INTERNATIONAL STANDARD

ISO/IEC 14846

Second edition
2003-04-01

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

Reference number
ISO/IEC 14846:2003(E)

© ISO/IEC 2003

--`,,`-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2003

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 either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2003 — All rights reserved

Not for Resale

Contents

Foreword v

Introduction vi

1 Scope 1

2 Conformance 1

3 Normative references 1

4 Terms and definitions 2

4.1 External definitions 2
4.2 Other definitions 3

4.2.1 Busy 3
4.2.2 Conference type connection 3
4.2.3 Impending intrusion warning notification 3
4.2.4 Isolation 3
4.2.5 Path retention 3
4.2.6 Served User PINX 3
4.2.7 Wanted user 3
4.2.8 Unwanted user 3
4.2.9 Unwanted User PINX 3
4.2.10 Wait on busy 3

5 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 9

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 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.9.1 Interaction with Calling Name Identification Presentation (SS-CNIP) **16**
6.9.2 Interaction with Connected Name Identification Presentation (SS-CONP) **16**
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**

Annexes

A - Signalling protocol for the support of Path Retention **21**

B - Protocol Implementation Conformance Statement (PICS) proforma **30**

C - Examples of message sequences **39**

D - Specification and Description Language (SDL) representation of procedures **47**

E - Imported ASN.1 definitions **60**

F - ASN.1 definitions according to ITU-T Recs. X.208 / X.209 **61**

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 14846 was prepared by ECMA (as 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.

This second edition cancels and replaces the first edition (ISO/IEC 14846:1996), which has been technically revised.

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Introduction

This International Standard is one of a series of 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 International Standard specifies the signalling protocol for use at the Q reference point in support of the Call Intrusion supplementary service. The protocol defined in this International Standard forms part of the PSS1 protocol (informally known as QSIG).

This International Standard is based upon the practical experience of ECMA member companies and the results of their active and continuous participation in the work of ISO/IEC JTC 1, ITU-T, ETSI and other international and national standardization bodies. It represents a pragmatic and widely based consensus.

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 ETS 300 387. 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 referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 11572:2000, *Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Circuit mode bearer services - Inter-exchange signalling procedures and protocol*

ISO/IEC 11574:2000, *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*

ISO/IEC 11579-1:1994, *Information technology - Telecommunications and information exchange between systems - Private integrated services network - Part 1: Reference configuration for PISN Exchanges (PINX)*

ISO/IEC 11582:2002, *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*

ISO/IEC 13863:1998, *Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Specification, functional model and information flows - Path replacement additional network feature*

--`,,`-`-`,,`,,`,`,,`---

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ISO/IEC 13869:2003, *Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Inter-exchange signalling protocol - Call Transfer supplementary service*

ISO/IEC 13873:2003, *Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Inter-exchange signalling protocol - Call Diversion supplementary services*

ISO/IEC 13874:2003 *Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Inter-exchange signalling protocol - Path Replacement additional network feature*

ISO/IEC 14843:2003, *Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Inter-exchange signalling protocol - Call Offer supplementary service*

ISO/IEC 14844:2003, *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*

ISO/IEC 14845:1996, *Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Specification, functional model and information flows - Call intrusion supplementary service*

ETS 300 387:1994, *Private Telecommunication Network (PTN); Method for the specification of basic and supplementary services*

ITU-T Rec. I.112:1993, *Vocabulary of terms for ISDNs*

ITU-T Rec. I.210:1993, *Principles of telecommunication services supported by an ISDN and the means to describe them*

ITU-T Rec. Q.950:2000, *Supplementary services protocols, structure and general principles*

ITU-T Rec. Z.100:1999, *Specification and description language (SDL)*

4 Terms and definitions

For the purposes of this document, the following terms and 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 (ITU-T 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)

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

- Private Integrated services Network eXchange (PINX) (ISO/IEC 11579-1)
- Rerouteing PINX (ISO/IEC 13873)
- Served user (ISO/IEC 14845)
- Signalling (ITU-T Rec. I.112)
- Supplementary Service (ITU-T 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

4.2.1 Busy

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

4.2.2 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.

4.2.3 Impending intrusion warning notification

A notification provided before communication is established between the served user and the wanted user.

4.2.4 Isolation

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

4.2.5 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.

4.2.6 Served User PINX

The PINX serving the served user.

4.2.7 Wanted user

The called user in the intruding call.

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

4.2.8 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.

4.2.9 Unwanted User PINX

The PINX of the unwanted user.

4.2.10 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 Acronyms

ANF	Additional Network Feature
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation no. 1
CICL	Call Intrusion Capability Level

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 11574.

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.

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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. The notation is in accordance with ITU-T Rec. X.680 and X.690. The ITU-T Rec. X.208 and X.209 superseded version is in annex F.

Table 1 - Operations in support of SS-CI

```
Call-Intrusion-Operations-asn1-97
                    {iso(1) standard(0) pss1-call-intrusion(14846) call-intrusion-operations-asn1-97 (2) }

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

IMPORTS             OPERATION, ERROR FROM Remote-Operations-Information-Objects
                        {joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}
                    EXTENSION, Extension{} FROM Manufacturer-specific-service-extension-class-asn1-97
                        {iso(1) standard(0)
                        pss1-generic-procedures(11582) msi-class-asn1-97(11)}
                    notAvailable, supplementaryServiceInteractionNotAllowed
                        FROM General-Error-List
                        {ccitt recommendation q 950 general-error-list (1)};

Call-Intrusion-Operations OPERATION ::= {pathRetain | serviceAvailable | callIntrusionRequest |
callIntrusionGetCIPL | callIntrusionIsolate | callIntrusionForcedRelease | callIntrusionWOBRequest |
callIntrusionCompleted | cfbOverride}

pathRetain          OPERATION ::= {
                    ARGUMENT        PathRetainArg       -- this operation may be used by other
                                                        -- Supplementary Services using other
                                                        -- values of the argument
                    RETURN RESULT       FALSE
                    ALWAYS RESPONDS     FALSE
                    CODE                local: 41}

serviceAvailable    OPERATION ::= {
                    ARGUMENT ServiceAvailableArg        -- this operation may be used by other
                                                        -- Supplementary Services using other
                                                        -- values of the argument
                    RETURN RESULT       FALSE
                    ALWAYS RESPONDS     FALSE
                    CODE                local: 42}

callIntrusionRequest OPERATION ::= {
                    ARGUMENT        CIRequestArg
                    RESULT          CIRequestRes
                    ERRORS      {notAvailable | notBusy | temporarilyUnavailable | notAuthorized |
                                unspecified | supplementaryServiceInteractionNotAllowed}
                    CODE                local: 43}

callIntrusionGetCIPL OPERATION ::= {
                    ARGUMENT            DummyArg
                    RESULT              CIGetCIPLRes
                    ALWAYS RESPONDS     FALSE
                    CODE                local: 44}
```

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

```
callIntrusionForcedRelease      OPERATION ::= {
                                ARGUMENT        DummyArg
                                RESULT          DummyRes
                                ERRORS          {notAvailable | unspecified |
                                    supplementaryServiceInteractionNotAllowed}
                                CODE            local: 46}

callIntrusionIsolate            OPERATION ::= {
                                ARGUMENT        DummyArg
                                RESULT          DummyRes
                                ERRORS          {notAvailable | unspecified |
                                    supplementaryServiceInteractionNotAllowed}
                                CODE            local: 45}

callIntrusionWOBRequest         OPERATION ::= {
                                ARGUMENT        DummyArg
                                RESULT          DummyRes
                                ERRORS          {notAvailable | unspecified |
                                    supplementaryServiceInteractionNotAllowed}
                                CODE            local: 47}

callIntrusionCompleted          OPERATION ::= {
                                ARGUMENT        DummyArg
                                RETURN RESULT       FALSE
                                ALWAYS RESPONDS     FALSE
                                CODE            local: 48}

PathRetainArg           ::= CHOICE {
                                serviceList             ServiceList,
                                extendedServiceList     SEQUENCE {
                                    serviceList         ServiceList,
                                    extension           Extension{{CIExtSet}}
                                        }
                        }

ServiceAvailableArg     ::= CHOICE {
                                serviceList             ServiceList,
                                extendedServiceList     SEQUENCE {
                                    serviceList         ServiceList,
                                    extension           Extension{{CIExtSet}}
                                        }
                        }

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{{CIExtSet}},
                                sequenceOfExtn  [2] IMPLICIT SEQUENCE OF Extension{{CIExtSet}}}

DummyRes                ::=     CHOICE{
                                null            NULL,
                                extension       [1] IMPLICIT Extension{{CIExtSet}},
                                sequenceOfExtn  [2] IMPLICIT SEQUENCE OF Extension{{CIExtSet}}}
```

--`,,`-`-`,,`,,`,`,`,,`---

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

```
CIRequestArg            ::=     SEQUENCE{
                                ciCapabilityLevel CICapabilityLevel,
                                argumentExtension       CHOICE{
                                        extension       [1] IMPLICIT Extension{{CIExtSet}},
                                        sequenceOfExtn  [2] IMPLICIT SEQUENCE OF Extension{{CIExtSet}}
                                        } OPTIONAL}

CIRequestRes            ::=     SEQUENCE{
                                ciUnwantedUserStatus CIUnwantedUserStatus,
                                resultExtension     CHOICE{
                                        extension       [1] IMPLICIT Extension{{CIExtSet}},
                                        sequenceOfExtn  [2] IMPLICIT SEQUENCE OF Extension{{CIExtSet}}
                                        } OPTIONAL}

CIGetCIPLRes            ::= SEQUENCE{
                                ciProtectionLevel CIProtectionLevel,
                                resultExtension     CHOICE{
                                        extension       [1] IMPLICIT Extension{{CIExtSet}},
                                        sequenceOfExtn  [2] IMPLICIT SEQUENCE OF Extension{{CIExtSet}}
                                        } OPTIONAL}

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
                        RETURN RESULT           FALSE
                        ALWAYS RESPONDS         FALSE
                        CODE                    local: 49}
                        -- used in the interaction with Call Forwarding Busy

CIExtSet EXTENSION ::= {…}

notBusy                 ERROR ::= { CODE        local: 1009}
                        -- used when an SS-CI request is received in
                        -- a Terminating PINX and the called user is not busy

temporarilyUnavailable  ERROR ::= { CODE        local: 1000}
                        -- used when conditions for invocation of SS-CI
                        -- are momentarily not met

notAuthorized           ERROR ::= { CODE        local: 1007}
                        --used when a SS-CI request is rejected
                        --because of insufficient CICL

unspecified             ERROR ::= {
                        PARAMETER Extension{{CIExtSet}}
                        CODE        local: 1008}

END                     -- of Call-Intrusion-Operations-asn1-97
```

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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-asn1-97
                                        {iso(1) standard(0)
                                        pss1-call-intrusion(14846) call-intrusion-notifications-asn1-97 (3)}

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

IMPORTS                         NOTIFICATION FROM Notification-class-asn1-97
                                {iso(1) standard(0)
                                pss1-generic-procedures(11582) notification-class-asn1-97(21)};

remoteUserAlerting          NOTIFICATION ::= {
                            ARGUMENT    NULL
                            CODE        local: 2000}

intrusionIsImpending        NOTIFICATION ::= {
                            ARGUMENT    NULL
                            CODE        local: 2003}

intrusionIsEffective        NOTIFICATION ::= {
                            ARGUMENT    NULL
                            CODE        local: 2004}

isolationThroughIntrusion   NOTIFICATION ::= {
                            ARGUMENT    NULL
                            CODE        local: 2005}

forcedReleaseAfterIntrusion NOTIFICATION ::= {
                            ARGUMENT    NULL
                            CODE        local: 2006}

endOfIntrusion              NOTIFICATION::= {
                            ARGUMENT    NULL
                            CODE        local: 2007}

Call-Intrusion-Notifications NOTIFICATION ::= { remoteUserAlerting | intrusionIsImpending | intrusionIsEffective |
isolationThroughIntrusion | forcedReleaseAfterIntrusion | endOfIntrusion}


END                     --of Call-Intrusion-Notifications-asn1-97
```

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, callIntrusionWOBRequest, callIntrusionCompleted, the NFE shall be included.

When conveying an invoke APDU of operations callIntrusionRequest, callIntrusionGetCIPL, callIntrusionForcedRelease, callIntrusionIsolate, callIntrusionWOBRequest, 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.

--`,,`-`-`,,`,,`,`,,`---
© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

--`,,,`---`,,`,,`,`,,`---

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 invokable, 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".

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 shall be restored to the state that existed prior to intrusion and a NOTIFY message containing notification description value "endOfIntrusion" shall be sent on the call reference of the established call.

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.6.2.6.2 Exceptional procedure

In state CI-GetCIPL-WOB or CI-Dest-Notify-WOB, if the called user answers (having made available the necessary resources, e.g. by releasing or placing on hold another call), the Terminating PINX shall stop timer T5 or T6, send a callIntrusionRequest return error APDU containing error notBusy together with a callIntrusionCompleted invoke APDU in a FACILITY message 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-Get-CIPL-WOB or CI-Dest-Notify-WOB, if the called user becomes not busy and alerting commences, the Terminating PINX shall stop timer T5 or T6, send a callIntrusionRequest return error APDU containing error notBusy together with notification value "remoteUserAlerting" in a FACILITY message and enter state CI-Dest-WOB.

6.6.3 Actions at the Unwanted User PINX

On receipt of a callIntrusionGetCIPL invoke APDU in a FACILITY message, the Unwanted User PINX shall send a FACILITY message to the Terminating PINX. The FACILITY message shall include a callIntrusionGetCIPL return result APDU with the CIPL of the unwanted user.

6.6.4 Actions at a Transit PINX

No special actions are required in support of SS-CI.

6.7 SS-CI impact of interworking with public ISDNs

On a call to a PISN from a public ISDN that does not support an equivalent service, SS-CI will not be requested.

On a call from a PISN to a public ISDN that does not support an equivalent service, the Outgoing Gateway PINX shall behave as specified in 6.6.2 for a Terminating PINX at which conditions for invocation of SS-CI are not met.

If the unwanted user is in a public ISDN, the Gateway PINX shall respond to the callIntrusionGetCIPL invoke APDU by supplying a CIPL on behalf of the unwanted user.

NOTE 6 - A Gateway PINX can supply the same CIPL for all calls or can introduce some discrimination, e.g. according to the direction of the call.

If the unwanted user is in a public ISDN that does not support an equivalent service, the Gateway PINX shall discard any SS-CI notification.

NOTE 7 - At the time of publication of this International Standard, no equivalent service has been specified for public ISDNs.

6.8 SS-CI impact of interworking with non-ISDNs

When interworking with a non-ISDN which does not support an equivalent service, the procedures defined in 6.7 for interworking with a public ISDN that does not support an equivalent service shall apply.

When interworking with a non-ISDN which supports an equivalent service, the two networks may cooperate in the operation of SS-CI. In this case, either the Originating PINX functionality or the Terminating PINX functionality or the Unwanted User PINX functionality will be provided in the non-ISDN. The Incoming or Outgoing Gateway PINX shall provide conversion between the signalling protocol specified in this International Standard and the signalling protocol of the other network.

6.9 Protocol interactions between SS-CI and other supplementary services and ANFs

This clause specifies protocol interactions with other supplementary services and ANFs for which stage 3 standards had been published at the time of publication of this International Standard. For interactions with supplementary services and ANFs for which stage 3 standards are published subsequent to the publication of this International Standard, see those other stage 3 standards.

NOTE 8 - Additional interactions that have no impact on the signalling protocol at the Q reference point can be found in the relevant stage 1 specifications.

NOTE 9 - Simultaneous conveyance of APDUs for SS-CI and another supplementary service or ANF in the same message, each in accordance with the requirements of its respective stage 3 standard, does not, on its own, constitute a protocol interaction.

6.9.1 Interaction with Calling Name Identification Presentation (SS-CNIP)

No protocol interaction.

6.9.2 Interaction with Connected Name Identification Presentation (SS-CONP)

No protocol interaction.

--`,,,`--`-`,,`,,`,`,,`---

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.9.3 Interaction with Call Completion to Busy Subscriber (SS-CCBS)

No protocol interaction.

6.9.4 Interaction with Call Completion on No Reply (SS-CCNR)

No protocol interaction.

6.9.5 Interaction with Call Transfer (SS-CT)

The following protocol interactions shall apply if SS-CT is supported in accordance with ISO/IEC 13869.

6.9.5.1 Notifications to User B of SS-CT

6.9.5.1.1 Actions at the Transferring PINX for transfer by join

If call transfer by join is performed at the SS-CI Originating PINX during state CI-Orig-WOB, the Transferring PINX shall initiate the normal procedures for transfer by join except that the behaviour shall be as if the secondary call basic call protocol control state were "Call Delivered". On receipt of a callIntrusionCompleted invoke APDU from the Secondary PINX, the Transferring PINX shall act as if a CONNECT message had been received, i.e. send a FACILITY message with a callTransferActive invoke APDU to the Primary PINX and enter state CT-Idle.

6.9.5.1.2 Actions at the Secondary PINX for transfer by join

If call transfer by join is performed and the Secondary PINX is also a SS-CI Terminating PINX in state CI-Dest-WOB, the Secondary PINX may send a "call is a waiting call" notification, as defined in ISO/IEC 11582, in a Notification indicator information element in a NOTIFY message to the Primary PINX using the call reference on which the callTransferComplete invoke APDU was received. If this notification is not sent, then when User C of SS-CT becomes not busy, no remoteUserAlerting notification shall be sent.

6.9.5.1.3 Actions at the Secondary PINX for transfer by rerouteing

If call transfer by rerouteing is performed and the SS-CI Terminating PINX is in state CI-Dest-WOB, the Secondary PINX shall act as if the secondary call had been in basic call protocol control state Call Received, i.e. send the callTransferSetup return result APDU in an ALERTING message. The ALERTING message may contain a notification "call is a waiting call", as defined in ISO/IEC 11582. If this notification is not sent, then when User C of SS-CT becomes not busy, no remoteUserAlerting notification shall be sent. When User C of SS-CT answers and a CONNECT message is sent, no callIntrusionCompleted invoke APDU shall be sent.

6.9.6 Interaction with Call Forwarding Unconditional (SS-CFU)

The following protocol interactions shall apply if SS-CFU is supported in accordance with ISO/IEC 13873.

6.9.6.1 Actions at the Rerouteing PINX

On receiving a callRerouting invoke APDU, the Rerouteing PINX shall include in the SETUP message to the Diverted-to PINX any callIntrusionRequest invoke APDU or pathRetain invoke APDU with bit ci-low, ci-medium or ci-high set to ONE that has been sent in the original SETUP message.

6.9.6.2 Actions at the Originating PINX

In order to invoke SS-CI without path retention after a call has encountered a busy diverted-to user, the Originating PINX shall include a callIntrusionRequest invoke APDU in addition to the divertingLegInformation2 invoke APDU in the SETUP message of the new call to the diverted-to user.

6.9.7 Interaction with Call Forwarding Busy (SS-CFB)

The following protocol interactions shall apply if SS-CFB is supported in accordance with ISO/IEC 13873.

6.9.7.1 Actions at the Rerouteing PINX

On receiving a callRerouting invoke APDU, the Rerouteing PINX shall include in the SETUP message to the Diverted-to PINX any callIntrusionRequest invoke APDU or pathRetain invoke APDU with bit ci-low, ci-medium or ci-high set to ONE that has been sent in the original SETUP message.

6.9.7.2 Actions at the Originating PINX

In order to invoke SS-CI without path retention directly at the last busy diverted-to user after a call has encountered two or more busy users that have been reached as a result of one or more invocations of SS-CFB, the Originating PINX shall include a callIntrusionRequest invoke APDU in addition to the divertingLegInformation2 invoke APDU in the SETUP message of the new call to the busy diverted-to user.

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

If SS-CI is to be invoked at the first busy user after a call has encountered two or more busy users that have been reached as a result of one or more invocations of SS-CFB, the Originating PINX shall act in one of the following ways:

– In order to invoke SS-CI without path retention at the first busy user, thereby overriding SS-CFB at that user, the Originating PINX shall include a callIntrusionRequest invoke APDU and a cfbOverride invoke APDU in a Facility information element in the SETUP message of the new call. When conveying the invoke APDU of operation cfbOverride, the NFE shall be included as defined for operation callIntrusionRequest and the Interpretation APDU shall be included with value discardAnyUnrecognisedInvokePdu.

– In order to invoke SS-CI with path retention at the first busy user, thereby overriding SS-CFB at that user, the Originating PINX shall include a pathRetain invoke APDU with bit ci-low, ci-medium or ci-high set to ONE and a cfbOverride invoke APDU in a Facility information element in the SETUP message of the new call. When conveying the invoke APDU of operation cfbOverride, the NFE shall be included as defined for operation pathRetain and the Interpretation APDU shall be included with value discardAnyUnrecognisedInvokePdu.

6.9.7.3 Actions at the Served (Called) User PINX

On receiving a SETUP message containing a callIntrusionRequest invoke APDU together with a cfbOverride invoke APDU, if the called user is busy, SS-CFB shall be overridden and the procedures of SS-CI shall apply.

On receiving a SETUP message containing a pathRetain invoke APDU with bit ci-low, ci-medium or ci-high set to ONE together with a cfbOverride invoke APDU, if the called user is busy, SS-CFB shall be overridden and the procedures of SS-CI shall apply.

6.9.8 Interaction with Call Forwarding No Reply (SS-CFNR)

No protocol interaction.

6.9.9 Interaction with Call Deflection (SS-CD)

No protocol interaction.

6.9.10 Interaction with Path Replacement (ANF-PR)

The following protocol interactions shall apply if ANF-PR is supported in accordance with ISO/IEC 13874.

6.9.10.1 Actions at an ANF-PR Requesting PINX

6.9.10.1.1 Sending of callIntrusionGetCIPL invoke APDU

As part of invocation of SS-CI, the SS-CI Terminating PINX may send a FACILITY message containing a callIntrusionGetCIPL invoke APDU while also acting as an ANF-PR Requesting PINX.

NOTE 10 - If the ANF-PR state is PR-Req-Initiating, the Requesting PINX should take steps to protect against release of the old connection before a response to the callIntrusionGetCIPL invoke APDU has been received. This can be achieved by responding to a pathReplaceSetup invoke APDU with a return error APDU containing error value temporarilyUnavailable, thereby causing ANF-PR to fail and ensuring that the old connection is kept. ANF-PR can be attempted again later.

If the ANF-PR state is PR-Req-Completing, the callIntrusionGetCIPL invoke APDU shall be sent using the new connection.

6.9.10.1.2 Receipt of callIntrusionGetCIPL invoke APDU

The response to a callIntrusionGetCIPL invoke APDU shall be sent on the connection on which the invoke APDU was received.

6.9.10.1.3 Sending of Notification to the unwanted user

An SS-CI Terminating PINX may send a NOTIFY message containing a notification to the unwanted user while also acting as an ANF-PR Requesting PINX.

NOTE 11 - If the ANF-PR state is PR-Req-Initiating, the Requesting PINX should take steps to protect against release of the old connection before the notification reaches the unwanted user's PINX (the ANF-PR Cooperating PINX). This can be achieved by responding to a pathReplaceSetup invoke APDU with a return error APDU containing error value temporarilyUnavailable, thereby causing ANF-PR to fail and ensuring that the old connection is kept. ANF-PR can be attempted again later.

If the ANF-PR state is PR-Req-Completing, the notification shall be sent using the new connection.

--`,,,`-`-`,,`,,`,`,,`---
© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.9.10.2 Actions at an ANF-PR Cooperating PINX

6.9.10.2.1 Sending of callIntrusionGetCIPL invoke APDU

As part of invocation of SS-CI, the SS-CI Terminating PINX may send a FACILITY message containing a callIntrusionGetCIPL invoke APDU while also acting as an ANF-PR Cooperating PINX.

If the ANF-PR state is PR-Coop-Establishment, the callIntrusionGetCIPL invoke APDU shall be sent using the old connection.

NOTE 12 - The Cooperating PINX should postpone release of the old connection until a response has been received.

If the ANF-PR state is PR-Coop-Retain, the Cooperating PINX shall postpone sending of the callIntrusionGetCIPL invoke APDU until completion of ANF-PR or send it again if no response is obtained.

6.9.10.2.2 Receipt of callIntrusionGetCIPL invoke APDU

The response to a callIntrusionGetCIPL invoke APDU shall be sent on the connection on which the invoke APDU was received.

6.9.10.2.3 Sending of Notification to the unwanted user

An SS-CI Terminating PINX may send a NOTIFY message containing a notification to the unwanted user while also acting as an ANF-PR Cooperating PINX. If the ANF-PR state is PR-Coop-Establishment, the notification shall be sent using the old connection.

If the ANF-PR state is PR-Coop-Retain, the Cooperating PINX shall postpone sending of the notification until completion of ANF-PR.

6.9.11 Interaction with Call Offer (SS-CO)

The following protocol interactions shall apply if SS-CO is supported in accordance with ISO/IEC 14843.

6.9.11.1 Actions at the Originating PINX

While SS-CO is in progress, the Originating PINX may request SS-CI by sending a callIntrusionRequest invoke APDU in a FACILITY message during basic call protocol state Outgoing Call Proceeding or Call Delivered, starting timer T1 of SS-CI and entering state CI-Wait-Ack. The procedures of SS-CI shall then apply.

6.9.11.2 Actions at the Terminating PINX

6.9.11.2.1 Normal Procedures

After SS-CO has been successfully invoked and prior to completion of SS-CO, on receipt of a callIntrusionRequest invoke APDU in a FACILITY message, the Terminating PINX shall act in accordance with SS-CI.

NOTE 13 - If SS-CI is successfully invoked, SS-CO returns to state CO-Idle, since a CONNECT message is sent.

6.9.11.2.2 Exceptional Procedures

The procedures of SS-CI shall apply. If SS-CI is rejected, SS-CO shall continue.

6.9.12 Interaction with Do Not Disturb (SS-DND)

No protocol interaction.

6.9.13 Interaction with Do Not Disturb Override (SS-DNDO)

The following protocol interactions shall apply if SS-DNDO

is supported in accordance with ISO/IEC 14844.

6.9.13.1 Actions at the Terminating PINX

On receiving a SETUP message containing a callIntrusionRequest invoke APDU together with a doNotDisturbOverrideQ invoke APDU, the procedures of SS-DNDO shall apply and, if DND is not active or is successfully overridden, the procedures of SS-CI shall apply.

6.10 SS-CI parameter values (timers)

6.10.1 Timer T1

Timer T1 shall operate at the Originating PINX during state CI-Wait-Ack and CI-Wait-Ack-WOB. Its purpose is to protect against an absence of response to a request for invocation or reinvocation of intrusion.

Timer T1 shall have a value not less than 30 s.

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.10.2 Timer T2

Timer T2 shall operate at the Originating PINX during state CI-Isolation-Request. Its purpose is to protect against an absence of response to a request for isolation.

Timer T2 shall have a value not less than 30 s.

6.10.3 Timer T3

Timer T3 shall operate at the Originating PINX during states CI-inForcedRelease-Request or CI-isForcedRelease-Request. Its purpose is to protect against an absence of response to a request for forced release.

Timer T3 shall have a value not less than 30 s.

6.10.4 Timer T4

Timer T4 shall operate at the Originating PINX during states CI-inWOB-Request or CI-isWOB-Request. Its purpose is to protect against an absence of response to a request for wait on busy.

Timer T4 shall have a value not less than 30 s.

6.10.5 Timer T5

Timer T5 shall operate at the Terminating PINX during states CI-GetCIPL-I and CI-GetCIPL-WOB. Its purpose is to protect against an absence of response to a request for the CIPL of the unwanted user.

Timer T5 shall have a value not less than 10 s.

6.10.6 Timer T6

Timer T6 shall operate at the Terminating PINX during state CI-Dest-Notify or CI-Dest-Notify-WOB. Its purpose is to control the delay between the impending intrusion warning notification and the execution of intrusion.

Timer T6 shall have a value not higher than 10 s.

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A
(normative)

Signalling protocol for the support of Path Retention

This annex is applicable to Originating PINXs that support SS-CI with path retention and to Terminating PINXs that support SS-CI. A similar annex will appear in other standards that make use of the generic mechanism for path retention.

A.1 Path Retention description

Path retention is a generic mechanism which can be used by supplementary services during call establishment.

Path retention is invoked by the Originating PINX either for one supplementary service or for several supplementary services at the same time. Invocation for a particular supplementary service means that the network connection is to be retained if the Terminating PINX encounters conditions in which it is appropriate to invoke that supplementary service. The Originating PINX is informed of the reason for retaining the connection so that it can decide (e.g. by consulting the calling user) whether to invoke the supplementary service. Under some circumstances in which the network connection is retained, more than one of the supplementary services for which path retention has been invoked may be applicable.

Successive retentions of the network connection by the Terminating PINX following a single invocation of path retention by the Originating PINX are possible as a result of different conditions being encountered at the Terminating PINX. When an attempt is made to invoke a supplementary service for which the network connection has been retained, a further condition can be encountered that can cause the network connection to be retained again for the same supplementary service or a different supplementary service.

Path retention is specified in terms of a Path Retention entity existing within the Coordination Function at the Originating PINX and at the Terminating PINX.

A.2 Path Retention operational requirements

A.2.1 Requirements on the Originating PINX

Call establishment procedures for the outgoing side of an inter-PINX link, 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.

A.2.2 Requirements on the Terminating PINX

Call establishment procedures for the incoming side of an inter-PINX link, 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.

A.2.3 Requirements on a Transit PINX

Call establishment 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 a Transit PINX, shall apply.

A.3 Path Retention coding requirements

A.3.1 Operations

The operations pathRetain and serviceAvailable as defined in 6.3.1 shall apply. Within the ARGUMENT of operation pathRetain, the element of type ServiceList may contain bits other than those named in 6.3.1, in order to request path retention for other supplementary services. Within the ARGUMENT of operation serviceAvailable, the element of type ServiceList may contain bits other than those named in 6.3.1, in order to indicate retention of the network connection for other supplementary services.

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.3.2 Information elements

APDUs of the operations pathRetain and serviceAvailable shall be coded in the Facility information element in accordance with ISO/IEC 11582.

When conveying an APDU of operation pathRetain or serviceAvailable, the NFE shall be included. In the case of an invoke APDU the destinationEntity data element of the NFE shall contain value endPINX.

When conveying an invoke APDU of operation pathRetain or serviceAvailable, the Interpretation APDU shall contain value discardAnyUnrecognisedInvokePdu.

A.3.3 Messages

The Facility information element shall be conveyed in the messages as specified in clause 10 of ISO/IEC 11582. The basic call messages shall be used for call establishment as specified in ISO/IEC 11572.

A.4 Path Retention state definitions

A.4.1 States at the Originating PINX

The procedures at the Originating PINX are written in terms of the following conceptual states existing within the Path Retention entity in that PINX in association with a particular call.

A.4.1.1 PRTO-Idle

Path retention is not operating.

A.4.1.2 PRTO-Requested

A pathRetain invoke APDU has been sent and the Originating PINX is waiting for a serviceAvailable invoke APDU from the Terminating PINX.

A.4.1.3 PRTO-Retained

A serviceAvailable invoke APDU has been received and the network connection is retained.

A.4.1.4 PRTO-Invoking

Invocation of a supplementary service is being attempted using a retained network connection.

A.4.2 States at the Terminating PINX

The procedures at the Terminating PINX are written in terms of the following conceptual states existing within the Path Retention entity in that PINX in association with a particular incoming call.

A.4.2.1 PRTT-Idle

Path retention is not operating.

A.4.2.2 PRTT-Requested

A pathRetain invoke APDU has been received and the Terminating PINX is waiting until conditions for retaining the network connection are encountered.

A.4.2.3 PRTT-Retained

A serviceAvailable invoke APDU has been sent and the network connection is retained.

A.4.2.4 PRTT-Invoking

Invocation of a supplementary service is being attempted using a retained network connection.

A.5 Path Retention signalling procedures for invocation and operation

A.5.1 Actions at the Originating PINX

The SDL representation of procedures at the Originating PINX is shown in A.9.1.

On sending a SETUP message for call establishment, if path retention is required for allowing the possibility of invoking one or more supplementary services on encountering certain conditions at the Terminating PINX, the Originating PINX shall include a pathRetain invoke APDU in the SETUP message and shall enter state PRTO-Requested. In the element of type ServiceList in the ARGUMENT, any bit corresponding to a supplementary service for which path retention is required shall be set to ONE and all other bits shall be set to ZERO.

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

On receipt of a serviceAvailable invoke APDU in a PROGRESS or a FACILITY message in state PRTO-Requested, the Originating PINX shall enter state PRTO-Retained.

In state PRTO-Requested, if the Originating PINX determines that retention of the network connection can no longer occur (e.g. on receipt of a CONNECT message), it shall enter state PRTO-Idle.

During state PRTO-Retained, invocation of any of the supplementary services indicated in the serviceAvailable invoke APDU may be requested. If invocation is requested (by sending the appropriate APDU in a FACILITY message), the Terminating PINX shall enter state PRTO-Invoking.

In state PRTO-Invoking, if the supplementary service concerned is successfully invoked, the Originating PINX shall either:

i) if there is a possibility of the network connection being retained again prior to completion of call establishment (e.g. to allow for the possibility of invoking another supplementary service or for the possibility of invoking the same supplementary service again), enter state PRTO-Requested again; or

ii) enter state PRTO-Idle.

In state PRTO-Invoking, if the supplementary service concerned fails to be invoked successfully, the Originating PINX shall either:

i) if the network connection is still retained to allow the possibility of invoking another supplementary service, enter state PRTO-Retained again; or

ii) enter state PRTO-Idle.

If, in any state other than PRTO-Idle, the call is released, state PRTO-Idle shall be entered.

A.5.2 Actions at the Terminating PINX

The SDL representation of procedures at the Terminating PINX is shown in A.9.2.

On receipt of a pathRetain invoke APDU in a SETUP message, the Terminating PINX shall enter state PRTT-Requested and record the list of supplementary services for which path retention has been requested, as indicated by the element of type ServiceList.

If, during state PRTT-Requested, a condition is encountered in which it is appropriate to invoke one or more of the supplementary services for which path retention has been requested, the Terminating PINX shall retain the network connection, send a serviceAvailable invoke APDU to the Originating PINX, start timer PRT1 and enter state PRTT-Retained. In the element of type ServiceList in the ARGUMENT, any bit corresponding to a supplementary service that can be invoked at this stage and for which path retention has been requested shall be set to ONE and all other bits shall be set to ZERO. This procedure replaces the normal procedure appropriate to the condition that has been encountered.

The serviceAvailable invoke APDU shall be sent either in a FACILITY message or, if a PROGRESS message is to be sent at the same time, in the PROGRESS message. A PROGRESS message containing a Progress indicator information element with CCITT Progress description no. 8 (in-band information or appropriate pattern now available) shall be sent if this Progress description has not already been sent for this call.

NOTE - It is necessary that this Progress description be sent, as a means of ensuring that basic call timer T310 is stopped at other PINXs. However, if this Progress description has already been sent in conjunction with an earlier serviceAvailable invoke APDU for this call, it need not be repeated.

In state PRTT-Requested, if the Terminating PINX determines that retention of the network connection can no longer occur (e.g. on sending a CONNECT message), it shall enter state PRTT-Idle.

In state PRTT-Retained, on receipt of an invocation request from the Originating PINX for any of the supplementary services for which the network connection has been retained, the Terminating PINX shall stop timer PRT1 and enter state PRTT-Invoking.

In state PRTT-Invoking, if the supplementary service concerned is successfully invoked, the Terminating PINX shall either:

i) if there is a possibility of the network connection being retained again prior to completion of call establishment (e.g. to allow for the possibility of invoking another supplementary service or for the possibility of invoking the same supplementary service again), enter state PRTT-Requested again; or

ii) enter state PRTT-Idle.

--`,,`-`-`,,`,,`,`,,`---
© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

In state PRTT-Invoking, if the supplementary service concerned fails to be invoked successfully, the Terminating PINX shall either:

i) continue to retain the network connection, return to state PRTT-Retained and start timer PRT1 if there are other supplementary services for which the network connection has been retained and that are still able to be invoked; or

ii) enter state PRTT-Idle and allow the call to proceed as specified for failure of the supplementary service concerned (e.g. initiate release of the call).

In case i), any APDU sent to the Originating PINX to indicate failure of the requested supplementary service shall be sent in a FACILITY message.

On expiry of timer PRT1, the Terminating PINX shall enter state PRTT-Idle and initiate call clearing in accordance with ISO/IEC 11572.

If, in any state other than PRTT-Idle, the call is released, state PRTT-Idle shall be entered and timer PRT1, if running, shall be stopped.

A.5.3 Actions at a Transit PINX

No special actions are required in support of path retention.

A.6 Path Retention impact of interworking with public ISDNs

On a call from a public ISDN that does not support an equivalent mechanism, path retention shall not be requested by the Incoming Gateway PINX.

On a call from a PISN to a public ISDN that does not support an equivalent mechanism, the Outgoing Gateway PINX shall, on encountering a condition in the public ISDN in which it is appropriate to invoke one or more of the supplementary services for which path retention has been requested, either:

i) proceed as if path retention had not been requested; or

ii) retain the network connection and allow invocation of the supplementary services concerned in accordance with A.5.2.

NOTE - If invocation of a supplementary service is requested while the network connection is retained, the Outgoing Gateway PINX is responsible for establishing a new network connection through the public ISDN in order to request invocation of the supplementary service. Failure to establish a new network connection (e.g. because of network congestion) can cause the Outgoing Gateway PINX to reject the supplementary service and release the call.

NOTE - At the time of publication of this International Standard, no equivalent mechanism has been specified for public ISDNs.

A.7 Path Retention impact of interworking with non-ISDNs

When interworking with a non-ISDN that does not support an equivalent mechanism, the procedures defined in A.6 for interworking with a public ISDN that does not support an equivalent mechanism shall apply.

When interworking with a non-ISDN that does support an equivalent mechanism, the two networks may cooperate in the operation of path retention. In this case, either the Originating PINX functionality or the Terminating PINX functionality will be provided in the non-ISDN. The Incoming or Outgoing Gateway PINX shall provide conversion between the signalling protocol specified in this International Standard and the signalling protocol of the other network.

A.8 Path Retention parameter values (timers)

Timer PRT1 operates at the Terminating PINX during state PRTT-Retained. Its purpose is to protect against absence of a supplementary service invocation request as a response to the serviceAvailable invoke APDU.

Timer PRT1 shall have a value not less than 60 s.

A.9 Specification and Description Language (SDL) - Representation of procedures (informative)

The diagrams in this annex use the Specification and Description Language defined in ITU-T Rec. Z.100 (1999).

Each diagram represents the behaviour of a Path Retention entity at a particular type of PTNX. In accordance with the protocol model described in ISO/IEC 11582, the Path Retention entity as a part of the Coordination Function uses the services of Generic Functional Procedures Control and Basic Call Control and provides services to the various SS Control entities.

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Where an output symbol represents a primitive to other parts of the Coordination Function, and that primitive results in a PSS1 message being sent, the output symbol bears the name of the message and any remote operations APDU contained in that message. In the case of a message specified in ISO/IEC 11572, basic call actions associated with the sending of that message are deemed to occur.

Where an input symbol represents a primitive from other parts of the Coordination Function, and that primitive results from receipt of a PSS1 message, the input symbol bears the name of the message and any remote operations APDU contained in that message. In the case of a message specified in ISO/IEC 11572, basic call actions associated with the receipt of that message are deemed to occur.

The following abbreviation is used:

inv. invoke APDU.

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.9.1 SDL representation of Path Retention at the Originating PINX

Figure A.1 shows the behaviour of a Path Retention entity within the Originating PINX.

Output signals to the right represent messages sent via protocol control, input signals from the right represent messages received via protocol control, and input signals from the left represent internal primitives.

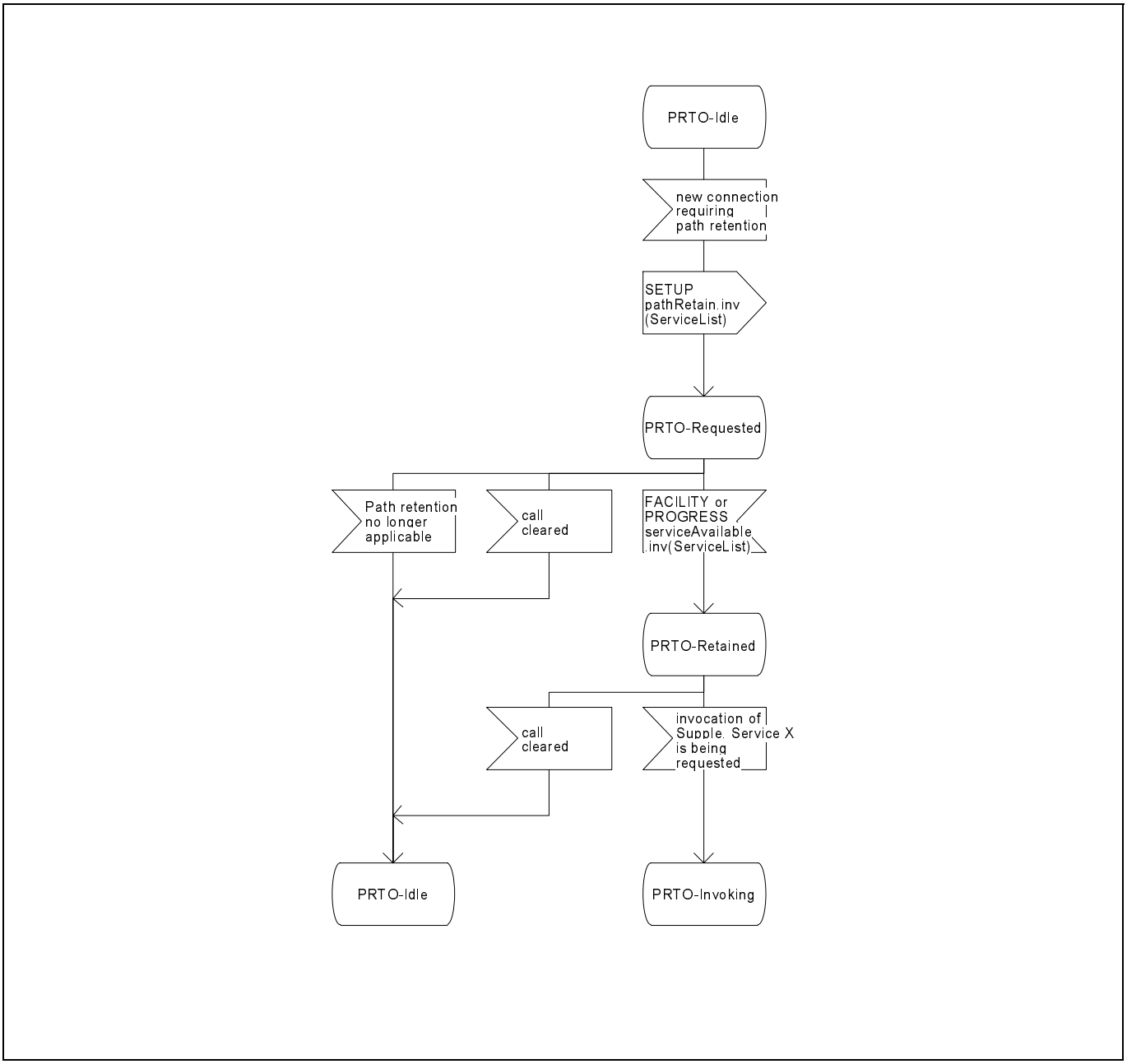


Figure A.1 (sheet 1 of 2) - SDL representation of Path Retention at the Originating PINX

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

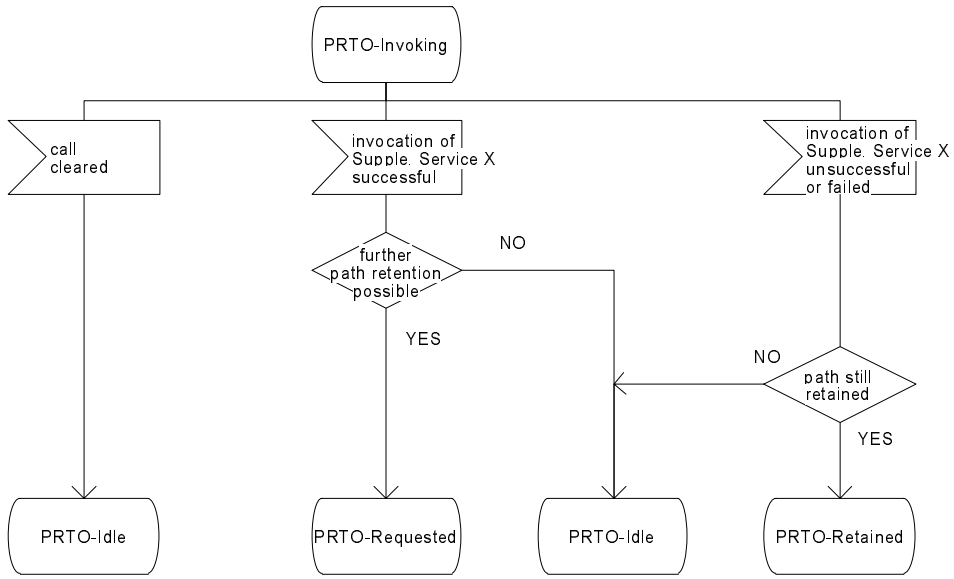


Figure A.1 (sheet 2 of 2) - SDL representation of Path Retention at the Originating PINX

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.9.2 SDL representation of Path Retention at the Terminating PINX

Figure A.2 shows the behaviour of a Path Retention entity within the Terminating PINX.

Output signals to the left represent messages sent via protocol control, input signals from the left represent messages received via protocol control, and input signals from the right represent internal primitives.

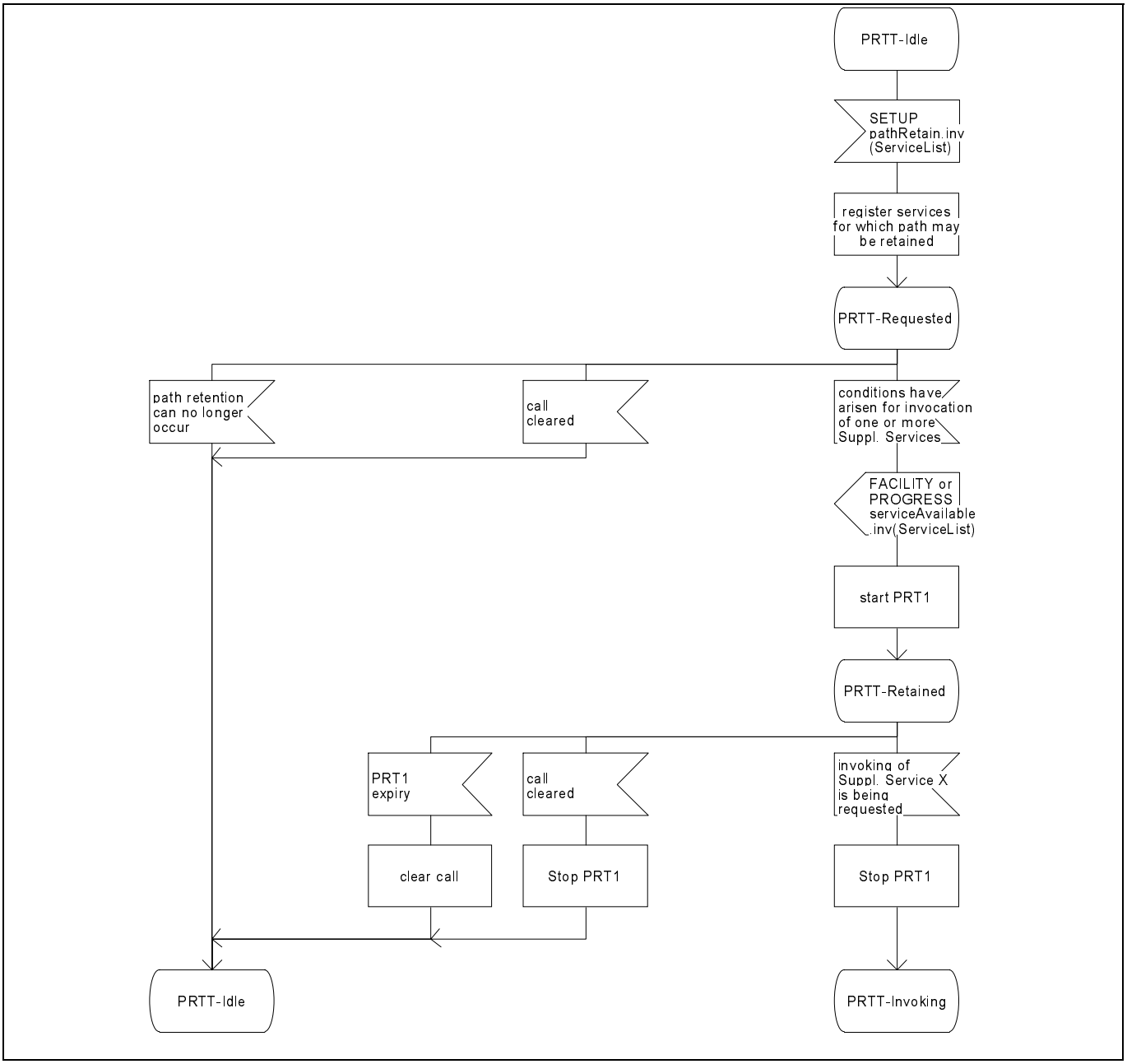


Figure A.2 (sheet 1 of 2) - SDL representation of Path Retention at the Terminating PINX

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

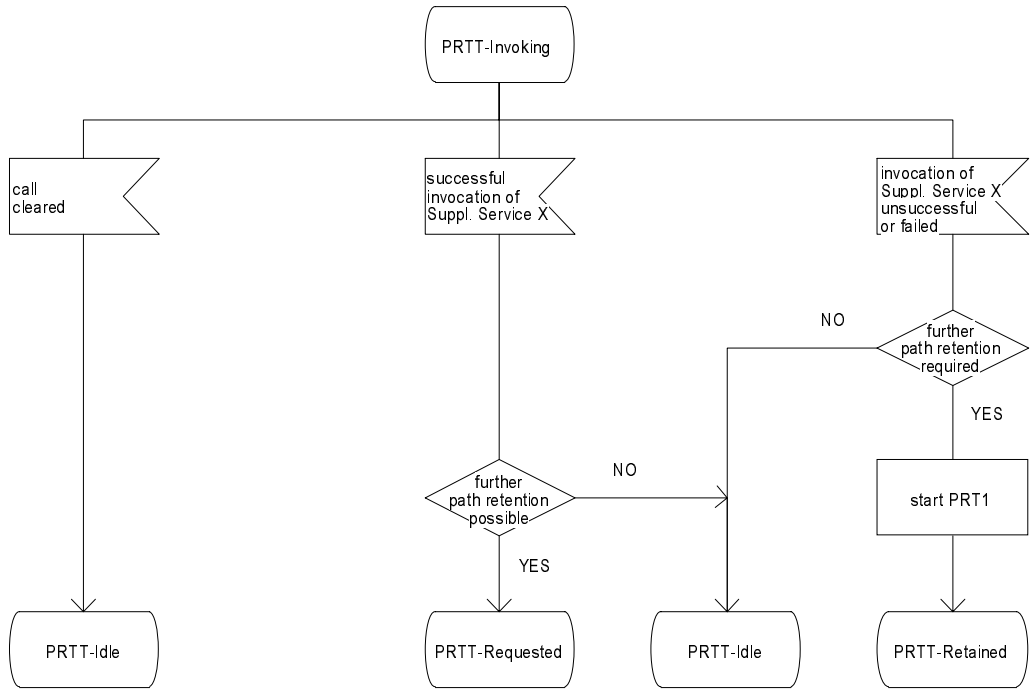


Figure A.2 (sheet 2 of 2) - SDL representation of Path Retention at the Terminating PINX

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B
(normative)

Protocol Implementation Conformance Statement (PICS) proforma

B.1 Introduction

The supplier of a protocol implementation which is claimed to conform to this International Standard shall complete the following Protocol Implementation Conformance Statement (PICS) proforma.

A completed PICS proforma is the PICS for the implementation in question. The PICS is a statement of which capabilities and options of the protocol have been implemented. The PICS can have a number of uses, including use:

– by the protocol implementor, as a check list to reduce the risk of failure to conform to the Standard through oversight;

– by the supplier and acquirer, or potential acquirer, of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the Standard's PICS proforma;

– by the user or potential user of the implementation, as a basis for initially checking the possibility of interworking with another implementation - while interworking can never be guaranteed, failure to interwork can often be predicted from incompatible PICSs;

– by a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

B.2 Instructions for completing the PICS proforma

B.2.1 General structure of the PICS proforma

The PICS proforma is a fixed format questionnaire divided into sub-clauses each containing a group of individual items. Each item is identified by an item number, the name of the item (question to be answered), and the reference(s) to the clause(s) that specifies (specify) the item in the main body of this International Standard.

The "Status" column indicates whether an item is applicable and if so whether support is mandatory or optional. The following terms are used:

m	mandatory (the capability is required for conformance to the protocol);
o	optional (the capability is not required for conformance to the protocol, but if the capability is implemented it is required to conform to the protocol specifications);
o.<n>	optional, but support of at least one of the group of options labelled by the same numeral <n> is required;
x	prohibited;
c.<cond>	conditional requirement, depending on support for the item or items listed in condition <cond>;
<item>:m	simple conditional requirement, the capability being mandatory if item number <item> is supported, otherwise not applicable;
<item>:o	simple conditional requirement, the capability being optional if item number <item> is supported, otherwise not applicable.

Answers to the questionnaire items are to be provided either in the "Support" column, by simply marking an answer to indicate a restricted choice (Yes or No), or in the "Not Applicable" column (N/A).

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.2.2 Additional information

Items of Additional Information allow a supplier to provide further information intended to assist the interpretation of the PICS. It is not intended or expected that a large quantity will be supplied, and a PICS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations.

References to items of Additional Information may be entered next to any answer in the questionnaire, and may be included in items of Exception information.

B.2.3 Exception information

It may occasionally happen that a supplier will wish to answer an item with mandatory or prohibited status (after any conditions have been applied) in a way that conflicts with the indicated requirement. No pre-printed answer will be found in the Support column for this. Instead, the supplier is required to write into the support column an x.<i> reference to an item of Exception Information, and to provide the appropriate rationale in the Exception item itself.

An implementation for which an Exception item is required in this way does not conform to this International Standard. A possible reason for the situation described above is that a defect in the Standard has been reported, a correction for which is expected to change the requirement not met by the implementation.

--`,,`-`-`,,`,,`,`,,`---

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.3 PICS proforma for ISO/IEC 14846

B.3.1 Implementation identification

Supplier	
Contact point for queries about the PICS	
Implementation Name(s) and Version(s)	
Other information necessary for full identification, e.g. Name(s) and Version(s) for machines and/or operating systems; system name(s)	

Only the first three items are required for all implementations; other information may be completed as appropriate in meeting the requirement for full identification.

The terms Name and Version should be interpreted appropriately to correspond with a suppliers terminology (e.g. Type, Series, Model).

B.3.2 Protocol summary

Protocol version	1.0
Addenda implemented (if applicable)	
Amendments implemented	
Have any exception items been required (see B.2.3)?	No [ ] Yes [ ] (The answer Yes means that the implementation does not conform to this International Standard)

Date of statement	

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.3.3 General

Item	Question/feature	Reference	Status	N/A	Support
A1	Support of SS-CI in Originating PINX of an intruding call	6.6.1	o.1		Yes [ ] No [ ]
A2	Support of SS-CI in Terminating PINX of an intruding call	6.6.2	o.1		Yes [ ] No [ ]
A3	Support of SS-CI in Unwanted User PINX See Note below	6.6.2	o		Yes [ ] No [ ]
A4	Behaviour as gateway to support SS-CI from user in PISN to user in public ISDN	6.7	o		Yes [ ] No [ ]
A5	Behaviour as gateway to support SS-CI from user in PISN to user in other network	6.8	o		Yes [ ] No [ ]
A6	Behaviour as gateway to support SS-CI from user in other network to user in PISN	6.8	o		Yes [ ] No [ ]
A7	Behaviour as gateway to support CIPL request from Terminating PINX to another network	6.8	o		Yes [ ] No [ ]
A8	Behaviour as gateway to support CIPL request from another network to an Unwanted User PINX	6.8	o		Yes [ ] No [ ]
A9	For which basic services can SS-CI be invoked?				Please indicate services: _____ _____ _____ _____

NOTE - Procedures of the Unwanted User PINX need not be supported if the unwanted users are to receive no protection.

--`,,`-`-`,,`,,`,`,,`---
© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.3.4 Procedures

Item	Question/feature	Reference	Status	N/A	Support
B1	Support of relevant ISO/IEC 11572 and ISO/IEC 11582 procedures	6.2.1, 6.2.2, 6.2.3	m		Yes [ ]
B2	SS-CI invocation without path retention in Originating PINX	6.6.1.1, 6.6.1.6	A1:o.2	[ ]	Yes [ ] No [ ]
B3	SS-CI invocation with path retention in Originating PINX	6.6.1.1, 6.6.1.6, A.2.1, A.5.1	A1:o.2	[ ]	Yes [ ] No [ ]
B4	SS-CI invocation without path retention in Terminating PINX	6.6.2.1, 6.6.2.6	A2:m	[ ]	Yes [ ]
B5	SS-CI invocation with path retention in Terminating PINX	6.6.2.1, 6.6.2.6, A.2.2, A.5.2	A2:m	[ ]	Yes [ ]
B6	Notification of intrusion impending in Terminating PINX	6.6.2	A2:o	[ ]	Yes [ ] No [ ]
B7	Notification of intrusion to calling user in Terminating PINX	6.6.2	B6:o	[ ]	Yes [ ] No [ ]
B8	Forced release request in Originating PINX	6.6.1.3	A1:o	[ ]	Yes [ ] No [ ]
B9	Forced release request in Terminating PINX	6.6.2.3	A2:o	[ ]	Yes [ ] No [ ]
B10	Isolate request in Originating PINX	6.6.1.2	A1:o	[ ]	Yes [ ] No [ ]
B11	Isolate request in Terminating PINX	6.6.2.2	A2:o	[ ]	Yes [ ] No [ ]
B12	Wait on busy request in Originating PINX	6.6.1.4	A1:o	[ ]	Yes [ ] No [ ]
B13	Wait on busy request in Terminating PINX	6.6.2.4	A2:o	[ ]	Yes [ ] No [ ]
B14	Reinvocation of SS-CI after wait on busy in Originating PINX	6.6.1.4	B12:m	[ ]	Yes [ ]
B15	Reinvocation of SS-CI after wait on busy in Terminating PINX	6.6.2.4	B13:m	[ ]	Yes [ ]
B16	SS-CI invocation in Unwanted User PINX	6.6.4	A3:m	[ ]	Yes [ ]

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.3.5 Coding

Item	Question/feature	Reference	Status	N/A	Support
C1	Sending of callIntrusionRequest invoke APDU and receipt of callIntrusionRequest return result and error APDU in Originating PINX	6.3.1	A1:m	[ ]	Yes [ ]
C2	Sending of pathRetain invoke APDU and receipt of serviceAvailable invoke APDU in Originating PINX	6.3.1	B3:m	[ ]	Yes [ ]
C3	Receipt of callIntrusionRequest invoke APDU and sending of callIntrusionRequest return result and error APDU in Terminating PINX	6.3.1	A2:m	[ ]	Yes [ ]
C4	Receipt of pathRetain invoke APDU and sending of serviceAvailable invoke APDU in Terminating PINX	6.3.1	A2:m	[ ]	Yes [ ]
C5	Sending of callIntrusionGetCIPL invoke APDU and receipt of callIntrusionGetCIPL return result APDU in Terminating PINX	6.3.1	A2:m	[ ]	Yes [ ]
C6	Receipt of callIntrusionGetCIPL invoke APDU and sending of callIntrusionGetCIPL return result APDU in Unwanted User PINX	6.3.1	A3:m	[ ]	Yes [ ]
C7	Sending of callIntrusionForcedRelease invoke APDU and receipt of callIntrusionForcedRelease return result APDU in Originating PINX	6.3.1	B8:m	[ ]	Yes [ ]
C8	Receipt of callIntrusionForcedRelease invoke APDU and sending of callIntrusionForcedRelease return result APDU in Terminating PINX	6.3.1	B9:m	[ ]	Yes [ ]
C9	Sending of callIntrusionIsolate invoke APDU and receipt of callIntrusionIsolate return result APDU in Originating PINX	6.3.1	B10:m	[ ]	Yes [ ]
C10	Receipt of callIntrusionIsolate invoke APDU and sending of callIntrusionIsolate return result APDU in Terminating PINX	6.3.1	B11:m	[ ]	Yes [ ]
C11	Sending of callIntrusionWOBRequest invoke APDU and receipt of callIntrusionWOBRequest return result APDU in Originating PINX	6.3.1	B12:m	[ ]	Yes [ ]
C12	Receipt of callIntrusionWOB invoke APDU and sending of callIntrusionWOBRequest return result APDU in Terminating PINX	6.3.1	B13:m	[ ]	Yes [ ]
C13	Receipt of callIntrusionCompleted invoke APDU in Originating PINX	6.3.1	A1:m	[ ]	Yes [ ]
C14	Sending of callIntrusionCompleted invoke APDU in Terminating PINX	6.3.1	A2:m	[ ]	Yes [ ]

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.3.6 Timers

Item	Question/feature	Reference	Status	N/A	Support
D1	Support of timer T1	6.10	A2:m	[ ]	Yes [ ] Value [ ]
D2	Support of timer T2	6.10	B10:m	[ ]	Yes [ ] Value [ ]
D3	Support of timer T3	6.10	B8:m	[ ]	Yes [ ] Value [ ]
D4	Support of timer T4	6.10	B12:m	[ ]	Yes [ ] Value [ ]
D5	Support of timer T5	6.10	A2:m	[ ]	Yes [ ] Value [ ]
D6	Support of timer T6	6.10	B6:m	[ ]	Yes [ ] Value [ ]
D7	Support of timer PRT1	A.8	A2:m	[ ]	Yes [ ] Value [ ]

B.3.7 Protocol interaction with Call Transfer (SS-CT)

Item	Question/feature	Reference	Status	N/A	Support
E1	Support of SS-CT (transfer by join)		o		Yes [ ] No [ ]
E2	Support of SS-CT (transfer by rerouteing)		o		Yes [ ] No [ ]
E3	Interactions between SS-CT by join and SS-CI for notification at Transferring PINX	6.9.5.1.1	c.1	[ ]	m: Yes [ ]
E4	Interactions between SS-CT by join and SS-CI for notification at Secondary PINX	6.9.5.1.2	c.2	[ ]	m: Yes [ ]
E5	Interactions between SS-CT by rerouteing and SS-CI for notification at Secondary PINX	6.9.5.1.3	c.3	[ ]	m: Yes [ ]

c.1: if (A1 and E1) then mandatory, else N/A

c.2: if (A2 and E1) then mandatory, else N/A.

c.3: if (A2 and E2) then mandatory, else N/A.

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.3.8 Protocol interactions with Call Forwarding Unconditional (SS-CFU)

Item	Question/feature	Reference	Status	N/A	Support
F1	Support of SS-CFU (Rerouteing PINX)		o		Yes [ ] No [ ]
F2	Support of SS-CFU (Originating PINX)		o		Yes [ ] No [ ]
F3	Interactions at Rerouteing PINX	6.9.6.1	F1:m	[ ]	m: Yes [ ]
F4	Interactions at Originating PINX	6.9.6.2	c.1	[ ]	m: Yes [ ]

c.1: if (A1 and F2) then mandatory, else N/A.

B.3.9 Protocol interactions with Call Forwarding Busy (SS-CFB)

Item	Question/feature	Reference	Status	N/A	Support
G1	Support of SS-CFB (Originating PINX)		o		Yes [ ] No [ ]
G2	Support of SS-CFB (Rerouteing PINX)		o		Yes [ ] No [ ]
G3	Support of SS-CFB (Served User PINX)		o		Yes [ ] No [ ]
G4	Interactions at Rerouteing PINX	6.9.7.1	c.1	[ ]	m: Yes [ ]
G5	Interactions at Originating PINX	6.9.7.2	c.2	[ ]	m: Yes [ ]
G6	Interactions at Served User PINX	6.9.7.3	c.3	[ ]	m: Yes [ ]

c.1: if ((A1 or A2) and G2) then mandatory, else N/A.

c.2: if (A1 and G1) then mandatory, else N/A.

c.3: if (A2 and G3) then mandatory, else N/A.

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.3.10 Protocol interactions with Path Replacement (ANF-PR)

Item	Question/feature	Reference	Status	N/A	Support
H1	Support of ANF-PR (Requesting PINX)		o		Yes [ ] No [ ]
H2	Support of ANF-PR (Cooperating PINX)		o		Yes [ ] No [ ]
H3	Sending of callIntrusionGetCIPL invoke APDU (actions at ANF-PR Requesting PINX)	6.9.10.1.1	c.1	[ ]	m: Yes [ ]
H4	Receipt of callIntrusionGetCIPL invoke APDU (actions at ANF-PR Requesting PINX)	6.9.10.1.2	c.2	[ ]	m: Yes [ ]
H5	Sending of Notification to the unwanted user (actions at ANF-PR Requesting PINX)	6.9.10.1.3	c.1	[ ]	m: Yes [ ]
H6	Sending of callIntrusionGetCIPL invoke APDU (actions at ANF-PR Cooperating PINX)	6.9.10.2.1	c.3	[ ]	m: Yes [ ]
H7	Receipt of callIntrusionGetCIPL invoke APDU (actions at ANF-PR Cooperating PINX)	6.9.10.2.2	c.4	[ ]	m: Yes [ ]
H8	Sending of Notification to the unwanted user (actions at ANF-PR Cooperating PINX)	6.9.10.2.3	c.3	[ ]	m: Yes [ ]

c.1: if (A2 and H1) then mandatory, else N/A.

c.2: if (A3 and H1) then mandatory, else N/A.

c.3: if (A2 and H2) then mandatory, else N/A.

c.4: if (A3 and H2) then mandatory, else N/A.

B.3.11 Protocol interactions with Call Offer (SS-CO)

Item	Question/feature	Reference	Status	N/A	Support
I1	Support of SS-CO (Originating PINX)		o		Yes [ ] No [ ]
I2	Support of SS-CO (Terminating PINX)		o		Yes [ ] No [ ]
I3	Interactions at the Originating PINX	6.9.11.1	c.1	[ ]	Yes [ ] No [ ]
I4	Interactions at the Terminating PINX	6.9.11.2	c.2	[ ]	Yes [ ] No [ ]

c.1: if (A1 and I1) then optional, else N/A.

c.2: if (A2 and I2) then optional, else N/A.

B.3.12 Protocol interactions with Do Not Disturb Override (SS-DNDO)

Item	Question/feature	Reference	Status	N/A	Support
J1	Support of SS-DNDO (Terminating PINX)		o		Yes [ ] No [ ]
J2	Interactions at the Terminating PINX	6.9.13.1	c.1	[ ]	m: Yes [ ]

c.1: if (A2 and J1) then mandatory, else N/A.

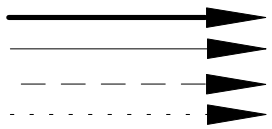
© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex C
(informative)

Examples of message sequences

This annex describes some typical message flows for SS-CI. The following conventions are used in the figures of this annex.

1 The following notation is used:



Basic call message containing SS-CI information
Basic call message without SS-CI information
Symbolic primitive carrying SS-CI information
Symbolic primitive without SS-CI information

xxx.inv	Invoke APDU for operation xxx
xxx.res	Return result APDU for operation xxx
xxx.err	Return error APDU for operation xxx
xxx.rej	Return reject APDU for operation xxx

2 The figures show messages exchanged via Protocol Control between PINXs involved in SS-CI. Only messages relevant to SS-CI are shown.

3 Only the relevant information content (i.e. remote operation APDUs) is listed below each message name. The Facility information elements containing remote operation APDUs are not explicitly shown. Information with no impact on SS-CI is not shown.

4 Some interactions with users are included in the form of symbolic primitives. The actual protocol at the terminal equipment interface is outside the scope of this International Standard.

5 CONNECT ACKNOWLEDGE, RELEASE, RELEASE COMPLETE messages are not shown.

6 The examples assume en-bloc sending.

7 The following abbreviations are used:

ciRequest	callIntrusionRequest
ciCompleted	callIntrusionCompleted
ciGetCIPL	callIntrusionGetCIPL
ciForcedRelease	callIntrusionForcedRelease
ciIsolate	callIntrusionIsolate
ciWOBRequest	callIntrusionWOBRequest
ci request	SS-CI request
ci impending	SS-CI is impending
ci confirm	SS-CI is confirmed
ci applied	SS-CI is effective
ci invokable	SS-CI is invokable
ci reject	SS-CI is rejected
ci completion	SS-CI is completed
ci terminated	SS-CI is terminated
WOB request	wait on busy is requested
WOB confirm	wait on busy is confirmed
WOB indication	wait on busy is indicated

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C.1 Example message sequence for normal operation of SS-CI without Path Retention

In this example all users are notified that the intrusion is impending. The intrusion results in a conference type connection involving all users.

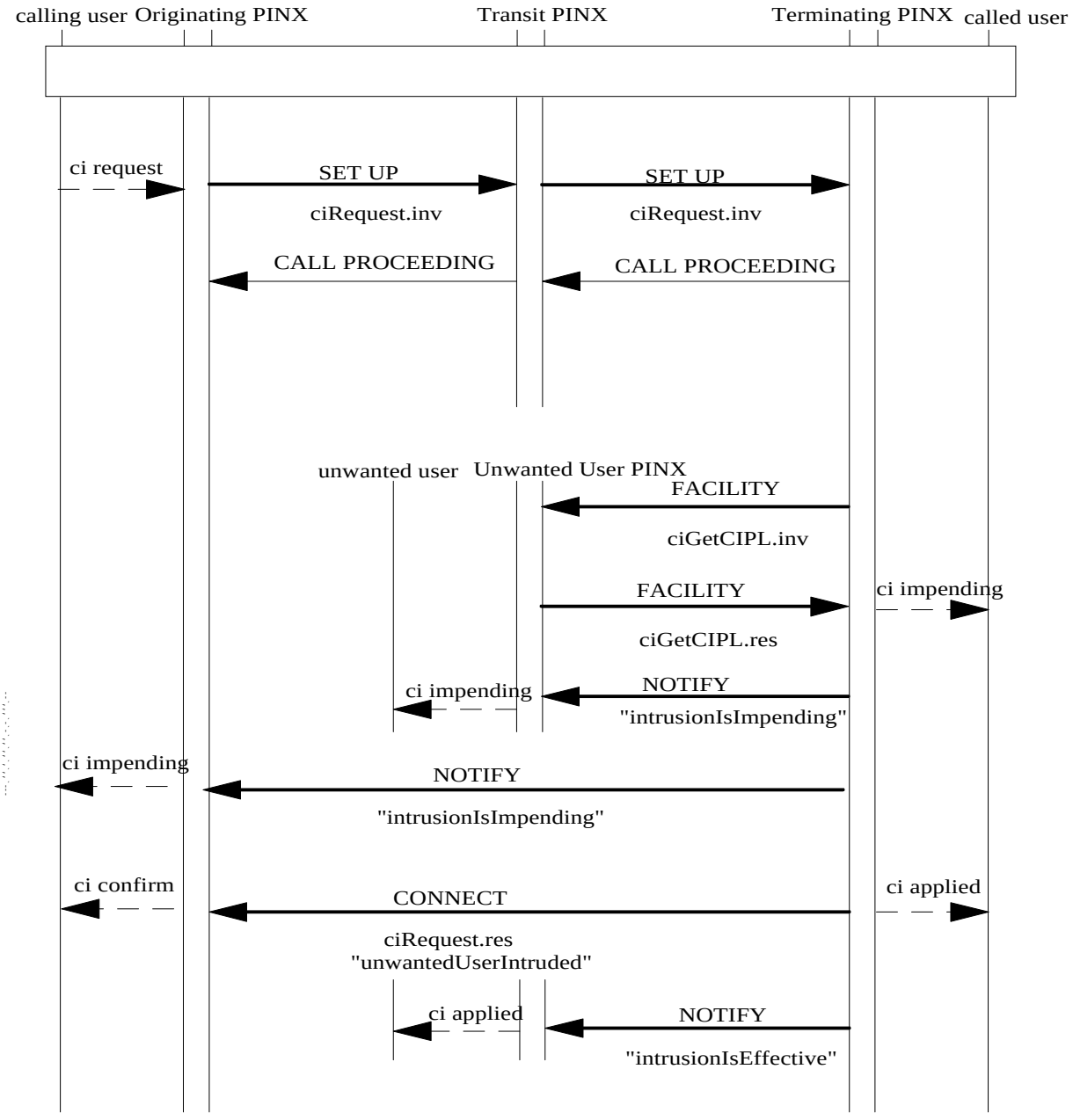


Figure C.1 - Message sequence for normal operation of SS-CI without Path Retention

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C.2 Example message sequence for normal operation of SS-CI with Path Retention

In this example the called user and the unwanted user are notified that the intrusion is impending. The intrusion results in the isolation of the unwanted user.

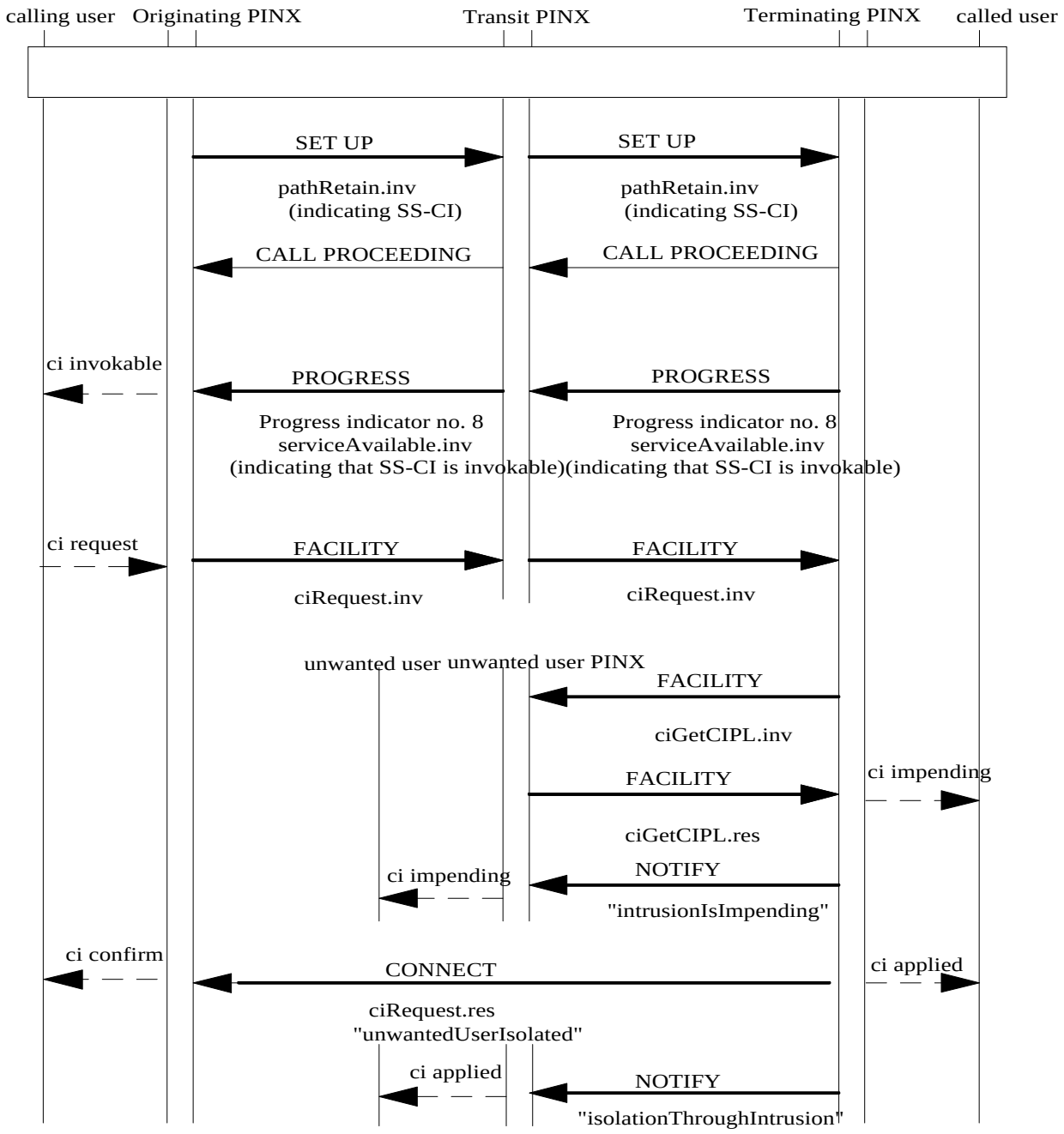


Figure C.2 - Message sequence for normal operation of SS-CI with Path Retention

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C.3 Example of unsuccessful invocation of SS-CI without Path Retention

In this example the request for SS-CI is rejected by the Terminating PINX on account of the CIPL of the unwanted user.

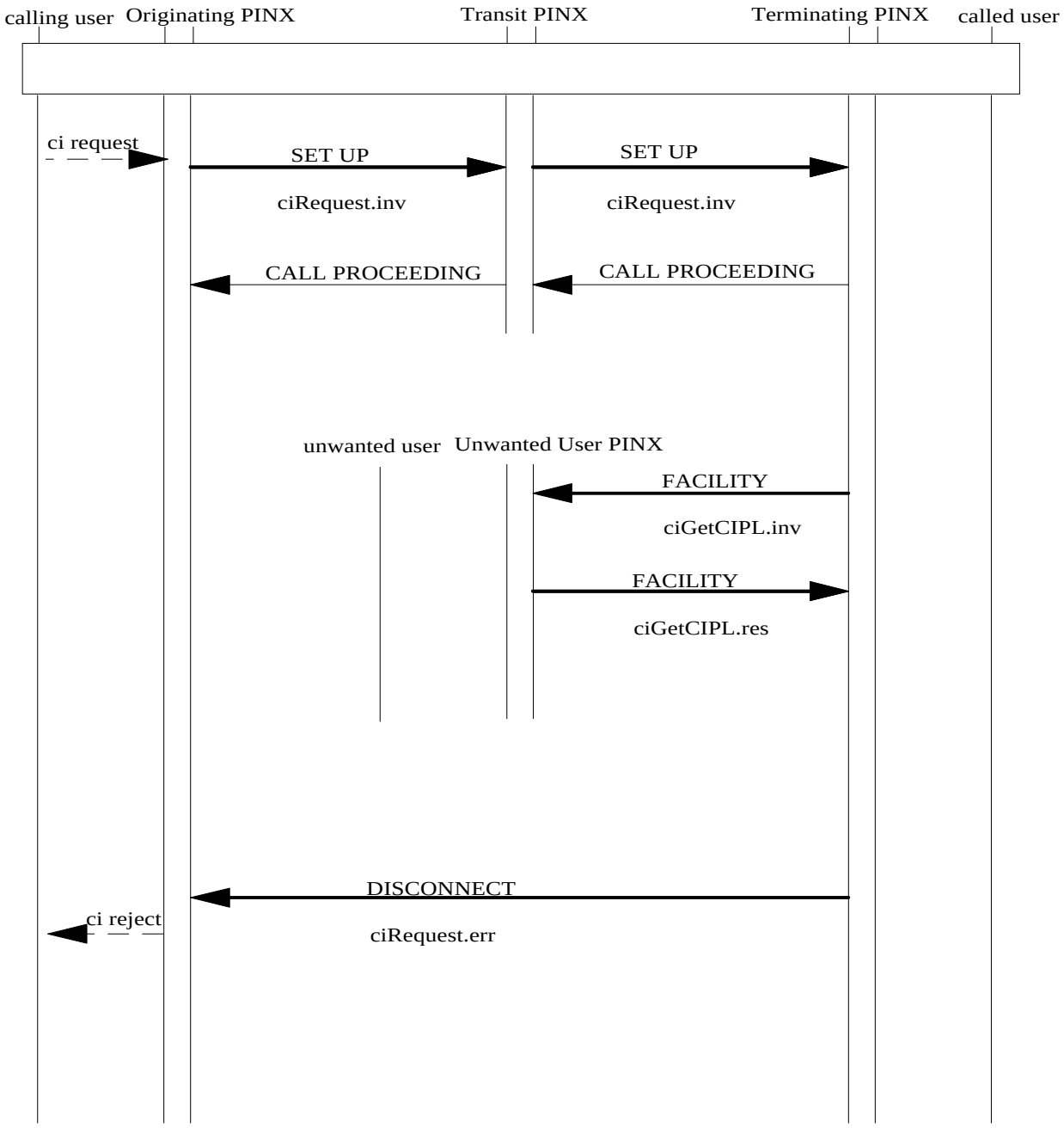


Figure C.3 - Message sequence for unsuccessful invocation of SS-CI

--`,,`-`-`,,`,,`,`,,`---

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C.4 Examples of completion of SS-CI

C.4.1 The established call is released

In this example, subsequent to successful invocation of call intrusion, the unwanted user releases the established call and a simple call is established between the calling user and the called user.

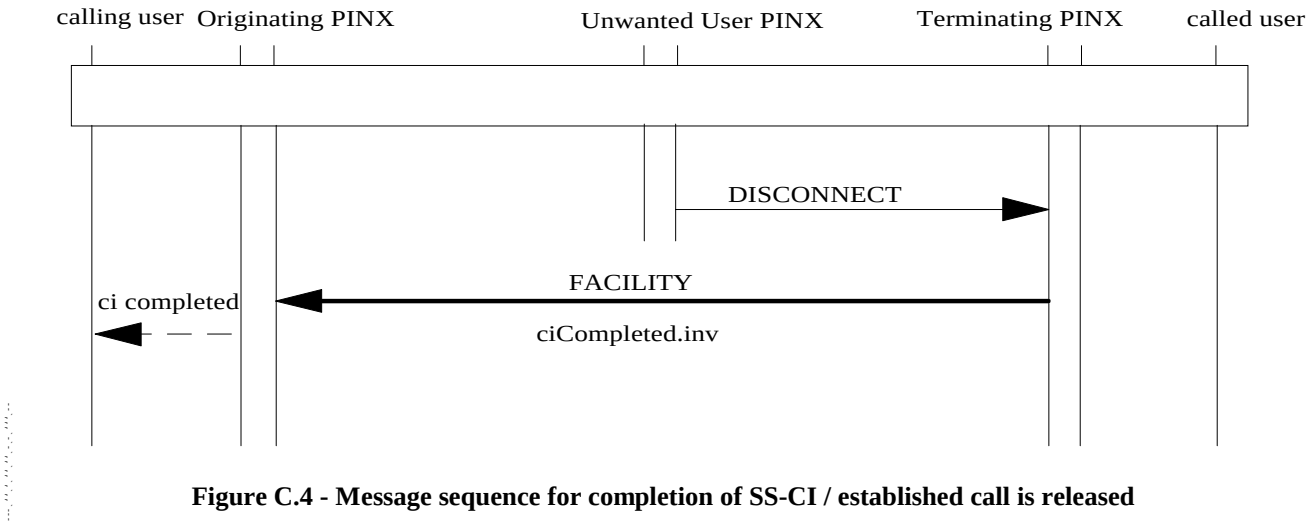


Figure C.4 - Message sequence for completion of SS-CI / established call is released

C.4.2 The intruding call is released

In this example the Originating PINX releases its call and the call is reestablished between the unwanted user and the called user.

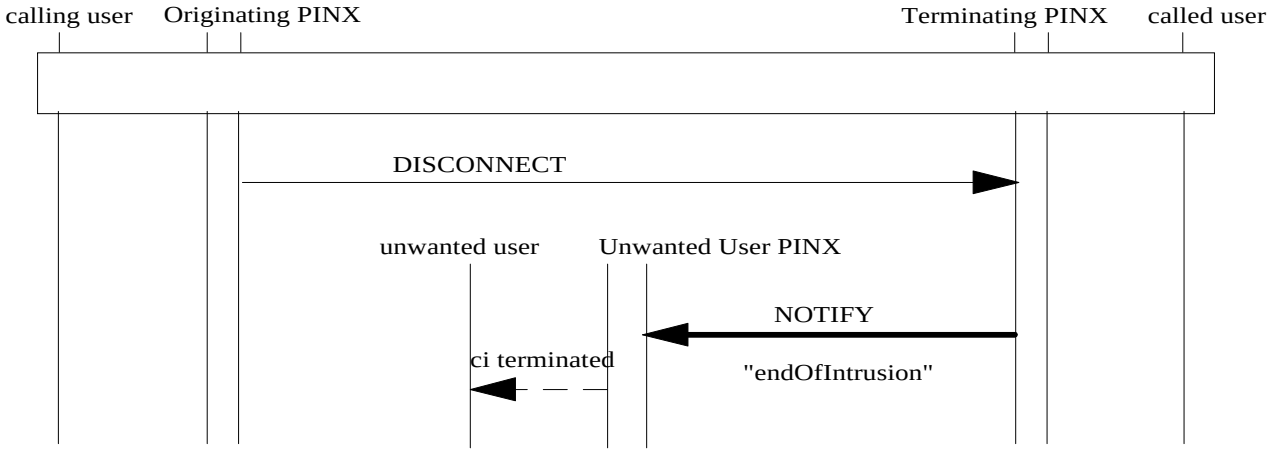


Figure C.5 - Message sequence for completion of SS-CI / intruding call is released

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C.5 Examples of invocation of SS-CI options

C.5.1 The Originating PINX forced releases the unwanted user

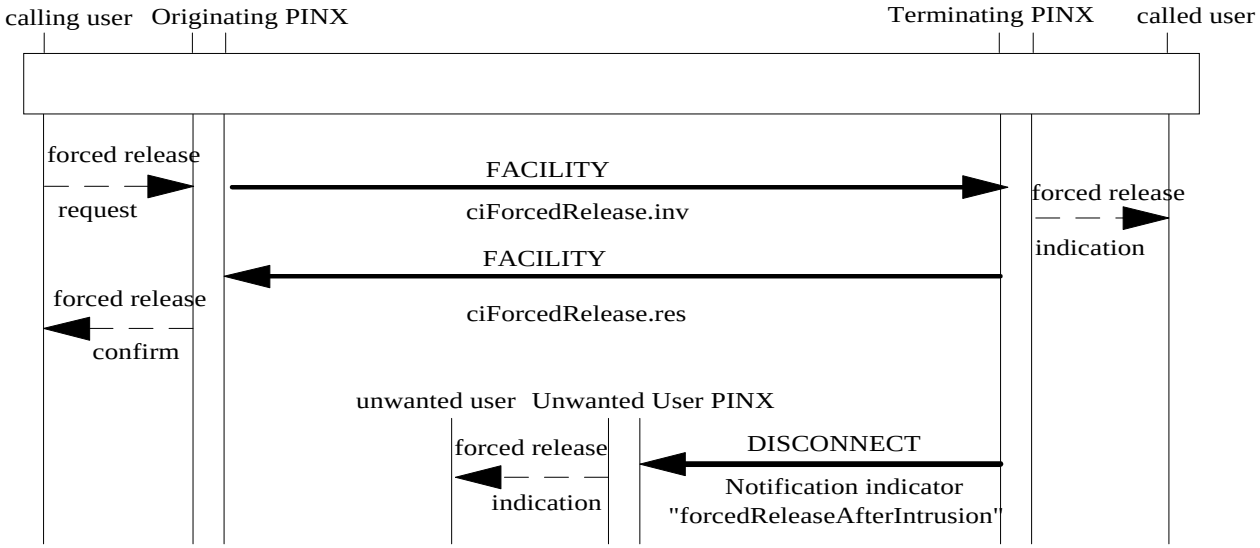


Figure C.6 - Message sequence for forced release of the unwanted user

C.5.2 The Originating PINX isolates the unwanted user

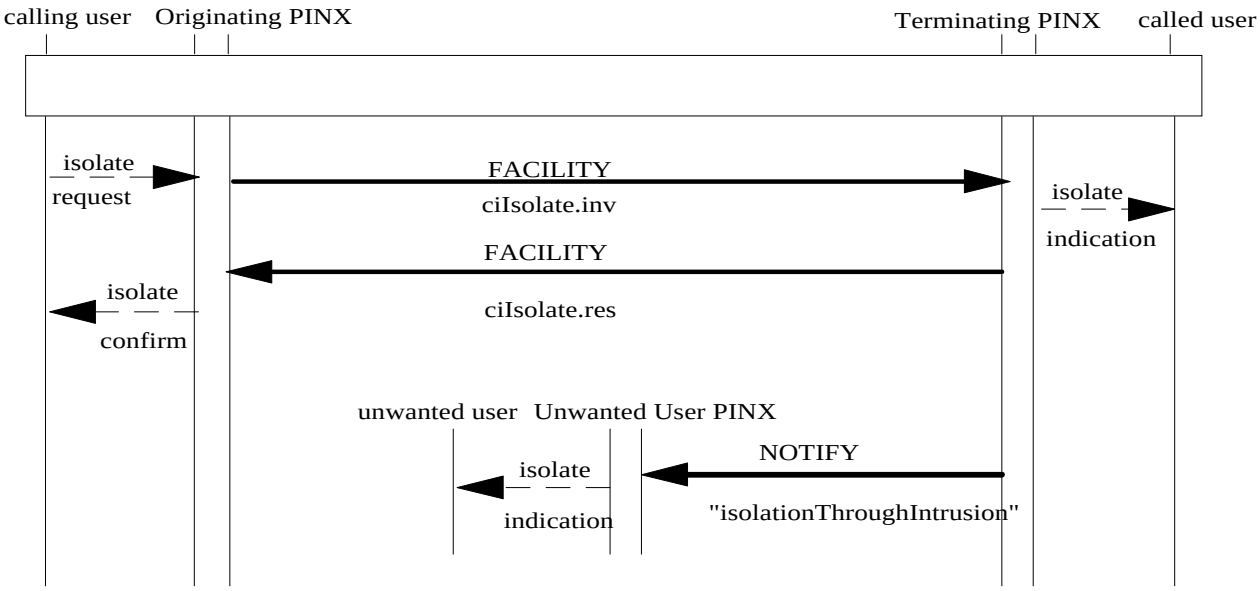


Figure C.7 - Message sequence for isolation of the unwanted user

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C.5.3 The Originating PINX invokes wait on busy

In this example, after invocation of WOB, the called user becomes not busy and answers.

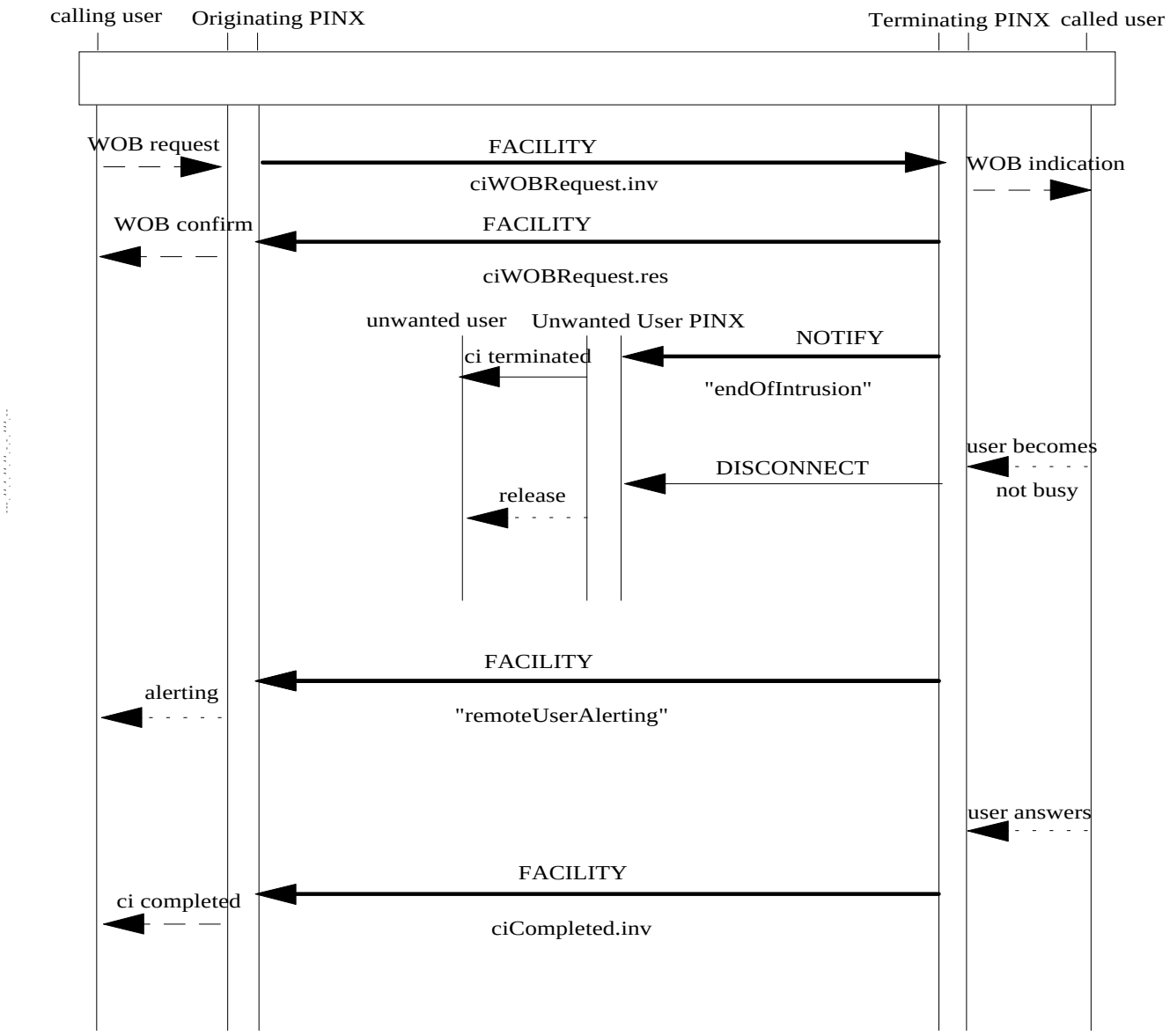


Figure C.8 - Message sequence for invocation of wait on busy

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C.5.4 The Originating PINX reinvokes intrusion during wait on busy

In this example, the called user and the unwanted user are notified that the intrusion is impending. The intrusion results in a conference type connection involving all users.

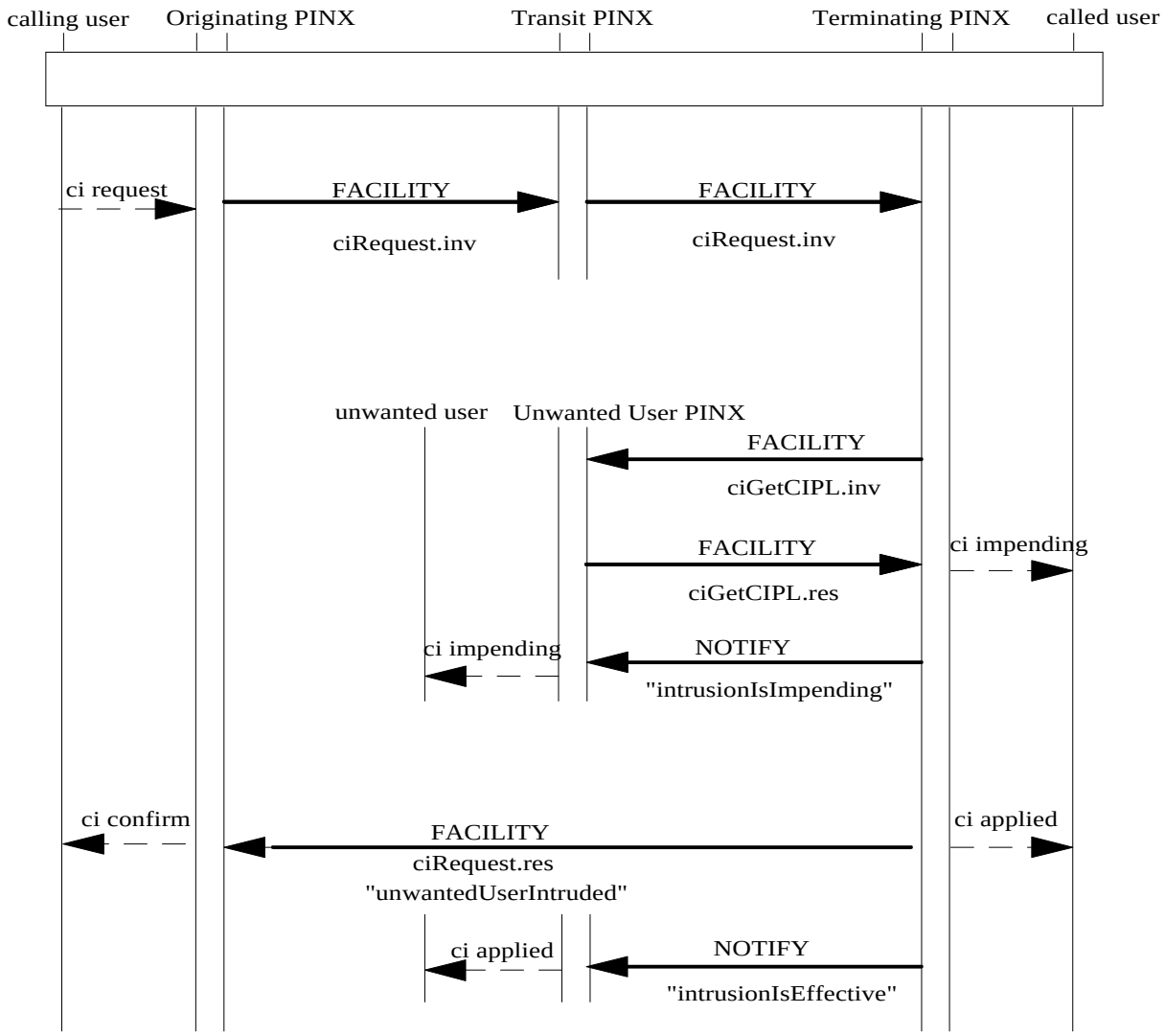


Figure C.9 - Message sequence for reinvocation of intrusion during wait on busy

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex D
(informative)

Specification and Description Language (SDL) representation of procedures

The diagrams in this annex use the Specification and Description Language defined in ITU-T Rec. Z.100 (1999).

Each diagram represents the behaviour of an SS-CI Supplementary Service Control entity at a particular type of PINX. In accordance with the protocol model described in ISO/IEC 11582, the Supplementary Service Control entity uses, via Coordination Functions, the services of Generic Functional Procedures Control and Basic Call Control.

Where an output symbol represents a primitive to the Coordination Functions, and that primitive results in a message being sent, the output symbol bears the name of the message and any remote APDU(s) or notification(s) contained in that message. In the case of a message specified in ISO/IEC 11572, basic call actions associated with the sending of that message are deemed to occur.

Where an input symbol represents a primitive from the Coordination Functions, and that primitive is the result of a message being received, the input symbol bears the name of the message and any remote operations APDU(s) or notification(s) contained in that message. In the case of a message specified in ISO/IEC 11572, basic call actions associated with the receipt of that message are deemed to have occurred.

The following abbreviations are used:

inv.	invoke APDU
res.	return result APDU
err.	return error APDU
rej.	reject APDU
ciRequest	callIntrusionRequest
ciGetCIPL	callIntrusionGetCIPL
ciCompleted	callIntrusionCompleted
ciIsolate	callIntrusionIsolate
ciForcedRelease	callIntrusionForcedRelease
ciWOBRequest	callIntrusionWOBRequest

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

D.1 SDL representation of SS-CI at the Originating PINX

Figure D.1 shows the behaviour of an SS-CI Supplementary Service Control entity within the Originating PINX.

Input signals from the left and output signals to the left represent primitives from and to the user, or an entity acting on behalf of the user.

Input signals from the right and output signals to the right represent primitives from and to the coordination functions in respect of messages sent and received. Protocol timer expiry and basic call release are also indicated by an input signal from the right.

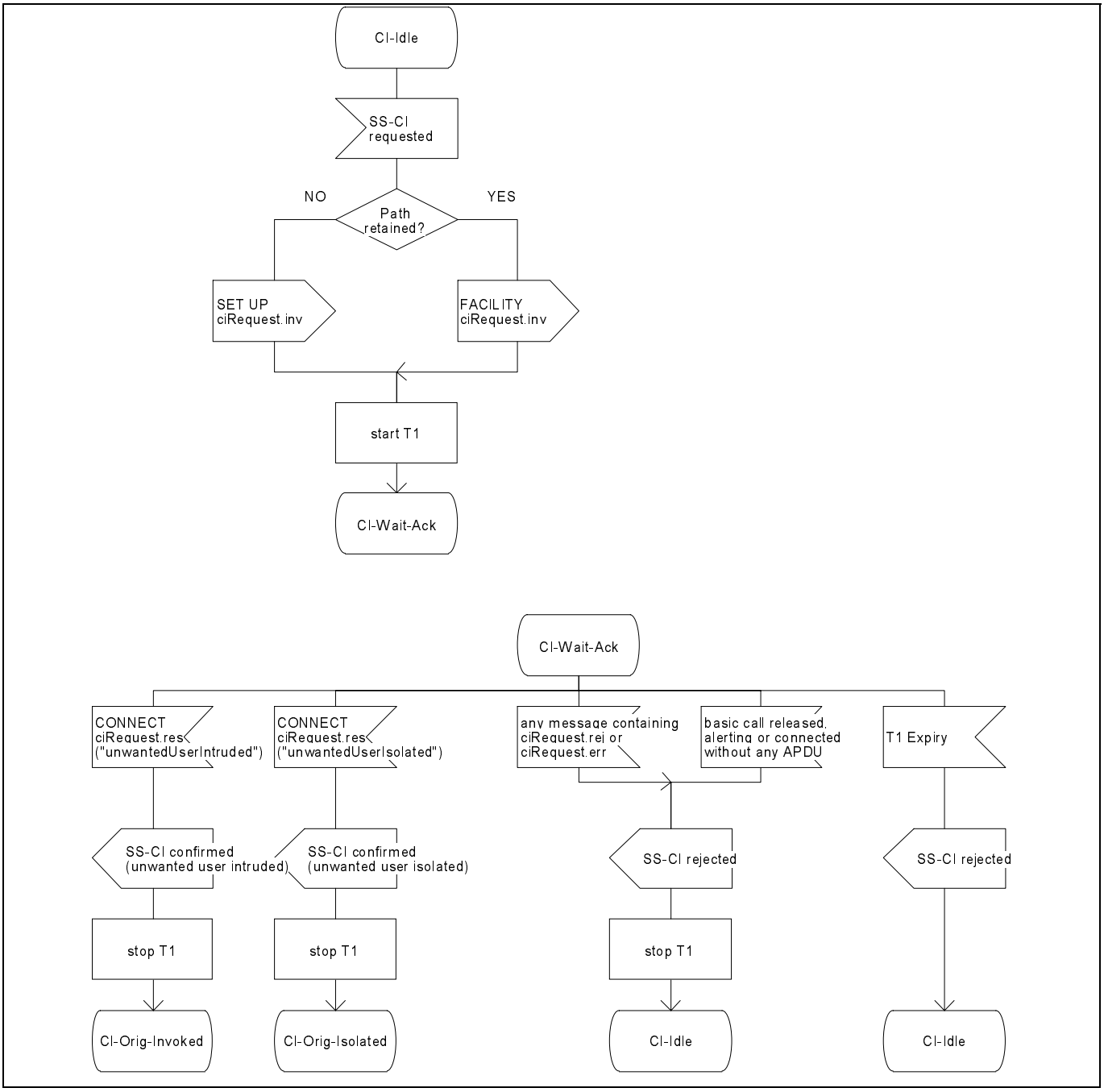


Figure D.1 (sheet 1 of 6) - Originating PINX SDL

--`,,`-`-`,,`,,`,`,,`---
© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

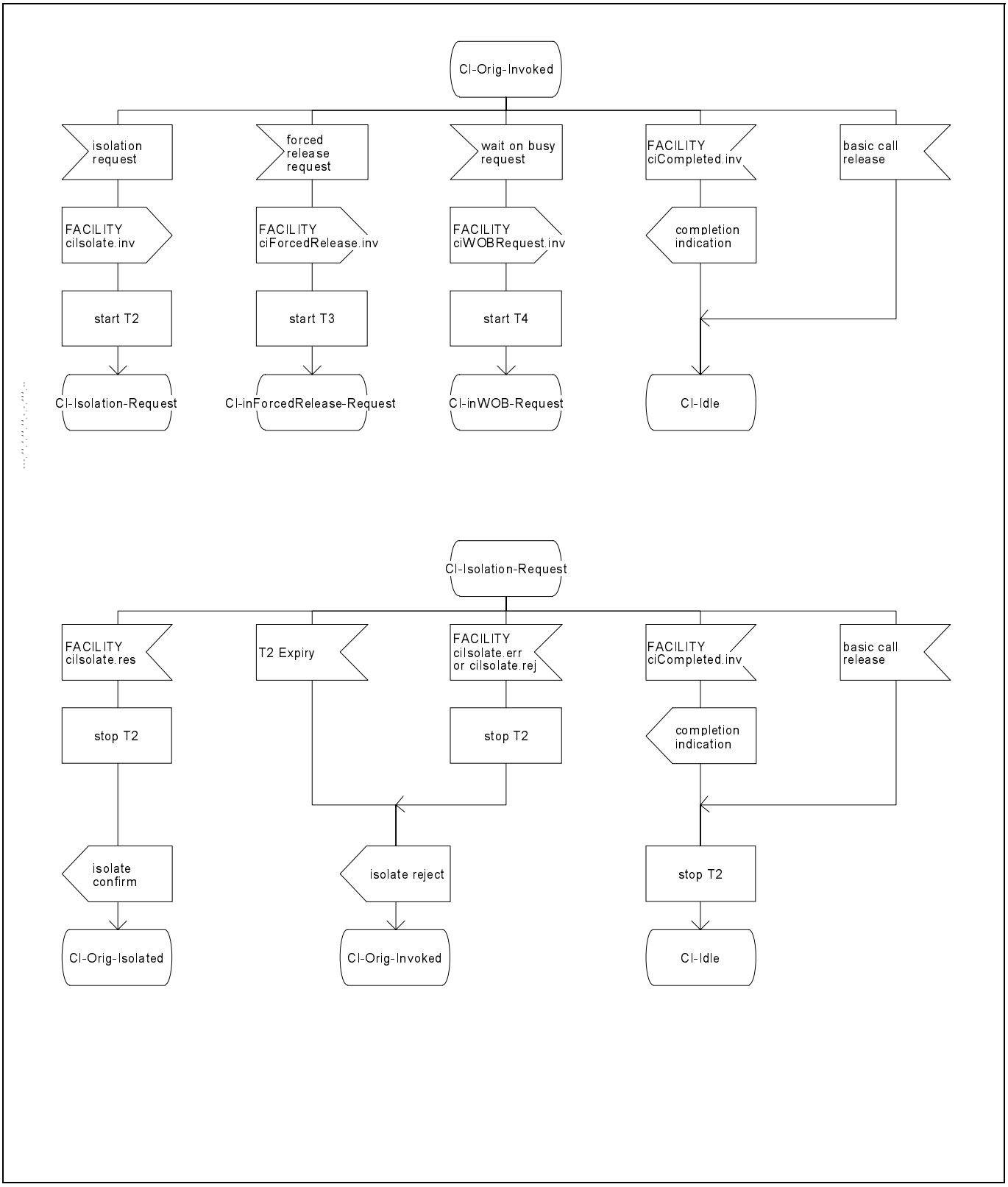


Figure D.1 (sheet 2 of 6) - Originating PINX SDL

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

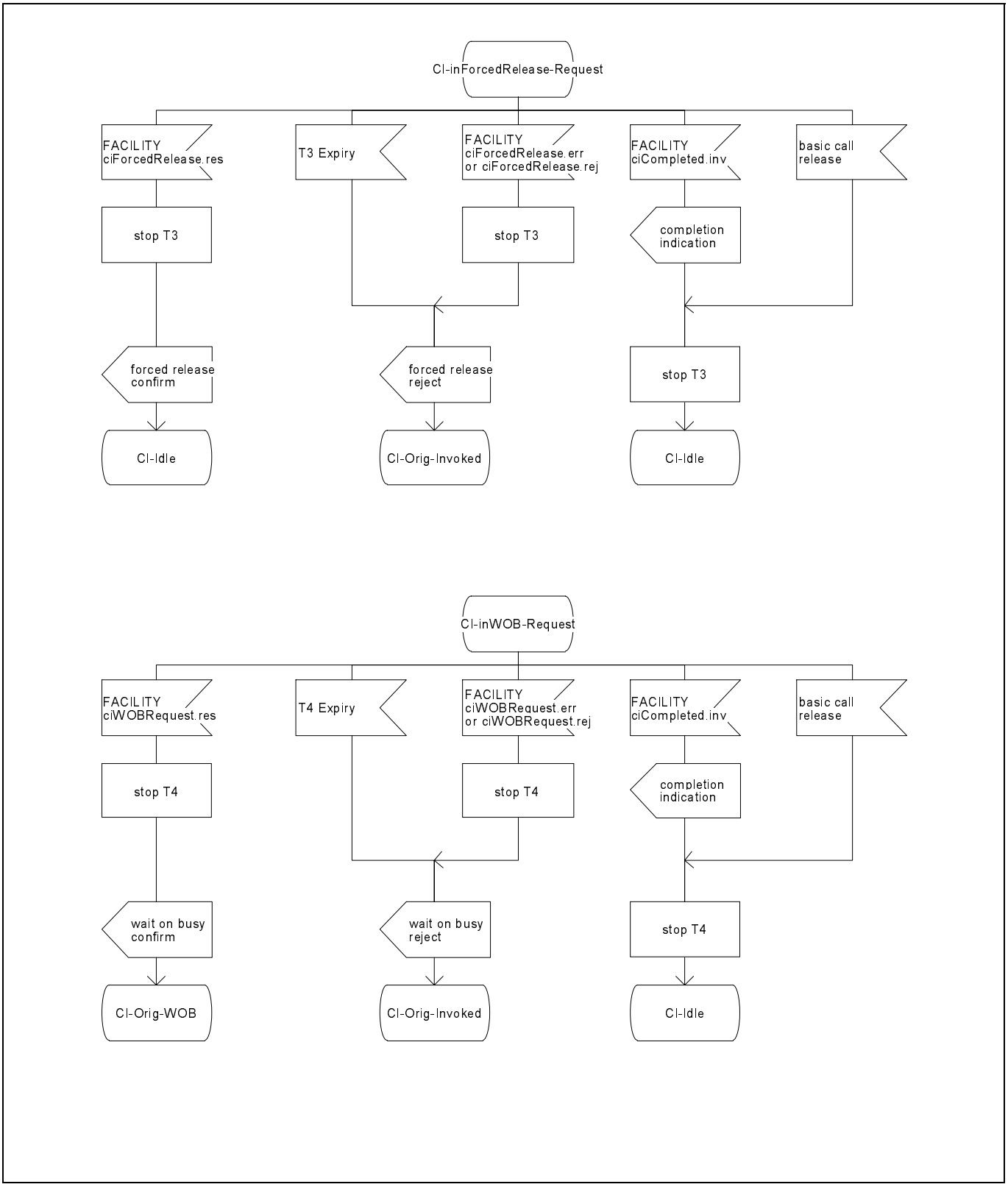


Figure D.1 (sheet 3 of 6) - Originating PINX SDL

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

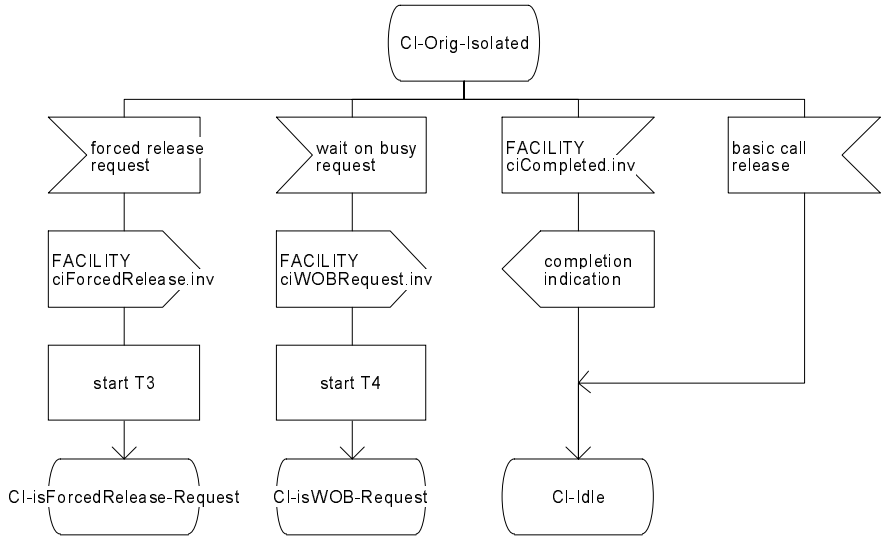


Figure D.1 (sheet 4 of 6) - Originating PINX SDL

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

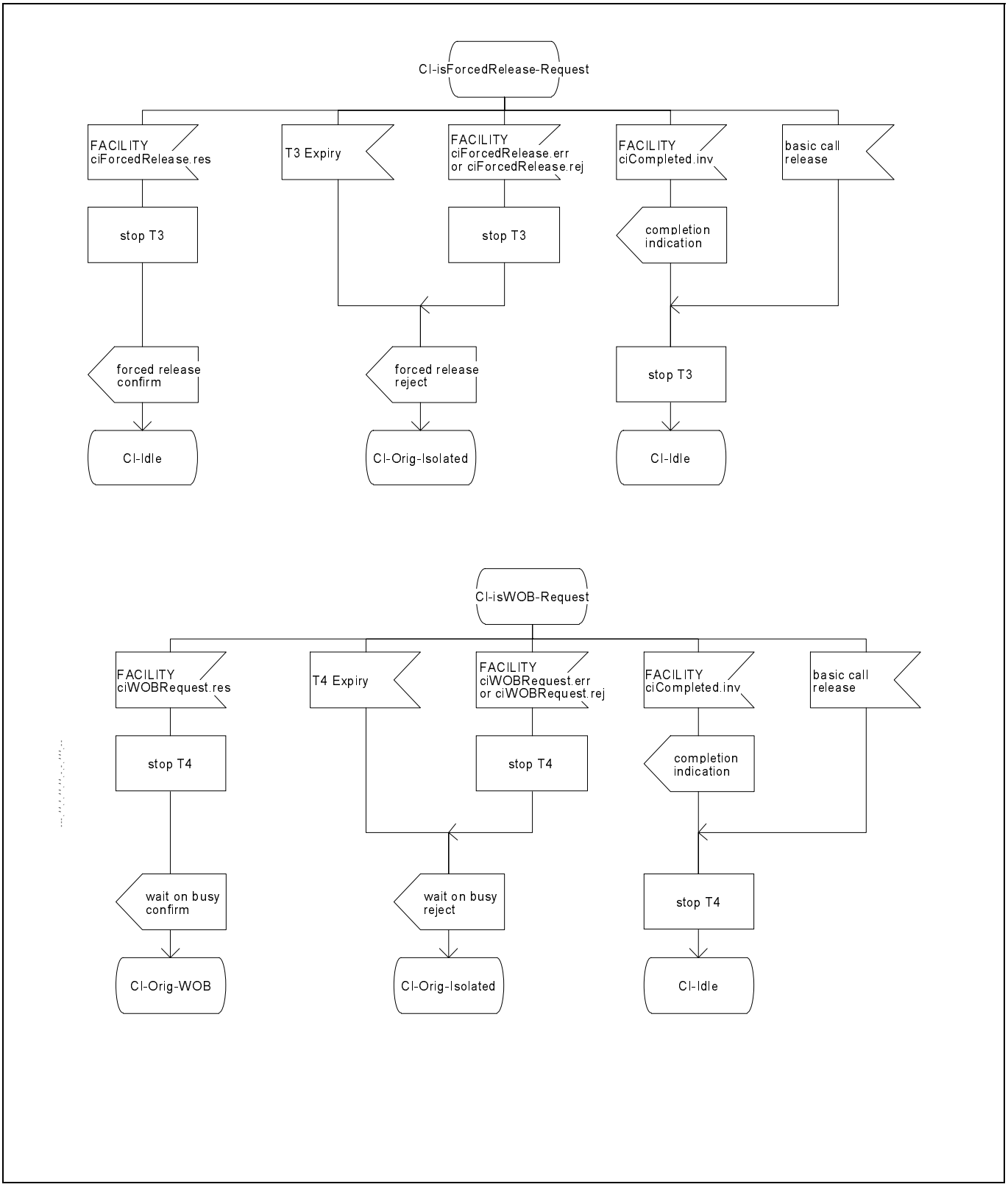


Figure D.1 (sheet 5 of 6) - Originating PINX SDL

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

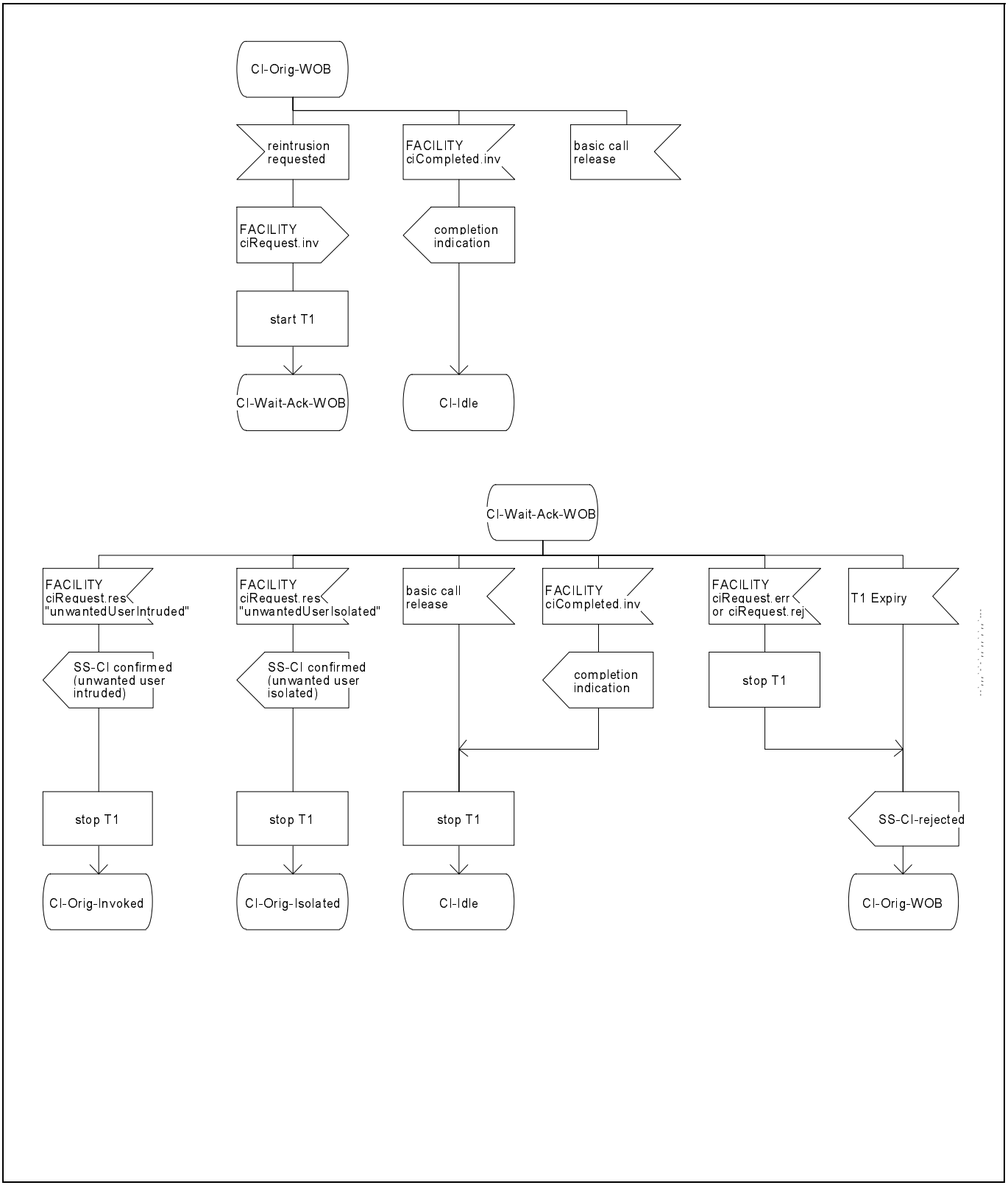


Figure D.1 (sheet 6 of 6) - Originating PINX SDL

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

D.2 SDL representation of SS-CI at the Terminating PINX

Figure D.2 shows the behaviour of an SS-CI Supplementary Service Control entity within the Terminating PINX.

Input signals from the left and output signals to the left represent primitives from and to the coordination functions. Protocol timer expiry and basic call release are also indicated by an input signal from the left.

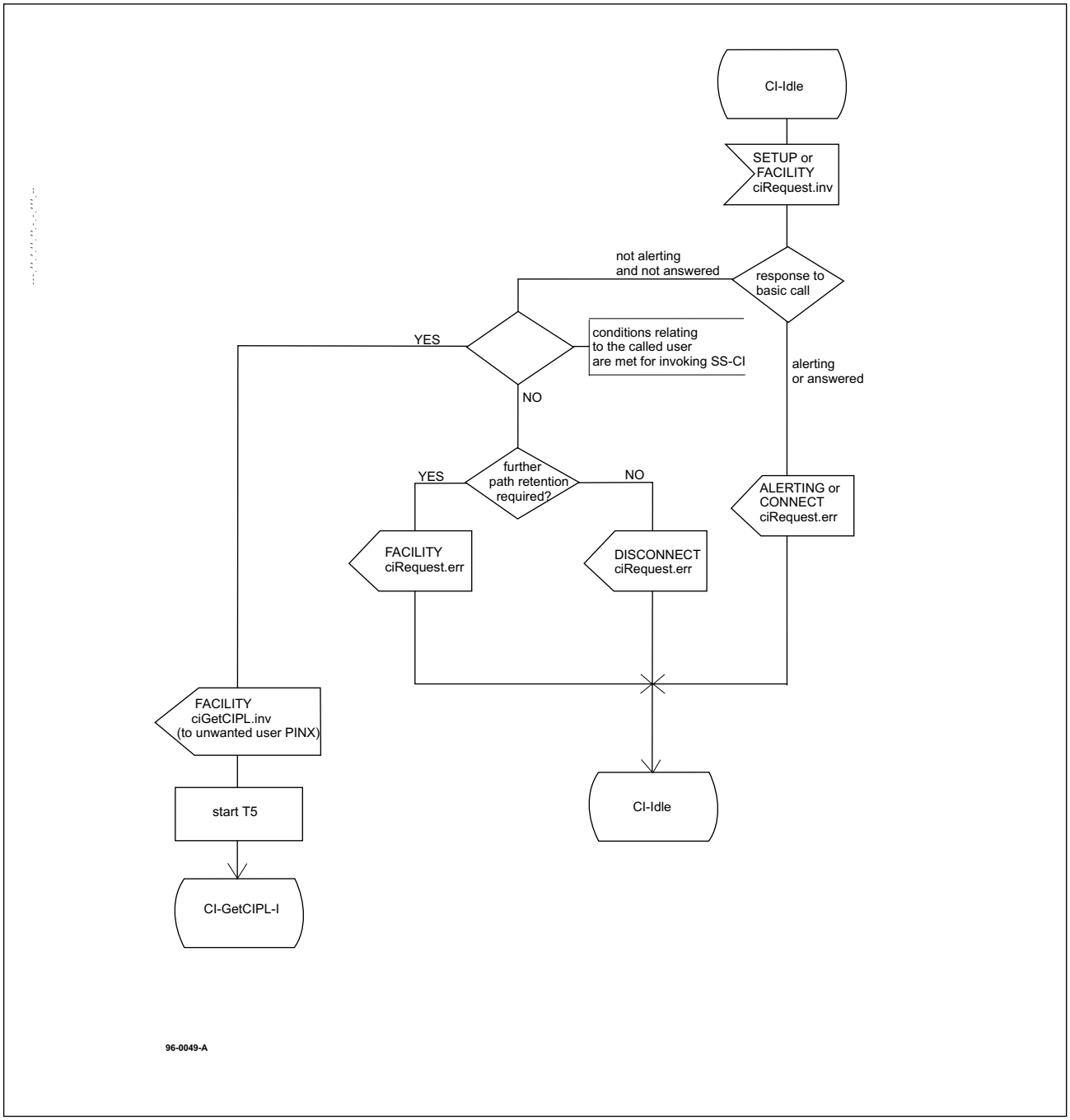


Figure D.2 (sheet 1 of 6) - Terminating PINX SDL

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

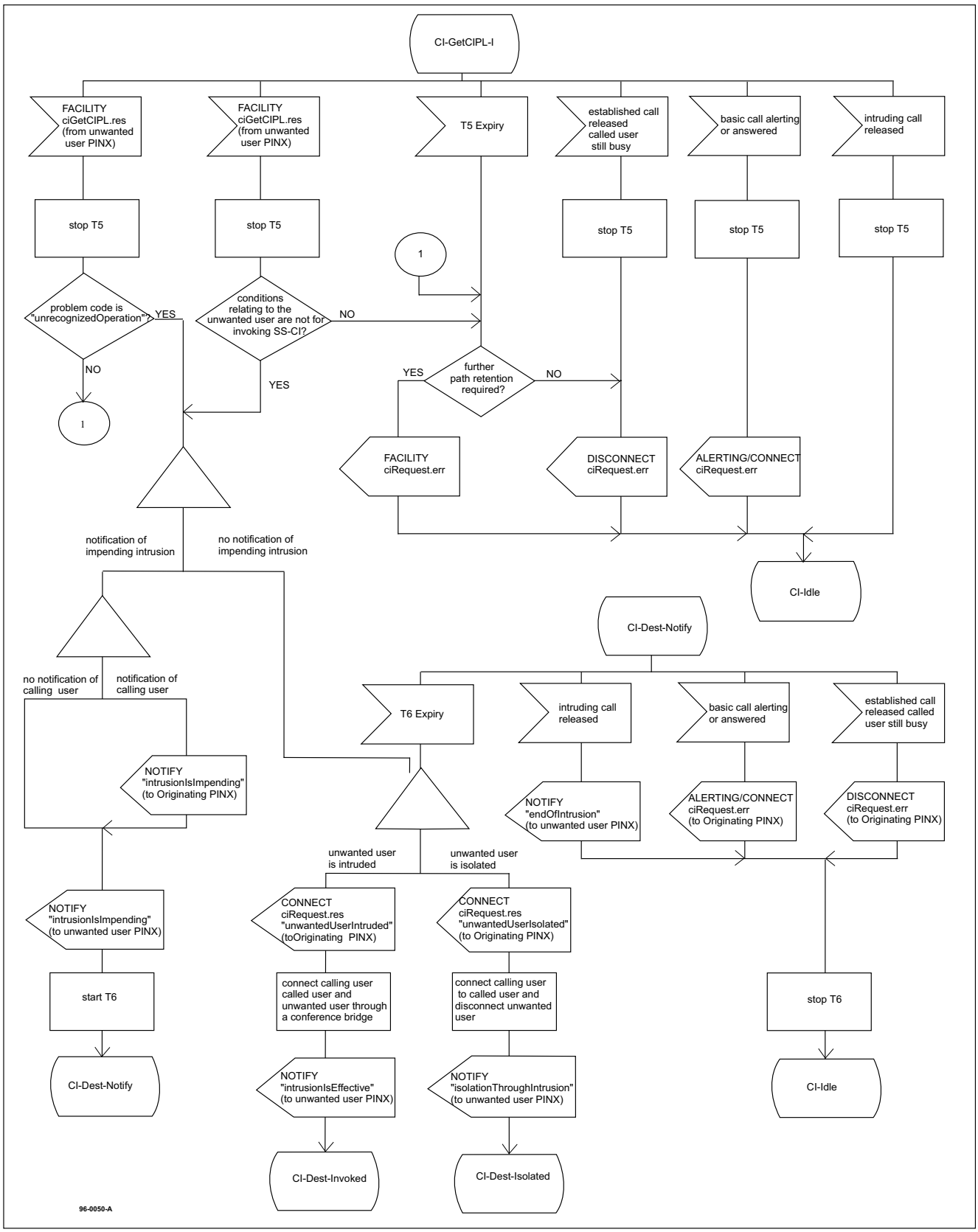


Figure D.2 (sheet 2 of 6) - Terminating PINX SDL

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

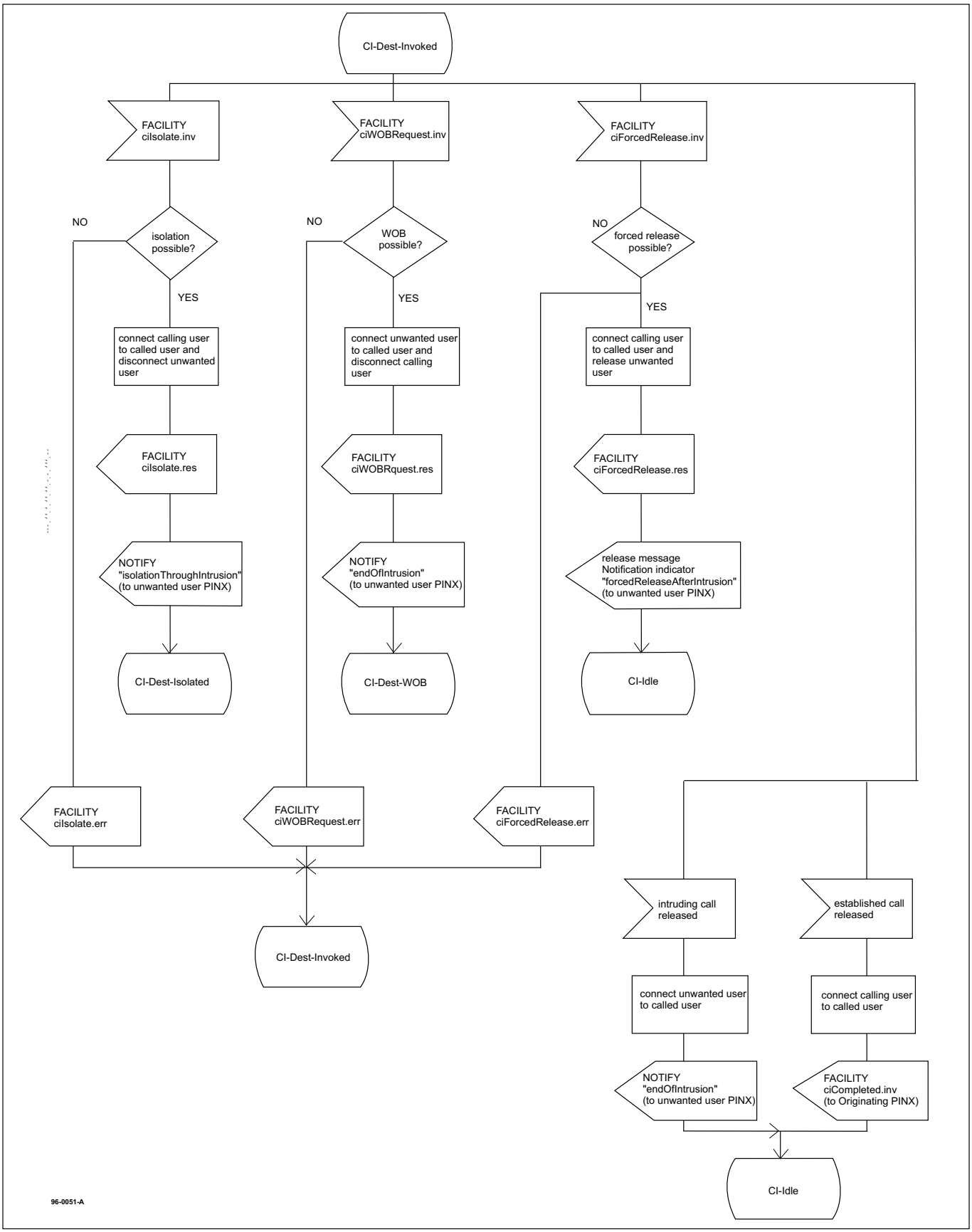


Figure D.2 (sheet 3 of 6) - Terminating PINX SDL

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

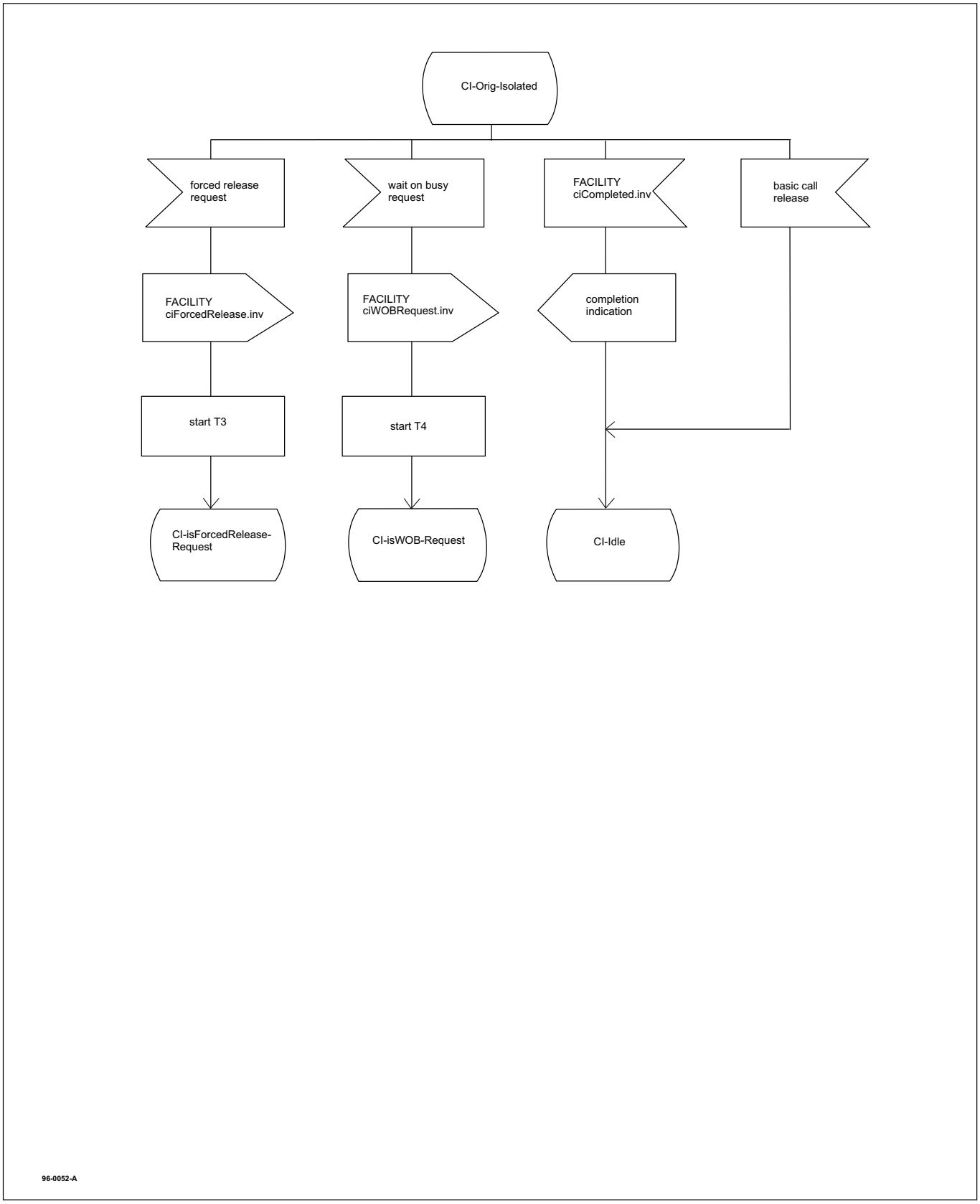


Figure D.2 (sheet 4 of 6) - Terminating PINX SDL

--`,,,`-`-`,,`,,`,`,,`---

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

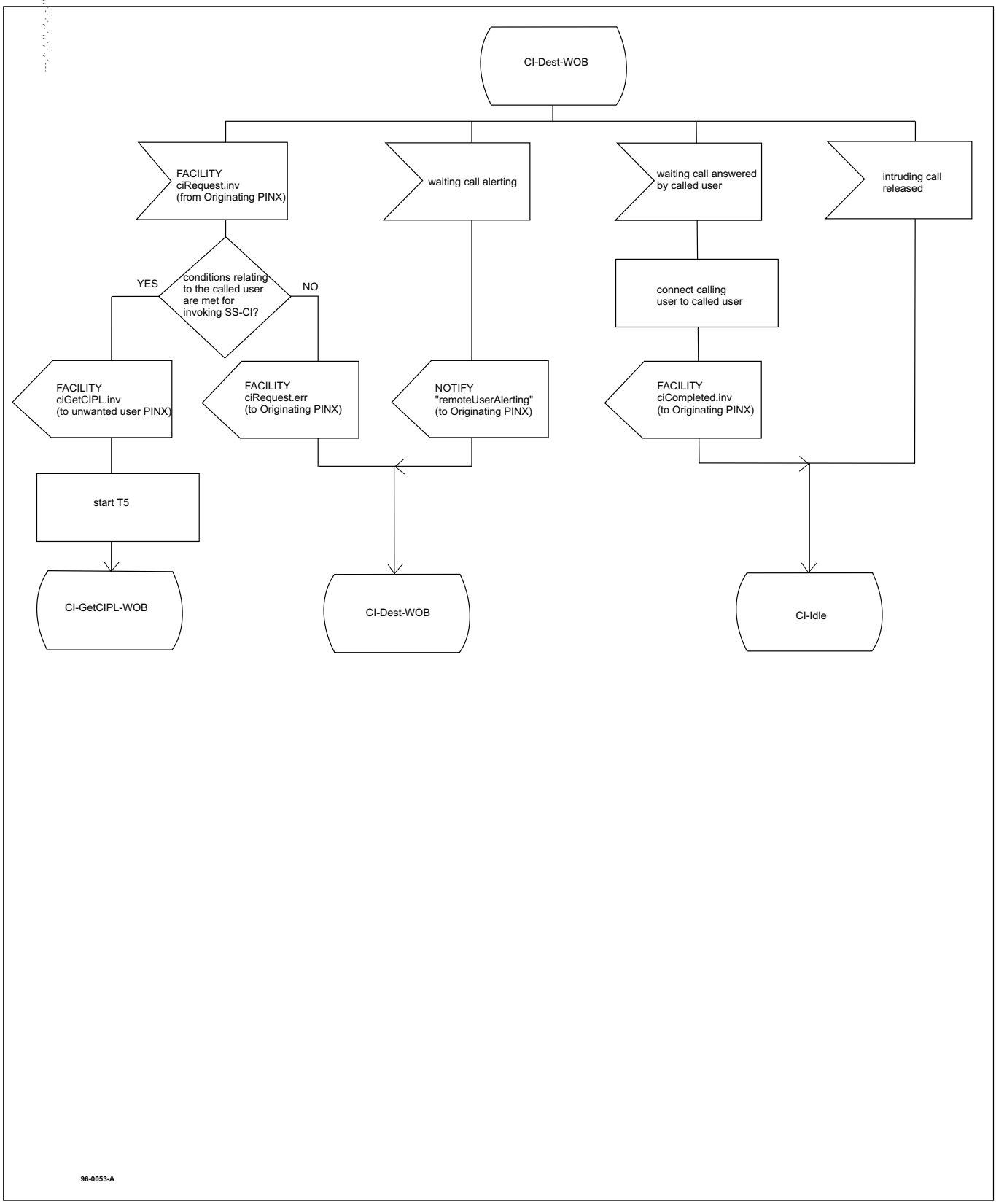


Figure D.2 (sheet 5 of 6) - Terminating PINX SDL

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

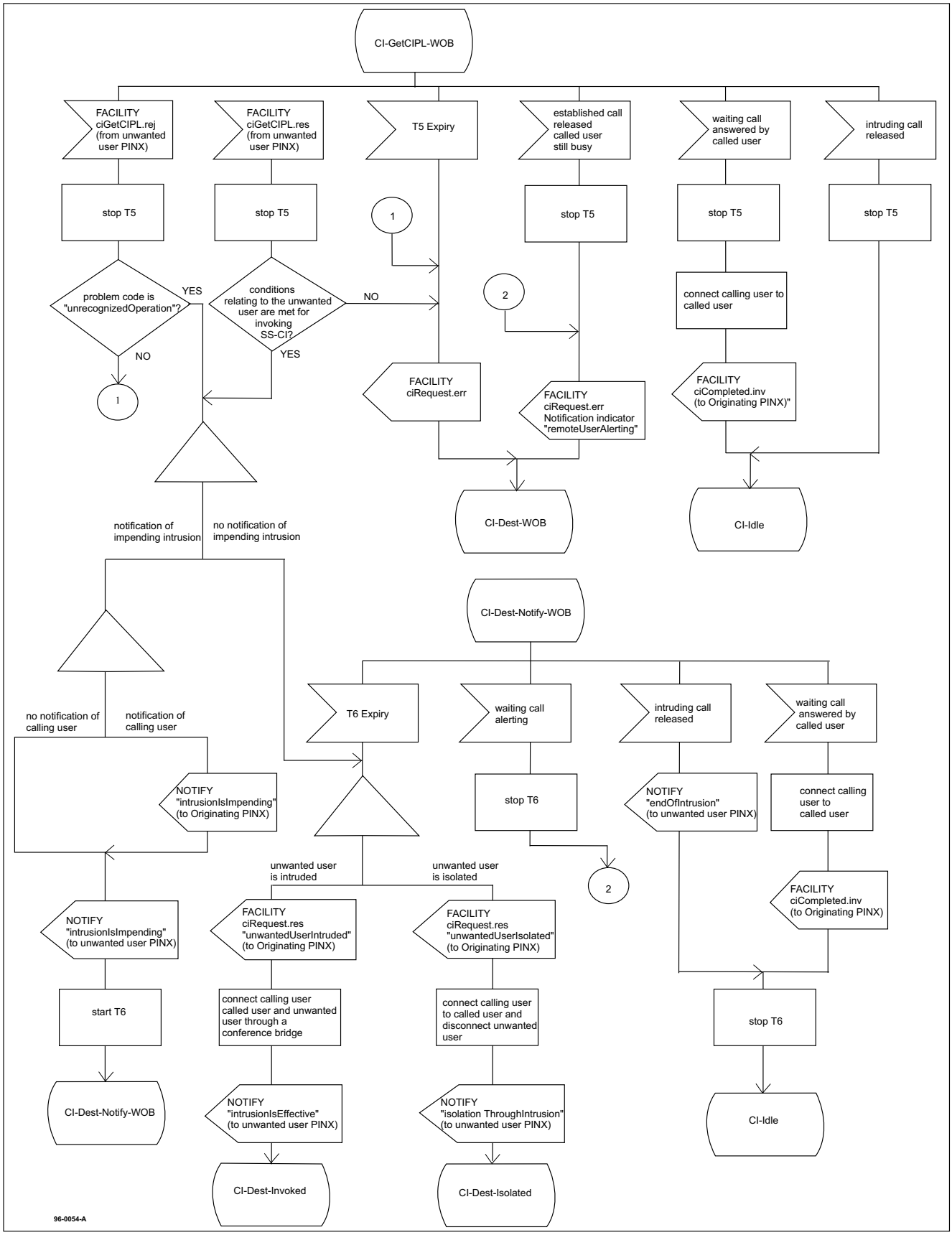


Figure D.2 (sheet 6 of 6) - Terminating PINX SDL

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex E
(informative)

Imported ASN.1 definitions

The content of this annex has been deleted to remove duplicate ASN.1 definitions defined elsewhere.

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex F
(normative)

ASN.1 definitions according to ITU-T Recs. X.208 / X.209

This annex lists all ASN.1 modules as they were defined in the second edition of ISO/IEC 14846, i.e. based on ITU-T Recommendations X.208 / X.209. Starting with this edition the ASN.1 modules within ISO/IEC 14846 comply with ITU-T Recommendations X.680 / X.690. Please note that regardless of which version of these modules is used as a base of a QSIG implementation, the line encoding remains unchanged. Changes in future editions to modules based on X.680 / X.690 ASN.1 are not reflected in the modules in this annex.

Table F.1 - Call-Intrusion-Operations – based on ITU-T Recs. X.208 / X.209

```
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       CIRequestArg
                             RESULT         CIRequestRes
                             ERRORS     {notAvailable, notBusy, temporarilyUnavailable, notAuthorized,
                                         unspecified, supplementaryServiceInteractionNotAllowed}

CallIntrusionGetCIPL    ::=  OPERATION
                             ARGUMENT       DummyArg
                             RESULT         CIGetCIPLRes

CallIntrusionForcedRelease::= OPERATION
                             ARGUMENT       DummyArg
                             RESULT         DummyRes
                             ERRORS         {notAvailable, unspecified,
                             supplementaryServiceInteractionNotAllowed}
```

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table F.1 - Call-Intrusion-Operations – based on ITU-T Recs. X.208 / X.209 (continued)

```
CallIntrusionIsolate        ::=  OPERATION
                                     ARGUMENT        DummyArg
                                     RESULT          DummyRes
                                     ERRORS          {notAvailable, unspecified,
                                     supplementaryServiceInteractionNotAllowed}

CallIntrusionWOBRequest ::=  OPERATION
                                     ARGUMENT        DummyArg
                                     RESULT          DummyRes
                                     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 CICapabilityLevel,
                                     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}
```

--`,,`-`-`,,`,,`,`,,`---

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table F.1 - Call-Intrusion-Operations – based on ITU-T Recs. X.208 / X.209 (concluded)

```
CIGetCIPLRes            ::= SEQUENCE{
                                ciProtectionLevel CIProtectionLevel,
                                resultExtension     CHOICE{
                                        extension           [1] IMPLICIT Extension,
                                        sequenceOfExtn      [2] IMPLICIT SEQUENCE OF
                                                                Extension} OPTIONAL}

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 CICL

Unspecified             ::=     ERROR PARAMETER Extension

unspecified             Unspecified ::= 1008

END                     -- of Call-Intrusion-Operations
```

© ISO/IEC 2003 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table F.2 - Call-Intrusion-Notifications – based on ITU-T Recs. X.208 / X.209

```
Call-Intrusion-Notifications
                                        {iso(1) standard(0)
                                        pss1-call-intrusion(14846) call-intrusion-notifications(1)}

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

IMPORTS                         NOTIFICATION FROM Notification-macro
                                {iso(1) standard(0)
                                pss1-generic-procedures(11582) notification-macro(10)};

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
```

--`,,`-`-`,,`,,`,`,,`---

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 33.040.35

Price based on 64 pages

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale