocol for the support of SS-CI

6.1 SS-CI description

SS-CI is a supplementary service which, on request from the calling user, enables the calling user to establish communication with a busy called user breaking into an established call between the called user and a third user (unwanted user).

SS-CI is applicable to all circuit mode basic services defined in ISO/IEC 11572.

6.2 SS-CI operational requirements

6.2.1 Requirements on an Originating PINX

Call establishment procedures for the outgoing side of an inter-PINX link and call release procedures, as specified in ISO/IEC 11572, shall apply.

Generic procedures for the call-related control of supplementary services, as specified in ISO/IEC 11582 for an End PINX, shall apply. In addition, the generic procedures for notification, as specified in ISO/IEC 11582 for an End PINX, shall apply.

6.2.2 Requirements on a Terminating PINX

Call establishment procedures for the incoming side of an inter-PINX link and call release procedures, as specified in ISO/IEC 11572, shall apply.

Generic procedures for the call-related control of supplementary services, as specified in ISO/IEC 11582 for an End PINX, shall apply. In addition, the generic procedures for notification, as specified in ISO/IEC 11582 for an End PINX, shall apply.

6.2.3 Requirements on a Transit PINX

Basic call procedures, as specified in ISO/IEC 11572 for a Transit PINX, shall apply.

Generic procedures for the call-related control of supplementary services, as specified in ISO/IEC 11582 for a Transit PINX, shall apply. In addition, the generic procedures for notification, as specified in ISO/IEC 11582 for a Transit PINX, shall apply.

For SS-CI the requirements are limited to the passing on of Facility information elements for which the destination, as indicated in the NFE, is not the Transit PINX.

6.2.4 Requirements on an Unwanted User PINX

Generic procedures for the call-related control of supplementary services, as specified in ISO/IEC 11582 for an End PINX, shall apply. In addition, the generic procedures for notification, as specified in ISO/IEC 11582 for an End PINX, shall apply.

6.3 SS-CI coding requirements

6.3.1 Operations

The operations defined in Abstract Syntax Notation number 1 (ASN.1) in table 1 shall apply.

Table 1 - Operations in support of SS-CI

Call-Intrusion-Operations		{iso(1) standard(0) pss1-call-intrusion(14846) call-intrusion-operations(0) }	
DEFINITIONS EXPLICIT TAGS		::=	
BEGIN			
IMPORTS		OPERATION, ERROR FROM Remote-Operation-Notation {joint-iso-ccitt(2) remote-operations(4) notation (0)} Extension FROM Manufacturer-specific-service-extension-definition {iso(1) standard(0) pss1-generic-procedures(11582) msi-definition(0)} notAvailable, supplementaryServiceInteractionNotAllowed FROM General-Error-List {ccitt recommendation q 950 general-error-list (1)};	
PathRetain	::=	OPERATION ARGUMENT PathRetainArg -- this operation may be used by other supplementary services -- using other values of argument	
ServiceAvailable	::=	OPERATION ARGUMENT ServiceAvailableArg -- this operation may be used by other supplementary services -- using other values of argument	
CallIntrusionRequest	::=	OPERATION ARGUMENT CRequestArg RESULT CRequestRes ERRORS {notAvailable, notBusy, temporarilyUnavailable, notAuthorized, unspecified, supplementaryServiceInteractionNotAllowed}	
CallIntrusionGetCIPL	::=	OPERATION ARGUMENT DummyArg RESULT CIGetCIPLRes	
CallIntrusionForcedRelease	::=	OPERATION ARGUMENT DummyArg RESULT DummyResult ERRORS {notAvailable, unspecified, supplementaryServiceInteractionNotAllowed}	
CallIntrusionIsolate	::=	OPERATION ARGUMENT DummyArg RESULT DummyResult ERRORS {notAvailable, unspecified, supplementaryServiceInteractionNotAllowed}	

Table 1 - Operations in support of SS-CI (continued)

CallIntrusionWORequest	::=	OPERATION	ARGUMENT	DummyArg
			RESULT	DummyResult
			ERRORS	{notAvailable, unspecified, supplementaryServiceInteractionNotAllowed}
CallIntrusionCompleted	::=	OPERATION	ARGUMENT	DummyArg
PathRetainArg	::=	CHOICE	{serviceList ServiceList, extendedServiceList SEQUENCE{ serviceList ServiceList, extension Extension } }	
ServiceAvailableArg	::=	CHOICE	{ serviceList ServiceList, extendedServiceList SEQUENCE{ serviceList ServiceList, extension Extension } }	
ServiceList	::=	BIT STRING	{ci-low(4), ci-medium(5), ci-high(6)} (SIZE(1..32)) -- bits other than ci-low, ci-medium, ci-high are reserved -- for other supplementary services	
DummyArg	::=	CHOICE{	null	NULL, extension [1] IMPLICIT Extension, sequenceOfExtn [2] IMPLICIT SEQUENCE OF Extension}
DummyRes	::=	CHOICE{	null	NULL, extension [1] IMPLICIT Extension, sequenceOfExtn [2] IMPLICIT SEQUENCE OF Extension}
CIRequestArg	::=	SEQUENCE{	ciCapabilityLevel CIPCapabilityLevel, argumentExtension CHOICE{ extension [1] IMPLICIT Extension, sequenceOfExtn [2] IMPLICIT SEQUENCE OF Extension} OPTIONAL}	
CIRequestRes	::=	SEQUENCE{	ciUnwantedUserStatus CIUnwantedUserStatus, resultExtension CHOICE{ extension [1] IMPLICIT Extension, sequenceOfExtn [2] IMPLICIT SEQUENCE OF Extension} OPTIONAL}	
CIGetCIPLRes	::=	SEQUENCE{	ciProtectionLevel CIPProtectionLevel, resultExtension CHOICE{ extension [1] IMPLICIT Extension, sequenceOfExtn [2] IMPLICIT SEQUENCE OF Extension} OPTIONAL}	

Table 1 - Operations in support of SS-CI (concluded)

CICapabilityLevel	::= ENUMERATED{ intrusionLowProt(1), intrusionMediumProt(2), intrusionHighProt(3)}		
CIProtectionLevel	::= ENUMERATED{ lowProtection(0), mediumProtection(1), highProtection(2), fullProtection(3)}		
CIUnwantedUserStatus	::= ENUMERATED{ unwantedUserIntruded(0), unwantedUserIsolated(1)}		
CfbOverride	::= OPERATION ARGUMENT DummyArg -- used in the interaction with Call Forwarding Busy		
pathRetain PathRetain			::= 41
serviceAvailable	ServiceAvailable		::= 42
callIntrusionRequest	CallIntrusionRequest		::= 43
callIntrusionGetCIPL	CallIntrusionGetCIPL		::= 44
callIntrusionIsolate	CallIntrusionIsolate		::= 45
callIntrusionForcedRelease	CallIntrusionForcedRelease		::= 46
callIntrusionWOBRequest	CallIntrusionWOBRequest		::= 47
callIntrusionCompleted	CallIntrusionCompleted		::= 48
cfbOverride	CfbOverride		::= 49
notBusy	ERROR	::= 1009	
	-- used when an SS-CI request is received in -- a Terminating PINX and the called user is not busy		
temporarilyUnavailable	ERROR	::= 1000	
	-- used when conditions for invocation of SS-CI -- are momentarily not met		
notAuthorized	ERROR	::= 1007	
	--used when a SS-CI request is rejected --because of insufficient CIDL		
Unspecified	::= ERROR PARAMETER Extension		
unspecified	Unspecified	::= 1008	
END	-- of Call-Intrusion-Operations		

6.3.2 Notifications

The following notification, defined in Abstract Syntax Notation number 1 (ASN.1) in table 2 shall apply.

Table 2 - Notifications in support of SS-CI

Call-Intrusion-Notifications			{iso(1) standard(0) pss1-call-intrusion(14846) call-intrusion-notifications(1)}		
DEFINITIONS EXPLICIT TAGS ::=					
BEGIN					
IMPORTS			NOTIFICATION FROM Notification-Data-Structure {iso(1) standard(0) pss1-generic-procedures(11582) notification-data-structure(7)};		
RemoteUserAlerting	::=	NOTIFICATION ARGUMENT NULL			
IntrusionIsImpending	::=	NOTIFICATION ARGUMENT NULL			
IntrusionIsEffective	::=	NOTIFICATION ARGUMENT NULL			
IsolationThroughIntrusion	::=	NOTIFICATION ARGUMENT NULL			
ForcedReleaseAfterIntrusion	::=	NOTIFICATION ARGUMENT NULL			
EndOfIntrusion	::=	NOTIFICATION ARGUMENT NULL			
remoteUserAlerting		RemoteUserAlerting	::=	2000	
intrusionIsImpending		IntrusionIsImpending	::=	2003	
intrusionIsEffective		IntrusionIsEffective	::=	2004	
isolationThroughIntrusion		IsolationThroughIntrusion	::=	2005	
forcedReleaseAfterIntrusion		ForcedReleaseAfterIntrusion	::=	2006	
endOfIntrusion		EndOfIntrusion	::=	2007	
END			--of Call-Intrusion-Notifications		

6.3.3 Information elements

6.3.3.1 Facility information element

The operations defined above shall be coded in the Facility information element in accordance with ISO/IEC 11582.

When conveying an APDU of operations callIntrusionRequest, callIntrusionGetCIPL, callIntrusionForcedRelease, callIntrusionIsolate, callIntrusionWOBRrequest, callIntrusionCompleted, the NFE shall be included.

When conveying an invoke APDU of operations callIntrusionRequest, callIntrusionGetCIPL, callIntrusionForcedRelease, callIntrusionIsolate, callIntrusionWOBRrequest, callIntrusionCompleted, the destinationEntity data element of the NFE shall contain value endPTNX.

When conveying the invoke APDU of operation `callIntrusionCompleted`, the Interpretation APDU shall be included and have the value `discardAnyUnrecognisedInvokePdu`.

When conveying the invoke APDUs of operations `callIntrusionRequest`, `callIntrusionGetCIPL`, `callIntrusionForcedRelease`, `callIntrusionIsolate` and `callIntrusionWOBRequest`, the Interpretation APDU shall be omitted.

Note 4 - Additional requirements for the conveyance of APDUs of operations `pathRetain` and `serviceAvailable` are given in A.3.2 of annex A.

6.3.3.2 Notification indicator information element

The notification defined above shall be coded in the Notification indicator information element in accordance with ISO/IEC 11582.

6.3.3.3 Other information elements

Any other information elements (e.g. Progress indicator) shall be coded in accordance with the rules of ISO/IEC 11572.

6.3.4 Messages

Messages used for call establishment and release shall be as specified in ISO/IEC 11572.

The Facility information element and the Notification indicator information element shall be conveyed in the messages as specified in ISO/IEC 11582.

6.4 SS-CI state definitions

6.4.1 States at the Originating PINX

The procedures for the Originating PTNX are written in terms of the following conceptual states existing within the SS-CI Supplementary Service Control entity in that PTNX in association with a particular call.

6.4.1.1 State CI-Idle

SS-CI is not operating.

6.4.1.2 State CI-Wait-Ack

The Originating PINX has requested SS-CI and is waiting for an acknowledgement from the Terminating PINX.

6.4.1.3 State CI-Orig-Invoked

SS-CI has been invoked successfully and the unwanted user has not been isolated.

6.4.1.4 State CI-inForcedRelease-Request

Following intrusion, the Originating PINX has requested the forced release of the unwanted user and is waiting for an acknowledgement from the Terminating PINX.

6.4.1.5 State CI-Isolation-Request

Following intrusion, the Originating PINX has requested the isolation of the unwanted user and is waiting for an acknowledgement from the Terminating PINX.

6.4.1.6 State CI-inWOB-Request

Following intrusion, the Originating PINX has requested WOB.

6.4.1.7 State CI-Orig-Isolated

SS-CI has been invoked successfully and the unwanted user has been isolated.

6.4.1.8 State CI-isForcedRelease-Request

Following isolation, the Originating PINX has requested the forced release of the unwanted user and is waiting for an acknowledgement from the Terminating PINX.

6.4.1.9 State CI-isWOB-Request

Following isolation, the Originating PINX has requested WOB.

6.4.1.10 State CI-Orig-WOB

Wait on busy is in progress.

6.4.1.11 State CI-Wait-Ack-WOB

While wait on busy is in progress, the Originating PINX has requested intrusion again and is waiting for an acknowledgement from the Terminating PINX.

6.4.2 States at the Terminating PINX

The procedures for the Terminating PINX are written in terms of the following conceptual states existing within the SS-CI Supplementary Service Control functional entity in that PINX in association with a particular call.

6.4.2.1 State CI-Idle

SS-CI is not operating.

6.4.2.2 State CI-GetCIPL-I

The Terminating PINX has requested the CIPL of the unwanted user after intrusion has been requested and is waiting for the result.

6.4.2.3 State CI-Dest-Notify

Following invocation of intrusion, the Terminating PINX has notified an impending intrusion to the unwanted user and is waiting the end of the impending phase before starting intrusion.

6.4.2.4 State CI-Dest-Invoked

SS-CI has been invoked successfully and the unwanted user has not been isolated.

6.4.2.5 State CI-Dest-Isolated

SS-CI has been invoked successfully and the unwanted user has been isolated.

6.4.2.6 State CI-Dest-WOB

Wait on busy is in progress.

6.4.2.7 State CI-GetCIPL-WOB

The Terminating PINX has requested the CIPL of the unwanted user after intrusion has been requested again during wait on busy and is waiting for the result.

6.4.2.8 State CI-Dest-Notify-WOB

Following invocation of intrusion during wait on busy, the Terminating PINX has notified an impending intrusion to the unwanted user and is waiting for the end of the impending phase before starting intrusion.

6.5 SS-CI signalling procedures for activation, deactivation and registration

Not applicable.

6.6 SS-CI signalling procedures for invocation and operation

The following procedures are call-associated.

SS-CI may be invoked in two ways depending on whether the network connection is retained when a call encounters a busy called user. Retention of the network connection makes use of a generic path retention mechanism, which is specified in annex A.

Some examples of message sequences are shown in annex C.

6.6.1 Actions at the Originating PINX

For a given call, the Originating PINX may choose one of the two following methods for invocation of SS-CI:

- invocation without path retention;
- invocation with path retention.

For invocation with path retention, the procedures specified below apply in conjunction with the procedures specified in A.5.1 of annex A.

For each method, if the basic call clears in circumstances other than those covered below, SS-CI shall terminate, any SS-CI timer shall be stopped, and state CI-Idle shall be entered (e.g. on calling user release, call failure, etc.).

The SDL representation of procedures at the Originating PINX is shown in D.1 of annex D.

6.6.1.1 Procedure for invocation of SS-CI

6.6.1.1.1 Normal procedure

To invoke SS-CI, the Originating PINX shall send a callIntrusionRequest invoke APDU, start timer T1 and enter state CI-Wait-Ack. For invocation without path retention, the APDU shall be sent in the SETUP message that establishes the call. For invocation with path retention, the APDU shall be sent in a FACILITY message using the call reference of a call for which the network connection has been retained in accordance with A.5.1 of annex A (path retention state PRTO-Retained) and for which the received serviceAvailable invoke APDU indicated that SS-CI is invokable. The argument shall convey the CICL of the calling user.

In state CI-Wait-Ack, on receipt of a CONNECT message including a callIntrusionRequest return result APDU with a result indicating intrusion on the unwanted user (value "unwantedUserIntruded"), the Originating PINX may confirm invocation of SS-CI to the calling user, shall stop timer T1 and shall enter state CI-Orig-Invoked.

In state CI-Wait-Ack, on receipt of a CONNECT message including a callIntrusionRequest return result APDU with a result indicating isolation of the unwanted user (value "unwantedUserIsolated"), the Originating PINX may confirm invocation of SS-CI to the calling user, shall stop timer T1 and shall enter state CI-Orig-Isolated.

6.6.1.1.2 Exceptional procedure

In state CI-Wait-Ack, on receipt of:

- any message containing a callIntrusionRequest return error or reject APDU, or
- an ALERTING, CONNECT or DISCONNECT message without a callOfferRequest return result, return error or reject APDU,

the Originating PINX shall stop timer T1 and enter state CI-Idle. Failure of SS-CI may be indicated to the calling user and the call shall continue in accordance with ISO/IEC 11572.

On expiry of timer T1, the Originating PINX shall enter state CI-Idle. Failure of SS-CI may be indicated to the calling user and the call shall continue in accordance with ISO/IEC 11572.

6.6.1.2 Optional procedure for invocation of isolation

6.6.1.2.1 Normal procedure

In state CI-Orig-Invoked, if isolation of the unwanted user is requested, the Originating PINX shall send a callIntrusionIsolate invoke APDU in a FACILITY message, start timer T2 and enter the state CI-Isolation-Request.

In state CI-Isolation-Request, on receipt of a callIntrusionIsolate return result APDU in a FACILITY message, the Originating PINX may indicate the result of the isolation request to the calling user, shall stop timer T2 and shall enter the CI-Orig-Isolated state.

6.6.1.2.2 Exceptional procedure

In state CI-Isolation-Request, on receipt of a FACILITY message containing a callIntrusionIsolationRequest return error or reject APDU, the Originating PINX may indicate failure of the isolation request to the calling user, shall stop timer T2 and return to state CI-Orig-Invoked; upon expiry of timer T2, the Originating PINX may indicate the rejection of the isolation request to the calling user and shall return to state CI-Orig-Invoked.

6.6.1.3 Optional procedure for invocation of forced release

6.6.1.3.1 Normal procedure

In state CI-Orig-Invoked or state CI-Orig-Isolated, if forced release of the unwanted user is requested, the Originating PINX shall send a callIntrusionForcedRelease invoke APDU in a FACILITY message, start timer T3 and enter respectively state CI-inForcedRelease-Request or state CI-isForcedRelease-Request.

In state CI-inForcedRelease-Request or state CI-isForcedRelease-Request, on receipt of a callIntrusionForcedRelease return result APDU in a FACILITY message, the Originating PINX may indicate the result of the forced release request to the calling user, shall stop timer T3 and shall enter the state CI-Idle.

6.6.1.3.2 Exceptional procedure

In state CI-inForcedRelease-Request or state CI-isForcedRelease-Request, on receipt of a FACILITY message containing a callIntrusionForcedRelease return error or reject APDU, the Originating PINX may indicate failure of the forced release request to the calling user, shall stop timer T3 and return to previous state CI-Orig-Invoked or state CI-Orig-Isolated; upon

expiry of timer T3, the Originating PINX may indicate the rejection of the forced release request to the calling user and shall return to previous state CI-Orig-Invoked or state CI-Orig-Isolated.

6.6.1.4 Optional procedure for invocation of wait on busy

6.6.1.4.1 Normal procedure

In state CI-Orig-Invoked or state CI-Orig-Isolated, if wait on busy is requested, the Originating PINX shall send a callIntrusionWOBRequest invoke APDU in a FACILITY message, start timer T4 and enter respectively state CI-inWOB-Request or state CI-isWOB-Request.

In state CI-inWOB-Request or state CI-isWOB-Request, on receipt of a callIntrusionWOBRequest return result APDU in a FACILITY message, the Originating PINX may indicate the result of the wait on busy request to the calling user, shall stop timer T4 and shall enter the state CI-Orig-WOB.

6.6.1.4.2 Exceptional procedure

In state CI-inWOB-Request or state CI-isWOB-Request, on receipt of a FACILITY message containing a callIntrusionWOBRequest return error or reject APDU, the Originating PINX may indicate failure of the wait on busy request to the calling user, shall stop timer T4 and return to previous state CI-Orig-Invoked or state CI-Orig-Isolated; upon expiry of timer T4, the Originating PINX may indicate the rejection of the WOB request to the calling user and shall return to previous state CI-Orig-Invoked or state CI-Orig-Isolated.

6.6.1.5 Procedure for reinvocation of intrusion during wait on busy

6.6.1.5.1 Normal procedure

In state CI-Orig-WOB, if call intrusion is requested again, the Originating PINX shall send a callIntrusionRequest invoke APDU in a FACILITY message. The Originating PINX shall start timer T1 and enter state CI-Wait-Ack-WOB.

In state CI-Wait-Ack-WOB, on receipt of a FACILITY message including a callIntrusionRequest return result APDU with a result indicating intrusion on the unwanted user (unwantedUserIntruded), the Originating PINX may confirm invocation of SS-CI to the calling user, shall stop timer T1 and shall enter state CI-Orig-Invoked.

In state CI-Wait-Ack-WOB, on receipt of a FACILITY message including a callIntrusionRequest return result APDU with a result indicating isolation of the unwanted user (unwantedUserIsolated), the Originating PINX may confirm invocation of SS-CI to the calling user, shall stop timer T1 and shall enter state CI-Orig-Isolated.

6.6.1.5.2 Exceptional procedure

In state CI-Wait-Ack-WOB, on receipt of a FACILITY message containing a callIntrusionRequest return error or reject APDU, the Originating PINX may indicate the failure of SS-CI to the calling user, shall stop timer T1 and return to state CI-Orig-WOB.

On expiry of timer T1, the Originating PINX shall enter state CI-Orig-WOB. Failure of SS-CI may be indicated to the calling user.

6.6.1.6 Procedure for completion of SS-CI

6.6.1.6.1 Normal procedure

In any state except CI-Idle and CI-Wait-Ack, on receipt of a callIntrusionCompleted invoke APDU in a FACILITY message, the Originating PINX may indicate completion of SS-CI to the calling user, shall stop any SS-CI timer and shall enter state CI-Idle.

6.6.1.6.2 Exceptional procedure

None.

6.6.2 Actions at the Terminating PINX

The Terminating PINX shall support the two methods of invocation.

For invocation with path retention, the procedures specified below apply in conjunction with the procedures specified in A.5.2 of annex A.

For each method, if the basic call clears in circumstances other than those covered below, SS-CI shall terminate, any SS-CI timer shall be stopped, and state CI-Idle shall be entered.

The SDL representation of procedures at the Terminating PINX is shown in D.2 of annex D.

6.6.2.1 Procedure for invocation of SS-CI

6.6.2.1.1 Normal procedure

If, while processing an incoming SETUP message in accordance with the procedures of ISO/IEC 11572, the called user is found to be busy, and if the SETUP message contained a callIntrusionRequest invoke APDU, the Terminating PINX shall not send a DISCONNECT message but shall check whether SS-CI is possible.

If, having retained a network connection in accordance with A.5.2 of annex A and having indicated in the serviceAvailable invoke APDU that SS-CI is invocable, a FACILITY message is received containing a callIntrusionRequest invoke APDU, the Terminating PINX shall check again whether the called user is busy and if so shall check whether SS-CI is still possible.

To check whether SS-CI is possible, the Terminating PINX shall check that the called user is involved in a compatible established call in basic call state Active, that the CIPL of the called user is lower than the received CICL of the calling user, and that there are no other reasons for denying intrusion (e.g. if the established call is already being intruded on). If as far as the Terminating PINX is concerned, SS-CI is possible, the Terminating PINX shall send a callIntrusionGetCIPL invoke APDU in a FACILITY message to the Unwanted User PINX, start timer T5 and enter the state CI-GetCIPL-I.

Note 5 - The method by which the Terminating PINX checks whether an established call is compatible with the intruding call is outside the scope of this International Standard.

In state CI-GetCIPL-I, on receipt of callIntrusionGetCIPL return result APDU in a FACILITY message, the Terminating PINX shall stop timer T5 and check that the CIPL of the unwanted user is lower than the CICL of the calling user.

If all conditions are met, the Terminating PINX may provide a notification of impending intrusion to users in the established call. If notification of impending intrusion is not to be given, execution of intrusion shall take place immediately. If notification of impending intrusion is to be given, the Terminating PINX shall send on the call reference of the established call a NOTIFY message containing notification value "intrusionIsImpending", may send on the call reference of the intruding call a NOTIFY message containing notification value "intrusionIsImpending", shall start timer T6 and shall enter state CI-Dest-Notify. Execution of intrusion shall commence on expiry of timer T6 in state CI-Dest-Notify.

Execution of intrusion shall result either in a conference type connection involving all three users (the calling user, the called user and the unwanted user) or in isolation of the unwanted user (disconnection of the unwanted user and connection of the calling user and the called user).

If a conference type connection is established, the Terminating PINX shall send using the call reference of the intruding call a CONNECT message containing a callIntrusionRequest return result APDU containing value "unwantedUserIntruded". The Terminating PINX shall also send a NOTIFY message containing notification value "intrusionIsEffective" using the call reference of the established call. The Terminating PINX shall enter state CI-Dest-Invoked.

If the unwanted user is isolated, the Terminating PINX shall send using the call reference of the intruding call a CONNECT message containing a callIntrusionRequest return result APDU containing value "unwantedUserIsolated". The Terminating PINX shall also send a NOTIFY message containing notification value "isolationThroughIntrusion" using the call reference of the established call. The Terminating PINX shall enter state CI-Dest-Isolated.

6.6.2.1.2 Exceptional procedure

On receipt of a SETUP or FACILITY message containing a callIntrusionRequest invoke APDU, if the called user is not busy the call shall continue in accordance with ISO/IEC 11572. The Terminating PINX shall return a callIntrusionRequest return error APDU containing error notBusy in the resulting ALERTING or CONNECT message and shall remain in state CI-Idle.

On receipt of a SETUP or FACILITY message containing a callIntrusionRequest invoke APDU, if the called user is busy but invocation of SS-CI is not possible (including the case where the received callIntrusionGetCIPL return result APDU indicates a CIPL that is too high) the intruding call shall be released in accordance with ISO/IEC 11572 or, if continued retention of the path is required, shall continue in accordance with A.5.2 of annex A. The Terminating PINX shall contain a callIntrusionRequest return error APDU containing an error other than notBusy in the resulting DISCONNECT or FACILITY message and shall remain in or enter state CI-Idle.

In the state CI-GetCIPL-I, on receipt of a callIntrusionGetCIPL reject APDU containing problem code "unrecognizedOperation" in a FACILITY message from the Unwanted User PINX, the Terminating PINX shall stop timer T5, and shall apply the procedures described in 6.6.2.1.1 for receipt of a return result APDU with the lowest value of CIPL.

On expiry of timer T5 or on receipt of a callIntrusionGetCIPL reject APDU containing a problem code other than "unrecognizedOperation", the Terminating PINX shall apply the procedures specified when the called user is busy and invocation of SS-CI is not possible. The error value used shall be "temporarilyUnavailable".

If, during state CI-Dest-Notify or state CI-GetCIPL-I, the called user becomes not busy and presentation of the intruding call becomes possible, a callIntrusionRequest return error APDU containing error notBusy shall be sent in the resulting ALERTING or CONNECT message, timer T6 or T5 shall be stopped and state CI-Idle shall be entered.

If, during state CI-Dest-Notify or state CI-GetCIPL-I, the established call is released but the called user remains busy, a callIntrusionRequest return error APDU containing error temporarilyUnavailable shall be sent in the resulting DISCONNECT message, timer T6 or T5 shall be stopped and state CI-Idle shall be entered.

6.6.2.2 Optional procedures for invocation of isolation

6.6.2.2.1 Normal procedure

In state CI-Dest-Invoked, on receipt of a callIntrusionIsolate invoke APDU in a FACILITY message from the Originating PINX, the Terminating PINX shall disconnect the unwanted user from the conference type connection and leave the calling and called users connected together. The Terminating PINX shall also send a callIntrusionIsolate return result to the Originating PINX, shall send to the Unwanted User PINX the notification description value "isolationThroughIntrusion" in a NOTIFY message and enter the state CI-Dest-Isolated.

6.6.2.2.2 Exceptional procedure

In the state CI-Dest-Invoked, on receipt of a callIntrusionIsolate invoke APDU in a FACILITY message from the Originating PINX, if isolation is not possible, the Terminating PINX shall send a callIntrusionIsolate return error APDU in a FACILITY message to the Originating PINX and remain in the state CI-Dest-Invoked.

6.6.2.3 Optional procedures for invocation of forced release

6.6.2.3.1 Normal procedure

In state CI-Dest-Invoked or CI-Dest-Isolated, on receipt of a callIntrusionForcedRelease invoke APDU in a FACILITY message from the Originating PINX, the Terminating PINX shall initiate release of the established call in accordance with the procedures of ISO/IEC 11572. From state CI-Dest-Invoked, the Terminating PINX shall disconnect the unwanted user from the conference type connection and leave the calling and called users connected together. The Terminating PINX shall also send a callIntrusionForcedRelease return result APDU to the Originating PINX, shall send to the Unwanted User PINX the notification description value "forcedReleaseAfterIntrusion" in the DISCONNECT message and enter the state CI-Idle.

6.6.2.3.2 Exceptional procedure

In the state CI-Dest-Invoked or CI-Dest-Isolated, on receipt of a callIntrusionForcedRelease invoke APDU in a FACILITY message from the Originating PINX, if forced release is not possible, the Terminating PINX shall send a callIntrusionForcedRelease return error APDU in a FACILITY message to the Originating PINX and remain in existing state CI-Dest-Invoked or CI-Dest-Isolated.

6.6.2.4 Optional procedures for invocation of wait on busy

6.6.2.4.1 Normal procedure

In state CI-Dest-Invoked or CI-Dest-Isolated, upon receipt of a callIntrusionWOBRequest invoke APDU in a FACILITY message from the Originating PINX, if WOB is possible the Terminating PINX shall disconnect the calling user from the conference type connection or from the called user, and shall reconnect the unwanted user to the called user. The Terminating PINX shall also send a callIntrusionWOBRequest return result APDU to the Originating PINX, shall send to the Unwanted User PINX the notification description value "endOfIntrusion" in a NOTIFY message and enter the state CI-Dest-WOB. The established call shall no longer be associated with the waiting intruding call and shall continue as if SS-CI had not occurred.

6.6.2.4.2 Exceptional procedure

In the state CI-Dest-Invoked or CI-Dest-Isolated, on receipt of a callIntrusionWOBRequest invoke APDU in a FACILITY message from the Originating PINX, if wait on busy is not possible, the Terminating PINX shall send a callIntrusionWOBRequest return error APDU in a FACILITY message to the Originating PINX and remain in respective states CI-Dest-Invoked or CI-Dest-Isolated.

6.6.2.5 Procedures for reinvocation of intrusion during wait on busy

6.6.2.5.1 Normal procedure

In state CI-Dest-WOB, on receipt of a callIntrusionRequest invoke APDU in a FACILITY message, the Terminating PINX shall check whether reinvocation of intrusion is possible.

To check whether reinvocation of intrusion is possible, the Terminating PINX shall check that the called user is involved in a compatible established call in basic call state Active, that the CIPL of the called user is lower than the received CICL of the calling user, and that there are no other reasons for denying intrusion (e.g. if the established call is already being intruded on). If, as far as the Terminating PINX is concerned, reinvocation of intrusion is possible, the Terminating PINX shall send a callIntrusionGetCIPL invoke APDU in a FACILITY message to the Unwanted User PINX, start timer T5 and enter the state CI-GetCIPL-WOB.

In state CI-GetCIPL-WOB, on receipt of callIntrusionGetCIPL return result APDU in a FACILITY message, the Terminating PINX shall stop timer T5 and check that the CIPL of the unwanted user is lower than the CICL of the calling user.

If all conditions are met, the Terminating PINX may provide a notification of impending intrusion to users in the established call. If notification of impending intrusion is not to be given, execution of intrusion shall take place immediately. If notification of impending intrusion is to be given, the Terminating PINX shall send on the call reference of the established call a NOTIFY message containing notification value "intrusionIsImpending", may send on the call reference of the intruding call a NOTIFY message containing notification value "intrusionIsImpending", shall start timer T6 and shall enter state CI-Dest-Notify-WOB. Execution of intrusion shall commence on expiry of timer T6 in state CI-Dest-Notify-WOB.

Execution of intrusion shall result either in a conference type connection involving all three users (the calling user, the called user and the unwanted user) or in isolation of the unwanted user (disconnection of the unwanted user and connection of the calling user and the called user).

If a conference type connection is established, the Terminating PINX shall send using the call reference of the intruding call a FACILITY message containing a callIntrusionRequest return result APDU containing value "unwantedUserIntruded". The Terminating PINX may also send a NOTIFY message containing notification value "intrusionIsEffective" using the call reference of the established call. The Terminating PINX shall enter state CI-Dest-Invoked.

If the unwanted user is isolated, the Terminating PINX shall send, using the call reference of the intruding call, a FACILITY message containing a callIntrusionRequest return result APDU containing value "unwantedUserIsolated". The Terminating PINX shall also send a NOTIFY message containing notification value "isolationThroughIntrusion" using the call reference of the established call. The Terminating PINX shall enter state CI-Dest-Invoked.

6.6.2.5.2 Exceptional procedure

On receipt of a FACILITY message containing a callIntrusionRequest invoke APDU while in state CI-Dest-WOB, if reinvocation of intrusion is not possible (including the case where the received callIntrusionGetCIPL return result APDU indicates a CIPL that is too high) the Terminating PINX shall send back a callIntrusionRequest return error APDU containing an appropriate error in a FACILITY message and shall remain in or reenter state CI-Dest-WOB.

In the state CI-GetCIPL-WOB, on receipt of a callIntrusionGetCIPL reject APDU containing problem code "unrecognized operation" in a FACILITY message from the Unwanted User PINX, the Terminating PINX shall stop timer T5, and shall apply the procedures described in 6.6.2.5.1 for receipt of a return result APDU with the lowest value of CIPL.

On expiry of timer T5 or on receipt of a callIntrusionGetCIPL reject APDU containing a problem code other than "unrecognizedOperation", the Terminating PINX shall send a callIntrusionRequest return error APDU containing error value "temporarilyUnavailable" in a FACILITY message to the Originating PINX and shall reenter state CI-Dest-WOB.

6.6.2.6 Procedures for completion of SS-CI

6.6.2.6.1 Normal procedure

In state CI-Dest-Invoked, or CI-Dest-Isolated, if the established call is released, the Terminating PINX shall send a callIntrusionCompleted invoke APDU in a FACILITY message to the Originating PINX and enter the state CI-Idle. The intruding call shall continue as a basic call in state Active and the calling and called users shall remain connected together.

In state CI-Dest-WOB, if the called user answers the waiting intruding call (having made available the necessary resources, e.g. by releasing or placing on hold another call), the Terminating PINX shall send a callIntrusionCompleted invoke APDU in a FACILITY message to the Originating PINX and enter state CI-Idle. The intruding call shall continue as a basic call in state Active and the calling and called users shall be connected together.

In state CI-Dest-WOB, if the called user becomes not busy and alerting commences, the Terminating PINX shall send a NOTIFY message containing notification value "remoteUserAlerting" and remain in the same state.

If the intruding call is released in any state, the Terminating PINX shall enter state CI-Idle and stop any SS-CI timer. If release occurs during state CI-Dest-Notify, CI-Dest-Notify-WOB, CI-Dest-Invoked or CI-Dest-Isolated, the established call