INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.1221

(09/97)

SERIES Q: SWITCHING AND SIGNALLING

Intelligent Network

Introduction to Intelligent Network Capability Set 2

ITU-T Recommendation Q.1221

(Previously CCITT Recommendation)

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4 AND No. 5	Q.120–Q.249
SPECIFICATIONS OF SIGNALLING SYSTEM No. 6	Q.250–Q.309
SPECIFICATIONS OF SIGNALLING SYSTEM R1	Q.310–Q.399
SPECIFICATIONS OF SIGNALLING SYSTEM R2	Q.400–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	**Q.1200–Q.1999**
BROADBAND ISDN	Q.2000–Q.2999

For further details, please refer to ITU-T List of Recommendations.

ITU-T RECOMMENDATION Q.1221

INTRODUCTION TO INTELLIGENT NETWORK CAPABILITY SET 2

Summary

Intelligent Network Capability Set 2 (IN CS-2) is the second standardized stage of the Intelligent Network (IN) as an architectural concept for the creation and provision of services, including telecommunication services, service management services and service creation services. This Recommendation gives an introduction to IN CS-2. It describes the main characteristics and overall capabilities of IN CS-2 and defines the service aspects, network aspects and functional relationships that form the basis of the IN CS-2 capabilities.

This Recommendation is the first in the Q.122x-Series of Recommendations devoted to IN CS-2, which builds on the architectural principles of IN as described in the Q.121x- and the Q.120x-Series of Recommendations.

The IN CS-2 Recommendations form a detailed and stable basis for implementing IN CS-2 telecommunication services. They also provide high-level guidelines for supporting service management services, service creation services and some partially supported telecommunication services. The IN CS-2 Recommendations are intended to give the same degree of technical information as the IN CS-1 Recommendations (1995).

Source

ITU-T Recommendation Q.1221 was prepared by ITU-T Study Group 11 (1997-2000) and was approved under the WTSC Resolution No. 1 procedure on the 12th of September 1997.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. The ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, the ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Recommendation Q.1221

INTRODUCTION TO INTELLIGENT NETWORK CAPABILITY SET 2

(Geneva, 1997)

1 Introduction

Intelligent Network Capability Set 2 (IN CS-2) is the second standardized stage of the Intelligent Network (IN) as an architectural concept for the creation and provision of services, including telecommunication services, service management services and service creation services. This Recommendation gives an introduction to IN CS-2. It describes the main characteristics and overall capabilities of IN CS-2 and defines the service aspects, network aspects and functional relationships that form the basis of the IN CS-2 capabilities.

Listed below are the acronyms used in this Recommendation:

BCSM	Basic Call State Model
CCAF	Call Control Agent Function
CCF	Call Control Function
CCIS	Common Channel Interoffice Signalling
CRACF	Call-related Radio Access Control Function
CS	Capability Set
CURACF	Call-Unrelated Radio Access Control Function
CUSF	Call-Unrelated Service Function
DTMF	Dual-Tone Multi-Frequency
FE	Functional Entity
GFP	Global Functional Plane
IAF	Intelligent Access Function
INAP	Intelligent Network Application Protocol
IN-SSM	IN-Switching State Model
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
OAM	Operation, Administration, and Maintenance
PBX	Private Branch Exchange
PE	Physical Entity
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
QOS	Quality of Service
RCF	Radio Control Function
SCE	Service Creation Environment
SCEF	Service Creation Environment Function
SCF	Service Control Function

SCUAF Service Control User Agent Function
SDF Service Data Function
SIB Service-Independent Building Blocks
SMAF Service Management Access Function
SMF Service Management Function
SRF Specialized Resource Function
SS7 Signalling System No. 7
SSF Service Switching Function
TMN Telecommunications Management Network
UPT Universal Personal Telecommunication

2 Phased standardization

The phased approach of IN capability sets has been described in Recommendation Q.1201.

In order to prepare for the next phases of IN (CS-3 and beyond), the IN CS-2 Recommendations contain both complete technical specifications (with complete support for physical architecture and detailed protocol description) and incomplete specifications that are intended to be the base for subsequent capability sets (with SIB description and the impact on the functional architecture). Capabilities which are only incompletely covered by IN CS-2 Recommendations are highlighted through special notes or caveats.

3 General description and scope of IN CS-2

3.1 Criteria for IN CS-2

IN CS-2 defines an initial subset of IN capabilities that meet the following general criteria:

a) IN CS-2 is a subset of the target Intelligent Network architecture;

b) IN CS-2 is a superset of IN CS-1, as defined in the IN CS-1 Recommendations (1995);

c) IN CS-2 is a set of definitions of capabilities that is of direct use to both manufacturers and network operators;

d) IN CS-2 provides network capabilities defined to support the set of IN CS-2 benchmark services or service features. These capabilities can also be used for the support of other services that may, or may not, be standardized by ITU-T.

The IN CS-2 architecture could be applied for PSTN, ISDN, and mobile networks.

3.2 Evolution of IN CS-2

The IN CS-2 Recommendations (Q.122x-Series) form a detailed and stable basis for implementing IN CS-2 telecommunication services. They also give high-level guidelines for supporting service management services and service creation services and some partially supported telecommunication services. Complete technical specifications of these services will be in the subsequent IN capability sets.

As IN CS-1, IN CS-2 takes into account the evolution requirement. It is defined to support the IN CS-2 benchmark services and service features without assumptions that are known to limit its evolution into future capability sets.

The IN CS-2 Recommendations are intended to give the same degree of technical information as the IN CS-1 Recommendations (Q.121x-Series).

4 Overview of IN CS-2 Recommendations

Table 1 contains an overview of the Recommendations that are specifically related to IN CS-2:

Table 1/Q.1221 – IN CS-2 Recommendations

Rec.	Title
Q.1220	Q.1220-Series Intelligent network capability set 2 Recommendation structure
Q.1221	Introduction to Intelligent Network Capability Set 2
Q.1222	Service plane for Intelligent Network Capability Set 2
Q.1223	Global functional plane for Intelligent Network Capability Set 2
Q.1224	Distributed functional plane for Intelligent Network Capability Set 2
Q.1225	Physical plane for Intelligent Network Capability Set 2
Q.1228	Interface Recommendation for Intelligent Network Capability Set 2
Q.1229	Intelligent network users guide for capability set 2
Q.1290	Glossary of terms used in the definition of intelligent networks

5 Service aspects

The services and service features that are to be supported by IN CS-2 are fundamental to the IN CS-2 Service-Independent Building Blocks (SIBs), call processing model and service control principles. Three types of services have been identified in IN CS-2: telecommunication service, service management service and service creation services. The last two types of services are first introduced in IN CS-2.

Tables 2 and 3 list IN CS-2 benchmark services and service features, which, in addition to IN CS-1 related telecommunication services/service features, can be used to identify and verify the service-independent capabilities of IN CS-2.

Appendix I provides short prose descriptions of the benchmark services and service features. It was used to develop the current Q.122x-Series of Recommendations and was intended for this purpose only. It is not to be used by service designers for service creation.

Table 2/Q.1221 – Target set of IN CS-2 telecommunication services

Benchmark telecommunication services

Internetwork Freephone (IFPH)	Call Transfer (CT)
Internetwork Premium rate (IPRM)	Call Waiting (CW)
Internetwork Mass calling (IMAS)	Hot line (HOT)
Internetwork televoting (IVOT)	Multimedia (MMD) [a)]
Global Virtual Network Service (GVNS)	Terminating Key Code Screening (TKCS) [a)]
Completion of Call to Busy Subscriber (CCBS) [a)]	Message Store and Forward (MSF)
Conference calling (CONF)	International Telecommunication Charge Card (ITCC) [a)]
Call Hold (HOLD)	Mobility services (UPT) [a)]

NOTE 1 – The above service names apply to the descriptions of targeted services (see Appendix I), and not to the user-network interface descriptions provided by ITU-T Study Group 1.

NOTE 2 – Network implementation aspects may be important for some services.

a) These services may be partially supported in IN CS-2. For example, they may be supported at the GFP level but not supported at the protocol level. Some of these services may also require capabilities beyond IN CS-2. Please note that SIBs are used for modelling purpose. They are not meant to be used as a standardized solution for service creation, even though some organizations may wish to use them for this purpose.

Table 3/Q.1221 – Target set of IN CS-2 telecommunication service features

Benchmark telecommunication service features

User Authentication (UAUT)	InterNetwork Service Identification (INSI)
User Registration (UREG/outgoing call registration)	InterNetwork Rate Indicator, Forward (INRI-F) [a)]
Secure Answering (SANSW)	InterNetwork Rate Indicator, Backward (INRI-B) [a)]
Follow-On (FO)	Real Time Flexible Rating (RTFR) [a)]
Flexible (call) Origination Authorization (FOA)	Originating Carrier Identification (OCI) [a)]
Flexible (call) Termination Authorization (FTA)	Terminating carrier identification (OTC) [a)]
Provision of Stored Messages (PSM)	Resource Allocation (RAL) [a)]
Multiple Terminal Address Registration (MTAR) [a)]	Delivery of Complementary Information (DCI) [a)]
Intended Recipient Identity Presentation (IRIP)	Service Indication (SIND)
Blocking/Unblocking of Incoming Calls (BUIC) [a)]	Service Negotiation (SNEG) [a)]
Terminal Authentication (TAUT) [a)]	Call Forwarding (CF)
Handover (HOV) [a)]	B-ISDN Multiple Connections Point to Point (BI-MCPP) [a)]
Terminal Location Registration (TLR) [a)]	B-ISDN Multi-Casting (BI-MCAST) [a)]

Table 3/Q.1221 – Target set of IN CS-2 telecommunication service features *(concluded)*

Benchmark telecommunication service features	
Terminal Attach/Detach (ATDT) [a)]	B-ISDN Conferencing (BI-CONF) [a)]
Terminal Paging (TPAG) [a)]	Call Connection Elapsed time Limitation (CCEL) [a)]
Radio Paging (RPAG) [a)]	Special Facility Selection (SFS) [a)]
Emergency Calls in Wireless (ECW) [a)]	Concurrent Features Activation with Bi-Control (CFA BC) [a)]
Terminal Equipment Validation (TEV) [a)]	Customized Call Routing with Public network (CCR-PU)
Cryptographic Information Management (CIM) [a)]	Customized Call Routing with Private network (CCR-PR)
Automatic Call Back (ACB) [a)]	Internetwork Service Profile Interrogation (ISPI)
Call Hold (HOLD)	Internetwork Service Profile Modification (ISPM)
Call Retrieve (CRET)	Internetwork Service Profile Transfer (ISPT)
Call Transfer (CT)	Reset of UPT registration for incoming calls (IRUR) [a)]
Call Toggle (CTOG)	Mobility Call Origination (MCO) (mobile call origination/UPT outcall)[a)]
Call Waiting (CW)	Mobility Incall Delivery (MID) (Mobile user call term./UPT incall delivery)[a)]
Meet-Me Conference (MMC) [a)]	Data Communication between different Protocol Terminals (DCPT) [a)]
Multi-Way Calling (MWC) [a)]	Charge Determination (CDET) [a)]
Call Pick-Up (CPU) [a)]	Charge Card Validation (CCV) [a)]
Calling Name Delivery (CND)	Call Disposition (CD) [a)]
Message Waiting Indication (MWI) [a)]	Enhanced Call Disposition (ECD) [a)]
Feature Use Charging (FUC) [a)]	User Service Interaction (USI) [a)]
Services On-Demand (SOD) [a)]	

[a)] These services may be partially supported in IN CS-2. For example, they may be supported at the GFP level but not supported at the protocol level. Some of these services may also require capabilities beyond IN CS-2. Please note that SIBs are used for modelling purpose. They are not meant to be used as a standardized solution for service creation, even though some organizations may wish to use them for this purposes

5.1 Telecommunication services

As in IN CS-1, IN CS-2 capabilities are intended to support *single-ended single-point-of-control* services and service features. Single-ended and single-point-of-control are to be described in 7.2.1 and 7.2.2.

5.2 Service management services

Service management services/service features are supported by IN CS-2. The following list (Table 4) represents service names but not user-network interface descriptions provided by ITU-T Study Group 1.

Table 4/Q.1221 – Target set of IN CS-2 service management services/service features

Benchmark service management services and service features

Service customization services	**Service monitoring services**
Telecommunications Service Customization (TSC)	Subscriber Service Report (SSR)
Service Control Customization (SCC)	Billing Report (BR)
Service Monitoring Customization (SMC)	Subscriber Service Status Report (SSSR)
Service control services	Subscriber Traffic Monitoring (STM)
Subscriber Service Activation/Deactivation (SSAD)	Subscriber service Management Usage Report (SMPUR)
Subscriber Monitoring Activation/Deactivation (SMAD)	**Other management services**
Subscriber Profile Management (SPM)	Subscriber Service Testing (SST)
Subscriber Service Limiter (SSL)	SMP Usage Report (SUR)
Subscriber Service Invocation (SSI)	Subscriber Security Control (SSC)

5.3 Service creation services

Service creation services/service features are supported by IN CS-2. The following list (Table 5) represents service names but not user-network interface descriptions provided by ITU-T Study Group 1.

Table 5/Q.1221 – Target set of IN CS-2 services creation services/service features

Benchmark service creation services and service features

Service specification services	**Service deployment services**
Feature interaction detection	SMP-created service data and SLP update
Cross-service feature interaction detection	Service distribution
Feature interaction rule/guidelines generation	SIB distribution
Service and SIB cataloguing	Data rule distribution
Created service resource utilization	Feature interaction rule distribution
Service development services	**Multiple SMP support**
Creation interface selection	Network tailoring
Creation initiation	Network element capability specification
Editing	Network element function/capability assignment
Combining	**Service creation management services**
Data population rule generation	SCE access control
SMP service creation	SCE usage scope

Table 5/Q.1221 – Target set of IN CS-2 services creation services/service features *(concluded)*

Benchmark service creation services and service features	
Syntax and data checking	SCE recovery
Service and SIB archiving	SCE release management
Service configuration control	SCE capability expansion
SIB configuration control	SCE conversion
Network configuration tracking capability	Cross-SCE service maintenance
Service verification services	SCE-to-SCE system consistency
SCE testing	SCE service/modular/system transference
Created service simulation	Conversion of created services
Created service live testing	Service management interaction

5.4 Network support of IN CS-2 services

The services are to be supported over various networks. For IN CS-2 applications the following networks are considered:

i) PSTN;

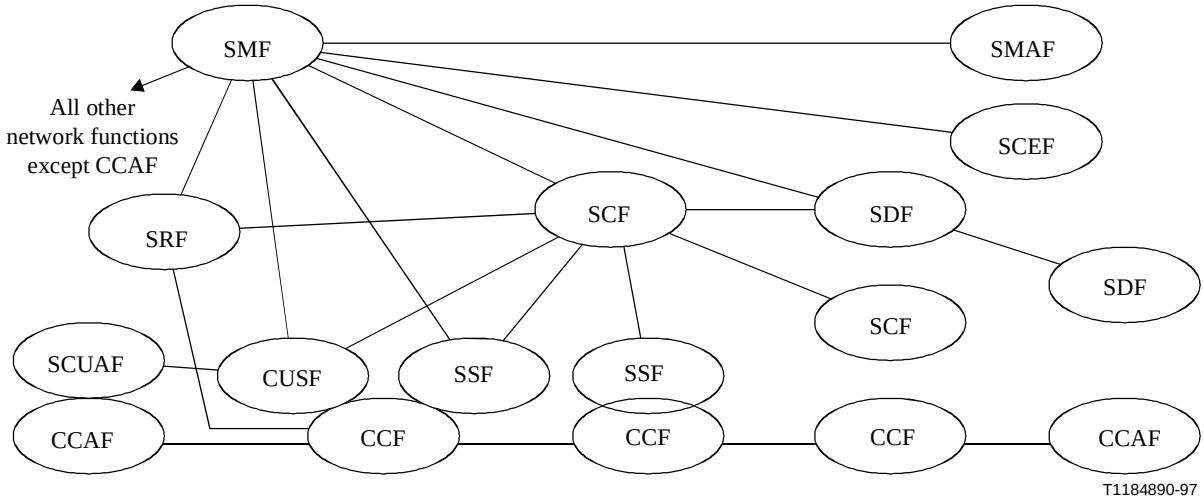
ii) ISDN (public and private networks);

iii) PLMN.

6 Network aspects

This clause provides an overview of the IN network functions and sets guidelines for the control architecture of IN CS-2. It also describes how the issues of feature interaction and service-feature consistency are handled in IN CS-2.

Figure 1 summarizes the IN network functions and their functional relationships.



CCAF	Call control agent function	SMF	Service management function
CCF	Call control function	SRF	Specialized resource function
SCEF	Service creation environment function	SSF	Service switching function
SCF	Service control function	CUSF	Call-unrelated service function
SDF	Service data function	SCUAF	Service control user agent function
SMAF	Service management access function		

Figure 1/Q.1221 – IN functions and functional relationships

6.1 Network functions

Call control and call unrelated control related functions

SSF – Service switching function: This function interfaces with CCF and SCF. It allows the CCF to be directed by the SCF.

SRF – Specialized resources function: This function provides a category of resources for access by other network entities. Examples of resources include DTMF sending and receiving, protocol conversion, speech recognition, and synthesized speech provision.

CCF – Call control function: This function refers to call and connection handling in the classical sense (e.g. that of an exchange).

CCAF – Call control agent function: This function provides the user access to the network.

CUSF – Call unrelated service function: This function handles call unrelated activities.

SCUAF – Service control user agent function: This function provides the user access to the network call unrelated service function.

Service control related functions

SCF – Service control function: This function contains the IN service logic and handles service related processing activity.

SDF – Service data function: This function handles access to service-related data and network data and provides consistency checks on data. It hides from the SCF the real data implementation and provides a logical data view to SCF.

Management related functions

SCEF – Service creation environment function: This function allows an intelligent network service to be defined, developed, tested and input to the SMF. The output of this function involves service logic and service data templates.

SMAF – Service management access function: This function provides an interface (e.g. screen presentation) for service subscribers and service administrators who have access to the SMF.

SMF – Service management function: This function involves service operation control, service provision control, service deployment control, service monitoring and billing.

6.2 Control architecture principles

As stated in clause 5 (Service aspects), the service scope of IN CS-2 shall be restricted to single-ended single-point-of-control services. This subclause identifies principles for the control architecture of IN CS-2, in the context of this service scope.

This subclause is organized around three control aspects:

– service invocation and control;

– end-user interaction with and without the SRF; and

– service management.

6.2.1 Service invocation and control

This control aspect involves the CCF, SSF and SCF.

As in IN CS-1, the following points capture key principles for IN CS-2:

1) The CCF retains ultimate responsibility for integrity and control of the local connection at all times.

2) The SSF-to-SCF relationship is, by definition, service-independent. Therefore, the CCF and SSF should never contain service logic specific to IN CS-2 supported services.

3) In the event of SCF malfunction, or time-out in the SCF to SSF response, the SSF/CCF combination should be capable of reverting to a default call completion sequence, with appropriate announcement(s) to the calling and/or called party.

4) The SSF should never have to interact with more than one SCF at any given time in order to complete a sequence of query/response interactions on behalf of a calling or called party.

5) Call hand-offs (transfer of responsibility) between SCFs, and between SSFs are permitted in IN CS-2. Nevertheless, the hand-off must be explicit, and must not violate principle 4).

6.2.2 End-user interactions

As part of the process of formulating a response to the SSF, the SCF may need to enter into a dialogue with the calling or called party. This would take the form of a prompt and collection sequence with the aid of an SRF, or the form of call unrelated/out-channel call related interactions, which are new in IN CS-2 (see 7.2.6 and 7.2.7 for more details).

As in IN CS-1, when the SRF is being used, the SCF in IN CS-2 does not have to enter into this dialogue directly. Instead, it instructs the SRF to carry out a prompt and collection sequence with the calling or called party on its behalf. In general, the actual implementation of IN services will govern the kind of transport systems and protocols (e.g. DTMF, D-channel user-to-user signalling, and data services) used to collect information from the user.

Again, the following key principles apply, when the SRF is being used in IN CS-2:

1) The SCF has full IN-supported service control of instruction formulation and sequencing with respect to the SRF and SSF.

2) As a corollary to principle 1), there shall be no direct service control interaction between the SSF and SRF for IN CS-2-based services. The SSF and SRF have a peer-peer relationship for the control of IN CS-2-based services, and both are subsidiary to the SCF.

3) The SCF will require the capability of suspending processing of an IN CS-2-based service on behalf of a calling or called party, and then resuming on behalf of the same party at a later time.

6.2.3 Service management

The control aspects covered in 6.2.1 and 6.2.2 address the real-time interactions between IN CS-2 functions on behalf of a particular calling or called party. In contrast, the service management aspect primarily addresses the network operator's interaction with the SSF, SCF, SDF, and SRF. This interaction normally takes place outside the context of a particular call or service invocation. Nonetheless, IN CS-2 must neither preclude nor constrain the capability of service customers to interact directly with customer-specific service management information (e.g. a personal service profile).

The following points capture key principles for IN CS-2:

1) The SMF may be used to add, change or delete IN CS-2-based service-related information or resources in the SSF/CCF, CUSF, SCF, SDF, and SRF. Such changes should not interfere with IN CS-2-based service invocations or calls that are already in progress.

2) The SMAF may be used to add, change, or delete appropriate customer-specific information. The mechanism and safeguards that are put into place by the network operator for this interaction may take advantage of IN CS-2 functions and capabilities.

3) The SCEF may be used by service providers to introduce new services. The task of deploying the service is the role of the SMF and is initiated from within the SMF.

6.3 Feature interactions

As in IN CS-1, the constraints placed on the IN CS-2 architecture have been put in place primarily to minimize and control feature interactions within single domains of responsibility. See 7.2.8 for more details.

The single-endedness of IN CS-2-based services means that all aspects of a call are under the control of one CCF/SSF and one SCF at any point in time [principle 4) in 6.2.1]. The SCF and SSF are therefore responsible for the handling of interactions between IN CS-2-based SSF/CCF capabilities, and non-IN features already provided in the basic network.

6.4 Consistency among IN CS-2 supported service features

The ultimate responsibility for consistency of operations within a set of IN CS-2-based service features lies with the network operator. Nonetheless, the software and data structures of the SCF and SDF, operation and control of these software and database structures via the SMF, and the tools provided by the SCEF, may be designed to aid the network operator in fulfilling this responsibility.

7 Functional relationships and interfaces

7.1 Functional relationships and control classes

Five groups of control capabilities, called control classes, have been identified to support the functional relationships:

1) Bearer connection control: the class of capabilities to establish, and clear the bearer connections (e.g. voice paths through the network), and provide surveillance.

2) Non-IN call control: the class of capabilities to invoke the user and provide the end-to-end control required for the non-IN delivery of supplementary services. The non-IN delivery does not involve the structured separation of the CCF, SSF, and SCF.

3) IN service-control: the class of capabilities that involve the structured separation of the SSF from SCF.

4) Service management control: the class of capabilities that involve service deployment, service provisioning, service operation control, and service monitoring.

5) Non-IN call unrelated control: the class of capabilities to establish, provide monitoring, and clear a non-bearer connection (e.g. out-channel interaction via the DSS 1 D-channel without a bearer connection).

Figure 2 depicts the classes of control capabilities required for the functional relationships. The following subsections further describe the control relationships for each control class, respectively. A control relationship is the relationship between a functional relationship and a control class.

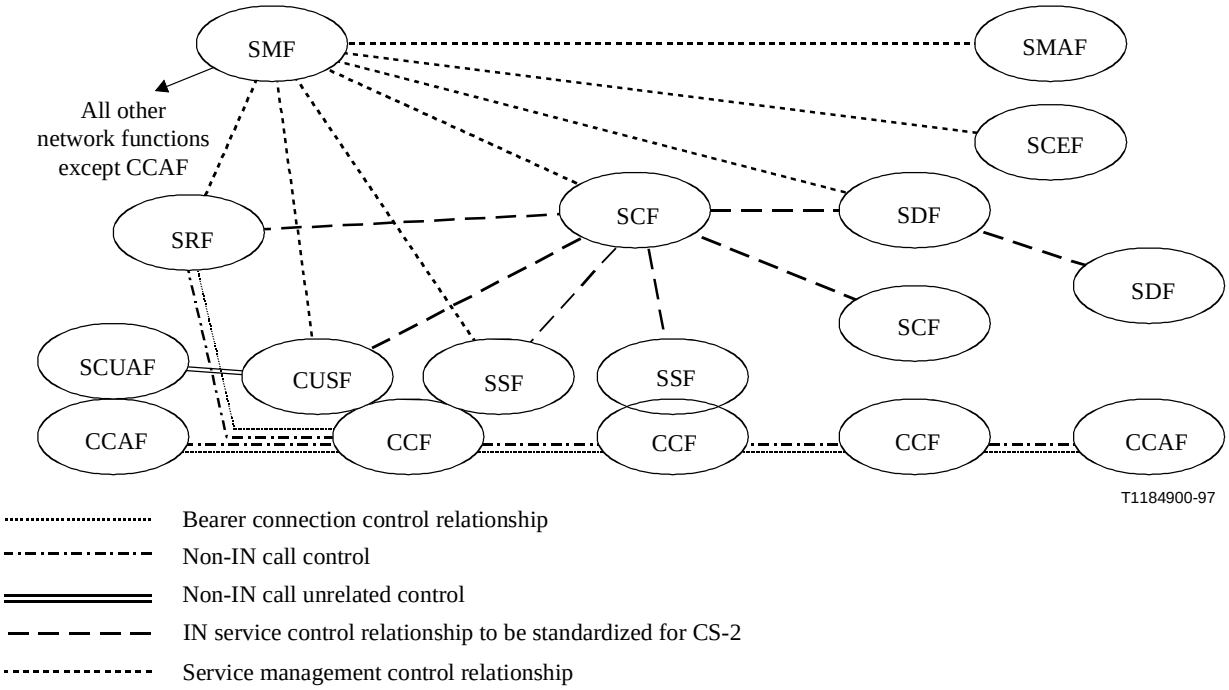


Figure 2/Q.1221 – Functional relationships and control classes for IN CS-2

7.1.1 Bearer connection control

Control relationships exist between the bearer connection control class and the CCAF-CCF, CCF-CCF, and CCF-SRF functional relationships, respectively. Standard interfaces are employed to realize these control relationships and are listed below by the involved functional relationships:

– CCAF-CCF: DSS 1/Q.931

– CCF-CCF: SS7/ISUP

– CCF-SRF: DSS 1/Q.931; SS7/ISUP

7.1.2 Non-IN call control

Control relationships exist between the non-IN call control class and the CCAF-CCF, CCF-CCF, and CCF-SRF functional relationships, respectively. Standard interfaces are employed to realize these control relationships and are listed below by the involved functional relationships:

– CCAF-CCF: DSS 1/Q.931

– CCF-CCF: SS7/ISUP

– CCF-SRF: DSS 1/Q.931; SS7/ISUP

7.1.3 IN service control

Control relationships exist between the IN service control class and the SCF-CUSF, SCF-SCF, SCF-SDF, SCF-SRF, SCF-SSF, and SDF-SDF functional relationships, respectively. They can be realized through SS7/TCAP/INAP.

IN CS-2 can support mid-call and topology manipulation capabilities, as noted in other Q.122x-Series of Recommendations. In addition, IN CS-2 may support services or service features which require ISUP or/and DSS 1 modifications.

7.1.4 Service management control

Control relationships exist between the service management control class and the SMF-CUSF, SMF-SCF, SMF-SCEF, SMF-SDF, SMF-SMAF, SMF-SRF, and SMF-SSF functional relationships, respectively. They can be realized through CMIP/Q.812. No modification to INAP (i.e. Q.1228) is foreseen for management aspects. In addition, no modification to the IN physical plane (i.e. Q.1225) is foreseen; namely, no additional Physical Entities (PEs) are required assuming basic PEs exist for management aspects.

7.1.5 Non-IN call unrelated control

There is a control relationships between the non-IN call unrelated control class and the SCUAF-CUSF functional relationship. Standard interfaces listed below are employed to realize this control relationship:

– SCUAF-CUSF: DSS 1/Q.932; SS7/ISUP

7.2 Key functions and interfaces

7.2.1 Single point multiple points of control

Single point of control describes a control relationship where the same aspects of a call are influenced by one and only one service control function at any point in time. Multiple points of control is the ability for multiple service logic instances to interact with a single call segment. The SSF/CCF may have to be able to manage interactions between IN service logic instances realized in different service logic instances that are simultaneously active on a single call. New capabilities beyond the single point of control capability are required to enable the SCF to control two call segments in different SSF/CCFs simultaneously.

Interfaces: SCF-SSF/CCF, SCF-SCF

7.2.2 Single-ended/multi-ended calls

A single-ended service feature applies to one and only one party in a call and is orthogonal (independent) at both the service and topology levels to any other parties participating in the call. Orthogonality allows another instance of the same or a different single-ended service feature to apply to another party in the same call as long as the service feature instances do not have feature interaction problems with each other.

Multi-ended is the ability for a service logic instance to interact with multiple call segments. The service logic instance may have to be able to manage IN call/connection processing among multiple call segments on a single call.

Interfaces: SCF-SSF/CCF, SSF-SSF, SCF-SCF

7.2.3 Mid-call interruption

Mid-call interruption supports SCF-SSF interaction during the alerting or active phase of a call (i.e. during ringing for the originating party or after the call reaching a stable state).

Interfaces: SCF-SSF/CCF.

7.2.4 Call party handling

Call party handling is the ability to manage various parties' participation in a call. Parties' bearer channels may be added, deleted, joined and/or separated from the other parties involved in the call.

Interfaces: SCF-SSF/CCF.

7.2.5 Enhanced SRF

Enhanced SRF capabilities are identified in 4.3.4/Q.1214 and 3.3.6/Q.1224. Examples include audio conference bridge, information distribution bridge, text-to-speech synthesis, protocol converters, automatic voice recognition and voice message sender/receiver. Capabilities such as voice message sender/receiver, text to speech synthesis, and automatic voice recognition can be supported using elementary operations (as in IN CS-1) or user interaction scripts (as in IN CS-2). The latter is based on the concept of task sharing between SCF and SRF; the SCF is responsible for the global service logic while the SRF is responsible for the user interaction logic. Other capabilities such as audioconference bridge and information distribution bridge are supported by using the hybrid approach for call party handling that an SRF as well as an SSF is involved in providing the services.

Interfaces: SRF-SCF, SSF-SCF.

7.2.6 Call unrelated user interaction

Call unrelated user interaction between the user and service processing is the ability to communicate information outside the context of a call, required for services/service features such as message waiting indication. As this capability is not supported by the BCSM, which is call related, the basic call unrelated state model (BCUSM) is introduced in IN CS-2.

Interfaces: SCF-CUSF, CUSF-SCUAF.

7.2.7 Out-channel call related user interaction

Out-channel call related user interaction provides the ability to communicate information within the context of a call on the out-channel signalling access (within the same call reference of a call) to support features such as user authentication.

Interfaces: SCF-SSF/CCF, SCF-SRF.

7.2.8 Service/feature interaction (service processing)

Service interaction during service processing focuses on the service interaction in the phase of service executions. It relates to the call control. To help characterize service interactions between non-IN supported services/features and IN supported services/features, it may be useful to map non-IN supported services/features to the IN-Switching State Model (IN-SSM). Non-IN supported services/features may be fully mapped, partially mapped, or unmapped. Placement of a non-IN supported service or service feature into one of these groups serves to characterize the information available to the Feature Interaction Manager/Call Manager (FIM/CM) during the operation of the feature. In characterizing service interactions for fully mapped non-IN-based services and service features, higher priority should be given to fully mapped non-IN-based services than to partially or unmapped non-IN-based services.

Interfaces: SCF-SCF, SCF-SDF, SCF-SRF, SCF-SSF/CCF

7.2.9 Internetworking

Internetworking is the process in which several networks (potentially of different types, such as IN-structured, non-IN-structured, public and private) cooperate to provide a service. The need for internetworking capabilities results from the fact that customers may want to access services which span multiple networks. A typical situation is when the data needed by a service (e.g. UPT, VPN and global network services) reside in a network that is different from the one in which the call has originated.

To meet the IN CS-2 internetworking need, extension of the IN models and architecture to a multi-network context as well as extension of existing functionalities defined in IN CS-1 to support interfaces between functional elements physically located in different network contexts has been provided by IN CS-2.

IN CS-2 identifies the SCF-SCF, SCF-SDF, SCF-IAF, SDF-SDF and SMF-SMF relationships for internetworking purposes. Distributed service logic, but not distributed service control, is supported. Additionally, internetwork management interactions and distributed data handling processes are supported.

7.2.9.1 Internetworking between IN-structured networks

General requirements for internetworking capabilities are presented in 2.2.6/Q.1201.

Although the involved networks may have different access types (e.g. PSTN and ISDN), as well as different levels of IN structure, IN CS-2 internetworking services are to be provided to customers in a consistent way, regardless of such differences.

Similar to Figure 1, which depicts the functional relationships between the IN functions within one network, Figure 3 depicts possible functional relationships between the IN functions that are located in two different networks.

The following observations can be made concerning the applicability of Figure 3 to IN CS-2:

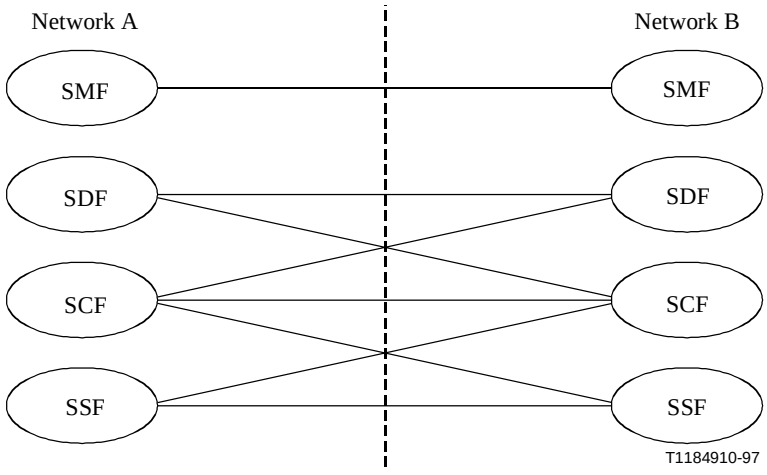


Figure 3/Q.1221 – Possible IN network interworking functional relationships

1) The SSF-SCF functional relationship across two networks is out of the scope of IN CS-2. As for IN CS-1, and as described in 2.2.6/Q.1201, which underlines the necessity to maintain the network security and network integrity, internetworking between the SSF in one network and the SCF in another one is not an IN CS-2 requirement.

2) IN CS-2 will support the SCF-SCF functional relationship across two networks when only one SCF directly interacts with the call. This restriction is necessary because IN CS-2 has no requirement for multiple point of control capability, where two SCFs are able to interact with the call at the same time. This internetworking relationship is new for IN CS-2 as it was not supported by IN CS-1.

3) As in IN CS-1, the SCF-SDF functional relationship across two networks is within the scope of IN CS-2.

4) The SDF-SDF functional relationship across two networks is within the scope of IN CS-2. This internetworking relationship is new for IN CS-2 as it was not supported by IN CS-1.

5) The SMF-SMF functional relationship across two networks is within the scope of IN CS-2. The assumed protocol should align with TMN generic protocols and the TMN X interface. This internetworking relationship is new for IN CS-2 as it was not supported by IN CS-1.

6) In IN CS-2, specific internetworking capabilities are assumed to be localized within the FEs which support an internetworking relationship, i.e. within the SCF, SDF and the SMF.

7) The internal architecture of one network is not visible from another network. However, functions needed for processing internetworking are to be visible from the other network (IN or non-IN).

7.2.9.2 Internetworking with non-IN-structured networks

The previous subclause defines the internetworking relationships for two networks, both of which have a structure compatible with the IN functional architecture. For IN CS-2, the Intelligent Access Function (IAF) provides access between the SCF of an IN-structured network and an entity of a non IN-structured network. This latter entity may be other networks or customers (e.g. private networks, simple databases used in the customer call routing service, terminals, and PABXs). It:

a) provides access to and from the SCF of the IN-structured network; and

b) maps the information between the internal and external representation.

As such, for the subscriber's each incoming call, information (such as dialled number, calling number, and caller entered digits) may be conveyed, for example, from a public network to a private one for the latter to determine how that call will be handled. A private network is defined as a network which provides services only to a specific set of users.

Similar to Figure 3, which depicts possible functional relationships between the IN functions that are located in two different IN-structured networks, Figure 4 depicts a possible functional relationship between the SCF located in an IN-structured network and the IAF located in a non-IN-structured network.

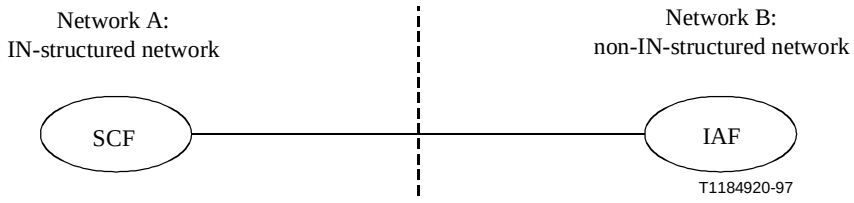


Figure 4/Q.1221 – IN to non-IN network interworking functional relationship

7.2.10 Security

Security is a general property which relates to safe and reliable operation. The high-level requirements of a secure system are:

- Confidentiality, which is defined in Recommendation X.800 as *the avoidance of the disclosure of information without the permission of its owner*. Thus, confidentiality may be considered as a property which ensures that conversations or interactions remain private;
- Integrity, which is defined in Recommendation X.800 as *the property that data has not been altered or destroyed in an unauthorized manner*. Integrity may then be considered as a property which ensures that operations occur as they are expected to;
- Availability, which may be considered as a property relating to the readiness of resources for authorized use;
- Accountability, which may be considered as a property which ensures that any operational request can be correctly attributed in case of doubt or dispute.

The components of an IN system must be assembled and operated in such a way as to provide a defined level of security.

To assist in this, any interface within the IN functional architecture may have the need to apply security assisting functions to the information flows passing across the interface such as:

- Network access security functions: This includes user/terminal authentication (i.e. the result of a process by which a service user proves his or her identity to an IN system), user profile verification (i.e. the verification that a user is authorized to use a functionality);
- Internetworking security functions: This includes peer entity authentication (i.e. a process which allows a communicating entity to prove its identity to another entity in the network), signalling data or TMN data integrity, non-repudiation, confidentiality, entity profile verification (i.e. the verification that an entity is authorized to use a functionality).

Recommendation Q.1228 defines a generic set of security mechanisms and procedures to offer some of the generic properties described above. In any particular circumstance, a set of network elements will be required to be configured according to some security scheme.

The definition of IN CS-2 offers the provision of certain security assisting functions at the SCF-SDF, SDF-SDF, and SCF-SCF interfaces. Additional security functions may be required depending on the security schemes in place.

Interfaces: SCF-SCF, SCF-SDF, SDF-SDF

7.2.11 IN-TMN

Applying TMN concepts, TMN functional architecture modeling aspects to the IN are identified in Recommendation Q.1224 and its associated annexes. Harmonization of IN/TMN using TMN concepts to define service management and network management is specified in 7.2.12.

Interfaces: See 7.2.12.

7.2.12 Service management

IN specific service management refers to the network capabilities that are necessary from a network operator's point of view, to support the proper operation of services. This includes management during deployment, provisioning and utilization phases. TMN functionality can be used to provide these capabilities. Service interaction during service management focuses on service interaction in the phase of service subscription, service registration and service activation.

The Service Management Function (SMF) is defined in 2.4/Q.1204. The actors who have access to the SMAF and thereby the SMF are service subscribers and service administrators. Service subscribers are users of the IN-supported services. (When subscribing for a particular IN-supported service, the service subscribers may choose some service features offered by the service provider

according to their needs.) Service administrators consist of both the service provider and network provider; they are responsible for the following areas of service support:

1) Service provisioning: introduction and allocation of the service logic with the ability to modify that service logic. Provisioning may also include changing certain service-related parameters prior to and during testing and distributing the related logic and data to other IN functional entities;

2) Service monitoring: monitoring service performance, receive trouble reports from service subscribers, and using the SMF to identify and correct the problem;

3) Security management: secure access to the functions of the SMAF.

The above activities so far have been performed only by service administrators; however, service subscribers need and demand more control over the specifics of the services. The capabilities of the service subscribers to control the subscribed services are named "customer control service capability". Specific controlling capabilities can be granted depending on specific services (e.g. the freephone-related capabilities may differ from the VPN-related capabilities).

In general, this set of capabilities would allow service subscribers to:

1) view and adjust the service parameters they subscribe to; and

2) request and receive reports.

Two technical approaches are supported in IN for the provision of the customer control service capability:

1) Access through the SMAF to the SDF: This would be done via dedicated terminals.

2) Access through the network via the CCAF: This approach is supported at service processing level, and the SDF is involved.

The second solution is constrained technically by the network-to-user interface and by the data available in the SDF. Full customer control service capability is only possible with the first solution.

The solution choice is specific to each service. For instance, simple customer control service capability, such as location registration in UPT from any terminal, would be based on the second solution. A more complex customer control service capability, such as VPN management would be based on the first solution.

The management-related functional relationships (i.e. SMF-SCF, SMF-SDF, SMF-SSF/CCF, SMF-SRF, and SMF-CUSF) are defined in IN CS-2 down to the distributed functional plane, with a high-level description of functions, functional model, functional relationships and interfaces (and guidance on the information model). The technical assumption is the alignment of IN and TMN. The assumed protocols to be used are the TMN generic protocols (e.g. common management information protocol, CMIP, as defined in Recommendation Q.812). No modification to INAP (Recommendation Q.1228) are foreseen for management aspects.

Within IN CS-2, the management relationships to be studied are: SMF-SCEF, SMF-SMAF, SMF-SSF/CCF, SMF-SCF, SMF-SDF, and SMF-SRF. The last four relationships describe the management of IN network elements.

The IN-specific management requirements concerning the service life cycle phases of creation, deployment, provisioning and utilization of IN-supported services are considered from a service plane point of view. Listed below are the requirements at the service and network level.

The service level requirements are:

– Install and configure the service script/software.

– Install and configure service management scripts/software (e.g. scripts for the introduction and allocation of subscriber specific data).
– Install and configure the service testing (for the provisioning of tests on line).
– Install and configure the service generic data.
– Install and configure the specialized resource data.
– Set the target time and date the service should be enabled (service is pending).
– Receive reports on installation and configuration.
– Receive information on service availability (to inform customer of problems).
– Workstation program configuration.
– Enable/disable (parts of) the service on a global (network-wide) level.
– Monitor and control the service performance.
– Monitor, control (e.g. setting conditions on alarm reporting) and correct the service faults.
– Update service generic data.
– Update specialized resource data.
– Tariffs initialization and modification.
– Remove service management scripts/software.
– Remove the service script/software.
– Remove the service testing.
– Remove the service generic data.
– Remove the specialized resource data.
– Receive reports on the removing actions.
– Set the target time and date the service should be disabled.
– Install customer data in the network.
– Handle complaints on service malfunctioning.
– Handle customer control requests (e.g. update customized announcements and change parameter settings).
– Remove customer data from the network.
– Obtain information on the usage of the service per service subscriber for billing (e.g. via usage records).

The network level requirements are:

– Test the installed software.
– Install and configure trigger data.
– Install and configure signalling routing data.
– Install and configure network elements.
– Configure the workstation program.
– Monitor and control the performance/QOS of the network element.
– Enable/disable the use of the resources of the network element involved in the "service execution".
– Reallocate specialized resources (e.g. following QOS criteria).
– Monitor, control and correct the network element.

– Test the network element.
– Update signalling routing data.
– Update trigger data.
– Update list of accountable events.
– Generate, collect and store usage information (e.g. for accounting purposes).
– Remove the installed software.
– Remove trigger data.
– Remove signalling routing data.
– Remove network elements.
– Handle complaints on network malfunctioning.

Interfaces: SMF to SMAF, SCEF, SCF, SDF, SRF, CUSF, and SSF/CCF

7.2.13 Service creation

IN service creation presents the operator's point of view for the creation of new services. These include service specification, service development, and service verification. Output is expected to be service logic for the execution aspects of a service, service logic for the management aspects of a service, and user data related logic and service data related logic. This includes partitioning of functionality between the SMF and SCEF.

The SCEF allows services provided in Intelligent Network to be defined, developed, tested and input to SMF. Output of this function would include service logic, service management logic, service data template and service trigger information. Based on this definition, it is possible to distinguish the following three phases of service creation activity (defined in 2.2.2/1201):

- service specification;
- service development;
- service verification.

The service specification phase involves the following:

- requirements specification based on customer/market input;
- analysis;
- feature interaction rules;
- OAM requirements;
- high-level design including evolution aspects.

The service development phase involves the following:

- detailed design:
  - feature design;
  - data schema;
  - test case generation;
  - engineering considerations;
- service logic and service management logic definition;
- development of service logic modules.

Note that the feature design may impact platform development but it should not be considered as part of the service creation services because the impact on the platform depends on the intrinsic

capabilities of the platform and it is vendor dependent. The output of the service development phase feeds into service verification phase.

The service verification phase involves the following:

- service logic syntactic checking;
- service logic and service management logic simulation;
- service logic module verification;
- network simulation;
- testing for service order requirement;
- engineering verification.

Service interaction focuses on service interaction in all phases of service creation. The output of this phase verifies that customer/market requirements are met.

Similarly, the SMF functionality can be subdivided into following phases:

- service deployment;
- service provisioning;
- monitoring and maintenance;
- service negotiation.

The service deployment phase involves the following:

- service configuration on each Functionality Entity (FE), i.e. SCF, SSF, SDF, and SRF;
- configuration verification;
- subscription template and customization;
- database initialization;
- resource allocation on each FE;
- distribution of service support data and logic on each FE;
- service activation and deactivation via trigger detection point data distribution.

Service interaction (from a service creation perspective) focuses on service interaction in the service deployment phase.

The service distribution activity involves transferring appropriate information about the service to other FEs, e.g. SCF, SDF, SSF, SRF.

The service provisioning phase involves the following activities:

- customer subscription data-fill based on service order template and service customization;
- validation, taking into account customer account information via SMAF;
- subscription provisioning, i.e. informing the subscriber that his order has been executed.

The service monitoring and maintenance phase involves the following activities:

- audit;
- operations measurement/log collection:
  - logic tracing;
  - fraud detection;
  - traffic management;
  - usage report;
  - performance analysis.

The service negotiation phase of the SMF is needed to ensure that there are sufficient network resources available to support the customer's request for IN supported services. This would include at least the following verifications:

– Ensure that the customer has access to the Service Switching Function (SSF).

– Ensure that the SSF/CCF supports the requested IN supported service.

– Ensure that all IN resources are available to support the requested IN supported service.

– Ensure that the requested IN supported service does not conflict with other existing IN supported services that the customer currently subscribes to. This requires an evaluation of potential feature interactions.

– Ensure that the customer has access to other switch-based services, such as ISDN, that may be required by the requested IN supported service.

– Ensure that the requested IN supported service does not conflict with existing switch-based services that the customer currently subscribes to.

Service interaction during service creation focuses on the service interaction in the phase of service creation and service deployment.

This provides a preliminary analysis of the SCEF and SMF functionalities.

Once the functional partitioning between SMF and SCEF are established, then specific functions pertaining to what an SCEF is expected to provide can be addressed in greater detail. An SCEF is unlike other network elements in that it is a tool, not a service execution platform. The implementation of a service design tool, including the extent of the functions is offered its end-user, should be independent of network configurations, i.e. platforms. It is proposed that the services be identified to reflect what information is required between the SCEF and the service management element. With respect to standardization of service creation, it is the interface to other network elements that should be seen as the focal concern. In particular, the SCEF to SMF interface should be specified.

Interfaces: SMF to SCEF

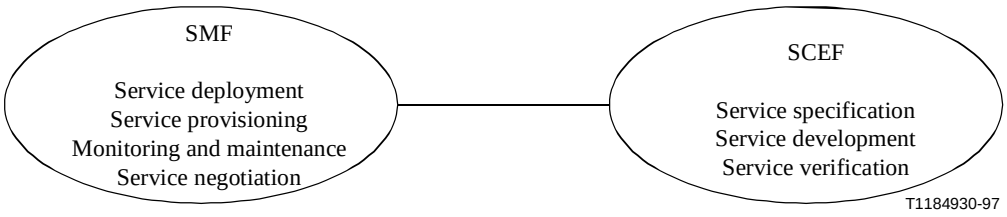


Figure 5/Q.1221 – Partitioning of functionality between SMF and SCEF

7.2.14 Personal mobility

Personal mobility allows a user to associate with and/or configure any terminal, according to individual needs to access telecommunication services. It also enables the user to customize various aspects of the offered features, thereby receiving personal telecommunication service features. Universal Personal Telecommunications (UPT) is an example of a telecommunications service supporting personal mobility.

IN CS-2 provides the network capabilities that are necessary to support personal mobility among heterogeneous access networks. In particular, IN CS-2 has extended the IN model and architecture to guarantee a correct handling of the user profile and service processing, independent of the user

access. The IN CS-2 relationships that may be involved in providing personal mobility services include the SCF-SDF, SDF-SDF, SCF-SCF and SCF-SSF.

APPENDIX I

IN CS-2 benchmark services and features

I.1 General

This Appendix provides short prose descriptions of the benchmark services and service features used to develop the current Q.122x-Series of Recommendations. These descriptions are not meant to be used by service designers for service creation. Note that some of the listed services and service features may be partially supported by IN CS-2 and not be supported at the protocol level.

I.2 Definitions

The following definitions have to be taken into consideration:

I.2.1 Telecommunication services

A telecommunication service is an information telecommunication service offered to subscribers by a service provider in areas where the (IN supported) service logic is executed to provide the service. A subscriber is a person or organization that is billed for use of a telecommunication service. A subscription is an instance of telecommunication service that is provided and billed to a particular subscriber.

I.2.2 Service management services

A service management service offers customization, control and monitoring functions to the telecommunication services for which it is provided. This may be a commercial offering to subscribers.

I.2.3 Service creation services

A service creation service offers specification, development, verification functions to the network operator.

I.3 Telecommunication services

I.3.1 General

It should be recognized that the services proposed are not an extensive list but are taken from categories of services that are important for the next phase of IN standardization. Work to enable this proposed set of services and service features will also enable other services that would also use these capabilities.

I.3.2 Definitions

More detailed definitions are to be found in Recommendation Q.1222.

I.3.2.1 A **telecommunication service** is characterized by one or more core service features, that can be optionally enhanced by other service features.

I.3.2.2 A **service feature** is a specific aspect of a telecommunication service that can also be used in conjunction with other telecommunication services/service features. A **core service feature** is a particular service feature fundamental to the telecommunication service, i.e. in the absence of this

service feature, the name of the telecommunication service does not make sense as a commercial offering to the service subscriber.

I.3.3 Mobility service features (UPT, FPLMTS)

These service features are aimed at, but not limited to, supporting UPT and FPLMTS. Other telecommunication services may utilize these service features.

I.3.3.1 Personal mobility features (UPT)

Personal mobility allows a user to appear at any network access point and initiate telecommunication services. Once recognized, the end user can access provisioned services and features according to a personal user profile, which can be customized by the subscriber or user. Please note that service features used in UPT but of more general nature (such as service indication, internetwork service profile interrogation, modification or transfer, reset of UPT registration for incoming calls) are described in 3.5.

I.3.3.1.1 User authentication (UAUT): This feature confirms the identity of a user with the network and the identity of the network with a user. UAUT takes place during interactions between the network and a user.

UAUT assumes that appropriate information is exchanged between the network and a user. A user has to provide his authentication data through the terminal or via an access device, which transmits the data to the network as well as establish a connection between the network and a user.

UAUT implies the use of security algorithms to check the validity of the information provided by a user.

Once the authentication has been performed, the visited network might keep the track of the authenticated user to avoid multiple use of UAUT.

I.3.3.1.2 User registration (UREG): This feature enables a user to register on a terminal access for the purpose of receiving or placing calls. This may be accomplished either from the terminal where the user wishes to register or from another terminal (remote registration) There are two aspects to this feature, which are both included in the list of UPT Set 1 features described in the Recommendation F.851 "UPT – Service description".

I.3.3.1.2.1 in-call registration is a means by which a user registers from the current terminal address for incoming calls to be presented to that terminal address. When registered, all the incoming calls to that user will be presented to the registered terminal for the duration specified by the user, or until a specific de-registration time. A new in-call registration made by the same user will cancel the previous in-call registration of that user. Several users may register for incoming calls to the same terminal address simultaneously. A user may also explicitly de-register for incoming calls.

I.3.3.1.2.2 Outgoing call registration (OGREG): The out-call registration allows a user from the current terminal address to register for outgoing calls to be made from that terminal address. When registered, all outgoing calls (except some calls like emergency calls) from the terminal address will be charged to the user account for the duration specified by the user in terms of time or number of calls, or until a de-registration takes place. Normally the user will not have to carry out any further authentication procedures in order to make outgoing calls. However, optionally a simplified authentication procedure may be used. A user may be registered for outgoing calls at several terminal addresses simultaneously, but at any time only one user may be registered for outgoing calls at the same terminal address. The user may prevent another user from de-registering him for outgoing calls. The user may also explicitly de-register for outgoing calls. A third party *may* prevent a user from registering at his terminal address for outgoing calls.

I.3.3.1.3 Secure answering (SANSW): Secure answering is a feature by which the service subscriber/user requires that incoming calls cannot be answered unless the answering party first successfully authenticates himself as the wanted subscriber. The use of this feature is strictly related to the privacy requirements from a service subscriber/user; although it has been considered only in the UPT description, it could be useful also for other services, e.g. freephone, VPN, and UMTS. (This feature is currently included in the list of UPT Set 1 optional features in Recommendation F.851 "UPT – Service description", with the name "called party specific secure answering of incoming UPT calls").

I.3.3.1.4 Follow-on (FO): This feature enables a user to make a series of service requests without going through the identification and authentication process before each service feature request. The identification and authentication are performed only for the first service request of the series. The user should be offered the choice after each service feature request to continue with a new service request.

I.3.3.1.5 Flexible (call) origination authorization (FOA): The FOA feature can take effect immediately prior to the time that an IN capable switch would authorize call origination, during the call set-up process. A customized algorithm, provided by the network provider or the subscriber, can then determine whether or not the call should be originated.

If the call is not authorized by the IN customized algorithm, then the call attempt is ended. If the call is authorized by the IN customized algorithm, then, depending on the feature subscriber profile, call processing can bypass switch-based authorization, or call processing can continue with switch-based authorization.

The FOA feature can be used by personal and terminal mobility services to provide authorization capability where a switch has restrictions on call origination authorization. Such restrictions could be a consequence of a switched-based call screening feature, on behalf of the "home" subscriber of a given access line. There exists the possibility that a mobile user may roam to such an access line, at which time restrictions may have to be removed.

I.3.3.1.6 Flexible (call) termination authorization (FTA): The FTA feature can take effect immediately prior to the time that an IN capable switch would authorize call termination, during the call set-up process. A customized algorithm, provided by the network provider or the subscriber, can then determine whether or not the call should be authorized.

If the call is not authorized by the IN customized algorithm, then the call attempt is ended. If the call is authorized by the IN customized algorithm, then, depending on the feature subscriber profile, call processing can bypass switched-based authorization, or call processing can continue with switch-based authorization.

The FTA feature can be used by personal and terminal mobility services to provide authorization capability where a switch has restrictions on call termination authorization. Such restrictions could be a consequence of a switched-based call screening feature, on behalf of the "home" subscriber of a given access line. There exists the possibility that a mobile user may roam to such an access line, at which time restrictions may have to be removed.

I.3.3.1.7 Provision of stored messages (PSM): When the service subscriber registers the location, the network automatically informs the subscriber of the service and sends the voice messages which were stored before.

I.3.3.1.8 Multiple terminal address registration (MTAR): This service feature enables a user to be registered for incoming calls on more than one terminal, with calls being offered to the terminals according to a certain algorithm (e.g. in sequence if there is no answer after a user-determined time (i.e. a user-configurable hunt group), and simultaneously).

I.3.3.1.9 Intended recipient identity presentation (IRIP): This service feature allows identification at the receiving terminal of the intended recipient of an incoming call. It is required to enable Secure Answering (SANSW) to be offered when there is more than one UPT user registered for incoming calls on the one terminal.

I.3.3.1.10 Blocking/unblocking of incoming calls (BUIC): This service feature enables any person, even if not a UPT user, to block and unblock calls incoming to UPT users currently registered on the third party's terminal.

I.3.3.2 Terminal mobility features (FPLMTS)

Terminal mobility provides a tetherless link between the user's terminal equipment and fixed network access points, thereby providing freedom of movement for the user during the use of telecommunication services and service features. The network is able to locate and identify a particular terminal as it appears within a network domain and while it is in motion, whether or not a call is currently taking place. Please note that service features used in FPLMTS but of more general nature (such as internetwork service profile interrogation, modification or transfer, mobile call origination or mobile user call termination) are described in 3.5.

I.3.3.2.1 Terminal authentication (TAUT): The TAUT feature is initiated within the mobility processes of location management (i.e. terminal location registration), call origination, call delivery and at other times as initiated by the network or terminal. In support of security, the feature ensures the validity of the terminal and the network. Also, the feature enables the establishment of a private control and communications channel between the network and a terminal. Authentication process should occur when a terminal authenticates either in its home network or visited network.

I.3.3.2.2 Handover (HOV): The handover (HOV) service feature enables a mobile terminal to change network access areas/points within a network or to an other network, while maintaining the call(s) and/or signalling relationship(s). Active services should be maintained, within the limits imposed by available radio and network resources. In the case of a lack of resources, active services could be modified (e.g. fall back to a lower grade of service quality) or interrupted.

Handover is a complex operation involving four types of entities. They are: the monitoring entity type, the initiating entity type, the performing entity type and the controlling entity type. There could be more than one entity of the same type involved in the handover operation, even during the same handover. Handover can be initiated by the terminal, or network entities.

The handover service feature consists of four processes: the handover monitoring process, the handover decision process, the handover execution process and the handover completion process.

Monitoring process: This process collects radio measurements, aggregates these data (e.g. averaging) and forwards them to the initiating entity. These data are to be used as indicators of the quality of the radio link and of the radio environment (e.g. signal profile and path loss) and also for determining the target cell during the decision process.

Decision process: The decision process comprises two sub-processes which can take place simultaneously. The first one determines when a handover must be triggered by comparing the data from the monitoring process with preset thresholds. The second one selects the target cell according to criteria defined for the handover. Otherwise stated, the decision process uses two sets of criteria: one for the triggering decision and the other for the selection of the target cell.

Execution process: The execution process reserves and allocates the resources and creates the new link and routes the traffic and the signalling of the handed-over communication on this new link. This process could include a macro diversity phase during which two links (the old and the new one) are both in use.

NOTE – The interrelationship between the resource reservation and the execution is not clear enough at this stage. Defining any precedence between the resource reservation and the execution operations in the network could impact on the handover processes at the radio interface. The way by which resource reservation at the radio interface and in the network are linked together for handover execution should be investigated. There is a need to consider the resource reservation process as an underlying process of the execution process.

Completion process: This process frees up any unused resources.

I.3.3.2.3 Terminal location registration (TLR): Terminal location registration is used when terminals notify the system of their location. This is a feature by which the location area information of a terminal is registered with the network. A location registration procedure is generally carried out (A) when the terminal changes the location area, or (B) when no previous location details are known (including updating of the location area information after network or terminal failure).

The location area information is used by the network to handle incoming calls to the terminal. Terminal location registration uses the terminal authentication service feature to validate the terminal. Case (B) also covers the situation when a terminal first appears in a network. The terminal location registration may be accompanied by the internetwork service profile transfer feature.

I.3.3.2.4 Terminal attach/detach (ATDT): The detach feature is used by the terminal to notify the network whether the terminal is temporarily not reachable. The network will modify the status information of the terminal.

The attach feature is used by the terminal to notify the network whether the terminal is reachable again. The network will modify the status information of the terminal.

I.3.3.2.5 Terminal paging (TPAG): This service feature enables the determination of the current location of a user or of a mobile terminal. It pages the terminal in the terminal location registration area based on the stored terminal location information, and determines the visited cell by the response from the terminal.

When several cells exist in a terminal location registration area, the following paging procedures may be used:

1) paging to all the cells in the terminal location registration area simultaneously;

2) paging to some of the cells in turn based on, e.g. priority and traffic statistics.

Different location registration area for macro, micro and pico cells can be overlaid at some locations within the service area. TPAG can be invoked by the network other than the network in which the terminal resides. Paging is executed in the network which covers the location area registered by mobile terminals. It can be executed before incoming calls are routed to the network (i.e. other network can invoke the paging execution to get the routing information).

I.3.3.2.6 Radio paging (RPAG): This service feature enables one-way personal selective calling with alert. The RPAG feature enables a user to send a message, either voice, tone, or alphanumeric, to a selected pager terminal or a group of terminals. This service feature also enables a user to request a receipt for such a message.

The length of both the sending message and reply message will be limited. The sending messages will not be sent on a real-time basis. The waiting duration for a reply message will also be limited. A sending user will send a message to a service centre. The service centre will then send the message through radio channels. For a message without reply receipt requested, the service centre may send the message again at a pre-determined time spacing to ensure reception. For a message requesting reply receipt, the service centre /paging control node will wait for a pre-determined time interval for a reply message, and send it again if no reply message is received. It will repeat this process till a maximum number of tries is reached. The reply message may be generated automatically by the pager terminal. It may also be generated by the paged user within a limited short time interval

(e.g. 30 seconds) after the message is received or the pager terminal will generate the reply message automatically. The service centre will store the reply message with a time-stamp for sender's retrieval. It should be clear that this service feature allows two-way message exchange, but not on a real-time basis, between a sender and a receiver.

I.3.3.2.7 Emergency calls in wireless (ECW): The ECW service feature allows emergency calls to have priority over all other calls to ensure service. Emergency calls can be readily connected without dropping other active calls and without the requirement of successful terminal authentication, privacy or user authentication. Some services restrictions which may apply to the terminal may be suspended (e.g. time-of-day restrictions). Once active, the emergency call has priority over other active calls (e.g. during handover). The ECW service feature consists of three processes.

The emergency call origination process: This process initiates a call with conventional terminal authentication, privacy, user authentication and user validation being performed. However, it does not depend on the success of these processes. The purpose of these processes is to obtain more available information about the user/terminal to facilitate assistance. This information and the location of the cell from which the call is originated should be available for forwarding to the emergency dispatcher, if required. The emergency call can not be denied if an RF channel can be found. The emergency call can be initiated by a user dialling the appropriate digits (e.g. 911) or by a terminal feature button. Either means of initiation can begin the process by placing a "normal" call or by invoking special signalling to the network.

The emergency call re-establishment – loss of RF contact process: This process occurs when the Radio System Function (RSF) is no longer able to receive RF signals from the terminal during an emergency call. The RSF will attempt to re-establish contact with the terminal. If successful, the reconnection processes undertaken are equivalent to those which follow the handover process, namely, the handover execution process and handover completion process.

The emergency call termination – dispatcher hang up process: This process occurs when the emergency operator goes on hook, which is the only means to normally end an emergency call. If the user returns the terminal to on hook condition, then the emergency call does not terminate; if necessary, the above process will be invoked. This emergency call should occur regardless whether a terminal is in its home network, or is in another network (i.e. local network).

I.3.3.2.8 Terminal equipment validation (TEVA): The TEVA feature should be considered as a part of the mobility processes of location management (i.e. terminal location registration), call origination, call delivery and at other times as initiated by the network or terminal. The feature enables FPLMTS network operator to identify stolen, lost, suspicious or non-type-approved terminal equipment and then track or prevent the use of this terminal equipment. A blacklist of the identities of individual stolen, lost or suspicious terminal equipment and a white list of the identities of type-approved terminal equipment will be needed.

Manufacturer should provide a terminal equipment identity, for example IMEI (International Mobile Equipment Identity), to be associated with a terminal equipment itself.

I.3.3.2.9 Cryptographic information management (CIM): Cryptographic information management is a service feature which manages the secret information associated with cryptographic security mechanism including: the enhanced authentication mechanism, the integrity mechanism, and the encipherment mechanism. This feature is concerned with the generation, distribution, storage, updating, and deletion of cryptographic information whose secrecy or integrity must be assured.

This feature is strongly related to User Authentication (UAUT) and Terminal Authentication (TAUT). Associated with each user and terminal is some information which only that user or

terminal and possibly the network knows. Authentication is based upon the user or terminal convincing the network that it knows the correct secret information through some cryptographic protocol and vice versa. Unlike simple password authentication schemes the secret information is never disclosed. Furthermore, during the authentication process, the user and service provider can generate some shared secret information which can be the basis of other security mechanisms.

The identity specific secret information is normally a key for a cryptographic algorithm. These key are classified either as asymmetric or symmetric keys depending on the type of algorithm used. With symmetric keys (associated with conventional secret key encryption algorithms) the network needs to know and assure the confidentiality of the value of the key. Alternatively, if the key is asymmetric (associated with public key encryption algorithms) then the network only needs a copy of the public key of the secret/public key pair. Although the public key does not have to be protected from disclosure, the key must be protected from modification so that the public key really corresponds to the secret key of the entity in question.

When public key schemes are used there is only limited security risk in distributing the authentication information to local service providers and the authentication algorithms could be standardized. Local authentication is possible.

With secret key schemes, the keys could be distributed to local service providers; however, this greatly increases the risk of disclosure. Again, a standard authentication algorithm could be used and local authentication is possible.

As an option with secret key schemes, the home service provider may not wish to disclose the secret key information but only distribute sufficient information for a limited number of authentication. Authentication in this case is essentially centralized. The type of information distributed depends on the authentication mechanism which may vary depending on the network involved. For example, the authentication process may need to proceed with only one message from the user to the service provider. The service provider would either have a list of expected authentication message from the home service provider and use these to check the identity locally, or the authentication message may need to be sent to the home service provider for remote authentication. The scheme chosen has implications for security and worldwide roaming.

As another option with secret key schemes, the home service provider may not wish to disclose the secret key information but only distribute sufficient information for a local key being generated. Those local key would be valid for a limited number of authentication. Authentication in this case is not centralized.

This service feature also provides for the management of cryptographic data associated with encryption. The type of data which should be encrypted depends on the network and may include: user information, especially for radio networks; user identity, and signalling data; and terminal identities.

I.3.4 Other services

I.3.4.1 Internetwork Freephone (IFPH): This service allows the served user having one or more installations to be reached from a specific network other than his/her network with a freephone number, and to be charged for this kind of call. The subscriber's network configuration is defined per subscriber direction using customer-specific information resident in multiple networks.

I.3.4.2 Internetwork Premium rate (IPRM): This service provides two-way interactive communication between callers in one network and service/information providers in another network. The calling party is charged with a premium rate for this kind of call. It can be available in the public telephone network, whereby a service provider having connections to the public network can be allocated a special telephone number by a network operator, known as premium rate number.

The service provider is able to earn revenue for each call successfully made to this premium rate number. In return, the service provider provides caller with some form of information service via the call connection. Calls to the premium rate number are charged to the caller at special rates.

I.3.4.3 Internetwork Mass calling (IMAS): This service is designed to accommodate large volumes of simultaneous calls to a single directory number in another network. It can provide one-way, non-interactive communication between each caller in a given network and a service/information provider in another network. Using this service, the network operator can temporarily allocate a single directory number to the served user. Alternatively, each time a call is made to this number by an end user from another network, for example, an announcement can be played to the end user asking him to input an additional digit to indicate a preference. The choice made can be recorded and a counter incremented. When the service has ceased, the network operator can supply details of the total "votes" cast for each preference to the served user and the special number can be re-allocated.

I.3.4.4 Internetwork televoting (IVOT): This service allows a service/information provider in one network to conduct voting or polling over the phone. The caller in another network votes by placing a call to a specific number corresponding to a voting/polling choice. The service provides communication between each caller in a given network and a service/information provider in another network. The service/information provider receives a tally of the number of calls to each number. Televoting enables subscribers to survey public opinions using the telephone network. Persons wishing to respond to an opinion poll can call televoting numbers to register their votes. The charging is to the discretion of the service subscriber. As an option, using this service, the network operator can temporarily allocate directory numbers to the served user. Each time a call is made to one of these numbers by an end user from another network, an announcement can be played to the end user, acknowledging the call, and a count of calls made to this number can be incremented. When televoting has ceased, the network operator can supply details of the total numbers of calls made to each number to the served user in a different network, and the special numbers can be re-allocated. Calls made to these special numbers may be charged at varying rates.

I.3.4.5 Global Virtual Network Service (GVNS): The global virtual network service is a global switched VPN service supported by multiple networks (e.g. offered to customers over PSTN and/or ISDN).

I.3.4.6 Completion of Call to Busy Subscriber (CCBS): This service enables a calling user encountering a busy destination to have the call completed when the busy destination becomes not busy, without having to make a new call attempt.

I.3.4.7 Conference calling (CONF): This service enables a group of users to be connected into a multi-party call.

I.3.4.8 Call Hold (HOLD): This service allows a user to place a call on hold and play an announcement to the held party, and to initiate a new call. The user can subsequently resume participation in the original call.

I.3.4.9 Call Transfer (CT): This service allows a user to place a call party on hold and to be offered dial tone to provide a destination number (optionally service logic can provide the destination number). Upon successful call set-up, the subscriber is released and the held party is connected to the new destination in a two-party active call.

I.3.4.10 Call Waiting (CW): This service allows a user to notify a subscriber of the occurrence of a call termination attempt, while that subscriber is participating in an active call. Upon the subscriber's request, the network is able to place on hold the call party participating in a previous active call, and allow the subscriber to accept the incoming call. The subscriber is then associated

with both calls and able to toggle between the two calls, causing the other call parties to toggle between hold and active conditions.

I.3.4.11 Hot line (HOT): The hot line service allows a user to place calls without providing, in the call request, the called party information required by the network to route the call. This routing information is stored in the network by prior subscription. The service also allows terminating restrictions to be provided to ensure that certain hot line subscribers only receive calls from other specified users. For the hot line receiving service, the user may receive calls only from a specified list of parties, a screening list before authorizing termination of the call.

I.3.4.12 Multimedia (MMD): This service allows a subscriber to receive or send an integrated communication consisting of mixtures of voice, data, image, and video information. A key capability will be the ability to synchronize and control delivery of information from disparate sources (e.g. voice and data). This will include controlling delivery from multiple sources to a single recipient and from a single source to multiple recipients.

The subscriber will also desire the ability to tailor a particular service to the type of terminating device or subscriber preference (i.e. turning off the video feed). Another key aspect of this service is that additional capabilities may be requested during the call (i.e. adding data capabilities to an existing voice connection).

I.3.4.13 Terminating Key Code Screening (TKCS): This service enables a subscriber to screen incoming calls by means of a user-defined key, i.e. pin code. The callers are required to enter this key. In case of success, either the subscriber is alerted or the busy tone is sent to the caller. In case of failure, appropriate information is sent to the caller. The subscriber may activate and deactivate the service.

I.3.4.14 Message Store and Forward (MSF): This service enables a user to send a message to be distributed to one or several destination users. Different types of messages (such as voice, data, and fax) may be supported and different methods of delivery and/or times of delivery (such as only to pre-subscribed mail-box holders or direct to any access) may be specified.

I.3.4.15 International telecommunication charge call (ITCC): This service allows the holders of a telecommunication charge card to make use of a variety of telecommunication services provided by the card acceptor (visited network) and have the charges billed to the customer's account number by the card issuer (home network). It is described in Recommendations E.113 and Q.86.7.

I.3.5 Other service features

I.3.5.1 Automatic Call Back (ACB): This service feature allows the called party to automatically call back the calling party of the last call directed to the called party.

I.3.5.2 Call Hold (HOLD): This service feature allows a user to interrupt his/her connection to an existing call, without releasing that call. Some of the resources which were dedicated to that call (e.g. bearer capability) become available for other uses.

I.3.5.3 Call Retrieve (CRET): This service feature allows a user to re-establish his/her connection to a call previously placed on hold.

I.3.5.4 Call Transfer (CT): This service feature allows a user who is a party in two separate calls, to cause the other two parties to those calls to be connected to each other, releasing him/her from both.

I.3.5.5 Call Toggle (CTOG): This service feature is applicable to a user who has one active call and one on hold. It allows him/her repeatedly to select the currently held party as the new connection, the previously connected party being automatically put on hold.

I.3.5.6 Call Waiting (CW): This service feature informs a user already engaged in a call that another party is trying to establish a connection to him/her. Signalling means are provided to enable the user to instruct the network as to what further action it should take.

I.3.5.7 Meet-Me Conference (MMC): This service feature allows the user to reserve a conference resource for making a multi-party call, indicating the date, time, and conference duration. At the specified date and time, each participant in the conference has to dial a designated number which has been assigned to the reserved conference resource, in order to have access to that resource, and therefore, the conference.

I.3.5.8 Multi-Way Calling (MWC): This feature allows the user to establish multiple, simultaneous telephone calls with other parties.

I.3.5.9 Call Pick-Up (CPU): This service feature enables a user to associate a call request to an already alerting call. The alerting call awaits answer while the user originating call pick-up signals to the network a desire to connect to the alerting call. The network then connects the call parties.

I.3.5.10 Calling Name Delivery (CND): This service feature gives to the network operator the capability to display/announce the name of the calling party to the calling name delivery user (the called party) prior to answer, thus allowing this user to screen or distinctively answer the call.

I.3.5.11 Services On-Demand (SOD): This service feature enables a user to request new services while initiating or involved in a call, e.g. multi-way calling at a pay phone. This includes the capability to invoke new services for the duration of the call.

I.3.5.12 Message Waiting Indication (MWI): This feature enables a user to be informed that messages for his attention are waiting.

I.3.5.13 Feature Use Charging (FUC): This feature enables the service provider to apply a certain charge to the use of any specified feature.

I.3.5.14 Internetwork Service Identification (INSI): This service feature permits the receiving network, in an internetwork call, to receive from the originating network an indication of the service used in the received call.

I.3.5.15 Internetwork Rate Indicator, Forward (INRI-F): This service feature is the ability to provide across networks, in the forward direction, an indication of the rate either being charged or to be charged for the presented call.

I.3.5.16 Internetwork Rate Indicator, Backward (INRI-B): This service feature is the ability to provide across networks, in the backward direction, an indication of the rate either being charged or to be charged for the received call.

I.3.5.17 Real Time Flexible Rating (RTFR): This service feature is the ability to vary in real time, for a given call, the billing rate, or the party being charged. This could be done at subscriber's direction, during a call or during call set-up.

I.3.5.18 Originating Carrier Identification (OCI): This service feature permits the receiving network, in an internetwork call, to receive an indication identifying the "originating carrier" (i.e. the originating network/network operator).

I.3.5.19 Terminating carrier identification (OTC): This service feature permits the receiving network, in an internetwork call, to receive from the originating network, an indication identifying the network where the call is destined to, or "terminating carrier" (i.e. the terminating network/network operator).

I.3.5.20 Resource Allocation (RAL): This service feature enables the allocation, in advance and for a certain period of time, of pooled resources (e.g. conference bridges) required for a service.

I.3.5.21 Delivery of Complementary Information (DCI): This service feature enables a calling user to supply to the network complementary information (e.g. an account number and a password) associated with the call set-up information.

I.3.5.22 Service Indication (SIND): This service feature enables the called party to receive an indication concerning the presented call (for instance, an application to the freephone service would be the indication that the charge is to be supported by the called party; an application to the call forwarding service would be the forwarding number).

I.3.5.23 Service Negotiation (SNEG): This service feature enables the parties involved in a call to negotiate the bearer services, teleservices and supplementary services to be provided for the call, depending on the services subscribed by the parties, the terminal and network capabilities, etc. This negotiation may take place both during call set-up and during the active call phase.

I.3.5.24 Call Forwarding (CF): As defined in Recommendation Q.1211. Nevertheless, this feature is listed here for inclusion in IN CS-2 because some useful capability had not been fully included in IN CS-1. Refer to Annex B of Recommendation Q.1211 for more detail and for a template description of this feature.

I.3.5.25 B-ISDN Multiple Connections Point-to-Point (BI-MCPP): This service feature enables a user to make a call between two points involving multiple connections, e.g. voice, audio, video, and/or data. This service feature may make use of B-ISDN point-to-point connection service feature (BI-PPC) and need other service features such as multi-connection.

I.3.5.26 B-ISDN Multi-Casting (BI-MCAST): This service feature enables the network to set up multiple connections among multiple parties where the connections are point-to-multipoint unidirectional. This service feature may make use of B-ISDN point-to-multipoint connection service feature (BI-PMC) and/or B-ISDN multipoint-to-point connection service feature(BI-MPC) and need other service features such as leaf control.

I.3.5.27 B-ISDN Conferencing (BI-CONF): This service feature enables the network to set up multiple connections among multiple parties where the connections are multipoint to multipoint. This service feature may make use of B-ISDN multipoint-to-multipoint connection service feature (BI-MMC) and other service features such as third party control.

I.3.5.28 Call Connection Elapsed time limitation (CCEL): This service feature allows a calling party to make calls and communicate with one or more parties within a duration time predefined on a subscription basis. A tone or an announcement may be provided to the parties (i.e. calling and called parties) to indicate that the call will be cleared in a short time.

I.3.5.29 Special Facility Selection (SFS): This service feature enables a call to be routed via a special facility (e.g. a virtual leased line) under the determination of service control.

I.3.5.30 Concurrent Features Activation with Bi-control (CFA-BC): This service feature enables a call to be influenced by some features at two different point concurrently, such as originating side and terminating side. With this feature, a set of features is pre-defined in one service logic and controlled by its context with bi-control relationship.

I.3.5.31.a Customized Call Routing with Public networks (CCR-PU): This service feature permits the public network to access other public networks for call processing and routing information. According to the subscriber's needs, the accessed public network determines each incoming call's appropriate destination, which could be local, national, or international telephone number. This action will remain under the sole control of the accessed public network, allowing for convenient updating, as well as confidentiality. CCR service feature can be provided either as a originating or as a terminating trigger feature.

I.3.5.31.b Customized Call Routing with Customers (CCR-CU): This service feature permits the public network to access customers systems for call processing and routing information. The accessed system (which may be in private network, simple database, a PABX, or a terminal) determines each incoming call's appropriate destination, which could be local, national, or international telephone number. This action will remain under the sole control of the accessed system, allowing for convenient updating, as well as confidentiality. CCR service feature can be provided either as a originating or as a terminating trigger feature.

I.3.5.32 Internetwork Service Profile Interrogation (ISPI): This service feature enables a user to interrogate (read only) the current contents of the user's service profile. The profile information could include information such as telecommunication services subscribed to, default parameters, activated supplementary services, current registrations for incoming and outgoing calls, etc.

The identification and authentication procedures should be required at beginning. The network will respond with the requested information to the user if the information can be disclosed. Any rejection could depend on the authentication procedure, service profile restriction.

I.3.5.33 Internetwork Service Profile Modification (ISPM): This service feature enables a user to modify (read and write) the appropriate user's service profile parameters that are allowed to be modified. Such parameters could be activation or deactivation of supplementary services, various default parameters, or PIN code.

The identification and authentication procedures should be required at beginning. The network will respond with the requested information to the user if the information can be modified. Any rejection could depend on the authentication procedure or service profile restriction.

I.3.5.34 Internetwork Service Profile Transfer (ISPT): This service feature enables service profile information to be transferred to other service profile storage locations in other networks. It is required to enable user profile information portability. The value of data which are simultaneously stored in some networks should be consistent. Information which is transferred to each visited network may depend on the contract with home network. The information updated in a visited network is transferred to the home network and conversely.

I.3.5.35 Reset of UPT registration for incoming calls (IRUR): This service feature enables any person (the third party), even if not a UPT user, to reset any UPT registrations for incoming calls on the third party's terminal.

I.3.5.36 Mobility Call Origination (MCO): The MCO feature covers both mobile call origination and UPT call termination. It is initiated within the mobility process of call origination. This feature does not require any location registration of terminal/users and allows a provision of customized authentication of terminal/user for call origination. This feature is independent of the registration states of the user and other users at the terminal.

For terminals, due to the radio access nature of third generation mobile system such as FPLMTS, the timing of the creation of the access bearers for FPLMTS should be flexible, i.e. the off-air call set-up scheme may be possible.

I.3.5.37 Mobility Incall Delivery (MID): The MID feature covers both mobile user call termination and UPT incall delivery.

I.3.5.38 Data communication between different protocol terminals (DCPT): This service feature enables a mobile terminal to handle data communication between different protocol terminals in the intra-network or internetwork environment. This service feature enables a mobile terminal to handle data communication between different protocol terminals in the intra-network or internetwork environment. This type of data communication service feature is performed by protocol conversion unit within SRF upon requesting the data communication from the subscriber.

I.3.5.39 Charge Determination (CDET): This service feature enables the calculation of charges related to a call. The charged party(s) may include FPLMTS subscribers, UPT subscribers and/or other calling parties. Charges may be based on usage and chargeable events/procedures (e.g. location update and service profile management). Two methods of charge determination are possible.

The first method is off-line charging. Relevant call information (i.e. a call record) is stored by the network at the end of a call. Call records are periodically processed off-line to calculate call charges. Call charge records are then transferred in batch-mode to the local billing centre, which may then forward them to the home service providers or home network designated locations for subsequent billing of their subscribers.

The second method is on-line charging. Charging information is calculated in real time during the call. This method supports calls from pay phones, charge metering and advice of charge. Some calls may involve both on-line and off-line charging (e.g. for split charging).

I.3.5.40 Charge Card Validation (CCV): This service feature provides the ITCC service an authentication feature to compare user-side information, provided to the visited network, with information stored in the home network. Authentication attempts and fails are to be recorded for security purposes.

I.3.5.41 Call Disposition (CD): This service feature provides the ITCC service the means to verify that the card has enough spare credit (e.g. the card usage value has not been exceeded) to give the permission to make the call. It implies that the usage of the card against the credit limit is tracked. The visited network sends to the home network an indication of the call card usage at the end of the call. The home network can accordingly decrement the current credit usage and, if exceeded, subsequent calls at authentication time are inhibited.

I.3.5.42 User Service Interaction (USI): This service feature enables a user to interact with, and thus to send or receive information to or from, a service in association with a call involving this service.

I.3.5.43 Enhanced Call Disposition (ECD): This service feature provides a means to cut down the call as soon as the card usage is exceeded. As soon as the card usage is exceeded, the call should be cut down and subsequent authentication requests should be inhibited according to pre-defined time basis (e.g. monthly and daily). As the card profile might imply different customers (such as the case for a multi-PIN card), concurrent usage, if any, should be tracked from different visited network locations. The previous requirements can be accomplished in different ways; anyway the home network is required to record the database access, in order to allows subsequent actions/requests during the same session. To accomplish the ECD requirements, the visited network gets a credit usage limit indication back in the authentication response. In this case the visited SCF is charged with real time control of the card usage and it has to cut down the call, if needed.

I.4 Service management services

I.4.1 General

This subclause intends to provide short prose descriptions of targeted service management services and service features.

I.4.2 Definition

I.4.2.1 service control service enables a subscriber to directly change the value of the parameters of his/her subscription to a telecommunication service and a service monitoring service after the service provisioning.

I.4.2.2 service control parameters are what a subscriber can directly control regarding a subscription to a telecommunication service and a service monitoring service. The service control parameters available for control within this subscription are specified by service customization parameters.

I.4.2.3 service monitoring service enables a subscriber to get information about the usage of a subscription to telecommunication service after the service provisioning.

I.4.2.4 service monitoring data are what a subscriber can directly monitor regarding a subscription to a telecommunication service.

I.4.2.5 service customization service provides the capability to select the type of telecommunication service feature, service control service, and service monitoring service to be provided to the subscriber after provisioning. Service customization is actually done by a network operator and possibly a service provider based on a subscriber's requirement during the service provisioning phase.

Service customization parameters define the services, parameters, and data which a subscriber can manipulate as part of his/her subscription to a telecommunication service, service control service, and service monitoring service. The service customization parameter value are set through negotiation with a network operator and/or service provider.

I.4.2.6 service management processes are the following types of activity performed by network operators/service providers:

– **service deployment** is the introduction of a service into the IN-structured network in a subscriber independent way;

– **service provisioning** is the initial installation and deployment of necessary resources and data in appropriate network elements to provide a service subscription to a specific subscriber;

– **management during the service utilization** contains service monitoring, service maintenance, service traffic management, audit administration, and billing activities.

The capability of the service management service can be recognized as follows:

a) Generic: Capabilities are generic for all services;

b) Service specific: Capabilities are service specific but common for service subscribers;

c) Service subscriber specific: Capabilities are service subscriber specific as well as service specific.

I.4.3 Service management service/service feature

I.4.3.1 Service customization service

I.4.3.1.1 Telecommunications Service Customization (TSC): Allows customization of telecommunication service to be provided to a specific subscriber according to requirements. There are two types of TSC:

– Generic TSC: Customization parameters for telecommunication service are service-specific but common for subscribers. A network operator sets subscriber-specific initial values for each necessary customization parameter to specify the telecommunication service features.

– Subscriber-specific TSC: TSC is fully subscriber-specific, so it requires the creation of subscriber-specific telecommunication service.

I.4.3.1.2 Service Control Customization (SCC): Allows customization of service control service to be provided to a specific subscriber according to requirements. There are two types of SCC:

– Generic SCC: Service control parameters for service control service are service-specific but common for subscribers. A network operator sets initial values for each necessary customization parameter to specify service control parameters available to the subscription.

– Subscriber-specific SCC: fully subscriber-specific, so it requires the creation of subscriber-specific service control parameters.

I.4.3.1.3 Service Monitoring Customization (SMC): Allows customization of service monitoring service to be provided to a specific subscriber according to requirements. There are two types of SMC:

– Generic SMC: Service monitoring data for service monitoring service are service-specific but common for subscribers. A network operator sets a subscriber-specific initial list of service monitoring data to be collected for a subscription.

– Subscriber-specific SMC: SMC is fully subscriber-specific, so it requires the creation of subscriber-specific service monitoring data collection lists.

I.4.3.2 Service control service

I.4.3.2.1 Subscriber Service Activation/Deactivation (SSAD): Allows the subscriber to activate/deactivate a subscription to a telecommunication service. While the service is deactivated, network provides the default announcement which indicates that the telecommunication service stops.

I.4.3.2.2 Subscriber Monitoring Activation/Deactivation (SMAD): Allows the subscriber to activate/deactivate a subscription to a service monitoring service.

I.4.3.2.3 Subscriber Profile Management (SPM): Allows the subscriber to manage his/her subscription to a telecommunication service profile and a service monitoring service profile, i.e. terminating destinations, announcements to be played, call distribution, and call originating areas for traffic monitoring.

I.4.3.2.4 Subscriber Service Limiter (SSL): Allows the subscriber to restrict the number of simultaneous usage of the telecommunication service.

I.4.3.2.5 Subscriber Service Invocation (SSI): Allows the subscriber to invoke the telecommunication service. The target telecommunication service should be designed to be invoked using SSI.

I.4.3.3 Service monitoring service

I.4.3.3.1 Subscriber Service Report (SSR): Allows the subscriber to get a report on the usage of service subscriptions. The report may involve some statistics, such as the number of calls and mean call duration under specific conditions like time of day, origination area and termination telephone.

I.4.3.3.2 Billing Report (BR): Allows the subscriber to get billing report of a chosen type. Several types of billing report may exist, e.g. total, terminating telephone basis, and group basis.

I.4.3.3.3 Subscriber Service Status Report (SSSR): Allows the subscriber to receive the following status on each subscription to a telecommunication service:

– performance (e.g. number of calls per measurement period);

– congestion (e.g. number of blocked calls per measurement period);

– fault (e.g. number of failed calls per measurement period).

I.4.3.3.4 Subscriber Traffic Monitoring (STM): Allows the subscriber to monitor real-time usage of service subscriptions (e.g. the number currently processing calls in mass calling service, and the length of queue in call-queueing service).

I.4.3.3.5 Subscriber service Management service Usage Report (SMPUR): Allows the subscriber to get a report on the usage of service control/monitoring service.

I.4.3.4 Other service management services

I.4.3.4.1 Subscriber Service Testing (SST): Allows the subscribers to perform their own test service subscriptions.

I.4.3.4.2 SMP Usage Report (SUR): Allows the subscriber to get a report on usage of SMP (e.g. number of login sessions, length of each, CPU usage, and mass storage usage).

I.4.3.4.3 Subscriber Security Control (SSC): Allows the subscriber to change security parameters (e.g. password).

I.5 Service creation services

I.5.1 General

This subclause intends to provide short prose descriptions of targeted service creation services.

I.5.2 Service specification services

I.5.2.1 feature interaction detection: Designed to aid detection of potential interactions between a new feature and existing features within a service (new or existing).

I.5.2.2 cross-service feature interaction detection: Designed to aid detection of potential interactions between a new feature and existing features across services (new or existing).

I.5.2.3 feature interaction rule/guidelines generation: Permits the specification of feature interaction rules for interactions within and across services (e.g. provisioning/rules governing which features can be provisioned together under specified conditions and network-level rules for run-time feature interaction management).

I.5.2.4 service and SIB cataloguing: Provides a system for cataloguing the services and service-independent building blocks (SIBs), their intended uses, their inputs, their outputs, etc. for reference and re-use.

I.5.2.5 created service resource utilization: Provides the capability to predict network resource utilization for services prior to deployment and to monitor actual resource utilization by a deployed service and limited testing use.

I.5.3 Service development services

I.5.3.1 creation interface selection: Permits the selection of different interface devices for obtaining access to a service creation environment (SCE) (e.g. graphic terminals or ASCII terminals).

I.5.3.2 creation initiation: Controls the process of initiating the creation of a new service or SIB (e.g. initial front-end loading activities, designation of permissible users).

I.5.3.3 editing: Permits the editing of partially-created or existing services or SIBs.

I.5.3.4 combining: Permits the creation of new services or SIBs as combinations of existing services and SIBs with new service logic to bind them together.

I.5.3.5 data population rule generation: Permits the creation of the data population mechanism that are required for both the deployed services and supported services in the Service Management System (SMP).

I.5.3.6 SMP service creation: Permits the creation of the SMP functions that are required to support the telecommunication services being created (e.g. OAM&P service logic programs for the SMP). Support is supplied as for all other services.

I.5.3.7 syntax and data checking: Permits systems checks (graphical or textual) and data definition checks as a part of the service or SIB creation process.

I.5.3.8 service and SIB archiving: Performs all the activities associated with storage, retrieval, and management of existing services and SIBs and services and SIBs still in the creation process.

I.5.3.9 service configuration control: Permits access to the appropriately defined current and former versions of each service so that the defined set is available for use as desired.

I.5.3.10 SIB configuration control: Permits access to the appropriately defined current and former versions of each SIB so that the defined set is available for use as desired.

I.5.3.11 network configuration tracking capability: Provides the functions necessary to ensure that the SCE has an accurate representation for as much of the network as it needs to perform the service creation functions.

I.5.4 Service verification services

I.5.4.1 SCE testing: Supports the localized testing of a created service or SIB in the SCE (e.g. debuggers, code tracers, graphics analysers).

I.5.4.2 created service simulation: Supports the use of simulation testing of created services prior to release to the network.

I.5.4.3 cated service live testing: Supports the distribution to the full network or to a limited set of network elements for "live" testing prior to making the new service generally available.

I.5.5 Service deployment services

I.5.5.1 SMP-created service data and service logic program update: Provides the ability to build and distribute updates to the installed services being controlled by an SMP (e.g. modifications to general data for a service, bug fixes).

I.5.5.2 Service distribution: Controls the distribution of services across a complex of related service creation entities. Service can be accessed and used at all sites in the associated system.

I.5.5.3 SIB distribution: Controls the distribution of SIBs across a complex of related service creation entities. The SIB can be accessed and used at all sites in the associated system.

I.5.5.4 Data rule distribution: Permits the distribution of updated data rules into the existing services and support entities.

I.5.5.5 Feature interaction rule distribution: Permits the distribution of updated feature interaction rules into the system to improve existing rules and account for additional services in the system.

I.5.5.6 Multiple SMP support: Permits the service creation entities to interact with different SMP implementations (e.g. permits one SCE to interact with SMPs of multiple vendors).

I.5.5.7 Network tailoring: Provides the functions necessary to modify the SCEs and all the service-description-related information when changes occur in the structure of the network the SCEs are interacting with (e.g. the addition, deletion, modification of network elements).

I.5.5.8 Network element capability specification: Permits the specification of the capabilities of network elements in a form that will be required for use during the service creation activities.

I.5.5.9 Network element function/capability assignment: Permits the assignment within the service creation entities of function or capability to network elements as they will be used by the created services (especially useful when multiple network elements are capable of performing the same function). This assignment may be only for a particular service being created or set as a default for all services that are created.

I.5.6 Service creation service management services

I.5.6.1 SCE access control: Provides the access security and limits the forms of access to those permitted for each registered user of an SCE.

I.5.6.2 SCE usage scope control: Permits the definition of levels of activity for utilization of the SCE capabilities (e.g. standard service creation activities, new service creation element generation, and system-level activities with unlimited permission).

I.5.6.3 SCE recovery: Permits the ability to recover the most recent versions of all activities, data, and service definitions after and SCE outage.

I.5.6.4 SCE release management: Controls the SCE version releases that are available for use (actively or by recall) on a particular platform element.

I.5.6.5 SCE capability expansion: Provides the ability to add new SCE functions (e.g. support functions such as editing service creation capabilities or improving implementations of existing capabilities).

I.5.6.6 SCE conversion: Converts the representation of the created service from the representation that is used on one service creation platform into a representation that can be used on another service creation platform.

I.5.6.7 cross-SCE service maintenance: Provides the functions necessary to ensure that the service creation infrastructures on different SCE implementations within related systems are capable of interworking as required.

I.5.6.8 SCE-to-SCE system consistency: Provides the functions necessary to ensure that all SCEs in the related complex have consistent data service representations and capabilities.

I.5.6.9 SCE service/modular/system transference: Provides the ability to transfer created or partially-created services, SIBs, and new SCE system creations across a complex of related SCEs.

I.5.6.10 conversion of created services: Permits the conversion of all existing service representations to the representations required in another SCE implementation (e.g. different SCE implementations or a new release of the same implementation).

I.5.6.11 service management interaction: Permits interaction with the SMP (e.g. obtains data not normally available to the SCE).

ITU-T RECOMMENDATIONS SERIES

Series A	Organization of the work of the ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communication
Series Z	Programming languages