Draft EG 201 367 V1.1.1 (1998-11)

ETSI Guide

Intelligent Network (IN);
Number Portability Task Force (NPTF);
IN and Intelligence Support for Service Provider Number Portability

Reference

DEG/NA-061501 (cno00icq.PDF)

Keywords

portability; IN, architecture, management

ETSI

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet

secretariat@etsi.fr
http://www.etsi.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1998.
All rights reserved.

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Guide (EG) has been produced by ETSI Technical Committee Network Aspects (NA), and is now submitted for the ETSI standards Membership Approval Procedure.

1 Scope

The present document covers network intelligence requirements, taking account of current and emerging Intelligent Network Standards, in order to assess the ability of Intelligence and an Intelligent Network to support Geographic and Non-Geographic number portability. The study will focus on a review of IN Capability Sets 1, 2 and identify any desirable enhancements to support number portability under IN CS3. The report will recognize that an IN solution can provide high functionality with fairly high throughput or traffic handling capability but Number portability may only require relatively low functionality. It should also be noted that IN Capabilities might exist in Originating, Donor, Transit or Recipient Networks. The report takes account of the requirement to minimize additional costs and avoid extended call set-up times. Billing aspects are outside the scope of the present document.

1.1 Purpose

The purpose of the present document is to provide scope guidance toward the following stages of the Number Portability Standards process.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] TR 101 119: "Network Aspects (NA); High level description of number portability".

[2] TR 101 118: "Network Aspects (NA); High level network architecture and solutions to support number portability".

[3] TR 101 122: "Network Aspects (NA); Numbering and addressing for Number Portability".

[4] TR 101 073: "Number portability for pan-European services".

[5] TR 102 081: "Network Aspects (NA); Signalling Requirements for Number Portability".

[6] Void.

[7] Void.

[8] Void.

[9] ETS 300 741: "Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for wide-area paging equipment".

[10] ITU-T Recommendation Q.1214: "Distributed functional plane for intelligent network CS-1".

[11] ITU-T Recommendation Q.1215: "Physical plane for intelligent network CS-1".

[12] ITU-T Recommendation Q.1218: "Interface Recommendation for intelligent network CS-1".

[13] ITU-T Recommendation Q.1224: "Distributed functional plane for Intelligent Network Capability Set 2".

[14] ITU-T Recommendation Q.1225: "Physical plane for Intelligent Network Capability Set 2".

[15] ITU-T Recommendation Q.1228: "Interface Recommendation for Intelligent Network Capability Set 2".

3 Definitions and abbreviations

3.1 Definitions

For the Generic Number Portability definitions please refer to Number Portability Task Force reports: TR 101 119 [1] and TR 101 118 [2], TR 101 122 [3] and TR 102 081 [5].

3.1.1 Donor Exchange

A Donor Exchange is the initial Exchange where a number was located before ever being ported.

3.1.2 Donor Network

A Donor Network is the initial Network where a number was allocated by the NPA before ever being ported.

3.1.3 Geographic Number (GN)

A Geographic Number (GN) is a Directory Number from that part of the national numbering scheme that is used to identify fixed line terminations. Prior to Number portability these numbers are geographical in that sense that they convey the location of the customer.

3.1.4 Geographic Number Portability (GNP)

See Service Provider Portability for Geographic Numbers.

3.1.5 Network Operator

A Network Operator is an entity that operates public telecommunications network in order to route calls.

3.1.6 Non Geographic Number (NGN)

Non-geographic Number (NGN) is a Directory number that is not a Geographic Number. A Non-geographic Number does not imply the Geographic location of the customer.

3.1.7 Non Geographic Number Portability (NGNP)

See Service Provider Portability for Non Geographic Numbers.

3.1.8 Number Translation Function

Number Translation Function is the function whereby a number (Routeing or Called Party), is translated to a destination number, possibly according to special conditions such as time of day, in order that calls can be completed.

3.1.9 Network Intelligence (NI)

The generic ability of a network to provide intelligence.

3.1.10 Intelligence

Intelligence is a network capability having the ability to dynamically effect call control and route calls according to an incoming number to a recipient network address. This is achieved by reference to a database to obtain, for example, a users profile, or time of day requirements. Intelligence can be provided by an Intelligent Network which has specified standard Interfaces between Service Control Functions, Switching Functions, Specialized Resource Functions and Database Functions.

3.1.11 Intelligent Network (IN)

See ITU-T Recommendation series Q.12xx.

3.1.12 Service Provider Portability for Geographic Numbers

Service Provider Portability for Geographic Numbers is a service that enables customers to resign their subscription with a Service Provider and to contract another subscription with another Service Provider without changing their Geographic Number, without changing their location, and without changing the nature of the service offered.

This service is also known as Geographic Number Portability (GNP) and as Local Number Portability (LNP).

3.1.13 Service Provider Portability for Non-geographic Numbers (NGNP)

Service Provider Portability for Non-geographic Numbers (NGNP) is a service that enables customers to resign their subscription with a Service Provider (Donor) and to contract another subscription with another Service Provider (Recipient) without changing their Non-geographic Number, and without changing the nature of the service offered.

This service is also known as Non-Geographic Number Portability (NGNP).

3.1.14 Service Provider Portability for Pan-European Services

Service Provider Portability for Pan-European Services is a service that enables a user to resign their subscription with their current Pan European Service Provider and subscribe to a competitor without changing their pan European Service Number.

3.1.15 Serving Exchange (SE)

A Serving Exchange (SE) is, within the present document, an Exchange within a Serving Network (SN) that makes a data base (Exchange internal or external) access to retrieve Routeing Number for a call to a Portable Number.

3.1.16 Serving Network (SN)

A Serving Network (SN) is, in the present document, a Network that makes a data base (Network internal or external) access to retrieve Routeing Number for a call to a Portable Number, i.e. it determines whether a number has been ported, and, if so, provides an appropriate routeing number. This functionality may be distributed.

3.1.17 Direct Dial In (DDI) - Variable Number Length

For lines terminating on a PABX, calls may be internally routed on public network incoming digits, in some networks; these incoming digit strings may be of variable length.

3.1.18 Masquerade (" spoofing ")

The pretence of an entity to be a different entity. This may be a basis for other threats like unauthorized access or forgery.

3.1.19 Unauthorized access

An entity attempts to access data in violation to the security policy in force.

3.1.20 Eavesdropping

A breach of confidentiality by monitoring communication.

Loss or corruption of information: The integrity of data (transferred) is compromized by unauthorized deletion, insertion, modification, reordering, replay or delay.

3.1.21 Replay of information

The repetition of previously valid commands and responses with the intention of corrupting service or causing an overload.

3.1.22 Repudiation

An entity involved in an event denies that involvement.

3.1.23 Forgery

An entity fabricates information and claims that such information was received from another entity or sent to another entity.

3.1.24 Denial of service

An entity fails to perform its task or forces an other entity to fail. Interfering with signalling may make such denial.

3.2 Abbreviations

For the purposes of the present document the following abbreviations apply:

ACL	Access Control List
CCBS	Call Completion to Busy Subscriber
CCF	Call Control Function
CCNR	Call Completion No Reply
CCPF	Call Control Portability Functions
CdPN	Called Party Number
CS	Carrier Selection
DB	Data Base
DBMS	Database Management System
DDI	Direct Dialling In
DN	Directory Number
GN	Geographic Number
GNP	Geographic Number Portability
GW	Gateway exchange
IAM	Initial Address Message
IN	Network Intelligence
INAP	IN Applicant Part
ISUP	ISDN User Part
LE	Local Exchange
NE	Network Element
NI	Network Intelligence
NGN	Non Geographic Number
NGNP	Non Geographic Number Portability
NP	Number Portability
NPA	Numbering Plan Administration

NPCF	Number Portability Control Functions
NPDF	Number Portability Data Functions
NPMF	Number Portability Management Functions
NPTF	Number Portability Task Force
PBX	Private Branch Exchange
PNO	Public Network Operator
POI	Point Of Interconnection (with PSTN)
QoR	Query on Release
REL	RELease
RI	Routeing Information
RN	Routeing Number
SCF	Service Control Function
SCCP	Signalling Connection Control Part
SCP	Service Control Point
SDF	Service Data Function
SDP	Service Data Point
SE	Serving Exchange
SMF	Service Management Function
SMP	Service Management Point
SN	Serving Network
SSF	Service Switching Function
SSP	Service Switching Point
SSCP	Service Switching and Control Point
TCAP	Transaction Capabilities Application Part
TE	Transit Exchange

4 General assumptions and Requirements on Intelligence support for NP

Network Intelligence (NI), with respect to Number Portability, provides the capability to obtain Routeing Information for ported / portable numbers, to enable routeing of incoming calls to the recipient network and to the recipient exchange.

4.1 Objectives

The objective of IN / Intelligence, with respect to Number Portability, is to provide number translation capabilities with a minimum impact on network performance or additional cost. It shall also provide increased flexibility when compared to traditional Exchange based solutions.

4.2 Requirements on Intelligence in the network to support NP

The following requirements, but not necessarily all, should be met according to implementer's requirements:

a) Overlap signalling, before and after number translation, to support variable length dialling plans

b) Triggering on number blocks (allowing NP) shall be supported.

   To support NP solution according to "all call query" principles.

c) Triggering on release (e.g. indicating "vacant" or "ported") shall be supported.

   To support NP solution according to "query on release (QoR)" principles.

d) Triggering on "number ported" shall be supported.

   To support NP solution according to "onward routeing by Donor LE" principles.

e) Generate a release with "re-Routeing information".

   To support NP solution according to "dropback" principles.

f) Generate a onward routeing with "re-routeing information".

   To support NP solution according to "onward routeing", "Query on Release" and the different "all call query" principles.

g) High throughput to allow all call query solutions (see TR 101 118 [2]).

The requirements above are identified to enable support of the different NP solutions described in TR 101 118 [2].

5 High Level Architectures and Solutions for NP

5.1 General information

In the TR 101 118 [2] several NP DB query triggers have been identified, they are:

a) "Query on Ported";

   At detection, in Donor Exchange, that called party number has been ported.

b) "Query on Release";

   At reception of a release message indicating that called party number may have been ported

   (e.g. reception of vacant or ported indication).

c) "All call Query";

   At reception of a called party number being part of a number block that allows NP.

These triggers are used to initiate a number translation by use of centralized network intelligence. The triggers can be initiated from Originating, Transit, Donor and Recipient Exchanges.

Queries, from the Exchanges, access a real-time database system, which responds with the Routeing Information back to the Exchange. A simple and straightforward Routeing service, translating the dialled number into a Routeing Information is required. Routeing Information contains the Routeing and/or Directory number.

Detailed explanation about the routeing information, for NP, can be found in TR 101 122 [3].

5.2 Generic Functional modelling of a solution for NP

A generic functional model for Number Portability, as outlined in figure 1, is described in TR 101 118 [2]. The functional entity model incorporates call control, NP triggering, NP service logic, NP data management and a real-time NP database.

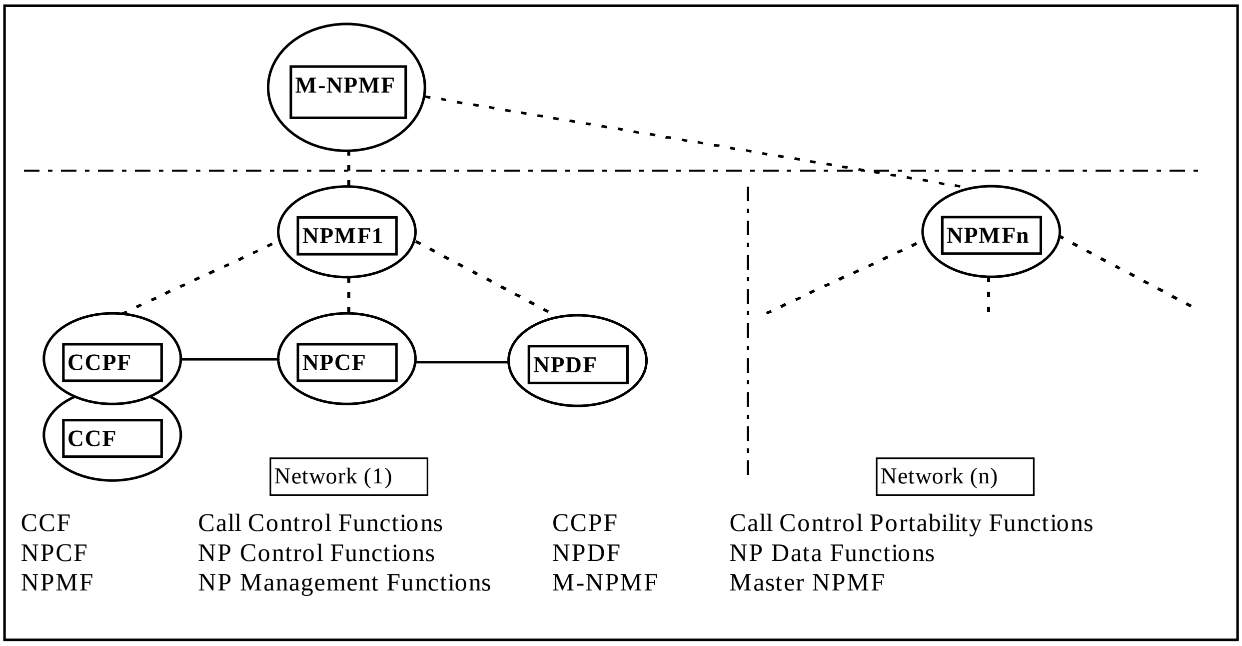


Figure 1: Generic Functional entity Model for number portability

The figure 1 is further elaborated, with respect to using IN functional entities, in the chapters analysing IN capability sets.

5.3 Generic Network Architecture for management of NP data

A generic Network Architecture for management of NP data, as outlined in figure 2, is described in TR 101 118 [2]. The network layout incorporates Master NP management functions (superior to operator internal level), Operator internal NP Management Functions and finally Network Elements (NE). The sum of NE's contains functions for call control, NP triggering, NP service logic and a real-time NP database, i.e. different NE's (within a particular Network) can do specialized NP related tasks but are not limited to one task only. I.e. the Generic network layout allows each network to have an own private: network structure, Routeing structure, management structure, NP task allocation and is finally free of choosing network components as long as external NP requirements are fulfilled.

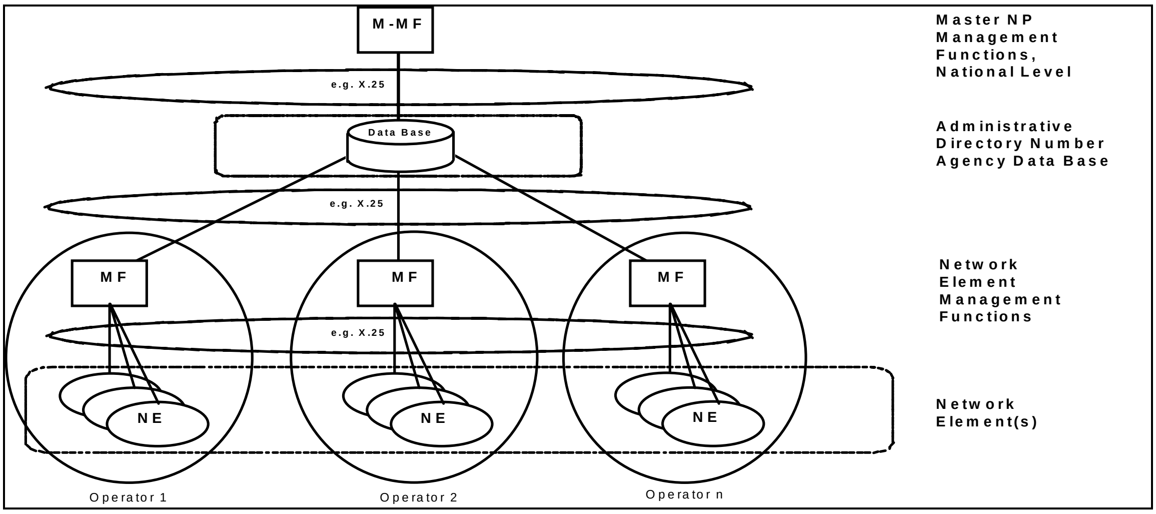


Figure 2: Generic Network architecture for management of NP data when data is maintained Nationally, and when NP data is replicated in each of involved Operators Network

The figure 2 is further elaborated, with respect to using IN elements, in the chapters analysing IN support for NP data management.

5.4 Generic Routeing and Addressing requirements to support NP

5.4.1 Transfer of Routeing Information

Signalling protocols supports already Pre-fixing of Directory Number but separate Routeing Number solutions requires signalling enhancements.

See TR 101 122 [3] for Pre-fix and Routeing Number principles / solutions of addressing the Recipient Network and Exchange.

5.4.2 Calling Party information

It has been identified the need for forward transfer of geographical information related to the calling party, in addition to the existing Calling Party Number, so that e.g. requirements on routeing to emergency numbers (closets office) can be fulfilled also in a number portability environment.

5.4.3 Routeing Numbers

In addressing the Recipient Network and Exchange the following addressable entities, depending on used structure for Routeing Number, are identified in TR 101 122 [3]:

Recipient Network:
in this option, the routeing number identifies the network where the customer is now located. Therefore the routeing process will need an additional information to be completed.

POI:
in this option, the routeing number identifies a gateway (POI) to the next network in the routeing process. Therefore the routeing process will need an additional information to be completed.

Recipient exchange:
in this option, the routeing number identifies the exchange the customer is now located. Therefore the routeing process within the recipient exchange will need additional information to be completed.

Subscriber / Access line / service:
in this option, the routeing number identifies the termination point. The ported customer identified by the RN is unique. Therefore the routeing process can be completed without any additional information.

Identification of any combination of the above entities could be used, again depending on used structure of RN.

5.4.4 Routeing loop detection

It has been decided (in NPTF) that the use of ISUP hop counters (confirmed in ISUP - 97) is an appropriate method for detecting routeing loops that might occur if NP Data Bases in different networks have contradicting data, see TR: "Signalling Requirements for Number Portability" for further information.

5.5 Generic Signalling Requirements to support NP

The signalling requirements identified by the TRs 101 119 [1], 101 118 [2] and 101 122 [3] are collected and described in TR 102 081 [5].

6 Service Provider Portability of Geographic Numbers

6.1 General Information

Geographic Numbers (GN), by their nature, are generally related to a particular (e.g. local) Exchange, i.e. each call to a GN shall be routed to the particular exchange that the called subscriber is connected to. Prior the introduction of Number portability it has been possible to address both by using the Number Block that called number is part of.

This traditional principle for Routeing of a call will need to change when introducing Service Provider Portability of Geographic Numbers, since the Number Block that the called number is part of will not always identify a particular operators Network or Exchange.

The NP related tasks for Service Provider Portability of Geographic Numbers (GN) incorporate therefor obtaining of routeing information identifying both Recipient Network and Exchange and Initiation of routeing towards the obtained destination. Obtaining the complete routeing information can be done by one NP DB query or by two or more steps.

For definitions and further information see TRs 101 119 [1] and 101 118 [2].

6.2 IN support for Service Provider Portability of Geographic Numbers

The requirement for IN support of Service Provider Portability of Geographic Numbers incorporate firstly the trapping (i.e. triggering of an IN NP DB query) of each call to a ported-out / portable number thereafter obtaining a routeing number and finally initiating call set-up towards the Recipient network and exchange. Management of NP data is elaborated in chapters addressing management issues.

The IN Architecture provides the basic relationship between the Service Control, Service Switching, Connection Control, Database and Specialized Resources Functions. There also are links with the Management and Service Creation Functions.

The interface between the switching network and the IN-NP DB is provided by the INAP (Intelligent Network Application Part) protocol.

Special requirements exists regarding support for cases where:

a) Number ranges have variable length;

   This might require multiple IN NP DB triggering, e.g. by request for more data, depending on number length knowledge in SSP.

b) DDI ranges have variable length (within a number range);

   This requires overlap signalling even after number translation all the way to the PBX, since the number length (per unique number) is controlled by the PBX owner.

The IN-triggering, to obtain a routeing number, is applicable both for circuit related signalling (call set-up) and for non-circuit related signalling (TCAP based services).

NOTE: Options a and b are only applicable for circuit related signalling, since the complete destination needs to be reached (i.e. all digits received) prior calling subscriber is able to activate e.g. CCBS and CCNR services.

6.3 IN Trigger Conditions, circuit related signalling to Geographic Numbers

6.3.1 General Information

Triggering of an IN NP DB query, during call set-up, can in principle be due to:

a) A Subscriber number being identified as ported-out, i.e. a "ported or vacant number" based trigger.

b) A received release message telling "e.g. number ported-out or vacant", i.e. a "release" based trigger.

c) A received call to "portable number", i.e. a "number block" based trigger.

For further information see TR 101 118 [2] clause "High Level Evolutionary Network models to support call set-up when Service Provider Portability is allowed for Geographic Numbers".

6.3.2 IN trigger per NP solution

6.3.2.1 High level NP solution "Onward Routeing"

The Onward Routeing NP solution, as described in TR 101 118 [2], could incorporate IN triggering based on a "ported number" based trigger.

6.3.2.2 High level NP solution "Dropback"

The Dropback NP solution, as described in TR 101 118 [2], could incorporate IN triggering based on any of: "ported number", "release" and "number block" based triggers.

6.3.2.3 High level NP solution "Query on Release"

The Query on Release (QoR) NP solution, as described in TR 101 118 [2], could incorporate IN triggering based on a "release" based trigger.

6.3.2.4 High level NP solution "All Call Query"

The All Call Query NP solution, as described in TR 101 118 [2], could incorporate IN triggering based on a "number block" based trigger.

6.3.3 Network Location for IN Trigger

6.3.3.1 IN Triggers in an Originating network

In an originating network the following IN triggers are valid:

a) "release" based trigger;

b) "number block" based trigger.

The triggers are applicable to Originating, Transit and Gateway exchanges.

6.3.3.2 IN Triggers in a Transit network

Same as for Triggers in Originating Network.

6.3.3.3 IN Triggers in a Donor Network

Same as for Triggers in Originating Network but in addition also Trigger on "ported number".

Trigger on "ported number" is only applicable in Donor Exchange.

Trigger on "release" and trigger on "number block" is applicable in Gateway, TE or even Donor Exchange.

6.3.3.4 IN Trigger in Recipient Network

In a Recipient network only the trigger on "number block" is applicable.

6.4 IN Trigger Conditions, Non-circuit related signalling to Geographic Numbers

6.4.1 General Information

Triggering of an IN DB query, during non circuit related signalling, can in principle be due to:

a) a Subscriber number being identified as ported-out, i.e. a single number based trigger;

b) a received call to "portable number", i.e. a number block based trigger.

For further information see TR 101 118 [2] clause "High Level Evolutionary model for NP and SCCP using services to Geographic Numbers".

6.5 Evaluating IN Capability Sets supporting NP of Geographic Numbers

6.5.1 General Information

The figure 3 shows an overview between NP DB query triggering method, DB access point, IN trigger, frequency of DB query and IN capability set supporting the trigger.

NP DB query Triggering Methods:	Database access point obtaining of Routeing Information		Frequency for database query	
	within switching system	IN trigger	Calls to	IN CS
Query on Ported	Donor / Serving Network	"Line_based_trigger_called_party"	ported numbers	CS2
Query on Release (1)	Serving Network	"Release with special cause value(-s)"	ported numbers	CS2
Query on Release (2)	Serving Network	Release without special cause value(-s)", e.g. on "vacant" indication	Ported and vacant numbers	CS1
All call Query (Fixed number block length)	Serving Network	"complete number"	all portable numbers	CS1
All call Query (Variable number block length)	Serving Network	"incomplete number"	all portable numbers	CS1

Figure 3: Overview between NP DB query triggering method and frequency of DB query

The figure 4 shows an overview of NP related actions required by SSF and SCF per routeing method.

NP Redirection Methods (after NP DB query):	Service Switching Functionality	Service Control Functionality	IN capability set support
Drop Back	a) Previous network supports Dropback: Generate a release of call with redirection Information. b) Previous network do not support Dropback: Generate an onward routeing using the obtained RN	Generate Drop-back message. Generate forward call set-up concatenated number Generate forward call set-up separated number	future CS CS1 future CS
Onward Routeing	Generate an onward routeing using the obtained RN.	Generate forward call set-up concatenated number Generate forward call set-up separated number ffs	CS1 future CS
All Call Query (Fixed number block length)	Generate an onward routeing using the obtained RN.	As above.	As above
All Call Query (Variable number block length)	Handle request for more digits. Generate an onward routeing using the obtained RN.	Request for more digits until RN is obtained. Generate call set-up as for Onward routeing.	As above

Figure 4: Overview of NP related actions required after SCF/SDF has been consulted

NOTE: Special requirements exists in the case where variable number length of e.g. DDI numbers are allowed, i.e. overlap signalling is be allowed also after number translation (regardless triggering method) since it is only the PBX owner that knows the complete number length.

6.5.2 IN CS1

6.5.2.1 IN CS1 Functional Entity Architecture supporting generic Functional modelling of NP

The generic requirements for a centralized network intelligence to provide number translation, for Number Portability reasons, can be mapped on an Intelligent Network architecture. The functional entities CCPF, NPCF, NPDF and NPMF, as outlined in figure 1, can easily be mapped onto the SSF, SCF, SDF and SMF respectively of an CS1 Intelligent Network architecture, as outlined in figure 5.

The M-NPMF can currently not be mapped onto IN functional entities.

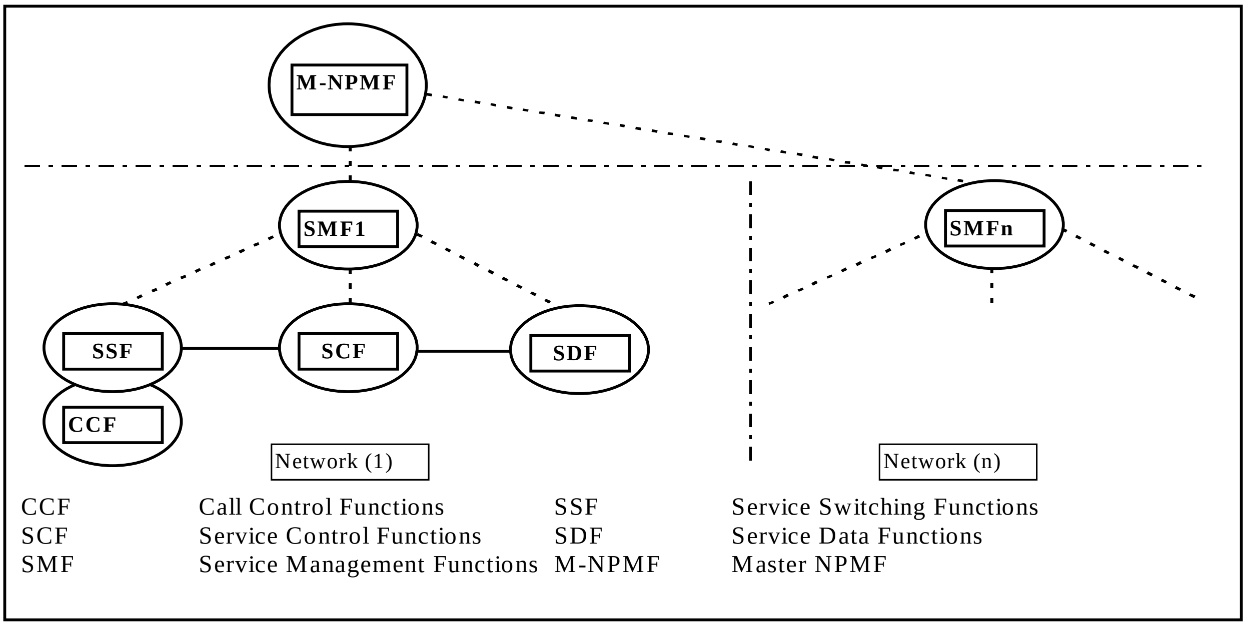


Figure 5: Functional entity Model e.g. based on an IN-CS1 structured number portability solution

6.5.2.2 IN CS1 Physical Entity Architecture supporting generic Architecture for NP

The generic functional entities, as related to providing number translation by an IN structured solution for NP as outlined in figure 2, can be mapped to IN Physical Entities: CCF&SSF to SSP, SCF to SCP, SDF to SDP and finally SMF to SMP. In addition there exists the SSCP which is a collocation of CCF, SSF and also SCF.

For further information see ITU-T Recommendations Q.1214 [10], Q.1215 [11] and Q.1218 [12] for CS1 Architecture Diagrams.

For more information on ETSI CS1 see ETS 300 741 [9].

6.5.3 IN CS2

6.5.3.1 IN CS2 Functional Entity Architecture supporting generic Functional modelling of NP

The Functional Entity architecture valid for IN CS1 is valid also for IN-CS2.

6.5.3.2 IN CS2 Physical Entity Architecture supporting generic Architecture for NP

The IN Architecture supporting generic Architecture for IN CS1 is valid also for IN-CS2.

For further information see ITU-T Recommendations Q.1224 [13], Q.1225 [14] and Q.1228 [15] for CS2 Architecture Diagrams.

6.6 Information flows for GNP when IN architecture is used

6.6.1 General Information

The following descriptions give some examples of possible scenarios for Geographic Number Portability Solutions where IN architecture is used to support NP related number translation and call control, The examples / solutions focuses on actions required by IN functional / physical entities.

A more complete list of high level scenarios and further explanation of pros and cons for the alternatives is found in TR 101 118 [2].

The special actions required for variable number length and variable DDI length is shown in some scenarios only but is applicable to all scenarios.

The Database's location is not the critical issues in the figures, instead the point where query is made and what caused the IN triggering are the important issues. Location of DB is mainly a NP data management issue and not a traffic issue.

IAM, REL, Dropback, etc. are only to be understood as logical signalling messages, i.e. the actual message name is dependent of used signalling system.

The variations of interconnections are only examples the actually used interconnection is network dependent.

Transit networks are optional and included only to give a better understanding of interconnection issues when routeing calls / services towards ported / portable Geographic Numbers.

6.6.2 Onward Routeing by donor LE combined with a second query in Recipient Network

The high level scenario addressed in this chapter is the case where the call is first routed to the Donor Network, optionally via Transit Network(-s) A and from there onward routed towards the recipient Network, optionally via Transit Network(-s) B, as outlined in figure 7.

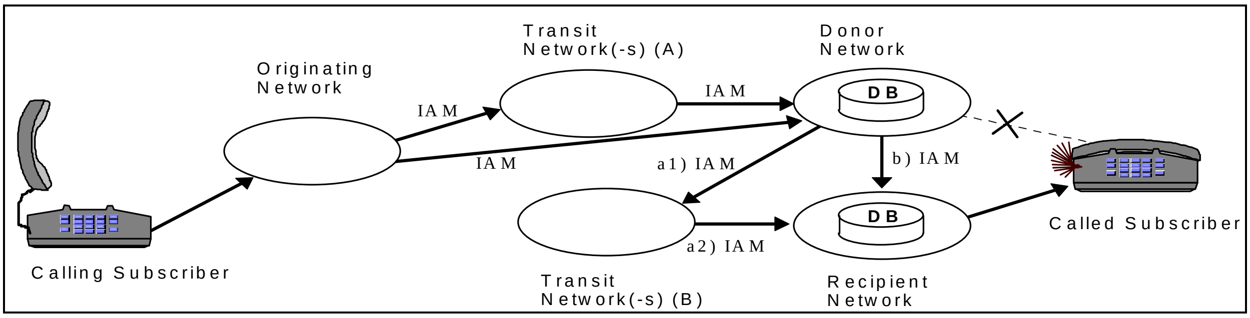


Figure 6: Onward Routeing by Donor combined with Query by Recipient Network

The figure 6 above can be opened / expanded to see how IN components can be used to perform the required NP tasks within both the Donor Network and Recipient Network, see figures 7 and 8 respectively. For simplicity reasons the Originating and Transit Networks are not expanded, since this does not give any additional value with the regard to IN structured aspects in Donor and Recipient.

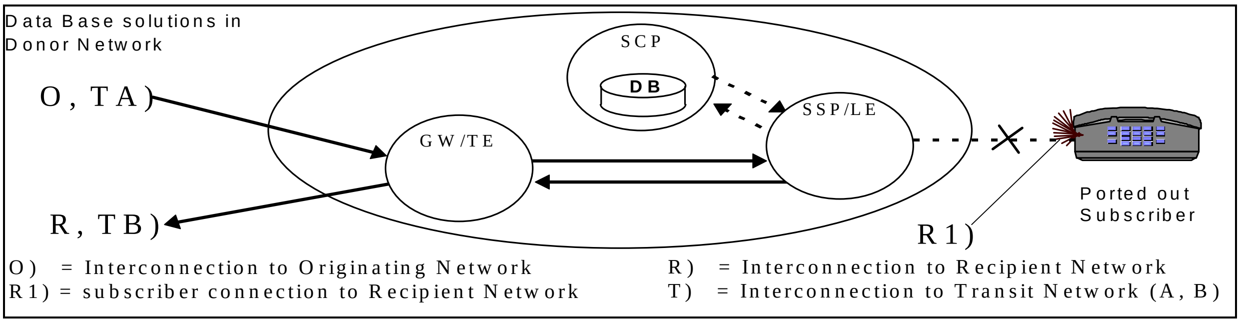


Figure 7: NP data stored switch external and queried by Donor Local Exchange(-s)

In figure 7 above, the Donor network is opened and we see that an exchange external NP DB solution has been chosen with the support of IN components SSP and SCP. The DB is accessed from Donor LE. The Routeing Information received from the DB indicates Recipient Network but not Recipient Exchange.

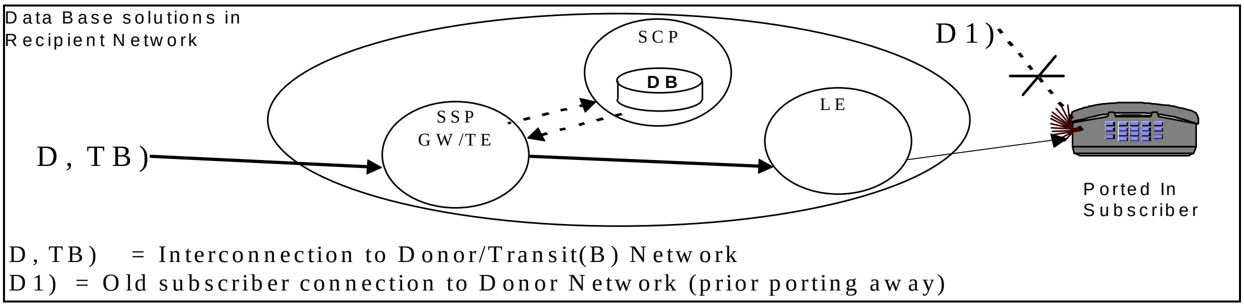


Figure 8: NP data stored switch external and queried by Recipient GW/TE Exchange(-s)

In figure 8 above, the Recipient Network is opened and we see that an exchange external NP DB solution has been chosen using IN components SSP and SCP. The DB is accessed from a Recipient GW/TE. The Routeing Information received from the DB indicates Recipient Exchange.

In the Information flows in figure 9 below, the Originating network routes the call to the network being in response of the number block that the called Directory Number (DN) is part of. The Donor network has armed a "line based" trigger, stating the number being ported-out. It then makes a NP DB query, using IN components, to retrieve a routeing number. The routeing number is then used to route the call onward towards the Recipient Network. When the call is received in the Recipient network a new query is performed, in similar way, to obtain a Routeing number to address the recipient exchange.

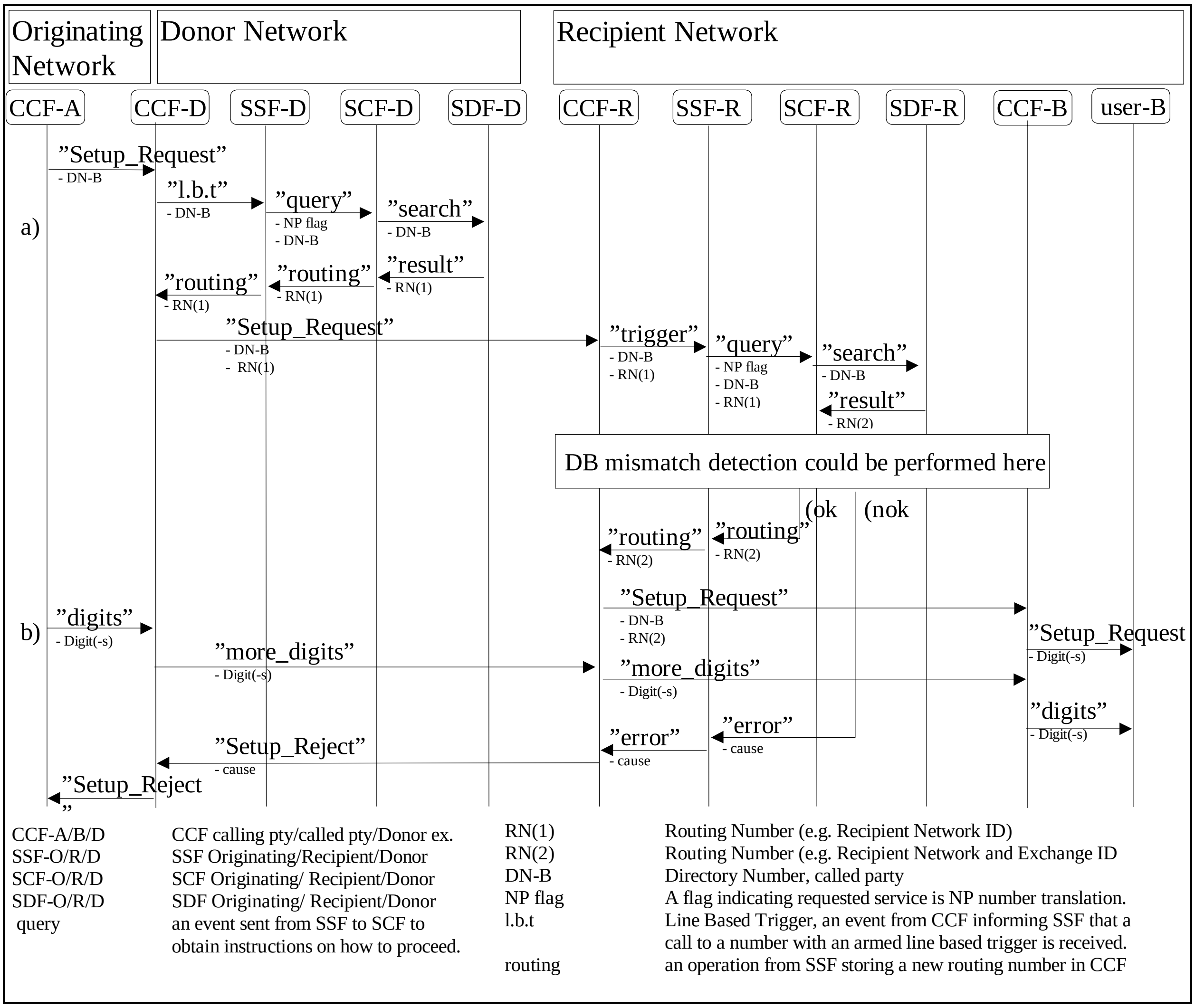


Figure 9: Information flows for IN structured support of figures 6, 7 and 8 (i.e. a two step "Onward Routeing" solution)

As can be read from the flows, the Donor Network is considered as the Serving Network since it performs both NP trap functions and obtaining of RN towards Recipient Network. The second query, in Recipient Network, is not required in the case that the first step obtains the complete address to the Recipient Exchange. The sending of RN between networks is optional.

NOTE 1: The DB mismatch detection principle in the figure shows one possible way of preventing loops to occur due to NP DB mismatch, this method is only possible if RN is sent between networks. Other ways of detecting database mismatch, e.g. use of ISUP hop counter, than the one shown in the figure does exist.

NOTE 2: Trigger on incomplete number is not applicable here since the Donor Exchange is reached prior IN triggering.

NOTE 3: The need for overlap sending of digits is only applicable where variable DDI ranges are used, i.e. is not necessary for fixed number length schemes.

6.6.3 Dropback from donor LE combined with a second query in Recipient Network

The high level scenario, as outlined in figure 11, addressed in this chapter is the case where the call is first routed to the Donor Network, optionally via Transit Network(-s) A, and from Donor a "Dropback" message is returned towards the Originating Network. The Transit Network passes on the "Dropback" to Originating Network. The Originating Network uses the received Routeing Information and re-routes the call towards the recipient Network, optionally via Transit Network(-s) B.

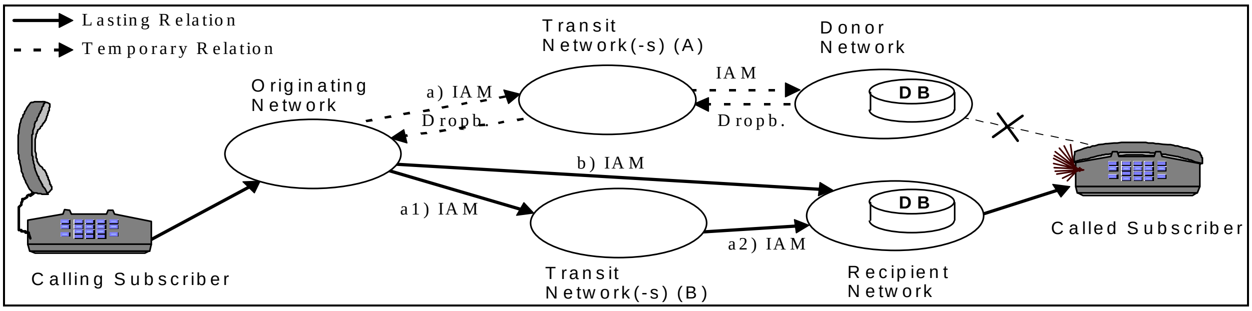


Figure 10: Dropback by Donor to Originating combined with Query by Recipient Network

The figure 10 above can be opened / expanded to see how IN components can be used to perform the required NP tasks within both the Donor Network and Recipient Network, see figures 11 and 12 respectively. For simplicity reasons the Originating and Transit Networks are not expanded, since this does not give any additional value with the regard to IN structured aspects in Donor and Recipient.

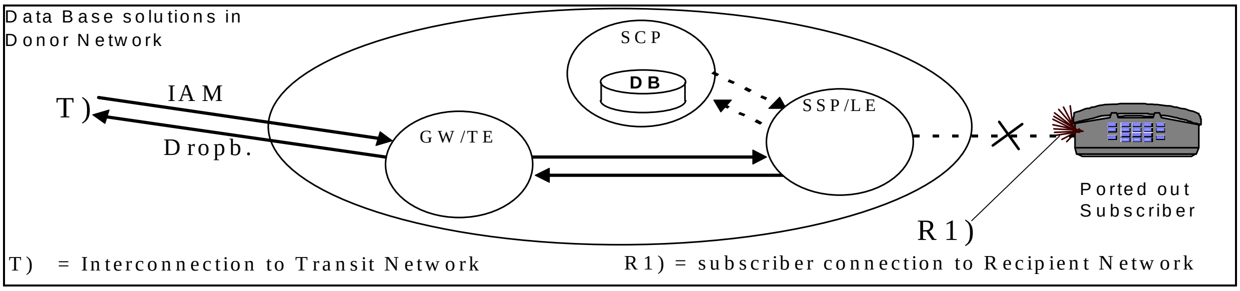


Figure 11: NP data stored switch external and queried by Donor Local Exchange(-s)

In figure 11 above, the Donor network is opened and we see that an exchange external NP DB solution has been chosen with the support of IN components SSP and SCP. The DB is accessed from Donor LE. The Routeing Information received from the DB indicates Recipient Network but not Recipient Exchange.

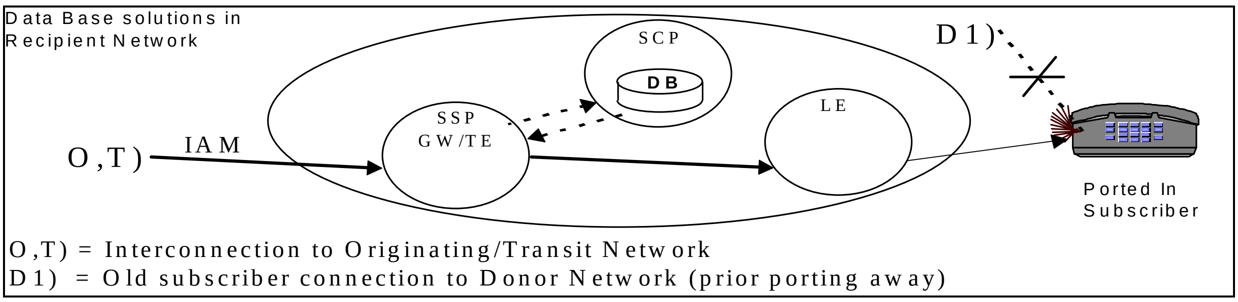
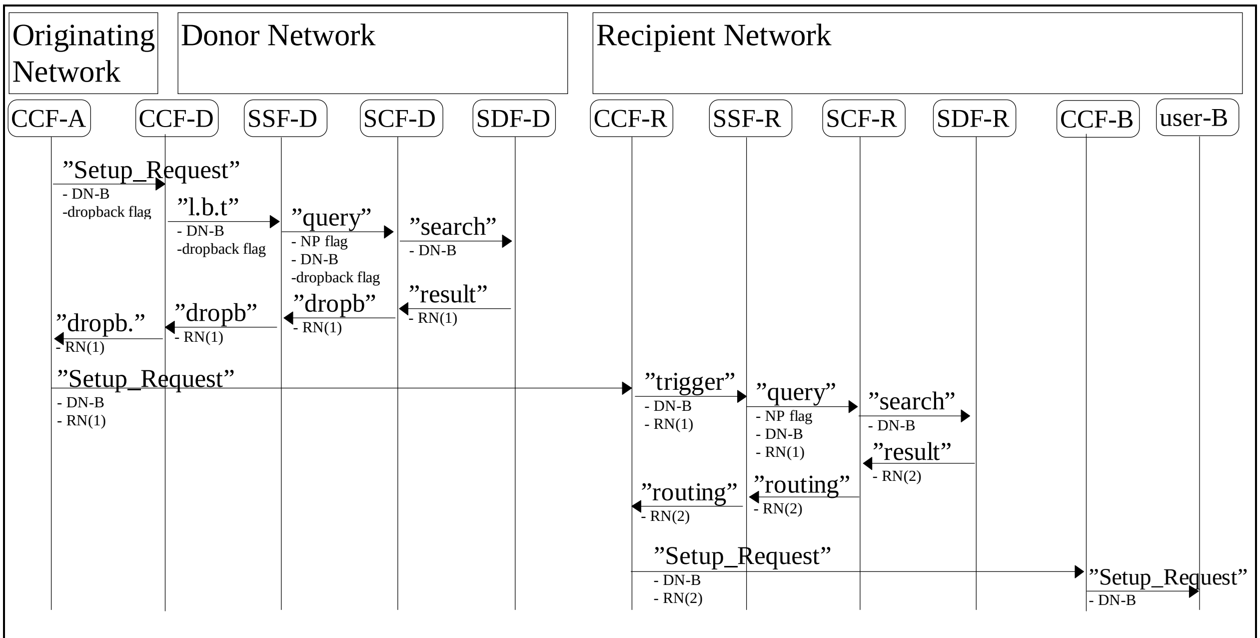


Figure 12: NP data stored switch external and queried by Recipient GW/TE Exchange(-s)

In figure 12 above, the Recipient Network is opened and we see that an exchange external NP DB solution has been chosen using IN components SSP and SCP. The DB is accessed from a Recipient GW/TE. The Routeing Information received from the DB indicates Recipient Exchange.

Also in the Information flows in figure 13 below, the Originating network routes the call to the network being in response of the number block that the called party number is party of. Also here the donor network has armed a "line based" trigger, stating the called number being ported-out. It then makes a NP DB query, using INAP, to retrieve a Routeing number, but in this case the Routeing number is returned to preceding network using a "Dropback" message.



CCF-A/B/D	CCF calling pty/called pty/Donor ex.	RN(1)	Routing Number (e.g. Recipient Network ID)
SSF-O/R/D	SSF Originating/Recipient/Donor	RN(2)	Routing Number (e.g. Recipient Network and Exchange ID
SCF-O/R/D	SCF Originating/ Recipient/Donor	DN-B	Directory Number, called party
SDF-O/R/D	SDF Originating/ Recipient/Donor	NP flag	A flag indicating requested service is NP number translation.
dropb	drop back of routeing information	l.b.t	Line Based Trigger, an event from CCF informing SSF that a call to a number with an armed line based trigger is received.
query	an event sent from SSF to SCF to obtain instructions on how to proceed.	routing	an operation from SSF storing a new routing number in CCF

Figure 13: Information flows for IN structured support of figures 10, 11 and 12 (i.e. a two step "Dropback" solution)

As can be read from the flows, the Donor Network is considered as the Serving Network since it performs both NP trap functions and obtaining of RN towards Recipient Network.

The second query, in Recipient Network, is not required in the case that the first step obtains the complete address to the Recipient Exchange.

NOTE: Overlap sending, after obtaining of RN, and DB mismatch detection are applicable options in this scenario in the same way as in figure 9.

6.6.4 Query on Release (QoR), from donor, combined with a second query in Recipient Network

The high level scenario, as outlined in figure 14, addressed in this chapter is the case where the call is first routed to the Donor Network, optionally via Transit Network(-s) A, and from Donor a "Release" message is returned, indicating "number Ported", towards the Originating Network. The Transit Network passes on the " Release" to Originating Network. The Originating Network traps the Release and makes a NP DB query to obtain Routeing Information (RI), it then uses the RI and re-routes the call towards the recipient Network, optionally via Transit Network(-s) B. Further alternatives, (e.g. trapping Release in Transit network) and explanation of the figures is found in TR 101 118 [2]. The examples / solutions focuses on actions required by IN functions.

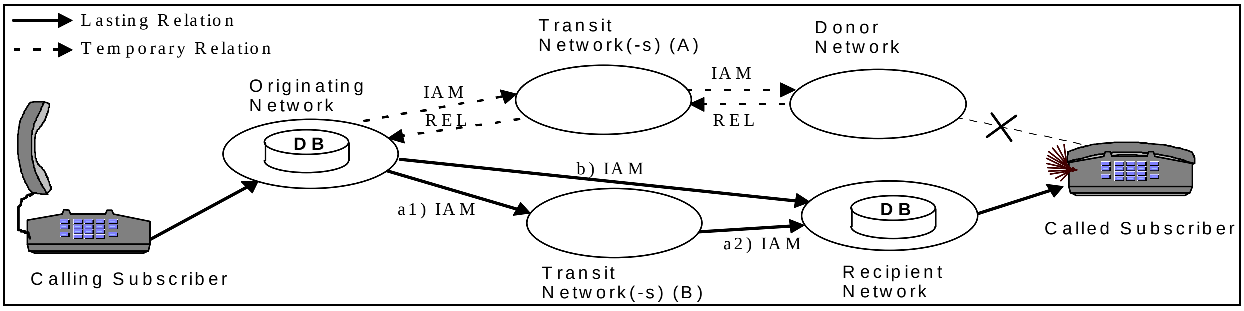


Figure 14: Query on Release by Originating combined with Query by Recipient Network

The figure 14 above can be opened / expanded to see how IN components can be used to perform the required NP tasks within both the Originating Network and Recipient Network, see figures 15 and 16 respectively. For simplicity reasons the Donor and Transit Networks are not expanded, since this does not give any additional value with the regard to IN structured aspects in Originating and Recipient.

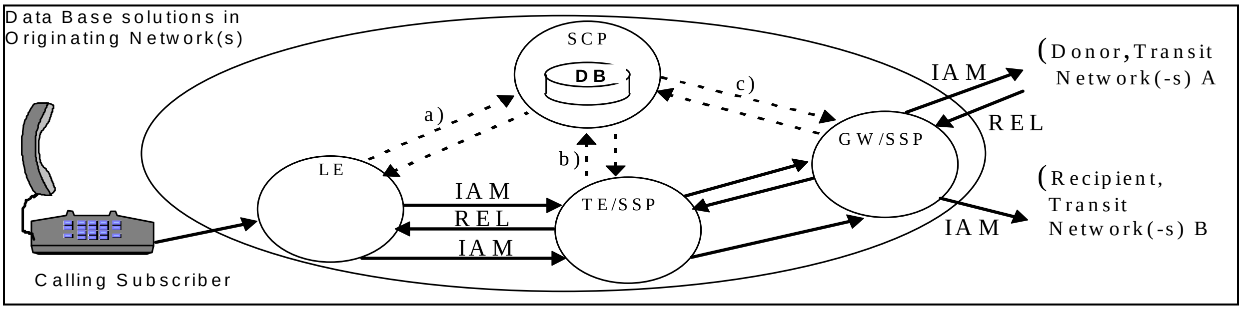


Figure 15: NP data stored Exchange external and queried by one of the Exchange(-s) in Originating Network

In figure 15 above, the Originating network is opened and we see that an exchange external NP DB solution has been chosen with the support of IN components SSP and SCP. The DB is accessed either from Originating LE, TE or GW. The Routeing Information received from the DB indicates Recipient Network but not Recipient Exchange.

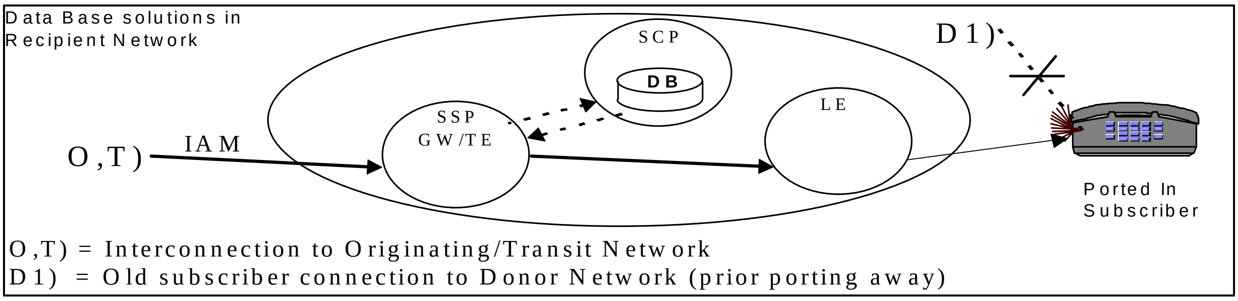


Figure 16: NP data stored switch external and queried by Recipient GW/TE Exchange

In figure 16 above, the Recipient Network is opened and we see that an exchange external NP DB solution has been chosen using IN components SSP and SCP. The DB is accessed from a Recipient GW/TE. The Routeing Information received from the DB indicates Recipient Exchange.

Also in the Information flows in figure 17 below, the Originating network routes the call to the network being in response of the number block that the called party number is party of. Also here the Donor network has detecting that the called number being ported-out. The Donor exchange then Releases the call with a certain indication, e.g. a cause value, telling number is ported-out. The Originating Network, after receiving this release, makes a NP DB query, using INAP, to retrieve a Routeing number. The Routeing number is then used to redirect the call towards Recipient Network. The actions in recipient are as in earlier solutions.

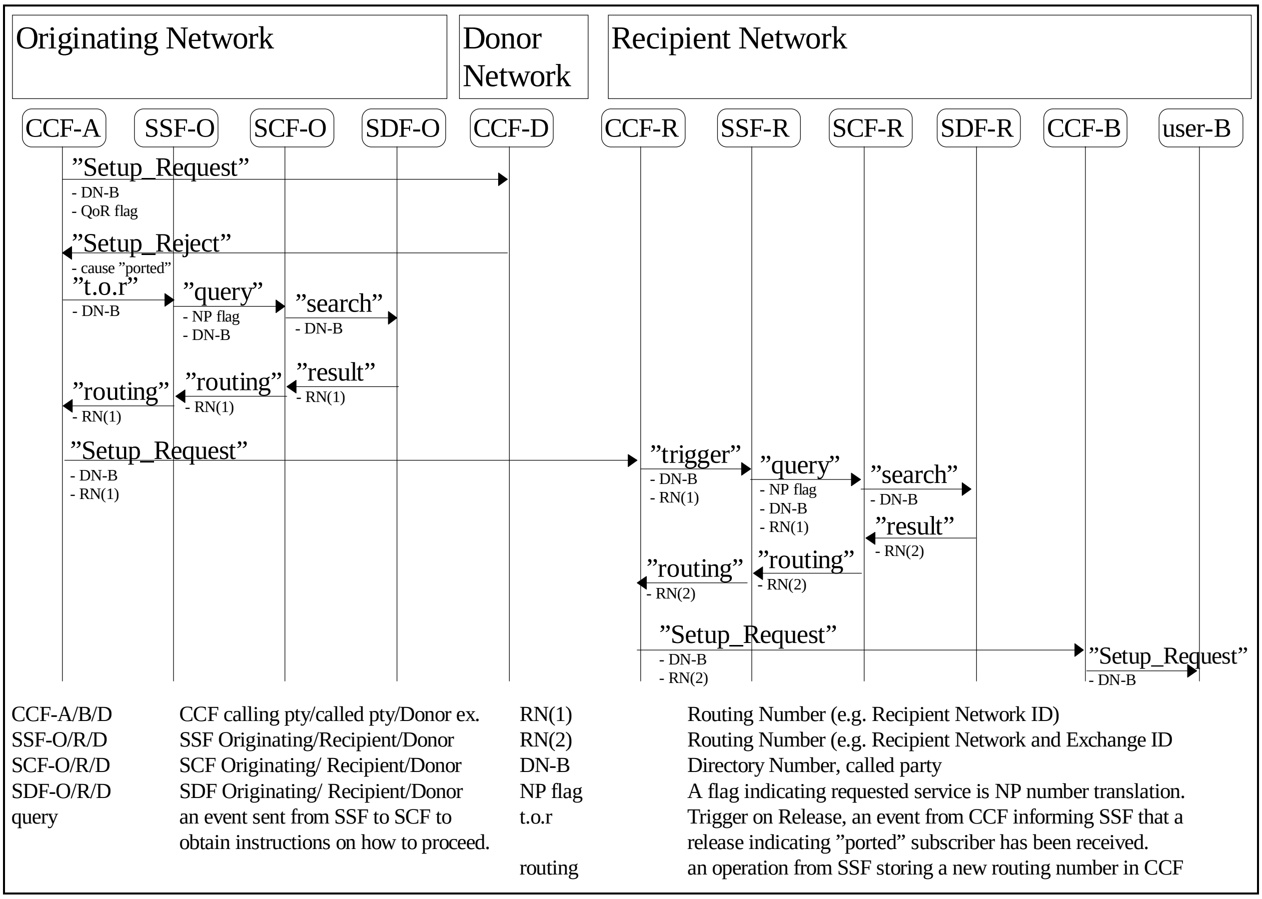


Figure 17: Information flows for IN structured support of figures 14, 15 and 16 (i.e. a two step "Query on Release" solution)

As can be read from the flows, the Originating Network is considered as the Serving Network since it performs both NP trap functions and obtaining of RN towards Recipient Network.

The second query, in Recipient Network, is not required in the case that the first step obtains the complete address to the Recipient Exchange.

NOTE: Overlap sending, after obtaining of RN, and DB mismatch detection are applicable options in this scenario in the same way as in figure 9.

6.6.5 All call query in Originating Network combined with a new query in Recipient Network

The high level scenario, as outlined in figure 18 below shows a NP solution where the Originating Network traps all calls to "portable numbers, makes a DB query on the CdPN to retrieve a partial Routeing Information (RI) to address the Recipient Network, routes the call towards the Recipient Network, optionally via Transit Network(-s). Further alternatives and explanation of the figures is found in TR 101 118 [2]. The examples / solutions focuses on actions required by IN functions.

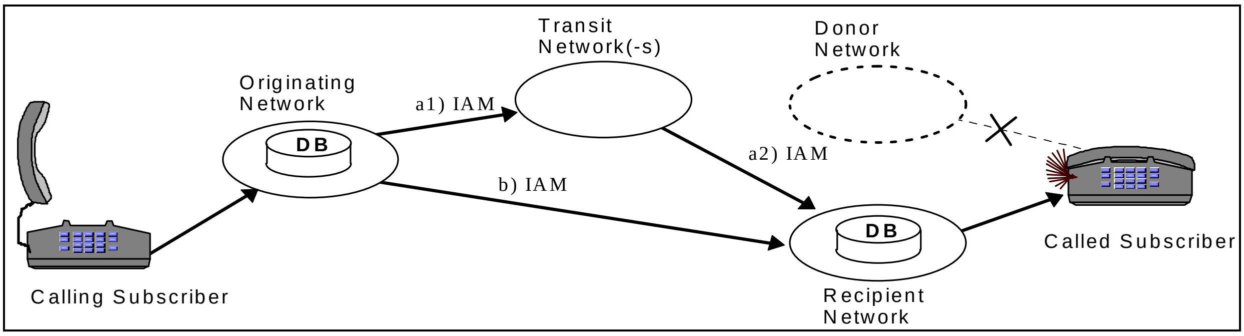


Figure 18: "All call Query" by Originating Network combined with Query by Recipient Network

The figure 18 above can be opened / expanded to see how IN components can be used to perform the required NP tasks within both the Originating Network and Recipient Network, see figures 19 and 20 respectively. For simplicity reasons the Transit Network(-s) are not expanded, since this does not give any additional value with the regard to IN structured aspects in Originating and Recipient.

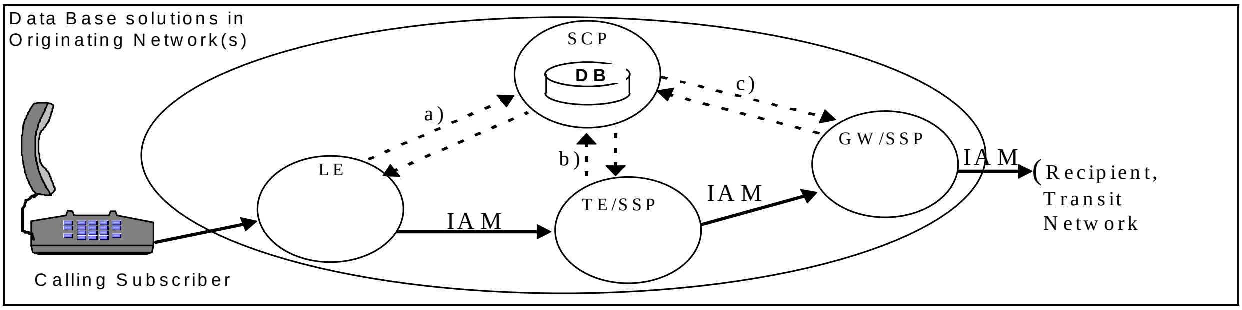


Figure 19: NP data stored Exchange external and queried by one of the Originating Exchange(-s)

In figure 19 above, the Originating network is expanded and we see that an exchange external NP DB solution has been chosen with the support of IN components SSP and SCP. The DB is accessed either from Originating LE (a), TE (b) or GW (c). The Routeing Information received from the DB indicates Recipient Network but not Recipient Exchange.

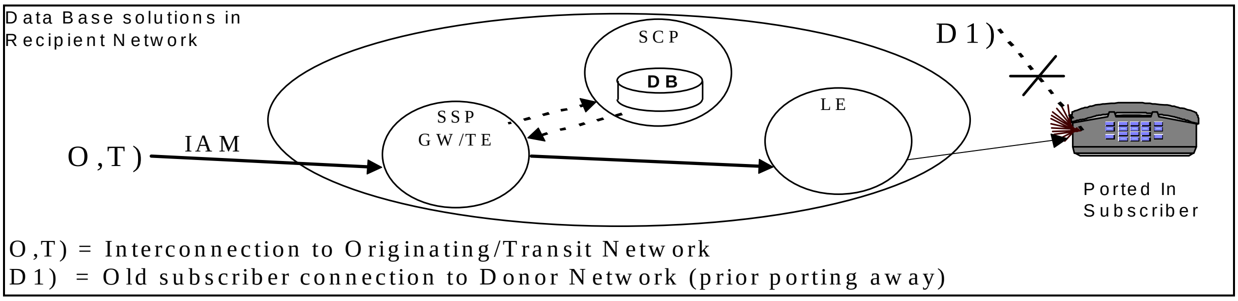


Figure 20: NP data stored switch external and queried by Recipient GW/TE Exchange(-s)

In figure 20 above, the Recipient Network is expanded and we see that an exchange external NP DB solution has been chosen using IN components SSP and SCP. The DB is accessed from a Recipient GW/TE. The Routeing Information received from the DB indicates Recipient Exchange.

In the solution outlined in figure 21 below, the Originating network has armed a "number block" based trigger, i.e. all outgoing calls with a called party number being part of this number block will lead to a NP DB query INAP, to retrieve a Routeing number. The query is performed using IN functional components. The Routeing number is then used to redirect the call towards Recipient Network. The actions in Recipient Network are as in earlier solutions.

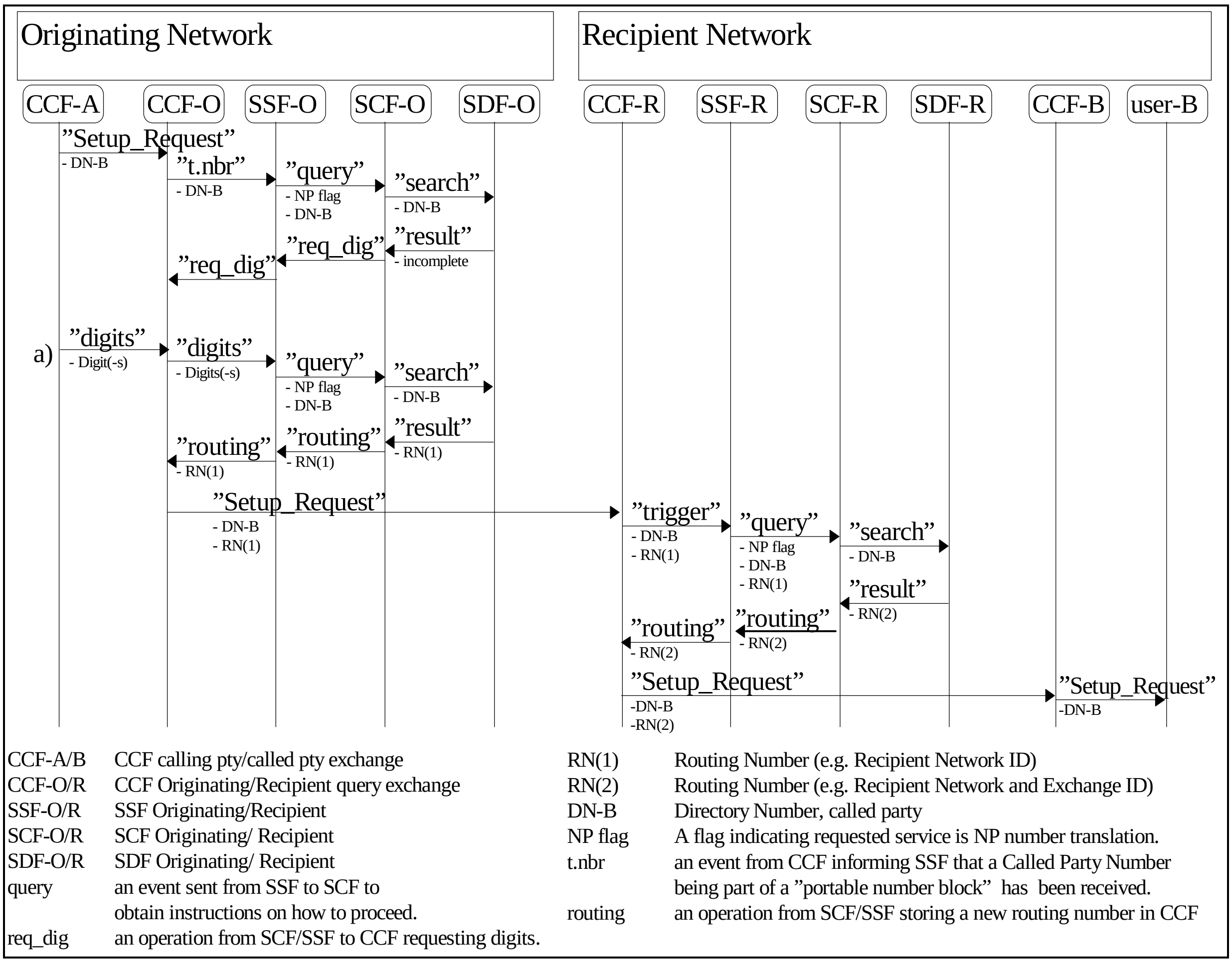


Figure 21: Information flows for an IN structured support of figures 18, 19 and 20 (i.e. a two step "all call query" solution)

As can be read from the flows, the Originating Network is considered as the Serving Network since it performs both NP trap functions and obtaining of RN towards Recipient Network.

The second query, in Recipient Network, is not required in the case that the first step obtains the complete address to the Recipient Exchange.

NOTE 1: The illustration of IN triggering on incomplete number and the request for additional digits from SCF-O), is only needed in the case that variable number block length is applied and the CCF-O/SSF-O do not "know" length for all number block(-s) with portable numbers.

NOTE 2: Overlap sending, after obtaining of RN, and DB mismatch detection are applicable options in this scenario in the same way as in figure 9.

7 Service Provider Portability of Non-Geographic Numbers

7.1 General Information

Non-Geographic numbers (NGN), by their nature, are generally processed on an 'IN like' basis, i.e. each call would be routed to an exchange with service switching functionality (SSF) for interaction with a service control (SCF) and database function (SDF) to obtain the appropriate destination address and routeing information.

It shall be noted that Non Geographic Numbers, are in most countries allocated in blocks to Service Providers (as for GN) but, elsewhere allocated either individually or to users. The solutions outlined in the present document, for portability of NGN, is mainly of interest where NGN's are allocated in blocks to Service Providers. This is because similar routeing principles apply for NGNP when NGN's are not allocated in blocks.

NP related tasks for Service Provider Portability of individual Non-Geographic Numbers incorporate identification of and routeing to Recipient Network (but not recipient exchange). The reason for no need, for NP reasons, to identify the recipient exchange is simply thanks to that the NGN itself is used to identify which exchange (SSP), in recipient network, that is capable of interacting with the relevant SCF (where the Service Logic for the called NGN service resides).

This section deal only with national NGN's and assumes that all national NGN blocks have the same fixed length.

For definitions and further information see TRs 101 119 [1] and 101 118 [2].

7.2 IN support for Service Provider Portability of Non-Geographic Numbers

The requirement for IN support of Service Provider Portability of Non-Geographic Numbers incorporate firstly the trapping (i.e. triggering of an IN NP DB query) of each call to a ported-out / portable NGN thereafter obtaining a routeing number and finally initiating call set-up towards the Recipient network. Management of NP data is elaborated in chapters addressing management issues.

The IN Architecture provides the basic relationship between the Service Control, Service Switching, Connection Control, Database and Specialized Resources Functions. There also are links with the Management and Service Creation Functions.

The interface between the switching network and the IN-NP DB is provided by the INAP (Intelligent Network Application Part) protocol.

The IN-triggering, to obtain a routeing number, is applicable both for circuit related signalling (call set-up) and for non-circuit related signalling (TCAP based services).

NGN blocks may not have the same fixed length, i.e. the problems / solutions for GNP related to variable number length are similar to NGNP.

7.3 IN Trigger Conditions, circuit related signalling to Non-Geographic Numbers

7.3.1 General Information

Triggering of an IN NP DB query, during call set-up, can in principle be due to:

a) a NGN being identified as ported-out, i.e. a "ported or vacant number" based trigger;

b) a received release message telling "e.g. number ported-out or vacant", i.e. a "release" based trigger;

c) a received call to "portable number", i.e. a "Non-Geographic number block" based trigger.

For further information please refer to TR 101 118 [2] chapter "Service Provider Portability for Non-Geographic Numbers (NGNP)".

7.3.2 IN trigger per NP solution

7.3.2.1 High level NP solution "Onward Routeing"

The Onward Routeing NP solution, as described in TR 101 118 [2], could incorporate IN triggering based on a "ported number" based trigger.

The difference here for NGNP and GNP is that the IN NP DB triggering will be the result after interrogation with SCF/SDF of Donor network (instead of interaction with Donor (e.g. Local) Exchange.

7.3.2.2 High level NP solution "Dropback"

The Dropback NP solution, as described in TR 101 118 [2], could incorporate IN triggering based on any of: "ported number", "release" and "number block" based triggers.

The difference here for NGNP, compared to GNP, is that the IN NP DB triggering will be the result after interrogation with SCF/SDF of Donor network (after interaction with Donor (e.g. Local) Exchange at GNP).

7.3.2.3 High level NP solution "Query on Release"

The Query on Release (QoR) NP solution, as described in TR 101 118 [2], could incorporate IN triggering based on a "release" based trigger.

The difference here for NGNP, compared to GNP, is that the IN NP DB triggering will be the result after interrogation with SCF/SDF of Donor network (instead of interaction with Donor (e.g. Local) Exchange.

7.3.2.4 High level NP solution "All Call Query"

The All Call Query NP solution, as described in TR 101 118 [2], could incorporate IN triggering based on a "number block" based trigger.

The same IN NP DB triggering is valid for both GNP and NGNP.

7.3.3 Network Location for IN Trigger

7.3.3.1 IN Triggers in an Originating network

In an originating network the following IN triggers are valid:

a) "release" based trigger;

b) "number block" based trigger.

The triggers are applicable to Originating, Transit and Gateway exchanges.

7.3.3.2 IN Triggers in a Transit network

Same as for Triggers in Originating Network.

7.3.3.3 IN Triggers in a Donor Network

Same as for Triggers in Originating Network but in addition also Trigger on "ported number".

Trigger on "ported number" is only applicable in Donor Exchange.

Trigger on "release" and trigger on "number block" is applicable in the Gateway, TE or even Donor Exchange.

7.3.3.4 IN Trigger in Recipient Network

NGNP related triggering is not applicable within the Recipient network since NP related routeing, for calls to NGN, ends when Recipient network is reached. Within recipient network routeing is based on the NGN itself.

7.4 IN Trigger Conditions, Non-circuit related signalling to Non-Geographic Numbers

7.4.1 General Information

Triggering of an IN DB query, during non circuit related signalling, can in principle be due to:

a) a Subscriber number being identified as ported-out, i.e. a single number based trigger;

b) a received call to "portable number", i.e. a number block based trigger.

For further information see TR 101 118 [2] chapter "High Level Evolutionary model for NP and SCCP using services to Geographic Numbers".

7.5 Evaluating IN Capability Sets supporting NP of Non-Geographic Numbers

7.5.1 General Information

The figure 22 shows an overview between NP DB query triggering method, DB access point, IN trigger, frequency of DB query and IN capability set supporting the trigger.

NP DB query Triggering Methods:	Database access point obtaining of Routeing Information		Frequency for database query	
	within switching system	IN trigger	Calls to	IN CS
Query on Ported	Donor / Serving Network	"Number_based_trigger_called_number"	ported numbers	CS2
Query on Release (1)	Serving Network	"Release with special cause value(-s)"	ported numbers	CS2
Query on Release (2)	Serving Network	Release without special cause value(-s)", e.g. on "vacant" indication	Ported and vacant numbers	CS1
All call Query	Serving Network	"complete number"	all portable numbers	CS1

Figure 22: Overview between NP DB query triggering method and frequency of DB query

The figure 23 shows an overview of NP related actions required by SSF and SCF per routeing method.

NP Redirection Methods (after NP DB query):	Service Switching Functionality	Service Control Functionality	IN capability set support
Drop Back	a) Previous network supports Dropback: Generate a release of call with redirection Information. b) Previous network do not support Dropback: Generate an onward routeing using the obtained RN	Generate Drop-back message. Generate forward call set-up concatenated number Generate forward call set-up separated number ffs	Future CS CS1 Future CS
Onward Routeing and All call Query	Generate an onward routeing using the obtained RN.	Generate forward call set-up concatenated number Generate forward call set-up separated number.	CS1 Future CS

Figure 23: Overview of NP related actions required after SCF/SDF has been consulted

7.5.2 IN CS1

7.5.2.1 IN CS1 Functional Entity Architecture supporting generic Functional modelling of NP

The generic requirements for a centralized network intelligence to provide number translation, for Number Portability reasons, can be mapped on an Intelligent Network architecture. The functional entities CCPF, NPCF, NPDF and NPMF, as outlined in figure 1, can easily be mapped onto the SSF, SCF, SDF and SMF respectively of an CS1 Intelligent Network architecture, as outlined in figure 24.

The M-NPMF can currently not be mapped onto IN functional entities.

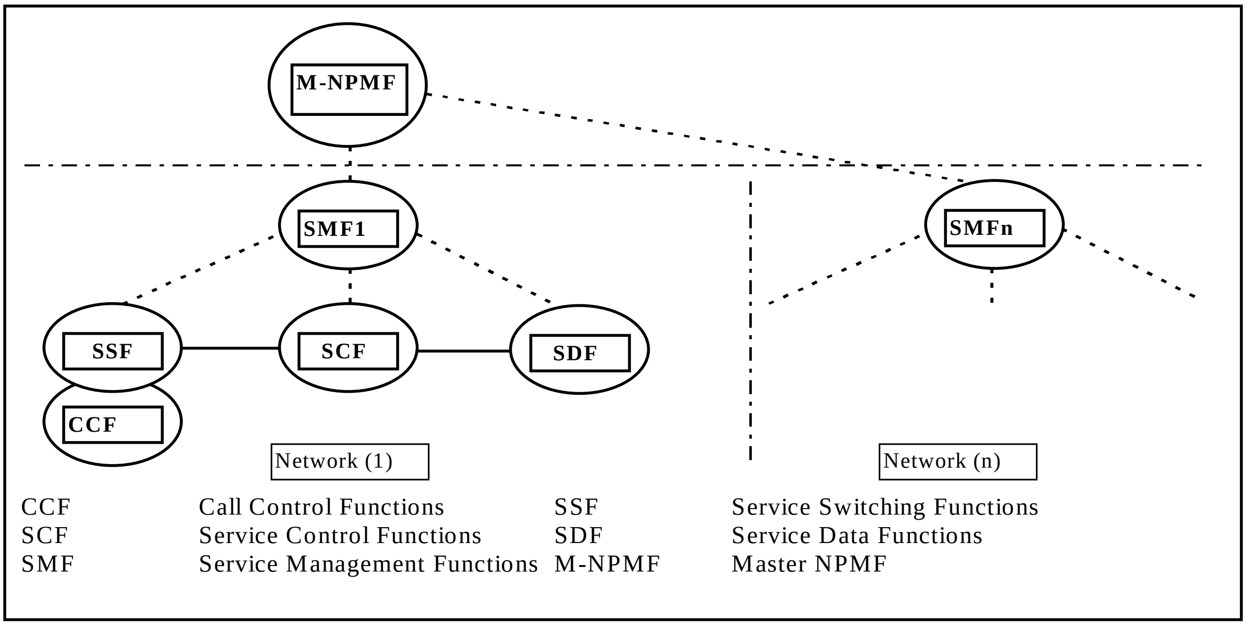


Figure 24: Functional entity Model for an IN-CS1 structured number portability solution

The architecture in the figure 24 provides a 'centralized **network** intelligence' as the M-NPMF merely manages data, is not part of the network in the diagram and does not have to have any intelligence. The centralized M-NPMF does provide any number translation as this performed in the SCF. The centralized M-NPMF provides data feeds to the SMFs and SMFs in turn to the SDFs.

7.5.2.2 IN CS1 Physical Entity Architecture supporting generic Architecture for NP

The generic functional entities, as related to providing number translation by an IN structured solution for NP as outlined in figure 2, can be mapped to IN Physical Entities: CCF&SSF to SSP, SCF to SCP, SDF to SDP and finally SMF to SMP. In addition there exists the SSCP which is a collocation of CCF, SSF and also SCF.

For further information see ITU-T Recommendations Q.1214 [10], Q.1215 [11] and Q.1218 [12] for CS1 Architecture Diagrams.

For more information on ETSI CS1 see ETS 300 741 [9].

7.5.3 IN CS2

7.5.3.1 IN CS2 Functional Entity Architecture supporting generic Functional modelling of NP

The Functional Entity architecture valid for IN CS1 is valid also for IN-CS2.

7.5.3.2 IN CS2 physical Architecture supporting generic Architecture for NP

The IN Architecture supporting generic Architecture for IN CS1 is valid also for IN-CS2.

For further information see ITU-T Recommendations Q.1224 [13] / Q.1228 [15] for CS2 Architecture Diagrams.

7.6 Information flows for NGNP when IN architecture is used

7.6.1 General Information

The following descriptions give some examples of possible scenarios for Non-Geographic Number Portability Solutions where IN architecture is used to support NP related number translation and call control, The examples / solutions focuses on actions required by IN functional / physical entities.

A more complete list of high level scenarios and further explanation of pros and cons for the alternatives is found in TR 101 118 [2].

The location of Databases is not the critical issues in the figures, instead the point where query is made and what caused the IN triggering are the important issues. Location of DB is mainly a NP data management issue and not a traffic issue.

IAM, REL, Dropback, etc. are only to be understood as logical signalling messages, i.e. the actual message name is dependent of used signalling system.

The variations of interconnections are only examples, the actually used interconnection is network dependent.

Transit networks are optional and included only to give a better understanding of interconnection issues when routeing calls / services towards ported / portable Non-Geographic Numbers.

7.6.2 Calls to National Non Geographic Numbers

7.6.2.1 Onward Routeing by Donor combined with NGN Service execution in Recipient

The high level scenario addressed in this chapter is the case where the call is first routed to the Donor Network, based on the Number Block the NGN is part of, and from there onward routed towards the Recipient Network as outlined in figure 25. In the Recipient Network the execution of ported-in NGN results in calling a subscriber. Further explanation of the figures is found in TR 101 118 [2]. Called subscriber is included for completeness reasons only, i.e. not part of NP related routeing.

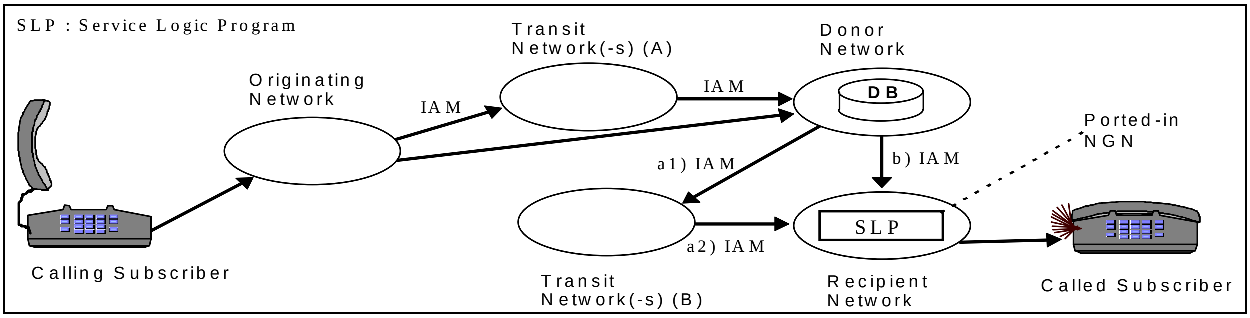


Figure 25: Onward Routeing by Donor combined with NGN Service execution by Recipient Network

The figure 25 above can be opened / expanded to see how IN components can be used to perform NP related tasks within both the Donor Network and Recipient Network, see figures 26 and 27 respectively. For simplicity reasons the Originating and Transit Networks are not expanded, this since this does not give any additional value with the regard to IN structured aspects in Donor and Recipient.

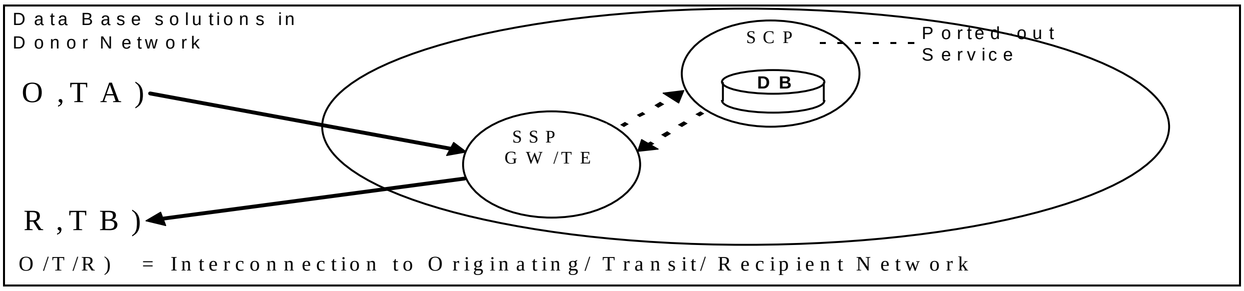


Figure 26: NGN Service execution attempt results in Routeing Information, due to ported-out Number

In figure 26 above, the Donor network is opened and we see that an attempt to execute the called NGN Service is done, but during this attempt it is detected that the called Service number has been ported-out. E.g. instead of obtaining Service Data, Routeing Information (RI) is received from the Service related DB. The RI indicates the Recipient Network (indication of Recipient Exchange is not relevant for NGNP).

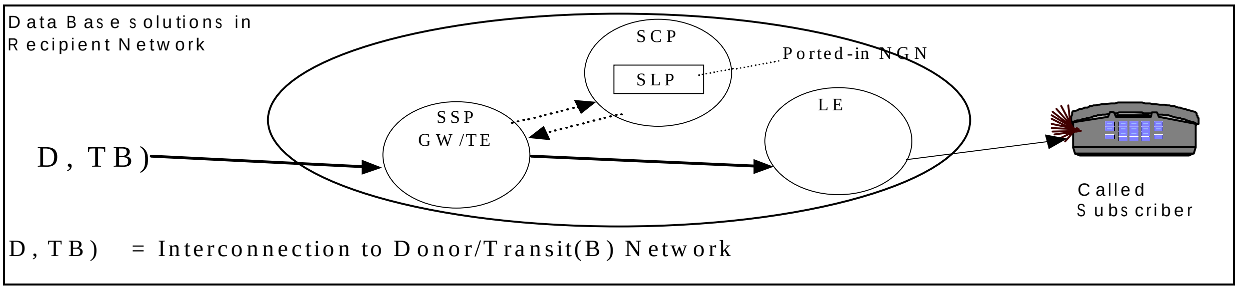


Figure 27: Execution of ported-in NGN Service in Recipient Network

In figure 27 above, the Recipient Network is opened and we see that the ported NGN Service is executed using IN components SSP and SCP. Routeing to relevant SSP is based on called Service Number i.e. this routeing step is not related to Number Portability since it only involves the execution of the NGN Service, it is only included for completeness. The called subscriber does not have to be attached to the recipient network but could be on a totally separate network and could, in turn, have GNP applied.

In the Information flows in figure 28 below, the Originating network routes the call to the network being in response of the number block that the called Non Geographic Number (NGN) is part of. The Donor Network receives the call and recognizes the number being part of a NGN number block in response of. The SCF-D is then invoked, then SCF-D queries the SDF-D to get customer / Service data (step "a" in the flow). The SDF-D has an indicator is set stating that the called Non Geographic Number is ported-out. Now SCF-D makes a second query to SDF-D (step "b" in the flow) to obtain Routeing Information (RI) to Recipient Network. SCF-D then initiates Onward Routeing of the call, towards the Recipient Network, without modifying any other call data than required for Routeing. Finally the Recipient Network traps the incoming call, executes the NGN Service and in this example routes the call further to a Called Party B.

A possible optimization is that the response from step "a" also contains the RI obtained by step "b", i.e. removing a single search and query flow. This optimization is not possible in case the NP related data is maintained in a different instance of SDF-D.

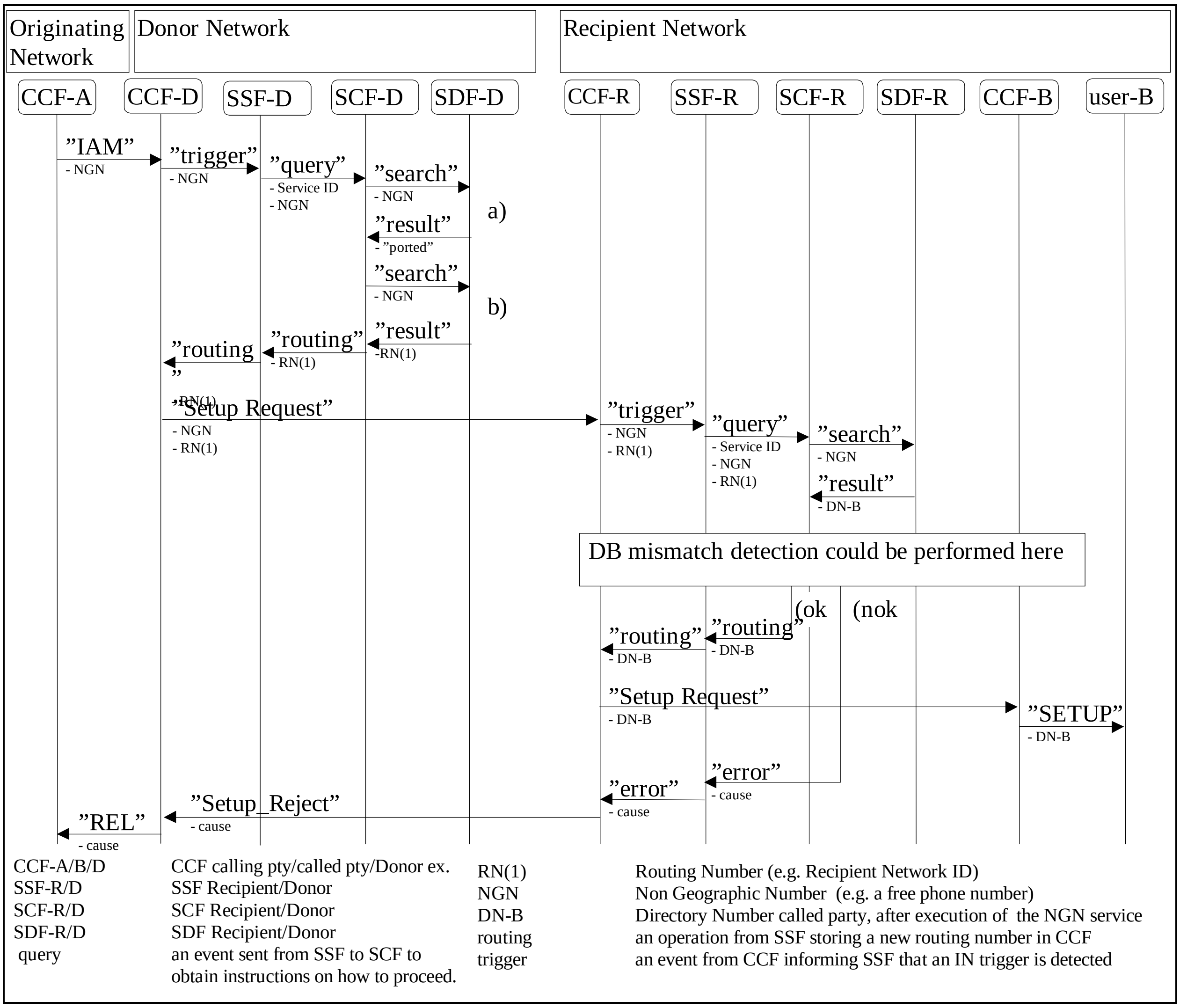


Figure 28: Information flows for IN structured support of figures 25, 26 and 27

As can be read from the flows, the Donor Network is considered as the Serving Network since it performs both NP trap functions and obtaining of RN towards Recipient Network. This scenario is only applicable when NGN blocks are assigned to operators.

NOTE: The DB mismatch detection principle in the figure shows one possible way of preventing loops to occur due to NP DB mismatch, this method is only possible if RN is sent between networks. Other ways of detecting database mismatch, e.g. use of ISUP hop counter, than the one shown in the figure does exist.

7.6.2.2 Dropback from Donor combined with NGN Service execution in Recipient

The high level scenario, as outlined in figure 29, addressed in this chapter, is the case where the call is first routed to the Donor Network, optionally via Transit Network(-s) A, and from Donor a "Dropback" message is returned towards the Originating Network. The Transit Network passes on the "Dropback" to Originating Network. The Originating Network uses the received Routeing Information and re-routes the call towards the recipient Network, optionally via Transit Network(-s) B. Further alternatives and explanation of the figures is found in TR 101 118 [2]. The examples / solutions focus on actions required by IN functions. Called subscriber is included for completeness, i.e. not part of NP related routeing. Whilst the routeing can occur in the way shown.

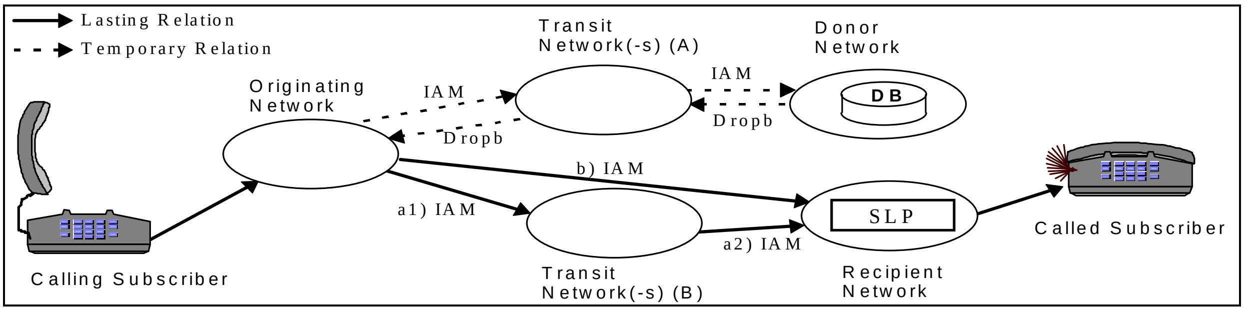


Figure 29: Dropback to Originating, combined with NGN Service execution in Recipient Network

The figure 29 above can be opened / expanded to see how IN components can be used to perform NP related tasks within both the Donor Network and Recipient Network, see figures 30 and 31 respectively. For simplicity reasons the Originating and Transit Networks are not expanded, this since this does not give any additional value with the regard to IN structured aspects in Donor and Recipient.

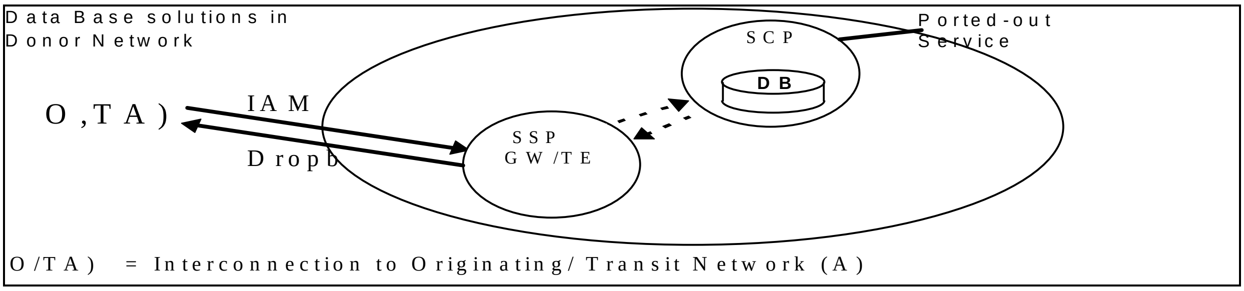


Figure 30: NGN Service execution attempt results in Routeing Information, due to ported Number

In figure 30 above, the Donor network is opened and an attempt to execute the called NGN Service is performed, but during this attempt it is detected that the called Service number has been ported-out. E.g. instead of obtaining Service Data, Routeing Information (RI) is received from the Service related DB. The RI indicates the Recipient Network (indication of Recipient Exchange is not relevant for NGNP).

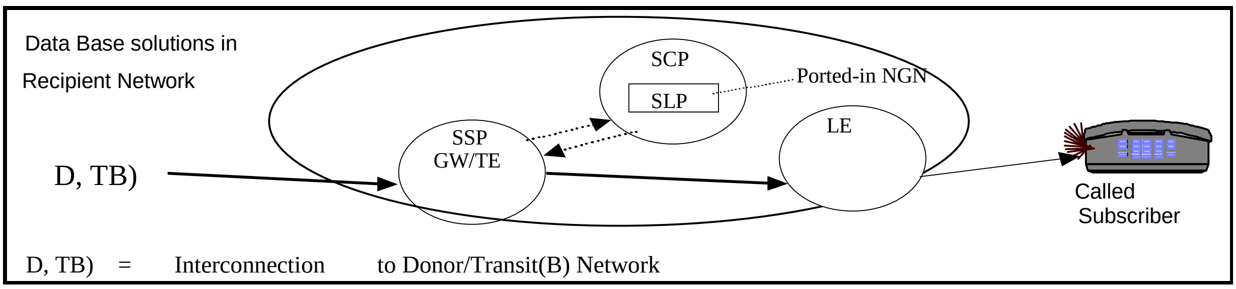


Figure 31: Execution of NGN Service in Recipient Network

In figure 31 above, the Recipient Network is opened and we see that the ported NGN Service is executed using IN components SSP and SCP. Routeing to relevant SSP is based on called Service Number i.e. this routeing step is not related to Number Portability since it only involves the execution of the NGN Service, it is only included for completeness.

Also in the solution, in figure 32 below, the Originating Network routes the call to the network being in response of the number block that the called Non Geographic Number (NGN) is part of. The Donor Network receives the call and recognizes the number being part of a NGN number block in response of. The SCF-D is then invoked, the SCF queries the SDF-D to get customer / Service data (step "a" in the flow). The SDF-D has an indicator is set stating that the called Non Geographic Number is ported-out. Now SCF-D makes a second query to SDF-D (step "b" in the flow) to obtain Routeing Information (RI) to Recipient Network. SCF-D then returns the Routeing number to preceding network using a "Dropback" message. The actions in Recipient are as in earlier solutions. Finally the Recipient Network traps the incoming call, executes the NGN Service and in this example routes the call further to a Called Party B.

A possible optimization is that the response from step "a" also contains the RI obtained by step "b", i.e. removing a single search and query flow. This optimization is not possible in case the NP related data is maintained in a different instance of SDF-D.

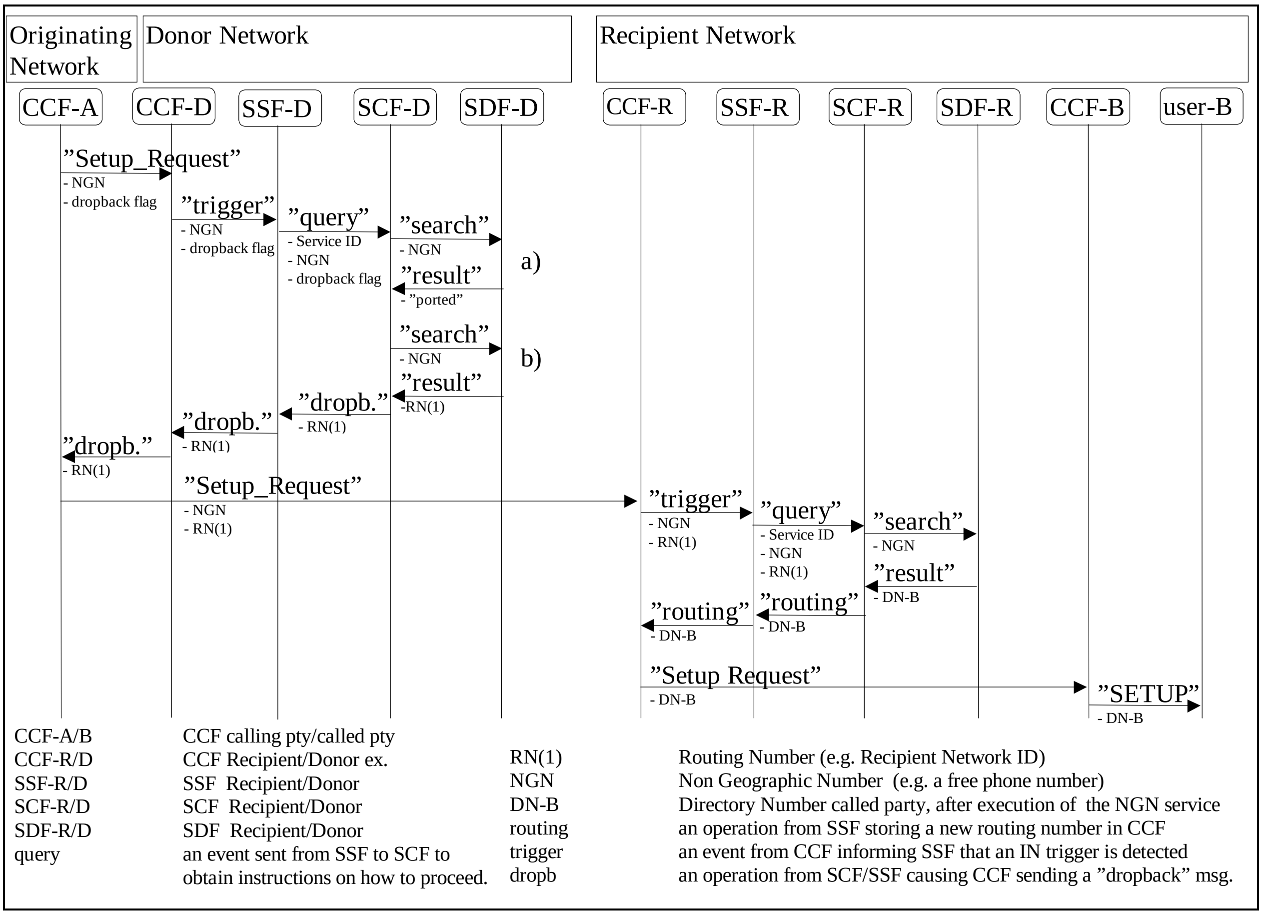


Figure 32: Information flows for IN structured support of figures 29, 30 and 31

As can be read from the flows, the Donor Network is considered as the Serving Network since it performs both NP trap functions and obtaining of RN towards Recipient Network. It may be possible for SDF to simultaneously return a ported return with the routeing number, i.e. concatenation of steps a and b above.

This scenario is only applicable when NGN blocks are assigned to operators.

NOTE: DB mismatch detection is an applicable option in this scenario in the same way as in figure 33.

7.6.2.3 Query on Release (QoR), from Donor, combined with NGN Service execution in Recipient

The high level scenario, as outlined in figure 33, addressed in this chapter is the case where the call is first routed to the Donor Network, optionally via Transit Network(-s) A, and from Donor a "Release" message is returned, indicating "Number Ported", towards the Originating Network. The Transit Network passes on the " Release" to Originating Network. The Originating Network traps the Release and makes a NP DB query to obtain Routeing Information (RI), it then uses the RI and re-routes the call towards the Recipient Network, optionally via Transit Network(-s) B. Further alternatives and explanation of the figures is found in TR 101 118 [2]. The examples / solutions focuses on actions required by IN functions. Called subscriber is included for completeness reasons only, i.e. not part of NP related routeing.

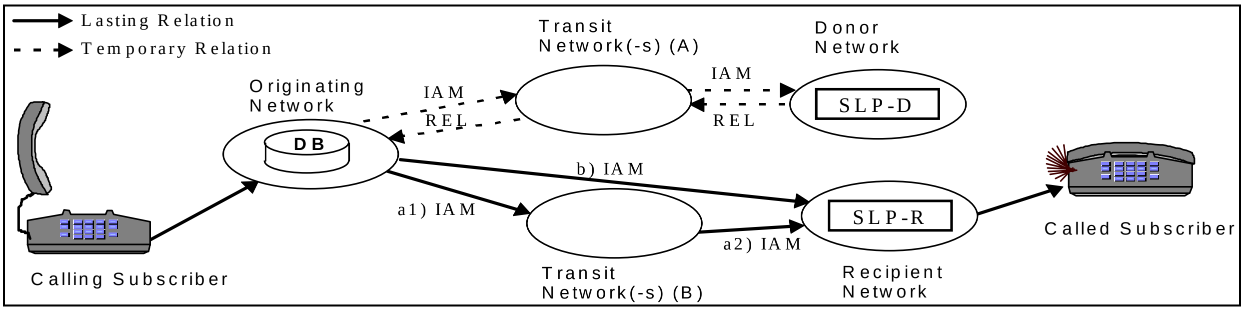


Figure 33: Query on Release by Originating combined with Query by Recipient Network

The figure 33 above can be opened / expanded to see how IN components can be used to perform the required NP tasks within the Donor, Originating and Recipient Network, see figures 34 and 35 respectively. The structure of Recipient is as for previous cases. For simplicity reasons the Transit Networks are not expanded, this since this does not give any additional value with the regard to IN structured aspects in Donor, Originating and Recipient.

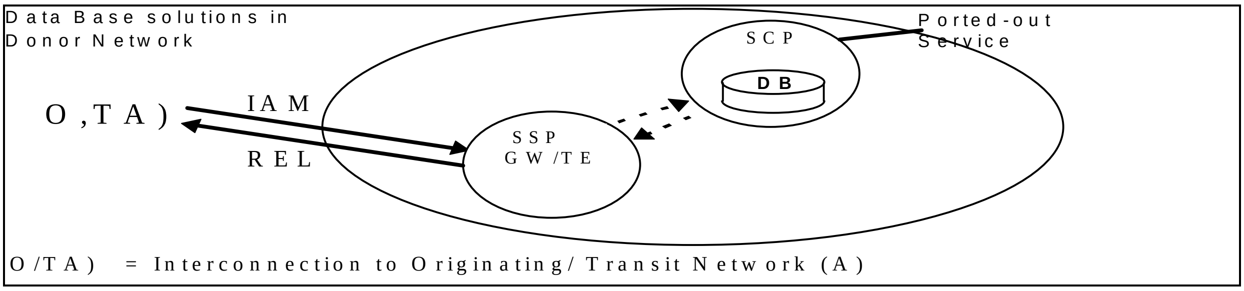


Figure 34: NGN Service execution attempt results in "Release", due to ported Number

In figure 34 above, the Donor network is opened and we see that an attempt to execute the called NGN Service is done, but during this attempt it is detected that the called Service number has been ported-out. E.g. instead of obtaining Service Data, a "ported" indication is received from the Service related DB.

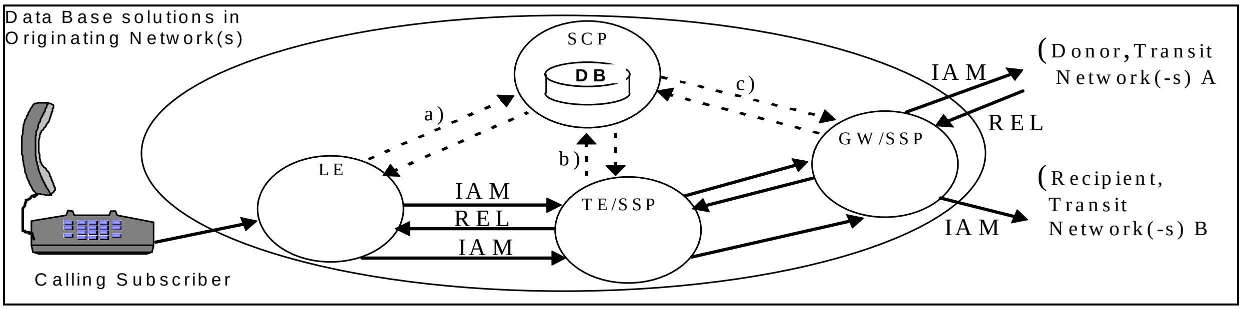
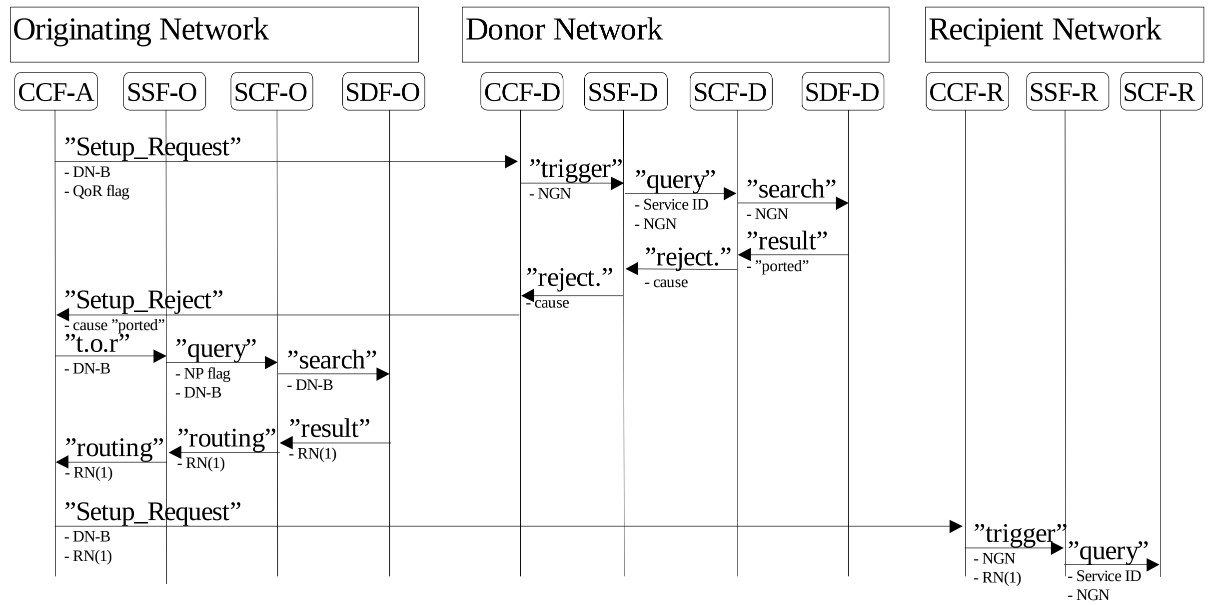


Figure 35: NP data stored Exchange external and queried by one of the Originating Exchange(-s)

In figure 35 above, the Originating network is opened and we see that an exchange external NP DB solution has been chosen with the support of IN components SSP and SCP. The DB is accessed either from Originating LE, TE or GW. The Routeing Information received from the DB indicates Recipient Network but not Recipient Exchange.

Also in the solution, in figure 36 below, the Originating network routes the call to the network being in response of the number block that the called Non Geographic Number (NGN) is part of. The Donor Network receives the call and recognizes the number being part of a NGN number block in response of. The SCF-D is then invoked, the SCF-D queries the SDF-D to get customer / Service data. The SDF-D has an indicator is set stating that the called Non geographic number is ported-out, this Information is returned to SCF-D. SCF-D then initiates a release of the call indicating that number is ported out. The CCF-D then Releases the call with a certain indication, e.g. a cause value, telling number is ported-out. The Originating Network, after receiving this release, makes a NP DB query, using INAP, to retrieve a Routeing Number. The actions in Recipient are as in earlier solutions.

The Donor SSP then Releases the call with a certain indication, e.g. a cause value, telling number is ported-out. The Originating Network, after receiving this release, makes a NP DB query, using INAP, to retrieve a Routeing number. The Routeing number is then used to redirect the call towards Recipient Network. The actions in recipient are as in earlier solutions.



CCF-A/R/D	CCF calling pty/Recipient/Donor exch.	RN(1)	Routing Number (e.g. Recipient Network ID)
SSF-O/R/D	SSF Originating/Recipient/Donor	NP flag	A flag indicating requested service is NP number translation.
SCF-O/R/D	SCF Originating/Recipient/Donor	t.o.r	an event from CCF informing SSF that a release indicating ”ported” subscriber has been received.
SDF-O/R/D	SDF Originating/Recipient/Donor		
query	an event sent from SSF to SCF to obtain instructions on how to proceed.	routing	an operation from SSF storing a new routing number in CCF
		QoR flag	an indication telling that Query on Release is supported.

Figure 36: Information flows for IN structured support of figures 33, 34 and 35 (i.e. a two step "Query on Release query" solution)

As can be read from the flows, the Originating Network is considered as the Serving Network since it obtains the RN towards Recipient Network.

This scenario is only applicable when NGN blocks are assigned to operators.

NOTE: DB mismatch detection is an applicable option in this scenario in the same way as in figure 33.

7.6.2.4 All call query in Originating Network combined with NGN Service execution in Recipient

The high level NP scenario, as outlined in figure 37 below, shows that the Originating network has armed a "number block" based trigger, i.e. all outgoing calls with a Non Geographic Number (NGN) being part of this number block will lead to a NP DB query, to retrieve Routeing Information (RI) to address the Recipient Network. The query is performed using IN functional components. Originating Network then routes the call towards the Recipient Network, optionally via Transit Network(-s). The actions in Recipient are as in earlier solutions. Further alternatives and explanation of the figures is found in TR 101 118 [2]. The examples / solutions focuses on actions required by IN functions. Called subscriber is included for completeness reasons only, i.e. not part of NP related routeing.

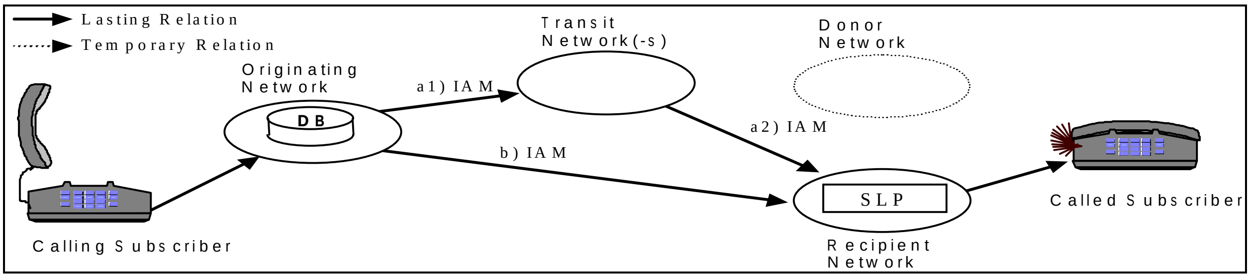


Figure 37: "All call Query" by Originating Network combined with NGN Service execution in Recipient

The figure 37 above can be opened / expanded to see how IN components can be used to perform the required NP tasks within both the Originating Network and Recipient Network, see figures 46 and 47 respectively. For simplicity reasons the Transit Network(-s) are not expanded, this since this does not give any additional value with the regard to IN structured aspects in Originating and Recipient. Donor Network is not involved, during call set-up, in this scenario.

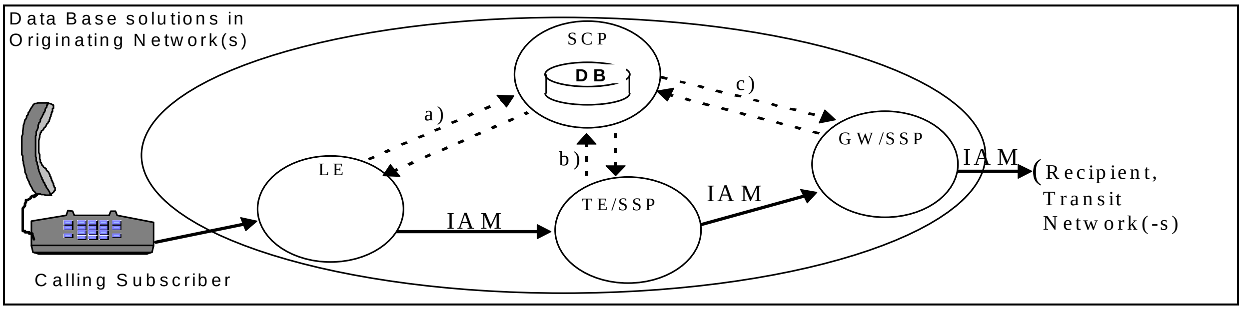


Figure 38: NP data stored Exchange external and queried by one of the Originating Exchange(-s)

In figure 38 above, the Originating network is expanded and we see that an exchange external NP DB solution has been chosen with the support of IN components SSP and SCP. The DB is accessed either from Originating LE, TE or GW. The Routeing Information received from the DB indicates Recipient Network but not Recipient Exchange.

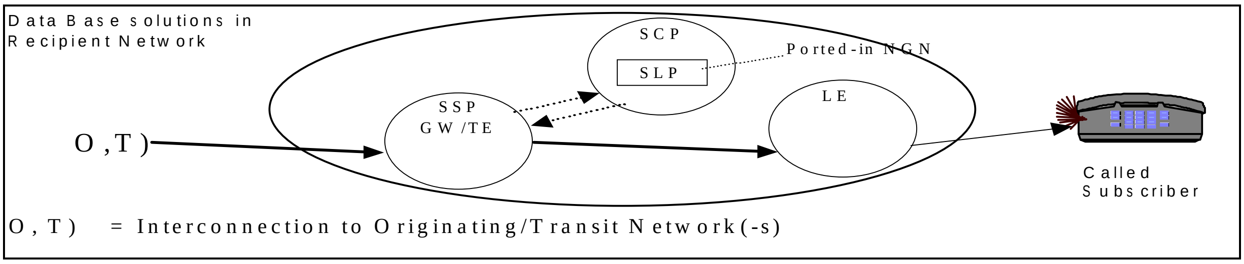


Figure 39: Execution of NGN Service in Recipient Network

In figure 39 above, the Recipient Network is opened and we see that the ported NGN Service is executed using IN components SSP and SCP. Routeing to relevant SSP is based on called Service Number i.e. this routeing step is not related to Number Portability since it only involves the execution of the NGN Service, it is only included for completeness reasons.

Also in the Information flows in figure 40 below, In this solution the Originating network has armed a "number block" based trigger, i.e. all outgoing calls with a called party number being part of this number block will lead to a NP DB query INAP, to retrieve a Routeing number. The query is performed using IN functional components. The Routeing number is then used to redirect the call towards Recipient Network. The actions in Recipient Network are as in earlier solutions.

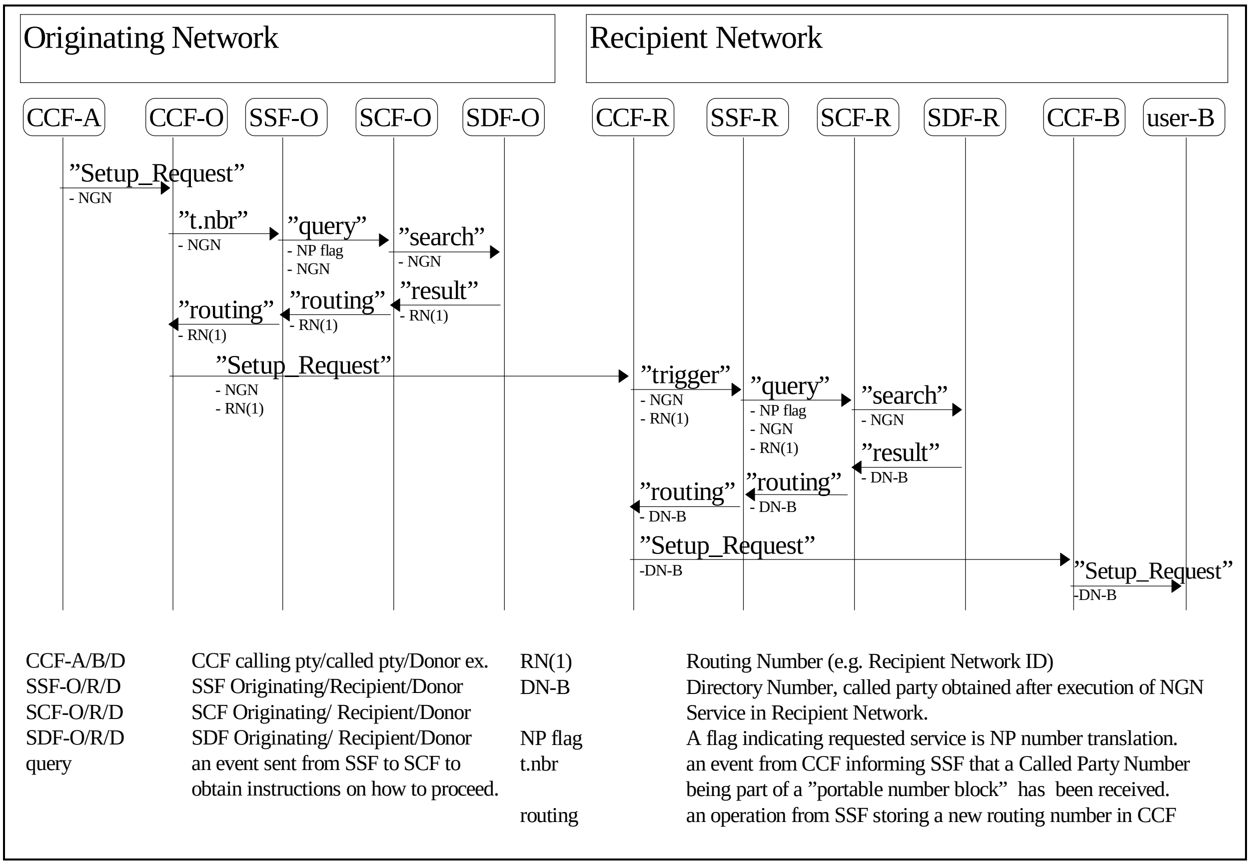


Figure 40: Information flows for an IN structured support of figures 37, 38 and 39 (i.e. a two step "all call query" solution)

As can be read from the flows, the Originating Network is considered as the Serving Network since it performs both NP trap functions and obtaining of RN towards Recipient Network.

This solution works even when NGN blocks are not allocated to Networks, i.e. when only individual numbers are allocated.

NOTE: DB mismatch detection is an applicable option in this scenario in the same way as in figure 28.

8 Management Aspects

8.1 Database Management

For reasons of efficiency, the Database may be distributed / replicated with updates being downloaded under the control of a Network Management System.

The Directory Number Agency administers the common resource of directory numbers within one number area, e.g. a country. It assigns number ranges to the each operator and administers ported numbers. The Directory Number Agency is the master database of a numbering area for a country.

8.2 IN structured NP management architecture

8.2.1 General information

The functional entities, as related to an IN structured solution for NP outlined in figure 2 can be mapped to IN elements: CCF + SSF to SSP, SCF to SCP, SDF to SDP and finally SMF to SMP as outlined in figure 41 below. In addition there exists the SSCP that is a collocation of CCF, SSF also SCF.

Please note that an SCP/SSCP might optionally contain also SDF functionality (still named SCP/SSCP).

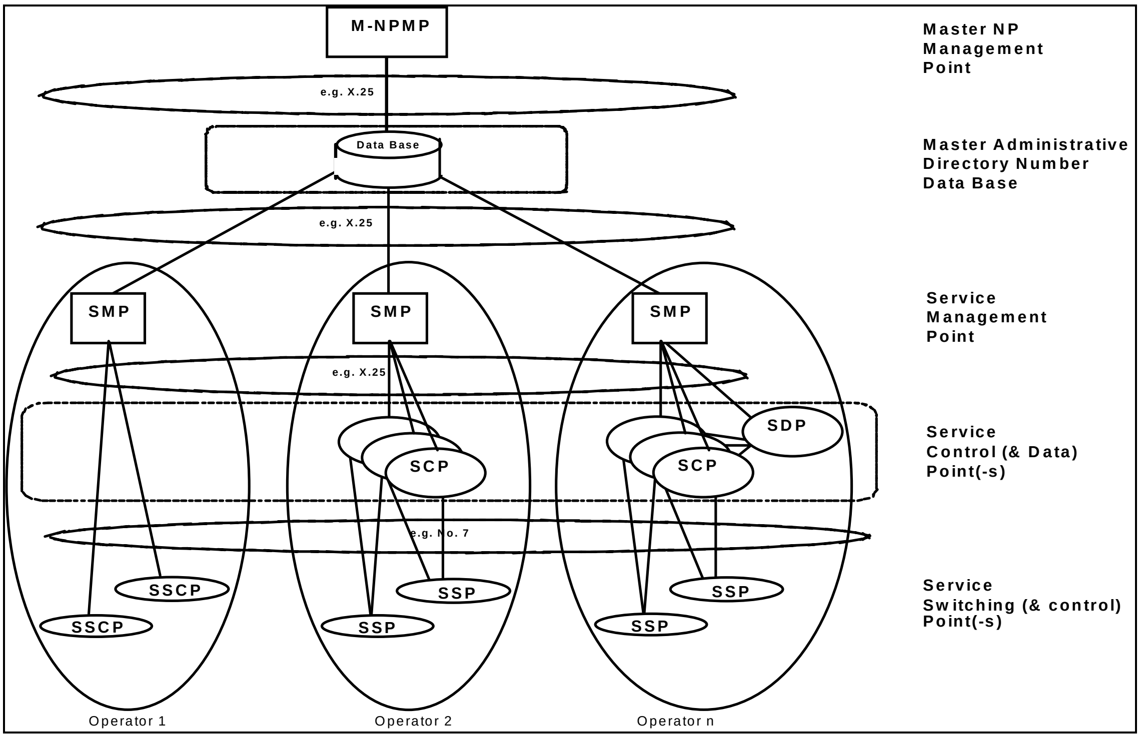


Figure 41: Network layout for management of NP data when data is maintained in an IN environment, and when NP data is replicated in each of involved Operators Network

The management system is mapped to the "SMP" in the Intelligent Network architecture. SSPs are integrated within switching exchanges in the networks. Depending on the method, the SSPs trigger either on ISUP release messages indicating "number ported" or "query on release" method or on each call in case of the "all call query" method to invoke the Routeing service. Since a call to a ported number located within another network may be recognized within the own exchange, the "query on release" case may occur also within the donor exchange. To be able to trigger these calls, it may be advantageous to provide SSPs in local exchanges. However it may be also possible at intermediate or terminating exchanges.

8.2.2 Number Portability Management Requirements

It is essential that adequate administrative procedures are in place to support the implementation of Number Portability. Aspects to be considered include the timing and alignment of the administrative procedures to ensure all involved operators are fully aware.

9 Interaction with Services and an IN structured NP solution

NP Services should not have any impact on Supplementary Services.

The provision of IN should not impact Number Portability.

9.1 Interaction Requirements for an IN structured NP solution

The introduction of Number Portability should not interfere with supplementary services.

However, routeing of non circuit related services (e.g. CCBS) need also access to NP DB to retrieve a global title routeing number.

9.2 Restrictions

All the services cannot be guaranteed to remain the same when a subscriber changes operators. For example, the subscriber has a IN service, which requires the subscriber to be connected to an SSP exchange. If the subscriber is no longer connected to an SSP exchange with the new operator, the same service may not be possible to be offered anymore.

If the originating subscriber is connected to an SSP-exchange and uses an IN service, there may be a need for two sequential SCP-queries in the same exchange: one for NP Number Translation and one for the other IN service. Some unwanted interactions may occur with NP service and other IN services. The order of the queries may be critical for correct functionality of both services.

Call Completion to Busy Subscriber (CCBS) and Call Completion No Reply (CCNR) services use SCCP level messages. The addressing of these messages should also be affected as a number is ported. This requires similar address translation procedures for SCCP messages as NP requires for call set-up messages.

10 Interconnect

The interconnection of networks providing Number Portability requires agreements on the form of transferring Routeing information between networks and also agreements on accounting for the use of donor network capacity. Following prior agreement to the format of routeing information, participating networks may not require the transfer of routeing information with ported calls.

10.1 Between IN Structured Networks

10.1.1 Onward Routeing

10.1.1.1 Routeing Aspects

The Donor Network shall be able to route the call to the Recipient Network (optionally via a Transit Network). This Routeing information need not contain the whole Routeing Number to the ported subscriber but only sufficient information for Routeing the call to the Gateway Exchange of the Recipient Network.

The Gateway Exchange of the Recipient Network shall be able to recognize that the incoming call has been re-routed from the Donor Network. A call to a ported number may be identified by appending a special Routeing prefix to the Donor Network of the ported number or e.g. adding a "ported-flag" in the signalling information.

For possible solutions other than a routeing pre-fix, please see TR 101 122 [3].

10.1.2 Commercial Aspects

A call that has been re-routed from the Donor Network to the Recipient Network is using transmission capacity of the Donor Network during the whole call. Every call to a ported-out number requires an SCP-query in the Donor Network. The donor operator has to reserve the ported-out Directory Numbers for use in another operator's network.

These procedures cause additional expenses for the Donor Network operator.

10.1.3 Dropback

10.1.3.1 Routeing Aspects

The Originating and Donor Networks shall be able to handle signalling messages with dropback information. If the Originating Network does not pass the "dropback flag" in the "set-up request" message, the Donor Network is not allowed to pass a "dropback" message backwards. Therefore it shall be mutually acceptable to both donor and originating networks.

The "dropback" message should contain sufficient Routeing information for the Originating Network to be able to route the call to the Recipient Network (optionally via a Transit Network). This Routeing information does not have to contain the whole Routeing Number to the ported subscriber but only sufficient information for Routeing the call to the Gateway Exchange of the Recipient Network.

10.1.3.2 Commercial Aspects

The Donor Network operator receives all calls to the ported-out numbers, makes an SCP-query and releases them with a dropback message with re-Routeing information. The donor operator has to reserve the ported-out Directory Numbers for use in another operator's network.

The recipient network shall be made aware of the use of dropback to the donor network. Procedures shall be made available to enable accounting for database queries on ported numbers.

These procedures cause additional expenses for the Donor Network operator.

10.1.4 Query on Release

10.1.4.1 Routeing Aspects

The Originating and Donor Networks shall be able to handle signalling messages with QoR information. If the Originating Network does not pass the "QoR flag" in the set-up request message, the donor network is not allowed to send backwards a "set-up reject" message indicating "number ported" . Therefore it shall be mutually accepted between donor and originating networks.

The "set-up reject" message does not contain any Routeing information, so the Donor Network operator does not have to store Routeing information for ported-out numbers. The Originating Network shall have sufficient Routeing information for Routeing the call to the Recipient Network. This Routeing information does not have to contain the whole Routeing Number to the ported customer but only sufficient information for Routeing the call to the Gateway Exchange of the Recipient Network.

To support Query on Release outside the NP Domain, transit operators shall have a 'proxy Query on Release' functionality.

10.1.4.2 Commercial Aspects

Every call to a ported-out number requires an SCP-query in the Originating Network. This causes additional expenses for the Originating Network operator.

The Donor Network operator receives all calls to the ported-out numbers and releases them with information "ported". The Donor Network operator has to reserve the ported-out Directory Numbers for use in another operator's network. These procedures cause additional expenses for the Donor Network operator.

10.1.5 All call Query

10.1.5.1 Routeing Aspects

All the operators in the NP domain have to have access to Routeing information for all portable numbers in the NP domain. This Routeing information does not have to contain the whole Routeing Number to the ported subscriber but only sufficient information for Routeing the call to the Gateway Exchange of the Recipient Network. As an alternative, operators may agree not to transfer routeing information across network boundaries, but only to transfer the Directory Number, and to let each operator retrieve Routeing information for routeing calls in their own network. Then the routeing information only needs to contain sufficient information for routeing the call to the Gateway Exchange to a next network on the route towards the Recipient Network."

10.1.5.2 Commercial Aspects

Every call to a NP domain requires an SCP-query in the Originating Network. This causes additional expenses for the Originating Network operator.

The Donor Network operator has to reserve the ported-out Directory Numbers for use in another operator's network. This causes additional expenses for the Donor Network operator.

10.2 Between IN and Non IN Structured Networks

This chapter considers the possibilities of NP implementations if one or more of the participating networks are non-IN structured. IN is not a requirement in these networks.

10.2.1 Onward Routeing

10.2.1.1 Non IN Originating Network

The fact that the Originating Network is non-IN structured has no effect on onward Routeing. No IN queries are needed in the originating network.

10.2.1.2 Non IN Donor Network

Re-Routeing has to be done by other means than IN query, e.g. exchange based Onward routeing service.

10.2.1.3 Non IN Recipient Network

Without IN functionality in the recipient network, the other networks shall pass the complete routeing information.

10.2.2 Dropback

10.2.2.1 Non IN Originating Network

The Originating Network can be non-IN structured.

10.2.2.2 Non IN Donor Network

If the Donor Network is not IN based, the generation of the dropback message with re-Routeing information should be possible with a switch-based service. If this is not possible, the NP service cannot be implemented with the dropback method.

10.2.2.3 Non IN Recipient Network

Without IN functionality in the recipient network, the other networks shall pass the complete routeing information.

10.2.3 Query on Release

10.2.3.1 Non IN Originating Network

Originating Network shall be able to make IN queries except where the query can be performed within an IN structured Network - possibly the Donor or Transit / Serving Network.

10.2.3.2 Non IN Donor Network

The donor Network does not have to be IN structured.

10.2.3.3 Non IN Recipient Network

Without IN functionality in the recipient network, the other networks shall pass the complete routeing information. The recipient network does not have to be an IN network.

10.2.4 All call Query

10.2.4.1 Non IN Originating Network

If the originating N/W is not IN then it shall pass calls that are not recognized as being translated on its own network (e.g. switched based) to transit network for surrogate query.

10.2.4.2 Non IN Donor Network

Donor network is not involved at call / service routeing for 'All call query'.

10.2.4.3 Non IN Recipient Network

Without IN functionality in the recipient network, the other networks shall pass the complete routeing information. The recipient network does not have to be an IN network.

10.3 Network integrity

Complete Routeing Numbers of subscribers do not have to be passed between operators. operators "An operator that receives the Directory Number and the information that the number has been ported, should be able to find the RN from its own database." Also in the dropback method, the dropback message does not have to contain the complete RN but the address to the Gateway Exchange of the Recipient Network operator.

11 Security aspects for an IN structured NP solution

11.1 Security

The aim of this section is to describe the various security threats and their associated methods of attack in relevance to the four proposed architectures for Number Portability using IN networks. The four architectures shall be outlined graphically and a brief explanation of the working mechanisms shall be given.

The architectures considered in the present document are:

1) Onward Routeing;

2) Call dropback;

3) Query on Release; and

4) All call query method.

Due to the differences in these architectures some attacks shall be relevant to one architecture whilst irrelevant to another.

11.2 Number Portability specific issues

To analyse security problems relevant to Number Portability the following four architectures should be considered and analysed for their respective flaws and limitations. These diagrams have been taken from TR 101 119 [1].

11.2.1 Onward Routeing Method

As depicted in figure 42 below, the originating network routes the call to the original destination recipient network based on the block identity in the telephone number of the called customer. The donor network then routes the call onward towards the recipient network.

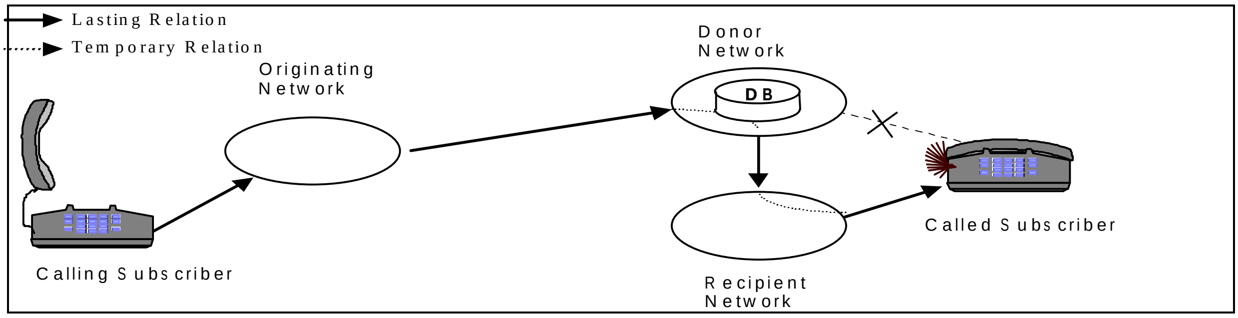


Figure 42: Onward Routeing method

The onward Routeing function is implemented in the Donor local switching system. The obvious disadvantage of this method is that all incoming successful calls to customers with a ported number result in connections via the donor network. Customers with ported numbers require network resources of the donor network as if they were still directly connected to it.

11.2.1.1 Security vulnerabilities

Database security: non-local to recipient network.

Network availability of donor network could possibly be affected.

Dependency on donor network for Routeing information - data and/or service availability / integrity may be affected.

Potential for fraud.

11.2.1.2 Counter measures

Congestion control.

Access control.

Security policy.

Audit system and integrity checks.

11.2.2 Call dropback and Query on Release

With the call drop back and Query on Release methods (figures 43 and 44 below), the Originating network routes the call to the (Donor) network based on the block identity in the telephone number of the called customer. However, the Donor network in the ported number case rejects the call. Upon call rejection the donor network re-routes the call to the recipient network. With call drop back the network resources consumed within the original destination donor network is restricted to the call set-up attempt including an interim user channel allocation. The connection eventually established after the re-Routeing does not consist of more interconnection sections than a connection to a non-ported number. (If released back to the original exchange only)

The Call dropback and Query on Release methods mainly differ with respect to which network maintains the Routeing data, i.e. the data to which serving recipient network the number has been ported.

11.2.2.1 Call dropback

The donor network maintains the Routeing data relating to its exported numbers. When a call is received for a ported number then this call is rejected with a release signal containing the identity of the recipient network. Based on this Routeing data the donor network re-routes the call to the recipient network.

The call drop back variant, as outlined in figure 43 below, is an evolution of the Onward routeing method. The required network functions are implemented in the switching systems. Particularly, the donor exchange maintains the Routeing data for its removed customers and supplies the Routeing data with the release each time a call arrives for a ported customer.

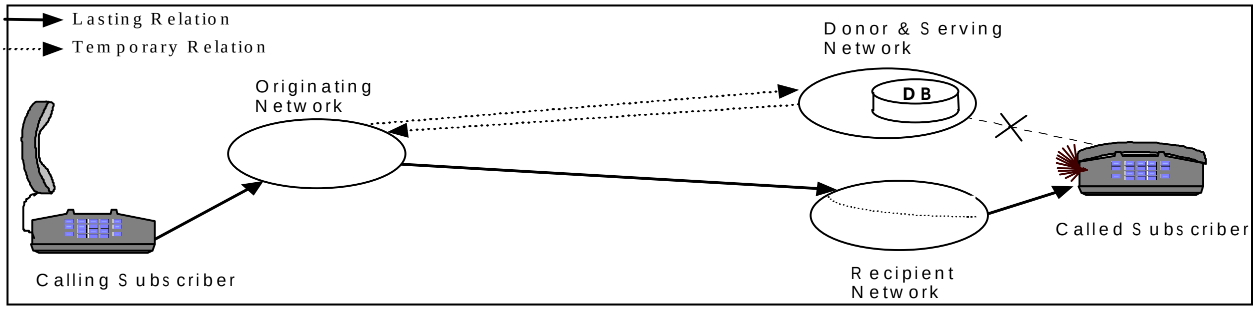


Figure 43: Call dropback - redirection

11.2.2.2 Security vulnerabilities

Database security: non-local to recipient network.

Loss or corruption of release message between operator networks.

Confidentiality of release message between Donor network and originating network.

Dependency on donor network for Routeing information - data and service availability may be affected.

Network availability of donor network.

Switching security issues.

Potential for fraud.

11.2.2.3 Countermeasures

Congestion control.

Access control.

Security policy.

Audit system and integrity checks.

11.2.2.4 Query on Release

With this variant, as outlined in figure 44 the donor network rejects the call by sending a backward release signal indicating the reason "ported" (or possibly "unequipped"). It is up to the originating network to determine whether it is a ported number and which is the recipient network.

For this purpose the originating network requires a database with access to current up-to-date. Routeing data for ported numbers across all networks.

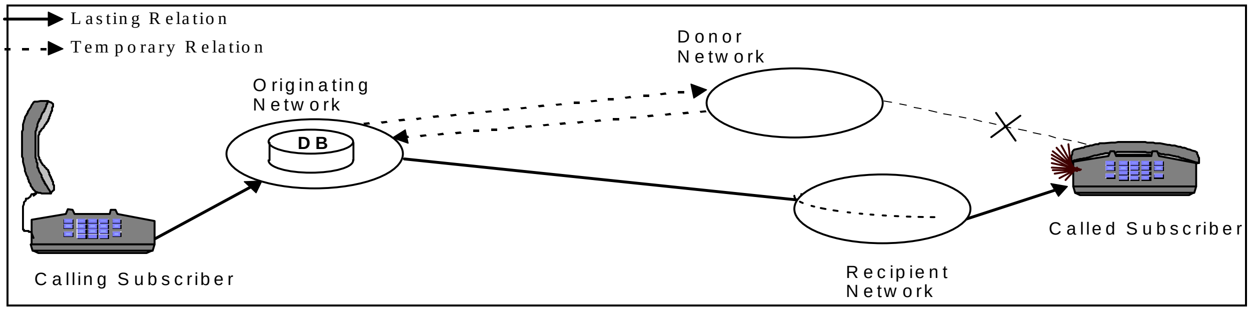


Figure 44: Query on Release method

11.2.2.5 Security vulnerabilities

Database security issues.

Loss or corruption of release signal data between operator networks.

Network availability of donor network.

Switching security issues.

11.2.2.6 Countermeasures

Congestion control.

Access control.

Security policy.

Audit system and integrity checks.

Standby system.

11.2.3 All call Query method

This principle of the All call query method is depicted in figure 45. For each call the originating network queries a database maintaining up-to-date Routeing data for ported numbers across all networks. Hence, calls can always be directly routed to the recipient network without affecting the donor network.

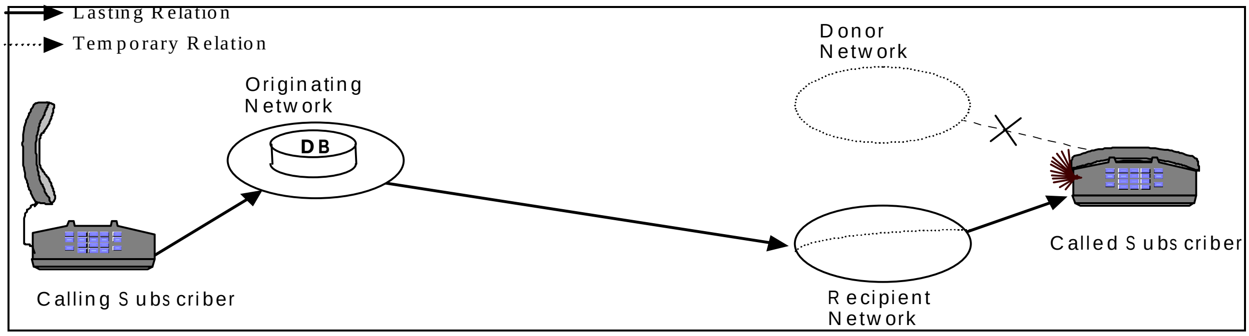


Figure 45: All call query method

11.2.3.1 Security vulnerabilities

Local database security issues.

Data integrity.

11.2.3.2 Countermeasures

Standby system.

Access control measures.

11.3 Database Security

Achieving security in a Database environment requires the identification of threats and a thorough analysis of the security policies pertaining to the database. All of the aforementioned proposed architectures in clause 11 implement the use of the operators database mechanisms. Some of the proposed architectures necessitate the use of a PNOs database for look-ups etc. which involves the traversal of the switched network to access the database. This highlights one of the greater security concerns for Number Portability which is access control to a PNOs database. This and other issues shall be investigated in the following sections. The figure 46 below outlines a Secure DBMS with external access from Public Network Operators (PNO).

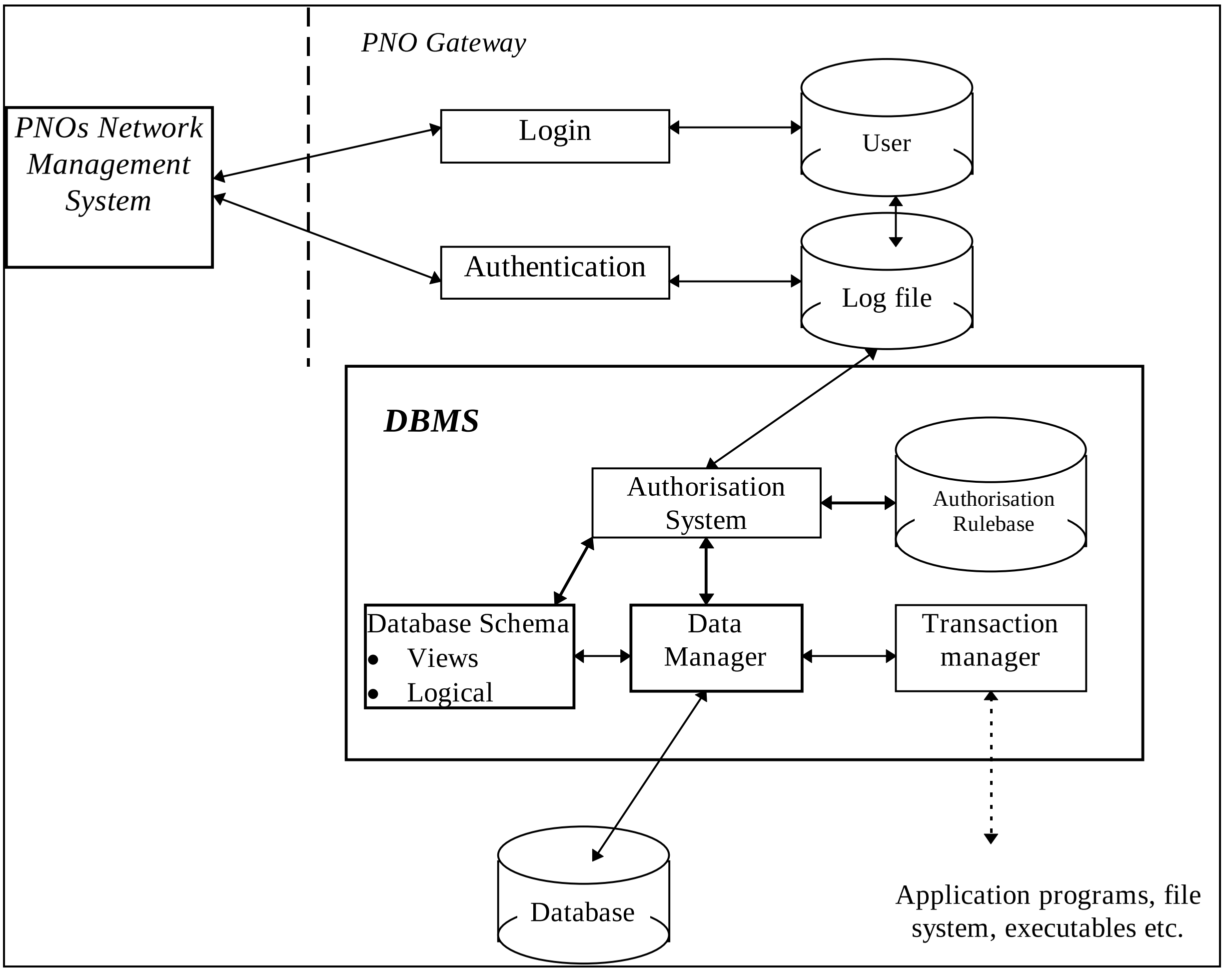


Figure 46: Secure DBMS with external access from PNO

11.3.1 Threats to Database security

Release of unauthorized information - This threat may manifest itself due to a number of reasons. The methods by which this may happen include hacking, social engineering and inference of unauthorized information from authorized information, incorrect access control lists or misconfiguration of network.

Improper modification of data - This may result from accidental or intentional usage. It includes all violations to data integrity by means of data handling or modification. These approaches to data modification are generally initiated by unauthorized access although this is not always the case. For example it is possible to modify stored data using a corrupted rulebase.

Denial of service by PNO database - The PNO database may prevent users from accessing data or resources for whatever reason.

Human error - This can result in potentially serious problems affecting data integrity, confidentiality or accessibility to data or resources. At worst human error can result in complete network failure.

*Misconfiguration of software / hardwar*e - Mis-configuration of hardware or software can result in serious error to all security requirements.

Natural disaster - Such as fire, water, wind and earthquake can all affect the security of the database by preventing access to system data.

Connectivity problems - Interconnection between operators may become unstable or break completely thus resulting in a loss of accessibility and possibly information in transit.

Availability of services - All systems should have adequate power and general service backup in case of failure.

11.3.2 Proposed counter measures

Protection from inference - Inference is the process of obtaining confidential data from non-confidential data. Inference generally affects statistical databases although multilevel databases etc. are also affected. It is generally recommended that as little confidential information as possible is stored in the database.

Access control - Access should only be given to authorized users. Access requests from PNOs should always be checked by the DBMS against the Access Control List (ACL). Database access control is more complicated than for files due to the granularity of data such as attributes, values etc. Data within a database is semantically related which raises the problem of a user inferring information without actually accessing it directly.

The Access Control System should theoretically consist of two major components that are heavily reliant on the operator's security policy:

A set of access policies and rules: This is information stored in the PNOs system describing the access methods to be adhered to by users upon access to the database.

Set of access control procedures - These should check the requests against the rules. Manipulation of data may then be permitted or denied.

Database integrity - The integrity of the database and its contents is primarily the responsibility of the DBMS and the site administrator whose task it is to make back-ups and recover data if necessary. For a system to be considered secure it requires integrity together with reliable and complete access control, authentication and anti-virus software.

Operational integrity of data - The data in the database should be logically consistent during simultaneous transactions. Locking techniques which lock data items for the period needed to execute the operation e.g. retrieving the identity of the serving network can enforce this.

Semantic integrity of data - This connotes ensuring the logical consistency of modified data by controlling data values in an allowed range.

Auditing and accountability - All non-call related actions on data items for both read and write should be recorded in an audit log that should be stored in a secure location. The security policy of the operator should state explicitly the granularity of data recorded by the audit log.

Authentication - All access to the database system should be authenticated by some means.

Security policy - The security policy of participating PNOs should be aligned with that of the database.

Resilient system - It is recommended that the system be logically or geographically distributed in case of failure.

Alarming - The system should be adequately alarmed to warn in case of suspicious activity.

Physical security - All performance critical or confidential systems should be physically secured. Suggested means include secure rooms etc.

11.4 Conclusions

Irrespective of the architecture being described there are certain requirements which apply across all scenarios. The following requirements have been identified as ubiquitous to Number Portability situation.

Careful marking of data - This entails that the services provided to a customer are clear and precise.

Well secured database - see subclause 11.2.

Careful update procedures.

Problem resolution procedure - The procedure for resolving problems anywhere on the network should be one of the first items detailed. If and when the scenario arises for this procedure to be referenced it should be unambiguous to the administrator.

Careful configuration and dimensioning of entire network and database. This encompasses the complete network security area.

12 Centralized / National Number Portability Database

For IN support of Number Portability, each call requires a database reference to determine if the dialled number has been ported and - if so - for a routeing translation to the current destination network.

For a centralized number portability database, it is essential that current number portability data is distributed effectively to ensure calls do not fail through non-availability. Risk is higher for ported numbers that depend on accurate data. The default route should be to the donor network.

History

Document history		
V1.1.1	November 1998	Membership Approval Procedure MV 9902: 1998-11-10 to 1999-01-08