ND1113:1999/06

PNO-ISC/INFO/013

Recommendations for Non-Circuit Related Signalling to support Service Provider Access Interface

Network Interoperability Consultative Committee
Oftel
50 Ludgate Hill
London
EC4M 7JJ
UK

http://www.oftel.gov.uk/ind_groups/nicc/

PNO-ISC INFORMATION DOCUMENT 013

Recommendations for Non-Circuit Related Signalling to support Service Provider Access Interface

NETWORK INTEROPERABILITY CONSULTATIVE COMMITTEE
Office of Telecommunications
50 Ludgate Hill
London EC4M 7JJ

0.2 Normative information

All enquiries about distribution reproduction, changes and clarifications should be addressed in the first instance to the Chairman of the NICC/PNO-IG/ISC at the address on the title page.

DISCLAIMER The contents of this information document have been agreed by the NICC. The information contained herein is the property of the NICC and is supplied without liability for errors or omissions.

SEE PAGE 2 FOR THE NORMATIVE INFORMATION

0.3 Contents

0.4 History

Revision	Date of Issue	Editor	Description
Issue 1	June 1999	J.D.Humphrey Marconi Communications	First published version

0.5 Issue control

PAGE	ISSUE	DATE
All	Issue 1	June 1999

0.6 References

[1] ITU-T Recommendation Q.1214 March ‘95 Distributed Functional Plane for Intelligent Networks Capability Set 1 (CS1)
[2] ITU-T Recommendation Q.1215 March ‘95 Physical Plane for Intelligent Networks Capability Set 1CS1

[3]‘ ETSI 300 374 (Part 1) Intelligent Network Application Protocol Capability Set 1 (CS1)
[4] ETSI 300 374 (Part 5)) Intelligent Network Application Protocol Capability Set 1 (CS1)
[5] ETSI EN 301 140-1 (Part 1)) Intelligent Network Application Protocol Capability Set 2 (CS2)CS2 Core INAP
[6] ETSI EN 301 140-5 (Part 5)) Intelligent Network Application Protocol Capability Set 2 (CS2) Distributed Functional Plane
[7] PNO-ISC Information Document 010 - Recommendations for Short Term Solutions to support Service Provider Access Interface
[8] ITU-T Recommendation Q.1225 Physical Plane for Intelligent Networks Capability Set 2 (CS2)
[9] ITU-T Recommendation Q.1224 Distributed Functional Plane for Intelligent Networks Capability Set 2 (CS2)
[10] ETSI EN 301 070-1 ISDN User Part (ISUP) Version 3 Interactions with the Intelligent Network Application Part (INAP)

0.7 Glossary of terms

ASE	Application Service Element
API	Application Programming Interface
APM	Application Transport Mechanism
CAMEL	Customised Applications for Mobile network Enhanced Logic
CCAF	Call Control Agent Function
CCF	Call Control Function
CS1/2/3	Capability Set 1/2/3
CUSF	Call Unrelated Services Function
DFP	Distributed Functional Plane
GSM	Global System for Mobile communication
HIRp	Handling Information Result
HIRq	Handling Information Request
IAM	Initial Address Message
IDP	Initial Detection Point
IETF	Internet Engineering Task Force
INAP	Intelligent Network Application Protocol
INSC	Intelligent Network Service Compatibility
IP	Internet Protocol
ISUP	ISDN User Part
LE	Local Exchange
MTP	Message Transfer Part
SCCP	Signalling Connection Control Part
SCF	Service Control Function
SCP	Service Control Point
SCUAF	Service Control User Agent Function
SDF	Service Data Function
SII	Service Interaction Indicator
SRF	Specialised Resources Function
SSF	Service Switching Function
SSP	Service Switching Point

0.8 Scope

This Information Document is limited to describing the possible IN architectures which could be used to realise Non-Circuit Related signalling in support of a Service Provider Access Interface.

SEE PAGE 2 FOR THE NORMATIVE INFORMATION

1 IN ARCHITECTURES

The IN standards provide a range of network capabilities which allow for distribution of functions and therefore options for interconnection between the IN domains. To satisfy the Service Provider Non-Circuit Related requirements, as defined in [7], four options are considered:

- ETSI CS1 Core INAP (SCF-SDF interface)
- ETSI CS1 Core INAP (SCF-SSF interface or interface subset)
- ETSI CS1 Core INAP (SCF-SSF interface or interface subset and SRF located in Service Provider domain)
- ETSI CS2 Core INAP (SCF-SCF interface)

The network architecture model assumed for the short term solution, refer [7], is also relevant to the options described in this section. The Service Provider domain may be attached to an originating, terminating or transit network. Since the Service Provider operates a distinct domain to the Network Operator, the IN interfaces selected for interconnection with the Service Provider will, by usage, be inter-network interfaces even if some of these interfaces are not designated as such within the standards. This may have implications on the licensing status of those Service Providers able to gain access to these interfaces.

1.1 ETSI CS1 Core INAP (SCF-SDF interface)

Figure 1 illustrates the application of IN CS1 functional architecture for Service Provider Access. For further information on the IN CS1 Functional Architecture refer to [1] and the mapping from the functional architecture to the Physical Entities refer to [2].

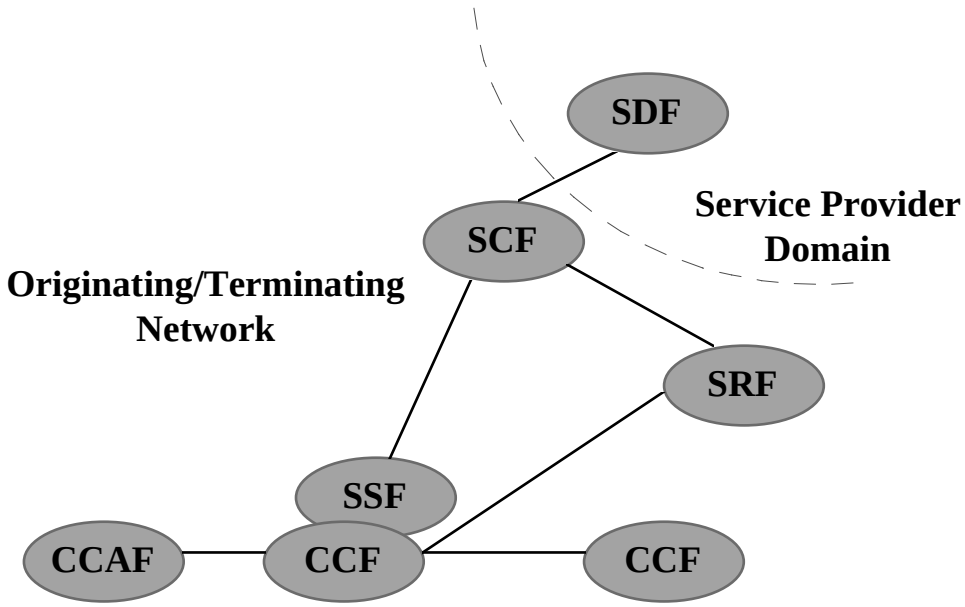

Figure 1 - Option 1 ETSI CS1 Core INAP

Notes:

1. ETSI CS1 Core INAP only supports one standardised interface for internetwork IN communication and that is SCF-SDF.
2. Both service logic and triggering would be provided by the Network Operator. This means that the Network Operator would create the Service Logic and the management of the trigger criteria would be under the control of the Network Operator. Obviously the Service Provider would provide the Network Operator with the Service Description and triggering requirements.
3. Access to the Service Providers SDF would be via X.500 based INAP protocol. For further information on the INAP protocol used on this interface and SCF-SSF and SCF-SRF interfaces refer to [2] [3] and [9]. Note that access to the SDF would mean that a common data model will be shared between the Service Provider and Network Operator providing the service logic.
4. Access to SRF capabilities would be controlled by the Network Operator (note that the SCF-SRF interface is not an open internetwork interface), this would mean that the usage of any existing announcements, or creation of new announcements, would be via agreement with the Network Operator.
5. Availability of signalling information to the Service Logic would depend on the capabilities of (a) SSP which triggers the service and (b) underlying network signalling and also SSP rollout status within the network.
6. Service Management would be under the control of the Network Operator. The Service Provider would provide the Network Operator with sufficient customer information to enable the service to be provisioned.
7. Billing information will be generated by the Network Operator and may be provided to the Service Provider as a part of the service. Billing and settlement arrangements between the Network Operator and the Service Provider would be expected to form part of the bilateral negotiations and are outside the scope of this document.

1.2 ETSI CS1 Core INAP (SCF-SSF interface or interface subset)

Using the same IN DFP architecture as described in the previous subsection, this option considers the use of the SCF-SSF interface. Either the full CS1 operation set is used or a subset of the operations is defined. A subset of operations would be similar to the CAMEL interface developed for GSM except that some of the CAMEL parameter extensions would not be required and a different Operation set may be required. For example, the Call Gap operation could be included and its use restricted to specific numbers owned by the Service Provider. The choice between the use of a full operation set and a subset is a matter for bilateral negotiation between the Network Operator and Service Provider. To simplify the use of an operation subset across SSF-SCF interface, a UK standard set of operations could be defined and this would be based on the UK extensions to INAP. Figure 2 describes this option.

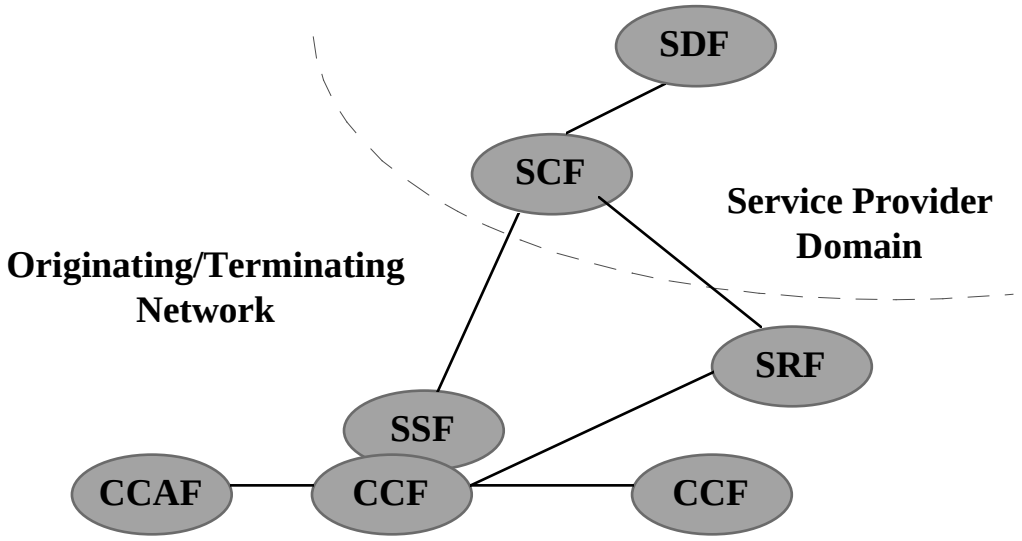

Figure 2 - Option 2 IN CS1 architecture using an SCF-SSF interface or interface subset

Notes:

1. The SCF capabilities and Service Creation Environment would be provided by and under the control of the Service Provider. However, to create the service will require network specific information from the network triggering the service (e.g. signalling information available from the network).
2. The Service Provider SCF could be connected to SSPs in different networks, therefore the Service Logic design should be sufficiently robust and generic to accommodate interworking with different SSP variants.
3. While management of the Service Creation Environment would be under the control of the Service Provider, some aspects of the Service Management would be controlled by the Network Operator. For example, provisioning of the service would require co-ordination between the Network Operator (for triggering, availability of signalling information, announcements, testing etc.) and Service Provider (service logic). Joint testing between the Network Operator and Service Provider is required when introducing new services and those service modifications involving changes to the signalling information flows across the interface.
4. Triggering would be controlled and managed by the Network Operator. The Service Provider must provide the Network Operator with the relevant service information (i.e. triggering information plus sufficient service information that would enable the Network Operator to determine the scope of the interactions across the SCF-SSF interface, for example, call rates, call duration, resources used, user interactions etc.). All triggers would be statically armed, dynamic triggers would not be supported. Triggers may be armed in some or all of the Network Operators SSPs, the decision as to which option to choose is a matter for bilateral negotiation between the Network Operator and Service Provider, this aspect is outside the scope of this document. The mechanism used by the Service Provider and Network Operator to manage the triggers and related data is also outside the scope of this document.
5. The inter-network use of the SCF-SSF and SCF-SRF interfaces is not recognised in CS1 (or CS2) therefore, security across these interfaces is limited, i.e. they assume intra-network use. Additional security arrangements may therefore be required by either the Network Operator or the Service Provider as part of bilateral negotiations that would need to take place between a Service Provider and a Network Operator for implementation of this interface between the two parties. Such arrangements are outside the scope of this document.
6. The SCF-SRF interface may not be a real-time interface but a management interface. The choice of a suitable interface to the SRF is a matter of bilateral negotiation between the Network Operator and the Service Provider, such arrangements are outside the scope of this document.

7. Access to the Service Providers SCF would be via the INAP protocol. Note that INAP would normally operate across MTP and SCCP however, in view of UK interconnect difficulties (e.g. number of Point Codes) it may be more appropriate to use other lower layer protocols to carry the INAP messages. For more information on the INAP protocol used on these interfaces refer to [2] and [3]
8. In the case where the full SCP-SSP interface is not used, and a subset only is required, the creation of this subset of the SCF-SSF INAP protocol would require new ASE's and Application Contexts to be defined. This means that implementations would require change and all SSPs within a network, which would trigger the Service Provider services, would need to be upgraded before they could be used.
9. Billing information will be generated by the Network Operator and may be provided to the Service Provider as a part of the service. To protect against misuse, INAP billing operations (FCI and SCI) may not be supported across the Service Provider interface (see 8 above). Even without INAP billing operations support, certain usage of the INAP protocol (SCF-SSF) can cause billing inaccuracies, or create problems for downstream billing systems, affecting customer or interadmin billing. Network Operators and Service Providers must cooperate to avoid such problems. Billing and settlement arrangements between the Network Operator and the Service Provider would be expected to form part of the bilateral negotiations and are outside the scope of the document.

1.3 ETSI CS1 Core INAP (SCF-SSF interface or interface subset and SRF located in Service Provider domain)

This option is distinguished from option 1.2 in that the SRF resides in the Service Provider Domain, refer to figure 3. This allows the SCF-SRF interface to be intra-network and allows the Service Provider to design and develop SRF functionality and to co-ordinate service management of SCF and SRF platforms.

IN supports a number of interconnection scenarios for the SRF and these are described in more detail in section 7.1.3 of ETSI CS1 Core INAP [3]. This option does not preclude any of these scenarios. For Service Provider access, the CCF-SRF interface would be an access type interface, typically DSS1. Or in the case where the Service Provider is licensed and already has the use of SS7-based NNI, then the Service Provider would have the option of using this for the CCF-SRF interface however, this may only be possible if the NNI supports the required faciities to enable the correlation of dialogues. The SRF need not necessarily be directly connected to the SSP handling the call. Also, networks which do not support a DSS1 access interface (e.g. GSM networks), may use an intermediate network to connect the SRF.

The SSF-SCF operations used would need to include support for an external Intelligent Peripheral. As with option 1.2, the specific details of the operations used across this interface would be agreed by bilateral negotiation between the Network Operator(s) and Service Provider.

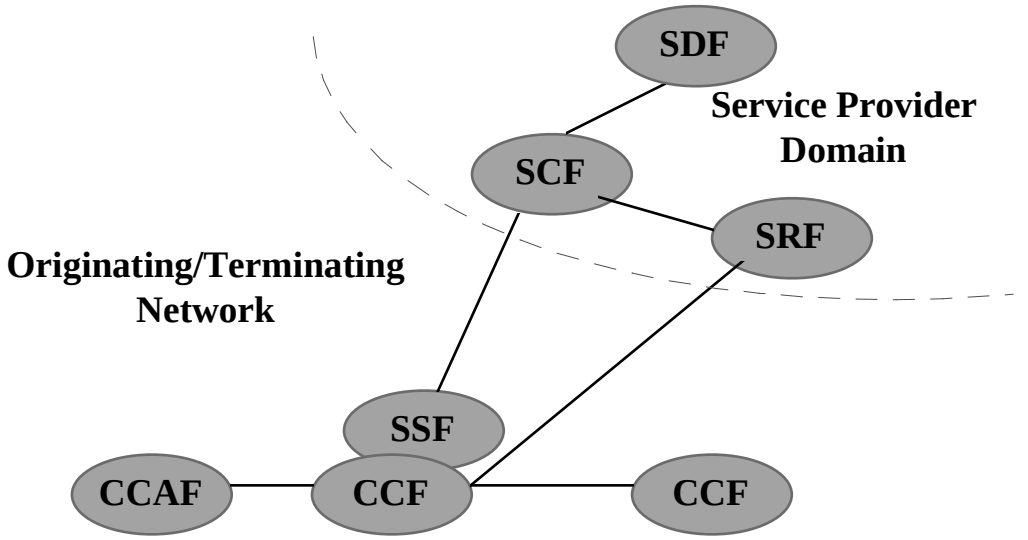

Figure 3 - ETSI CS1 Core INAP (SCF-SSF interface or interface subset and SRF located in Service Provider domain)

Notes:

1. The SCF capabilities and Service Creation Environment would be provided by and under the control of the Service Provider. However, to create the service will require network specific information from the network triggering the service (e.g. signalling information available from the network).
2. The Service Provider SCF could be connected to SSPs in different networks, therefore the Service Logic design should be sufficiently robust and generic to accommodate interworking with different SSP variants.
3. While management of the Service Creation Environment would be under the control of the Service Provider, some aspects of the Service Management would be controlled by the Network Operator. For example, provisioning of the service would require co-ordination between the Network Operator (for triggering, availability of signalling information, testing etc.) and Service Provider (service logic, announcements). Joint testing between the Network Operator and Service Provider is required when introducing new services and those service modifications involving changes to the signalling information flows across the interface.
4. The inter-network use of the SCF-SSF interface is not recognised in CS1 (or CS2) therefore, security across this interface is limited, i.e. they assume intra-network use. Additional security arrangements may therefore be required by either the Network Operator or the Service Provider as part of bilateral negotiations that would need to take place between a Service Provider and a Network Operator for implementation of this interface between the two parties. Such arrangements are outside the scope of this document.
5. Triggering would be controlled and managed by the Network Operator. The Service Provider must provide the Network Operator with the relevant service information (i.e. triggering information plus sufficient service information that would enable the Network Operator to determine the scope of the interactions across the SCF-SSF interface, for example, call rates, call duration, resources used, user interactions etc). All triggers would be statically armed, dynamic triggers would not be supported. Triggers may be armed in some or all of the Network Operators SSPs, the decision as to which option to choose is a matter for bilateral negotiation between the Network Operator and Service Provider, this aspect is outside the scope of this document. The mechanism used by the Service Provider and Network Operator to manage the triggers and related data is also outside the scope of this document..
6. Access to the Service Providers SCF would be via the INAP protocol. Note that INAP would normally operate across MTP and SCCP however, in view of UK interconnect difficulties (e.g.

number of Point Codes) it may be more appropriate to use other lower layer protocols to carry the INAP messages. For more information on the INAP protocol used refer to [2] and [3]

7. Access to SRF capabilities would be controlled by the Service Provider.
8. In the case where the full SCP-SSP interface is not used, and a subset only is required, the creation of this subset of the SCF-SSF INAP protocol would require new ASE's and Application Contexts to be defined. This means that implementations would require change and all SSPs within a network, which would trigger the Service Provider services, would need to be upgraded before they could be used.
9. Billing information will be generated by the Network Operator and may be provided to the Service Provider as a part of the service. To protect against misuse, INAP billing operations (FCI and SCI) may not be supported across the Service Provider interface (see 8 above). Even without INAP billing operations support, certain usage of the INAP protocol (SCF-SSF) can cause billing inaccuracies, or create problems for downstream billing systems, affecting customer or interadmin billing. Network Operators and Service Providers must cooperate to avoid such problems. Billing and settlement arrangements between the Network Operator and the Service Provider would be expected to form part of the bilateral negotiations and are outside the scope of the document.

1.4 ETSI CS2 Core INAP

IN CS2 introduces two new interfaces which can be used for internetworking namely, SDF-SDF and SCF-SCF. This option only considers the use of the new SCF-SCF interface. With this scenario the Service Provider SCF would communicate with the network operator SCF to provide the service. The suitability of other new CS2 capabilities also needs to be considered.

For further information on the IN CS2 Functional Architecture refer to [6] and [9] and the mapping from the functional architecture to the Physical Entities refer to [8].

It should be noted that ETSI CS2 Core INAP is not yet an approved specification, final vote and approval was expected by end '98.

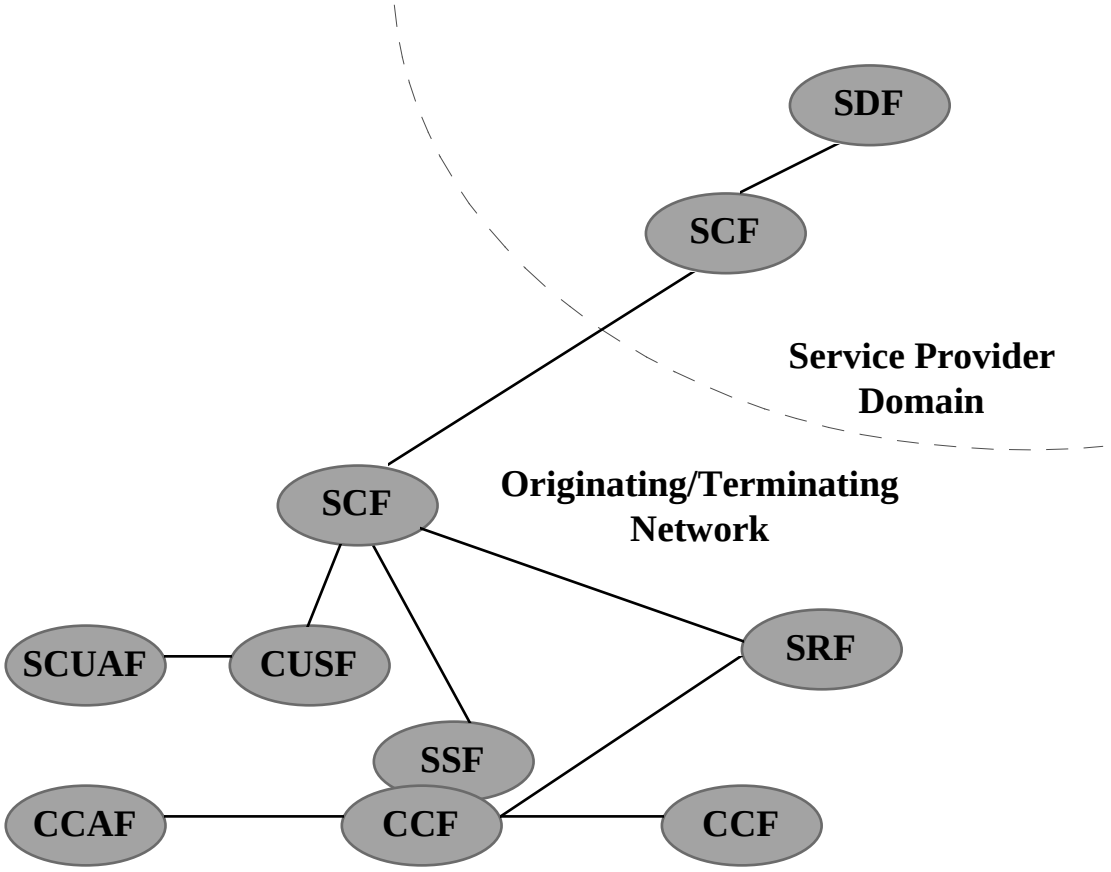

Figure 4 - Option 3 ETSI CS2 Core INAP

Notes:

1. Inter network security across the SCF-SCF interface is specified in [5].
2. Some aspects of the Service Management would be controlled by the Network Operator. For example, provisioning of the service would require co-ordination between the Network Operator (for triggering, availability of signalling information, announcements, testing etc.) and Service Provider (service logic). To ensure that the network can support all the necessary functions required the Service Provider would need to provide a basic Service Description.
3. The SCF capabilities and Service Creation Environment would be provided by and under the control of the Service Provider. However, to create the service will require network specific information from the network triggering the service (e.g. signalling information available from the network).
4. Triggering would be controlled and managed by the Network Operator. The Service Provider must provide the Network Operator with the relevant service information (i.e. triggering information plus sufficient service information that would enable the Network Operator to determine the scope of the interactions across the SCF-SSF interface, for example, call rates, call duration, resources used, user interactions etc). All triggers would be statically armed, dynamic triggers would not be supported. Triggers may be armed in some or all of the Network Operators SSPs, the decision as to which option to choose is a matter for bilateral negotiation between the Network Operator and Service Provider, this aspect is outside the scope of this document. The mechanism used by the Service Provider and Network Operator to manage the triggers and related data is also outside the scope of this document.
5. The use/access to SRF capabilities needs to be determined. For performance reasons the use of the “local” SRF would be the preferred option however, this means that the Network Operator and Service Provider would need to agree on the set of announcements to be used and the

requirements for collecting information from the Service Provider customer. Another option to consider is the SRF being located within the Service Provider Domain. Refer [3] for further information on the options for SRF interaction.

6. Access to the Service Providers SCF would be via the INAP protocol. Note that INAP would normally operate across MTP and SCCP however, in view of UK interconnect difficulties (e.g. number of Point Codes) it may be more appropriate to use other lower layer protocols to carry the INAP messages. For more information on the INAP protocol refer to [5].
7. Billing information will be generated by the Network Operator and may be provided to the Service Provider as a part of the service. Billing and settlement arrangements between the Network Operator and the Service Provider would be expected to form part of the bilateral negotiations and are outside the scope of this document.

2 SERVICE INTERACTION

The purpose of this section is to describe the principles of the service interaction mechanisms available to support IN to ISDN Supplementary Service interaction and IN to IN service interaction. Use of these mechanisms is an essential element in the management of interactions between Network Operator provided services and Service Provider provided services.

2.1 Service Interaction Indicator

The Service Interaction Indicator is a generic mechanism to control the interaction between IN and Network Based Supplementary Services by enabling the IN service to allow/deny or modify ISDN Supplementary Service execution. This indicator is only used across the SCF-SSF interface in the following IN CS2 operations as an optional parameter:

- *Connect*
- *ContinuewithArgument*
- *InitialDP*
- *InitiateCall Attempt*

For a definition of the Service Interaction Indicator refer to ETSI Core INAP CS2 [5]. In addition, for a definition of the mapping between ISUP Indicators and IN Service Interaction Indicators refer to ETSI endorsement of the ITU-T Recommendation Q.1600 [10]. Figure 5 illustrates the basic principles of this mechanism.

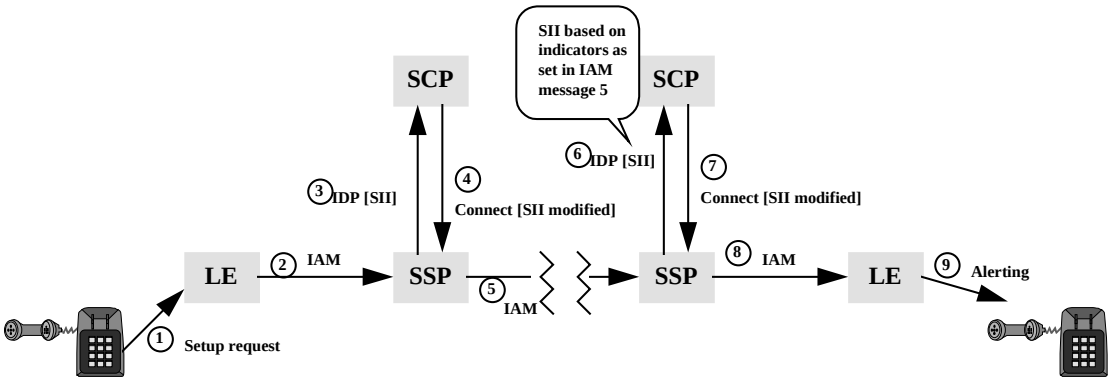

Figure 5 - Service Interaction Indicator Mechanism

2.2 SCF-SCF Service Interaction

SCF-SCF interaction does not make direct use of the Service Interaction Indicators parameter, 3 parameters have been created for the purpose of exchanging supplementary service information between the controlling and supporting SCF. The parameters are:

- *ActivableServices* - this is an optional parameter containing the list of supplementary services that have been activated by the user. Only the information that is available to the controlling SCF can be

provided, this just means deriving the services from the information contained in the *InitialDP* operation. This parameter is transported in the *HandlingInformationRequest* operation.

- *InvokableService* - this is an optional parameter containing the list of supplementary services that have been invoked by the user. Only the information that is available to the controlling SCF can be provided, this just means deriving the services from the information contained in the *InitialDP* operation. This parameter is transported in the *HandlingInformationRequest* operation.
- *SupplementaryServices* - this optional parameter is used by two operations, *HandlingInformationResult* and *NetworkCapabilities* (request and response). In the case of *HandlingInformationResult*, the supporting SCF may provide a list of supplementary Services that have been activated by the user. The *NetworkCapabilities* operation can be used by the supporting SCF to request the controlling SCF for a list of the services supported by the network, this can then be used to determine the level of support which can be provided to the user.

Figure 6 illustrates the principles of this mechanism.

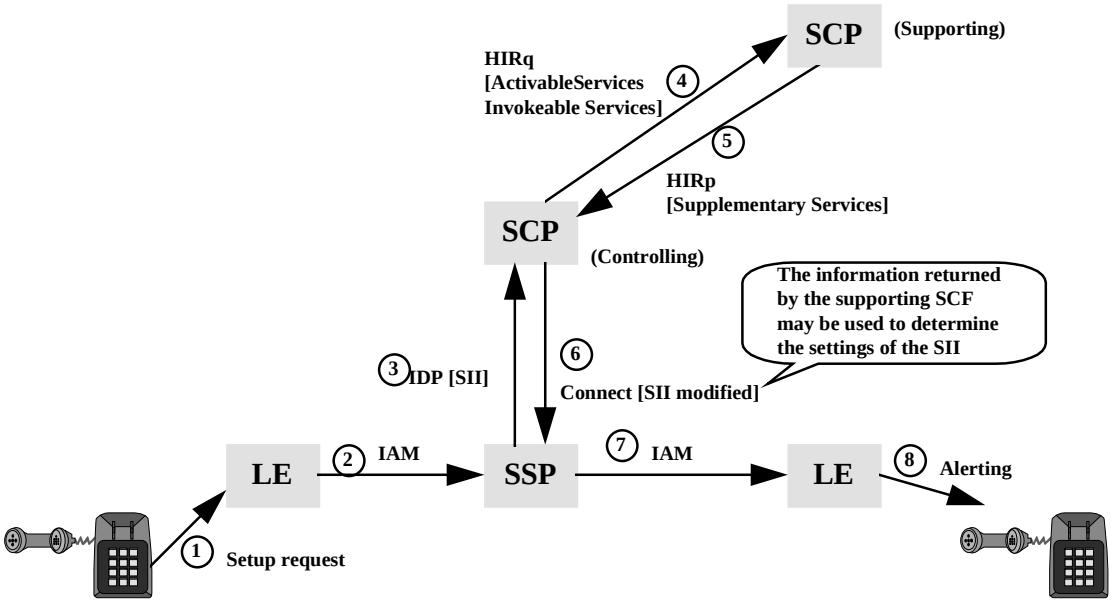

Figure 6 - SCF-SCF Service Interaction Mecahism

2.3 IN/IN Service Interaction - Service Compatibility Indicator

For CS2 additional service compatibility checks have been introduced into the trigger procedure for an IN service. These checks are based on *ServiceCompatibilityID*s which need to be assigned to an IN service by the network operator via trigger table administration. As more than one SSF may be involved in the call it is required that the second IN service is informed about the *ServiceCompatibilityID* of the first IN service. If these SSFs are located in different SSPs (which may also be in different networks) the *ServiceCompatibilityID* is transported by ISUP both in the forwards direction and backwards direction. This indicator is only of relevance for IN Services, there is no impact on existing ISDN supplementary services.

Two INAP parameters have been defined to carry the *ServiceCompatibilityID*:

a) *INServiceCompatibilityResponse*
This is an optional parameter which is created by the SCF service logic, the content of this parameter is a *ServiceCompatibilityID* (known as *Entry*). The parameter may be carried in one of the following operations:

Connect
ContinueWithArgument
InitiateCallAttempt

The parameter is only used by the SSF application procedures to create (or overwrite) the content of the *INServiceCompatibilityIndication*, described below.

b) *INServiceCompatibilityIndication*
This optional parameter is a sequence of *ServiceCompatibilityID*s (known as *Entry*) and is created by the SSF application procedures based on the *INServiceCompatibilityResponse* parameter provided by the SCF. This parameter will be transported by ISUP and will be provided to ISUP during the call establishment phase, i.e. on generation of the IAM from the SSP. If a *INServiceCompatibilityIndication* is received at a preceding or subsequent SSP, then this must be passed to the SSF application procedures where it will be stored and in the case of a subsequent SSP, the information will be passed up to the SCF in the *InitialDP* operation.

The INAP definition of this parameter is as follows:

```
INServiceCompatibilityIndication ::= SEQUENCE SIZE (1..numOfInServiceCompatibilityIndLength) OF Entry

Entry ::= CHOICE {
        agreements          [0] OBJECT IDENTIFIER,
        networkSpecific     [1] Integer4
        }
```

One entry denotes one *ServiceCompatibilityID*. There may be more than one *ServiceCompatibilityID* carried within a message, the maximum number is for further study. The ISUP interworking to support this parameter is in the process of being defined, currently there are proposals to limit the transfer of information to the forwards direction only to limit the volume of traffic generated by this mechanism. Further refinements to this mechanism are still be considered for IN CS3 enhancements.

Figure 7 illustrates the principles of this mechanism.

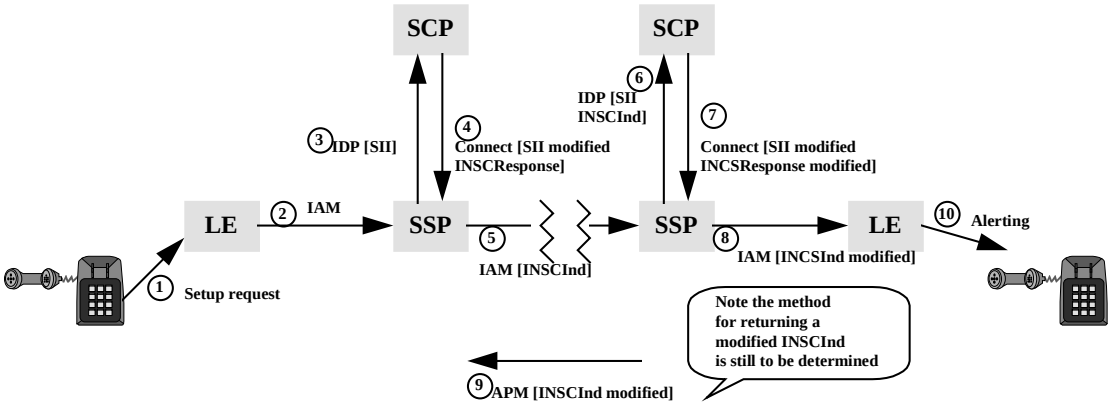

Figure 7 - IN/IN Service Compatibility Indicator Mechanism

2.4 Conclusions

The mechanisms described above are still evolving. For example, there will be further enhancements to the IN-IN service compatibility mechanisms to provide improved support for Multiple Points of Control,

this is the case where more than one SCP controls the call at the same time. The ISUP signalling support to transport this IN-IN service compatibility information has still to be defined. In addition, the SCP-SCP service compatibility mechanism appears to be limited, in terms of capabilities and definition, therefore it is expected that this mechanism will also be revised in the future.

Generally service interaction problems will appear as faults and will be reported as such by the Service Provider to the Network Operator for resolution, due to the Network Operator's greater visibility of the network. This should be taken into consideration in developing the procedures for fault reporting and resolution between the network operator and the Service Provider, again forming part of the necessary bilateral negotiations (see also section 4 below).
To avoid these limitations it is recommended that Network Operators and Service Providers identify potential service interactions and, where possible, eliminate them.

3 SECURITY AND NETWORK INTEGRITY

The IN recommendations (references [3] [4] and [5]) describe a number of mechanisms, namely:

- **Entity Authentication** - these mechanisms are available on the interfaces which are designated as internetwork, SCF-SDF, SDF-SDF, SCF-SCF. This enables an entity in one network to authenticate an entity in another network to confirm that it is what it claims to be, this is generally achieved via the exchange of key information.
- **User Authentication** - via SRF interaction with the user, password (e.g. PIN) verification can be performed.
- **Application Control** - within the INAP protocol an Application Context negotiation mechanism is defined. The Application Context identifies the purpose of a dialogue with another entity, the information provided identifies which version of a protocol will be used and which operations (and parameter set) will be used during the dialogue. If any errors are detected (e.g. use of an unspecified operation) the dialogue will be aborted. The Application Context information is exchanged immediately on opening a dialogue.

Depending on the interfaces used for interworking between the Network Operator and Service Provider, additional security arrangements may be deemed necessary. Such additional arrangements are not described in this document, this is a matter for bilateral negotiation between the Network Operator and Service Provider.

As indicated in the previous section, for service interactions there are no complete solutions therefore no guarantees can be provided for network integrity as a result of a service interaction problem. As before, it is therefore recommended that Network Operators and Service Providers jointly identify potential service interactions and, their potential effect on network integrity so that these can be avoided by joint action.

4 ERROR HANDLING

There are several categories of errors to consider:

- Fault reporting (e.g. who does the customer complain to?);
- Fault distribution (e.g. network domain or service provider domain?);
- Misuse of protocol operation-operation.

The first two can be considered as administrative and management issues at the customer level. These types of error are outside the scope of this document. Otherwise, providing standard protocols are used across the interfaces described in section 1 of this document then the mechanisms which have been defined as part of the standard should be sufficient to cope with failure conditions at the interconnection interface level.

5 FUTURE EVOLUTION

The IN based solutions described in this document are capable of supporting the Service Provider non-circuit related requirements as described in [7]. However all of these solutions are limited in so far as they all rely on a significant amount of service information being passed between the Service Provider and Network Operator. This means that the Service Provider is not in total control of the services being provided. The independence of the Service Provider to create services is constrained.

IN continues to evolve, a planned feature of CS3 is to support interconnection with IP networks. The capabilities defined to support this interworking may also be of use of Service Provider Access.

There is currently some ETSI work on a Service Provider Access interface which may result in a more customised IN interface for the Service Providers. The conclusion to this work, in the form of a protocol specification, is not expected till the end of 1999. In addition, there are a number of research studies looking at the creation of a common API, the IETF are also giving some consideration to Service Provider Access mechanisms. Unfortunately at the present time there is nothing other than IN, which is sufficiently mature enough for consideration as a Service Provider interface that would meet the requirements.

In summary, what is described in this document is just the story so far, research work is currently ongoing in a number of areas which may provide an interface(s) which would be ultimately more suitable for the Independent Service Provider.

END OF PNO-ISC/INFO/013