Version FNP3v2F - March 31st 2014

Fixed Number Portability Task Force:

PT3: Database and operational aspects

Fixed Number Portability Provisioning Processes

&

Common Reference Database for Number Location

Content

1 Scope

The purpose of the document is to define the operational aspects and the database needed for the support of Number Portability in Belgium. It describes how the Participants communicate to establish a consistent environment, i.e. the method and contents of information exchanges.

In line with the scope of output from other project teams this document is focused on database elements and interactions with and between the parties involved in supporting number portability. The interactions described here are not influenced by potential bilateral communication schemes which are to be transparent for the functions highlighted in this document.

The scope of Number Portability described in this document covers both, Geographic and Non-Geographic Number Portability, as described in the law of 21 March 1991 article 105bis §6.

This document starts with a list of documents in the 'References' with additional information related to the concepts of operator number portability. These references are followed with a section on definitions and abbreviations of term defined in this and other FNPTF-PT documents. Also an overview of the processes is provided as they are specified by this contribution.

Section four is a general description of the database content and the responsibilities of the organisation responsible to operate the database. Also a high-level architecture of the system is shown, including the facilities which allow the database to communicate with its users.

The following two sections specify the processes of operation and the messages exchanged for this purposes. Also specific timing requirements are highlighted. The elements described in these sections are the backbone for co-ordination and co-operation as required to make number porting possible. They support the various aspects of internal workflow and processes of the Participants which are related to their commercial activities, the implementation of number porting requests, problem solving and customer services. Internal processes are not considered however because this is specific per Participant.

Section seven provides details of database content, responsibilities and functions that are required for the production of the document to tender.

The annexes clarify aspects of number portability, which are complementary to the specifications of given sections. They cover such topics, as SLA's, the problem of loops, complex installations, error codes, etc.

Billing and accounting related topics were not considered for this deliverable.

Version NPG3v1F (17-SEP-1999) describes, in addition to the "database & operational aspects" for Geographic Number Portability, the full role of the CRDC/CRDB as available at the launch of Number Portability. It also serves as the basis for NGFNP (please, refer to the corresponding NG-PT3 deliverable for details).

Version NP3v2F (30-AUG-2000) includes a section on escalation processes, and describes the actions to be taken for particular exceptions

Version NP3v1F (08-AUG-2001) integrates the specifications for Geographic and Non-Geographic Number Portability with the new enhancements and processes agreed on for the implementation into a new CRDB system as well as the process entry for the Broadcast Other Participants in the now spitted Technical Phase . The FNP Broadcast process is now an independent process allowing Participants not involved in the CRDB FNP Initiation and FNP Activation process to enter a own FNP RFS Broadcast messages into the FNP reference database.

Version FNP3v1F (24- March-2003) reflects the changes agreed and implemented in the CRDC that was accepted by the sector and put into production by 5 December 2002. The CRDB is a common used platform for the Fix and Mobile Number Portability provisioning and Common Reference for Number Location Database for all type of fixed and mobile numbers, each with its own processes but same interface for the NP Broadcast information and same common reference data base for new routing information of ported numbers and national number location of served numbers per operator.

Validation tasks, new or enhanced processes were added and the CRDB will manage different data tables involved to validate Number Portability transactions.

Reports were added to facilitate unique transactional of statistical values or volumes. The CRDC is enhanced with 3rd party access interfaces, one for the general public, accessible through the internet, and a second for the Judicial Authorities protected by individual login and password.

Additional information recorded under an agreed identification, “the Coded ID” mainly used in the common reference database for number location, reflects the impact or specific condition of a number used in the national network of a Belgian licensed operator.

For Fixed Number Portability a Participant FOLO has the possibility to process NP provisioning messages on a manual, semi-automated or fully automated manner.

The Version FNP3v1F (28 May-2004) reflects the changes and updates agreed by the Participants to enhance the CRDC. These updates are accepted by the sector and need to be put into production in the NP process applications running in September 2005. The CRDB is a common used platform for the Fix and Mobile Number Portability provisioning and Common Reference for Number Location Database and Information for all type of fixed and mobile numbers, each with its own processes but same interface for the NP Broadcast information and same common reference data base for the routing information of ported numbers and national number location of served numbers per operator.

New specific process related actions activated by the CRDC will produce a new FNP message towards the involved Participants , some stages in the FNP activation phase will only generate a notification towards the CRDC helpdesk for follow up or escalation purposes. New is also a System Down or Up status, information generated by a Participant through its GUI interface or by the CRDC Helpdesk. System down status issued by a Participant will generate a notification towards the CRDC helpdesk as well as in a real-time monitoring dashboard available to all CRDC Participants. When a System down status is observed for a specific Participant the CRDC shall generate a fault code when a FNP Recipient operator intends to send a FNP execution message and this till the status is back in a “System UP” state. The CRDC helpdesk monitoring the access link(s) towards the CRDC can initiate, after consultation of the involved party or after the escalation process with agreement of the NPA SM a System Down status in the name of the involved Participant.

To reduce the flow of irrelevant Broadcast messages emitted by the CRDC to all Participants , especially for GUI users or a recognised Hosting Party, annex L of this document describes a FNP Broadcast filtering method per Broadcast type permitting to receive only the FNP Broadcasts the Participant is involved with.

The new Version FNP3V2F (March 31st 2014) reflects the changes and updates introduced by the Royal Decree of July 2nd 2013, applicable as of October 2013. These are mainly related to timers, simplified validation rules and opening hours.

2 References

[1] NPTF-PT1 Number Portability Task Force - PT1: Service Description Number Portability for Geographical Numbers

[2] NPTF-PT2 Number Portability Task Force - PT2: Network Architecture and Signalling

[3] NPTF-PT3 - FNPG3v3F - Number Portability Task Force – PT3: Database and operational aspects – RELEASE 1

[4] NGFNPTF-PT3 - FNPG3v1F – Non-Geographical Number Portability Task Force – PT3: Database and operational aspects

[5] NPTF-PT4 Number Portability Task Force: - PT4: Economic aspects

[6] NPTF-PT7 Number Portability Task Force – PT5 : Regulatory Issues – Operator Number Portability for Geographic Numbers

[7] GFNPTF-PT1 Number Portability Task Force - PT1: Service Description Number Portability for Non Geographical Numbers

[8] NGNPTF-PT2 Number Portability Task Force - PT2: Network Architecture and Signalling

[9] NGNPTF-PT4 Number Portability Task Force: - PT4: Economic aspects

[10] MNPTF-PT3 Number Portability Task Force: - Mobile PT3: Database and operational aspects

[11] MNPTF-PT4 Number Portability Task Force : Mobile PT4 : Economic aspects

[12] Technical Interface Specifications (NPA document)

[13] Detailed Functional Design (NPA documents)

[14] Fix Number Portability Basic Service Level Agreement edition 03 July 2003 (BIPT Website)

3 Definitions, Abbreviations and Overview

3.1 Definitions

The following definitions and abbreviations are in addition to the ones specified in other contributions on the subject of Geographic Number Portability. They will be used in the context of different project teams working on the implementation of GFNP in Belgium.

For definitions, please refer also to FNPTF PT1 document entitled “Service Description Number Portability for Geographic Numbers”, section 4.1.

- **Block Portability (BP)** - for definition, see PT1
- **Broadcast Other Participants (BO)** – for definition, see hereunder
- **Call Trap Function (CTF)** - for definition, see PT1
- **Database Query Function (DQF)** - for definition, see PT1
- **Directory Number (DN)** - for definition, see PT1
- **Donor Network /Exchange (DON/DOE)** - for definition, see PT1
- **Donor Platform** - for definition, see [7]
- **Atypical Traffic** – for definition, see [7]
- **Geographic Number (GN)** - for definition, see PT1
- **Geographic Number Portability (GFNP)** - for definition, see PT1
- **Location Portability (LP) (also called Number Mobility (NM))** - for definition, see PT1
- **Mobile Station International ISDN Number (MSISDN)**
- **Mobile Number Portability (MNP) – for definition , see MNPTF – PT1**
- **Network Operator (NO)** - for definition, see PT1
- **Network Operator Portability (OP)** - for definition, see PT1
- **Non Geographic Number - for definition**, see [7]
- **Non Geographic Number Portability** – for definition, see [7]
- **Number Allocated Network Operator (NANO)** - for definition, see PT1
- **Originating Network(ORN)** - for definition, see PT1
- **Originating Exchange (ORE)** - for definition, see PT1
- **Point of Interconnection (POI)** - for definition, see PT1
- **Ported Number (PN)** - for definition, see PT1
- **Ported-In Number (PIN)** - for definition, see PT1
- **Ported-Out Number (PON)** - for definition, see PT1
- **Range Analysis Function (RAF)** - for definition, see PT1
- **Real-time Database (RTDB)** - for definition, see PT1
- **Recipient Network (REN)** - for definition, see PT1
- **Recipient Exchange (REE)** - for definition, see PT1
- **Recipient Platform** - for definition, see [7]
- **Reference Database (RFDB)** - for definition, see PT1
- **Routing Information (RI)** - for definition, see PT1

- **Routing Information Addition Function (RIAF)** - for definition, see PT1
- **Routing Number (RN)** - for definition, see PT1
- **Routing Prefix (RP)** - for definition, see PT1
- **Second Number (SN)** - for definition, see PT1
- **Service Portability (SP)** - for definition, see PT1
- **Serving Network (SEN)** - for definition, see PT1
- **Serving Network Functionality (SNF)** - for definition, see PT1
- **Service Portability (SP)** - for definition, see PT1
- **Service Provider** – for definition, see [7]
- **Service Subscriber** – for definition, see [7]
- **Transit Network(TRN)** - for definition, see PT1
- **Transit Exchange (TRE)** - for definition, see PT1

Definitions specific to the database and operational aspects of number portability in Belgium are the following:

- **Common Reference Database (CRDB)**

  The common reference database used by the Participants.

  The involved parties have the same information for normal real-time operational activities. However, due to the proprietary nature of such solutions no explicit specifications are given for the storage capability for actual network data.

- **Common Reference Database Centre (CRDC)**

  3rd Party contracted by the NPA to run, manage and maintain the CRDB and its NP processes, processes agreed between Participants and approved by the NRA.

  "CRDC" means in the document ; the total solution providing, maintaining, administering and operating Operator Portability and service management system, including, but not limited to:

  - the data processing system used to provide a centralised reference database,
  - the common reference database Software (including Enhancements or Maintenance Modifications),
  - agreed additional Services,
  - centralised reference database centre utilities, hardware, Third Party software, peripherals, communi-cations equipment and services, and
  - other facilities used at its centralised reference database centre to provide agreed services. E.g. the Public Web interface www.crdc.be for Number Location usage.

- **Donor**

  Means the operator of the Donor network (GNP and/or NGNP) or the service provider (NGNP) thereby ceasing to serve the Subscriber

- **Recipient**

  Means the operator of the Recipient network (GNP and/or NGNP) or the service provider (NGNP) thereby serving the Subscriber

- **Licensed operator**

  Means an operator, with NP obligations, who is responsible to support the operational procedures and processes as described in this document.

- **Network Portability Due Date** or **FNP Due Date**

  The date and time indicating the moment after which the GNP or NGNP service can be activated must be defined within the FNP activation Service Window.

- **Party or Participant**

  Means the users of the CRDB as approved by the body responsible for the CRDC; e.g. the CRDC, the Donor, the Recipient or another licensed operator (GNP and/or NGNP) or service provider (NGNP); not the Subscriber

- **3rd Party**:

  Party that has some privileges to retrieve public number location information from a CRDB front-end

  or NP private historical and/or common reference data from the CRDB.

- **Service User**

  The user, calling a non-geographical number.

- **End User**

  The end user is the entity who has been assigned the DN by the service Subscriber in the case of a non-geographic number.

- **Subscriber**

  Means the entity or person who is assigned a DN and who requests to the Recipient to port his DN, the service Subscriber (see definition in PT1) or the end-user of the DN.

- **Atypical Traffic**

  An atypical traffic pattern (f.i. massive traffic and explosive traffic) deviates from normal traffic pattern (in terms of call attempts per second and Erlang values) such that specific modifications are required at the interconnection and network level before the numbers generating traffic can be ported in order to guarantee a correct call treatment after the number(s) are ported.

- **Hot line or Support Desk**

  Supported service method and application system(s) from the CRDC to assist the Participants or recognised 3rd party users of the CRDB, for periods of time contractually agreed.

- **Transaction**

  Handling to process, end to end, a message through the CRDC system from the Participant's legacy installation towards another Participant or back to them.

- **Transaction Time**

  The total time needed by the CRDC to handle incomming messages, to validate and process them as well as to forward an acknowledgement , status condition or answer to the emitting party. End to end , In /out handling starting and ending on the access point (Router) of the Virtual Private Network, managed by the CRDC.

- **Non Profit Association for Number Portability In Belgium [NPA]**

  Entity managed by a representation of the Fix and Mobile operators in Belgium, that has as task to manage the contracted party that implemented and operate the CRDC and to support the members of the association for all NP related provisioning or data reference matters as well as to interface with 3rd parties who needs to have reference data for their own business usage. The NPA is represented by its board for contractual and management matters and by the NPA Service Manager for daily operational tasks or support.

- **Number Location utility**

  Two Public access methods have been put in place, the first access by use of an Interactive Voice Response Unit (IVR), managed and maintained by each operator on its own network and a second one based on a Web interface, managed by the CRDC, that provides information to the user when a correct mobile, geo or non-geographical number is typed in the query field. The outcome of the query is based on the CRDB reference data reflecting when a number is ported in by a Participant.

  The calling numbers (short numbers) for the IVR unit are language dependant; 1299 (Nl), 1399 (Fr), 1499 (D) and 1450 (E). The web interface uses the same structure; **www.1299.be (**Nl) etc…

  As of the new Royal Decree in 2013, the IVR is no longer a legal requirement and becomes optional. The web interface however remains an obligation.

- **NPA Service Manger**

Function granted to an own NPA or 3rd party resource to manage in name of the NPA the daily operational issues that have generated an escalation request from a Participant or hosting party, to validate the reports requested by the NRA and to manage any valid and accepted change requests of CRDC operational data or application change(s). The NPA Service Manager has a specific and own profile in the CRDC providing supervision on Participant's or Hosted NP transactions with an adequate reporting tool to settle accurately and efficiently these activities. NPA SM function could be extended for the supervision and management of Number Location Information (NLI) services or other annexed services to the CRDC, services running inside or through an external interface system(s) but connected on the CRDC.

- **Hosting party for NP Participant(s)**

Party recognised by the NPA, offering NP transaction services towards the CRDC for requesting NP Participant(s) and seen as a 3rd party resource. Host shares for its contracted NP Participant(s) an own connection(s) (link) to access the CRDC following the specifications. It logs in with the individual NP Participant ID using the Participant's "mnemonic" for the operational follow-up of NP transactions. Host is bind to respect e.g. NP regulated operational matters like NP Service Windows, Escalation procedures, published NP SLA parameters as well as the NPA "CRDC Usage" contracted duties. A Hosting service can be offered by a CRDC Participant or through a 3rd Party recognised by the NPA and mandated by the NP Participant requesting such services.

- **Repository Solution for 3rd party providing Number Location Information (NLI)**

NLI Repository solution is a separate module on the CRDC that contains the changes of the Number Location Information (NLI) based on current activated Fix Geographical and Non-Geographical ported numbers, as well as from MSISDN mobile numbers. NLI updated files are compared to a complete snapshot of the number locations (bulk synchronisation file) for a given date. The delta information compared to the latest bulk synchronisation file is posted in a repository module interfaced with the CRDC and entitled third parties having a subscription as 3rd Party for NLI, to access the repository system and can then download the NLI delta files. Location of Ported Numbers have to be compared with the by the BIPT, per OLO, allocated number blocks. (DB on BIPT Website).

3.2 Abbreviations and Acronyms

For abbreviations, please refer also to the NPTF PT1, NG-NPTF PT1 or MNPTF PT1 documents.

The letter "F" before an abbreviation or process step means mainly a Fixed Number Portability topic, an "M" or none a mobile topic. E.g. FNPTF- PT3, MNPTF-PT3, FNP RFS broadcast and NP broadcast.

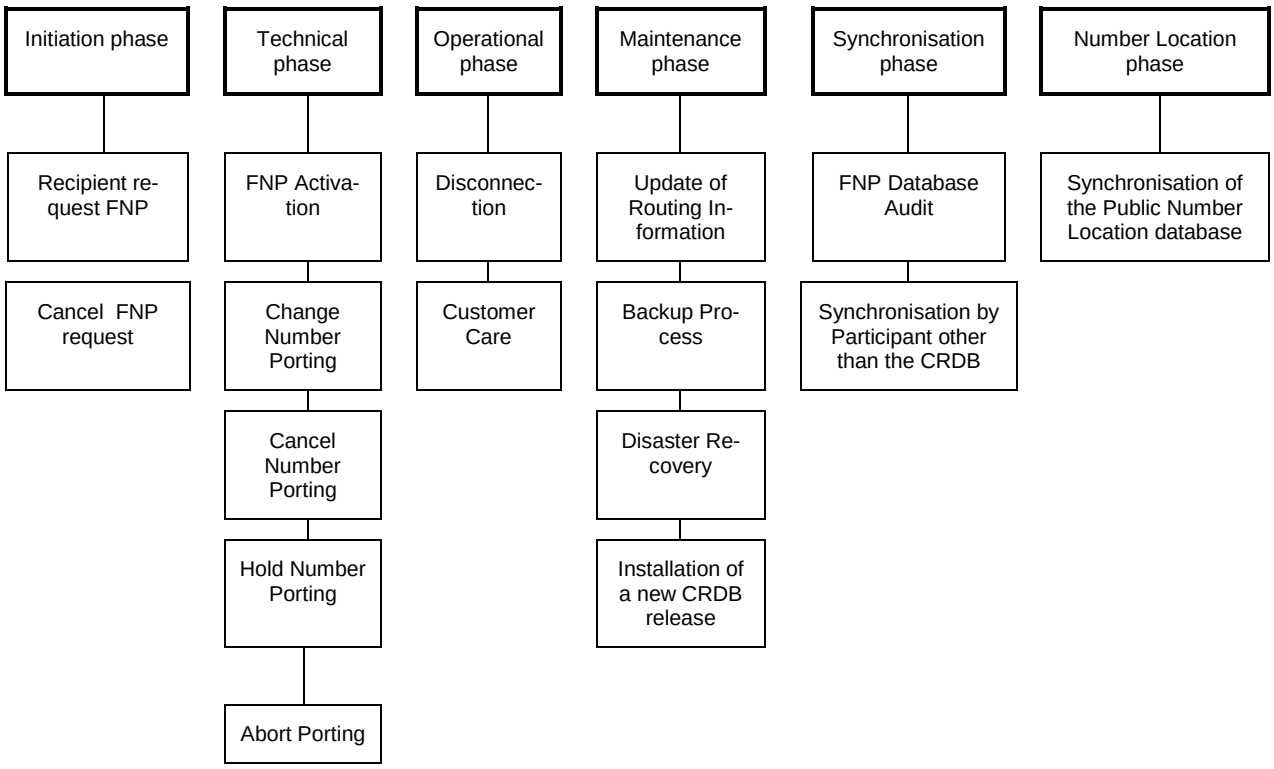
Documents could be consulted on the BIPT website.

ACC	Additional Conveyance Cost
APP	Applications
ARPA	Advanced Research Projects Agency
ASP	Application Service Provider
BO	Broadcast Other Participant
BP	Block Portability
BR	Block Reallocation
CCBS	Call Completion to Busy Subscriber
CCITT	International Telegraph and Telephone Consultative Committee
CLI	Calling Line Identity
CTF	Call Trap Function
CRDB	Common Reference DataBase
CRDC	Common Reference Database Centre
DB	Database
DDI	Direct Dialling In
DN	Directory Number (Geographical Number)
DNS	Domain Name System
DNSSEC	DNS Security
DOE	Donor Exchange
DON	Donor Network
DQF	Database Query Function
DWH	Data WareHouse
ENUM	Conversion protocol from Telephony to DNS (Electronic Number-

	ing)
ETNS	European Telephony Numbering Space
FMSP	Fixed Mobile Service Portability
FNP	Fix Number Portability
FNPR	Fix Number Portability Request
FOLO	Fix Other Licensed Operator
FTM	Fix To Mobile
FTP	File Transfer Protocol
FVMO	Fix Virtual Network Operator
GMSC	Gateway Mobile Switching Centre
GN	Geographic Number
GNP	Geographic Number Portability
GRPS	General Packet Radio Service
GUI	Graphical User Interface
HLR	Home Location Register
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
INT	Internet Services
IP	Internet Protocol
IPNG	Internet Protocol Next Generation
ISDN	Integrated Services Digital Network
ISO	International Organisation for Standardisation
ITU	International Telecommunication Union
LIDB	Line Information Database
LLU	Local Loop Unbundling
LoA	Letter of Authorisation
LP	Location Portability
MGT	Network Management
MN	Mobile Number
MNPTF	Mobile Number Portability Task Force
MNP	Mobile Number Portability
MPIN	Mobile Ported-In Number
MOLO	Mobile Other Licensed Operator
MPN	Mobile Ported Number
MSC	Mobile Switching Centre
MSISDN	Mobile Station International ISDN Number
MSRN	Mobile Subscriber Routine Number
MTF	Mobile to Fix
MVNO	Mobile Virtual Network Operator
MWI	Message Waiting Indicator
NANO	Number Allocated Network Operator , see also NRH
NDC	National Destination Code
NGN	Non-Geographical Number (Marketing number)
NIC	Network Information Centre
NIS	Network Information Services
NLI	Number Location Information
NM	Number Mobility
NO, NetwOper	Network Operator
NOC	Network Office Code
NOC	Network Operation Centre
NOP	Network Operator Portability
NPA	Non Profit Association for Number Portability in Belgium
NP-DB	Number Portability Database
NPTF	Number Portability Task Force
NRA	National Regulatory Authority
NRH	Number Range Holder
NSN	National Significant Number
OPS	Operational Requirements
ORE	Originating Exchange
ORN	Originating Network

OSI	Open System Interconnection
PIN	Ported-In Number
PN	Ported Number
POI	Point of Interconnection
PON	Ported-Out Number
PSTN	Public Switched Telephone Network
RAF	Range Analysis Function
REE	Recipient Exchange
REN	Recipient Network
RFDB	Reference Database
RI	Routing Information
RIAF	Routing Information Addition Function
RIPE	Reseaux IP Europeens
RIR	Routing Information Retrieval Cost
RN	Routing Number
RP	Routing Prefix
RTDB	Real-time Database
RTG	Routing
SEC	Security
SEN	Serving Network
SIM	Subscriber Identity Module
SM	Service Manager
SMS	Short Message Service
SN	Second Number
SNF	Serving Network Functionality
SP, ServProv	Service Provider
SRF	Signalling Relay Function
TC	Transaction Capability
TRE	Transit Exchange
TRN	Transit Network
TSP	Telephony Service Provider
TSV	Transport
UMTS	Universal Mobile Telecommunication System
USV	User Services
VLR	Visitors Location Register
VMSC	Visited Mobile Switching Centre
VoIP	Voice Over IP
VPN	Virtual Private Network
xDSL	x Data Subscriber Line
XML	Extensible Market Language

3.3 Overview



3.3.1 Initiation Phase

The objective of the initiation phase is to prepare the porting of a (non-)geographical numbers from the Donor to the Recipient. The conclusion of this phase is the agreement on a FNP Due Date for the actual porting of the Subscriber or a reject of a request.

All requests for non-geographic FNP (including Free Phone (FPH), Split Charges (SPL), Universal Access Numbers (UAN), Personal Number Services (PNS), Premium Rate (PRM), kiosk, …) have an indication whether the intended traffic profile will be “ATYPICAL” or “NON-ATYPICAL”.

The CRDC shall generate fault codes to prevent the relay of incorrect or incomplete information created by a Participant towards another.

A Recipient is able to request a cancellation after a FNP Request, during the validation period, E.g. When a customer changes his mind.

3.3.2 Technical Phase (Activation and Broadcast phase)

Implementation starts after a new FNP request is identified and all related data is collected via exchange of FNP data with the CRDB. All key parties supporting FNP - Recipient, Donor, CRDC, the other Participants will be ready to provide the service to the Subscriber by the end of this technical phase. Alternatively, it is possible that the request is cancelled or aborted before the actual activation of FNP takes place. There exists a special case where the Recipient is back the original Donor, and the process of porting can be undone.

The technical phase is split in activation and a broadcasting phase, were the broadcasting phase starts with a successful porting event.

A difference is observed between the GFNP and NGFNP Activation in the Technical phase:

The porting of geographical numbers is classified in different complexity classes; “Simple or Complex” depending if the FNPR belongs to a full or partial porting coupled to an installation type.

The porting of non-geographical numbers is classified under the “complex” installation with respect to the values for timers at the moment of porting.

Before the Execution of the porting, the FNPR could be put on hold by the Donor, cancelled or the due date changed by the Recipient.

During the Broadcast phase, but before the FNP Broadcast the Recipient can request the abortion of the port.

3.3.3 Operational Phase

Day-to-day changes to the operational environment with impact on individual ported Subscribers are specified in this process.

3.3.4 Maintenance Phase

Processes specified under this maintenance phase concern day-to-day updates of database information and planned actions for restoration of data or measures to do so.

3.3.5 Synchronisation Phase

The synchronisation phase includes processes which are used as day-to-day activity to keep consistency between databases of the CRDC and Participants.

3.3.6 Number Location Phase

A public accessible web interface permits to the general public or to the judicial authorities (*) to retrieve number location information and (*) historical data .This information is updated (synchronisation) every night based on the final broadcast for a ported number during the technical phase. This update occurs mainly for geographical, non-geographical and mobile numbers ported or disconnected but also for numbers subject to a specific condition recognised by the sector with an agreed specific Coded ID.

4 Database Content and Responsibilities

4.1 General

The CRDB stores information of common interest to all parties who contribute to operator FNP in Belgium. This information refers to common data; Subscriber specific information used for operator FNP and historical data for the provisioning of this service. Normally, all information as described in this document will be accessible to all parties under equal conditions. Temporarily, this principle will be violated when porting is taking place and synchronisation of the information must be completed.

The criteria referred to and used for the described concepts of database and operations are:

- The requests for number portability are an initiative of the Subscriber,
- This request is accepted by the Donor,
- The impact on the Subscriber for the implementation of FNP is minimal,
- There is efficient co-operation between centralised and decentralised functions of Participants and CRDC.

The Common Reference DataBase and the Common Reference Database Centre - for the definition of terms, represent the responsibilities highlighted in this section please, see elsewhere in the document. The responsibilities of CRDB/CRDC relate to the guaranteed, completeness, integrity and availability of the information and confidentiality.

The specific functions, data elements and/or values related to ‘CRDB content’ and ‘CRDC Responsibilities’ are specified in the sections ‘Database’ and ‘Operational aspects’, respectively. The purpose of qualitative descriptions in this section is to provide the context for subsequent sections ‘Interactions’, ‘Messages’, ‘Database’ and ‘Operational Aspects’.

Currently **unspecified** elements of processes in this document and stored data are:

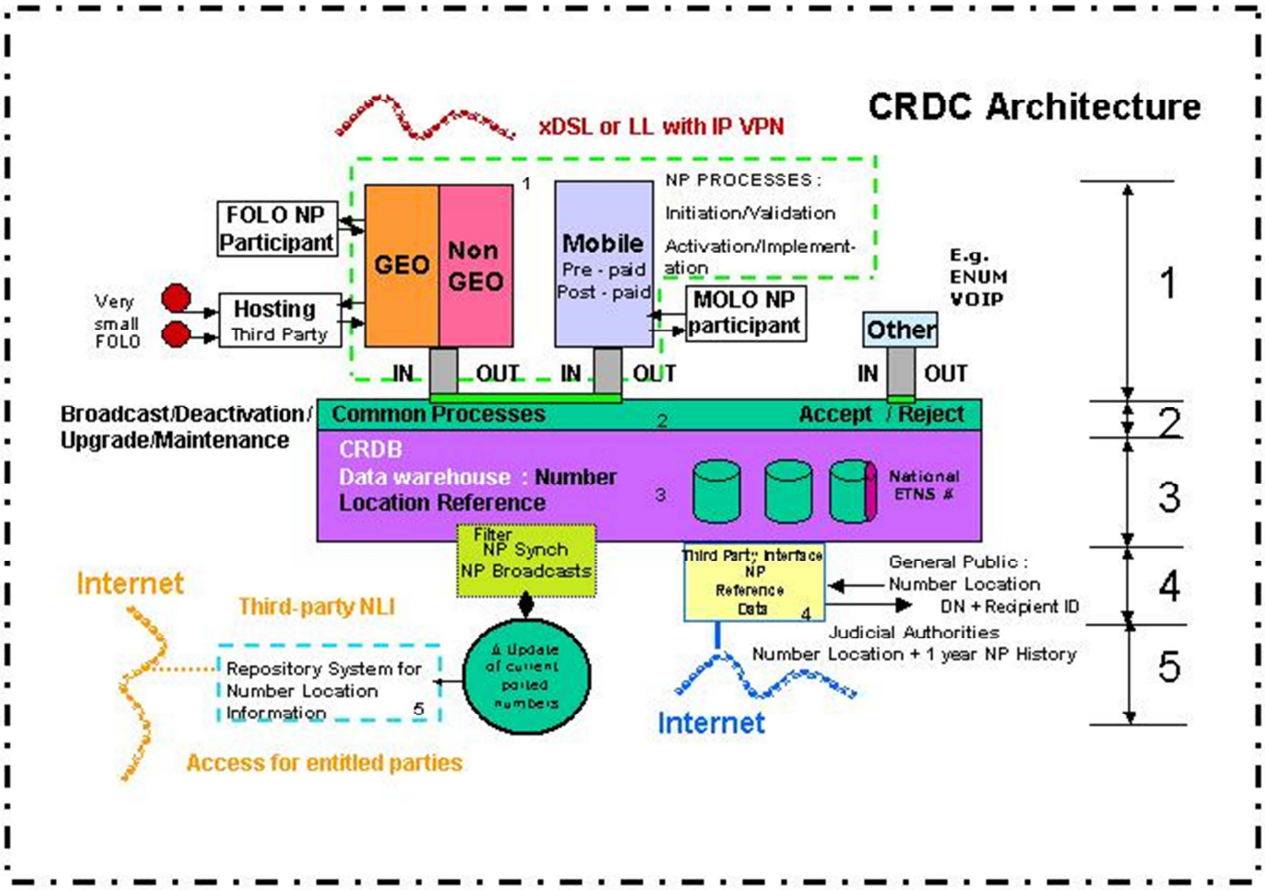
- **Partial Number blocks Reallocation,**
- **Local FNP,**
- **National FNP.**

Depending on the recommendation of STC or expansion of the scope of the PT3 task some of the above topics may be clarified in future releases of this document.

The responsibilities in this section specify in general terms the task of the CRDC. Detailed descriptions are given below in the sections that clarify the processes and exchanged information. Also specific requirements and constraints are therefore clarified respectively in “Processes for Interaction” and Messages”.

The FNPTF-PT3 document shall prevail in order of ranking compared to any other FNP issued document produced by whichever involved party.

The following schematic overview shows the different area’s of CRDC responsibilities:



Other: also the remote access for the NPA Service Manager.

4.1.1 CRDC Role

The CRDC will be responsible for the administration and operational support services required by Participants in their use of the CRDC/CRDB production and Test System. The CRDC will be involved in ported number administration monitoring. Mechanised enforcement capabilities may or may not exist in the CRDC to assist the CRDC in the monitoring and control functions.

4.1.2 Operational Functions

The primary roles of the CRDC are to assist Participants in obtaining reliable access to the CRDC and to support all Participants encountering operator ported number service provisioning problems resulting from CRDC operation. To meet this need, the CRDC must support the following functional areas: System Administration, Participant Support, maintenance tasks, monitoring tasks and System Support on Production and Test System.

4.1.3 Administrative Functions

Administrative functions include all management tasks required to run the CRDC. The CRDC must be accountable for all his personnel, legal, and financial management associated with the CRDC. These include, but are not limited to staffing, equipment and site procurement, facilities, and the own accounts payable obligations, which are part of day to day management. The CRDC must provide for the administration of its staffing, contractual, financial, maintenance, insurance, levy and operational needs. Proposals must specify how this will be accomplished.

The CRDC will be responsible for working with the NPA SM to update on request data tables requiring a change, tables impacting FNP operations & Management tasks. The CRDC is also responsible for; distributing the most current version of ported numbers and administration guidelines. The CRDC will notify the other Participants ASAP before any change.

4.1.4 System Administration

System administration ; the CRDC operational group is responsible for CRDC logon administration, Participant staff access and Participant data security, Participant notification of scheduled system downtime, and management and administration of the CRDB information tables required to link Participant records with the correct ported number & service functions, features, and network routing information.

4.1.5 CRDB functions

The CRDB application has as functions to facilitate under a unified and agreed FNP process flow the FNP phases and to log specific events for a certain period of time. The final goal of the CRDB is to keep on a real time basis the history of all "FNP RFS broadcast messages" and to keep its database clean and up to date by purging obsolete records after a FNP disconnection or number ported back to original Donor event. By subsequent ports to a third or xth Participant, the first port activated from the original Donor will still be recorded and documented in the CRDB as reference date and time of a first "port-Out" of this number.

The CRDB will maintain FOLOs data related tables and use these tables to validate the FNPR and if invalid reject the porting request with the appropriated fault code.

The tables are referred in section 7.2; e.g. the National Operator number block allocation tables, the Participants exchange identification routing numbers tables, Participant's mnemonic, pooled number blocks (e.g. ETNS numbers), etc…

The active allocated blocks referred as the National number block allocation data tables need to be provided and updated via the CRDC with input coming through the NPA Service Manager and originally from the BIPT and the exchange identification routing numbers table has to be provided with its updates on a automate basis from each involved Participant.

4.1.6 Test System

The Test System is a System that will be used for a FNP testing environment in order to allow testing the porting of numbers, to train people and to test all functionalities of software running on the Production System, patches before implementation on the production system and any new CRDB release. The Test System will be accessed through the same link for Participants already in production or on request of a Participant through the Internet. The Test System will be accessible through the Internet for new Participants to conduct their conformance testing.

4.1.7 NLI Repository Solution

The NLI Repository Solution, permit entitled 3rd parties to retrieve delta files (NP changes, due to subsequent ports or disconnections) for a certain period, compared to the last available NLI data file. The Solution is accessible through the Internet (https) and a login and password is needed to enter the repository solution. Access is all-time possible except during the maintenance duties of the NLI Solution Module. Information provided in the delta file contains the MNP & FNP Broadcast messages as well as the MNP and FNP Disconnect Messages. The CSV file will contain the following fields:

Timestamp of the message, Message type (broadcast or disconnection), Recipient identification, MSISDN for mobile ports and NumberFrom to NumberTo for Fixed ports.

The initial bulk synchronisation file will be generated on the start of the subscription or on explicit request of the 3rd party subscribing to the NLI Solution.

4.2 Detailed descriptions of the various functions (CRDC)

4.2.1 Logon Administration

Key Responsibilities

- Assist with new logon requests
- Verify logon signature approval
- Initialise logon ID, password per Participant's agreed user (involved individual Staff member), and security level
- Update data base and add new Participants

- Notify Participants of logon activation
- Resolve problems with existing logon IDs or passwords
- Resolve all log-on problems in real-time 24/7
- Password Management for FNP Participant's Staff and other integrated services accessible to third parties.
- Remote NPA Service Manager access (ISDN or xDSL)
- Log all problems within a Trouble Ticketing system
- Log access time and period spend on the CRDC as NPA SM + idle time longer than 30' (generate a time out)

4.2.2 Participant Record Security

Key Responsibilities

- Establish Participant boundaries through Participant access permission classes
  - Class that:
  - Can send a FNP request.
  - Can request an audit.
  - Can request a cancel.
  - Is member of the HOTLINE
  - Is member of the administrators.
- Assign new Participants to the correct security permission class
- Exercise absolute control of access to Participant records
- Monitor and report unauthorised system access attempts
- The logon Administrator is responsible for determining the correct group based on the organisation that originates the request.

4.2.2.1 NPA SM Security

- o Manage NPA SM profile and privileges

4.2.3 Scheduled System Unavailability Notification

Key Responsibilities

- Notify Participants and NPA SM in advance of planned or known system unavailability.
- The notification should be sent two weeks in advance via electronic way and a registered letter.

4.2.4 Software Release Acceptance Testing

Key Responsibilities

- Update software test plans
- Install new Software release on the Test Server
- Allocate staff for performing tests
- Execute test plans
- Generate and resolve testing trouble reports
- Document test results
- Certify CRDB software and release for operation
- Support ,"Software Acceptance Testing" phases by the Participants

4.2.5 Table Administration (Service)

Key Responsibilities (see also 7.2 for the CRDB data tables)

- Create and maintain CRDB data tables
- Map table information to appropriate codes
- Create and maintain descriptive data table labels. Includes but are not limited to:
  - Location Routing Number (LRN) tables
  - Participant information tables
  - Participant codes
  - CodedId table(s)
  - NP Broadcast type of message per specific Participant's profile
  - Timers table as published in the latest FNP Basic SLA document (NRA Website)
- FNP split/mass table changes.

4.2.6 Participant Problem Resolution (HOT LINE or/and Support Desk)

Key Responsibilities

- Clarify feature capabilities for Participants
- Resolve Participant record input and modification problems
- Support link problem resolution with data-link protocol analysis capabilities
- 24/24 hours – 7 days/week
- Resolve all download failures.
- Manage reporting of Trouble Ticketing System
- Manage the support Desk facilities (see annex K)

4.2.7 Software Update Notification

Key Responsibilities

- Notify Participants and NPA SM of upcoming CRDB software releases
- Updated documentation should be included as part of the software update.

4.2.8 Training Administration and documentation

Key Responsibilities

- Can be another qualified contractor (transparent to Participants).
- Serve as primary contact for course schedules/registration information
- Ensure availability of all CRDC/CRDB training
- Must produce the training material.

4.2.9 Document Order Administration

Key Responsibilities

- Process documentation requests
- Initiate documentation update distribution
- Provide documentation description, ordering information and price list literature
- Document security
- Provide a Business continuity plan

4.2.10 Training and Documentation Participant Feedback

Key Responsibilities

- Getting appropriate Participant recommendations reflected in CRDC/CRDB system documentation and training material
- Organise training sessions when relevant (main new Software release) or requested
- Provide and maintain a Repository System for the Participants

4.2.11 Conformity testing for New Participants

Key Responsibilities

- Conduct the certification management
- Provide Conformity testing statistics
- Provide support to the new Participant(s) during the compliance testing period

4.2.12 Download Problem Resolution

Key Responsibilities

- Analyse and resolve exception report issues resulting from unsuccessful updates to Participants' networks
- The HOTLINE must resolve all download failures.
- Manage the Participant's trouble ticket database, support adequately and timely the open tickets and forward a solution to the reported problems.
- If a communication problem exists it should be possible to communicate changes by a non-electronic way (fax, phone,). Therefore it should be possible to make use of the system from a GUI interface.
- Log all the operational issues within a trouble ticket system

4.2.13 CRDC/ CRDB Report Administration

Key Responsibilities

- Generate and distribute CRDB reports to all requesting Participants who are entitled to receive reports
- Validate the accuracy of report contents
- Generate and distribute reports to CRDB Participants who are entitled to receive reports and do not have local print facilities
- Resolve report interpretation problems
- They should provide reports and optional customised reports.
- Provide tool(s) or adequate support to provide "Participant's consolidated reporting" for the NRA
- Build the reports with an agreed constructive business logic
- Document the used (agreed) business logic per report type to generate a report
- Differentiate Participant as report requestor and involved Participant in the NP cases reported
- Maintain the reports list and content up to date (see list under annex D)
- Report connection history with the monitored parameters per access type

4.2.14 CRDC Interface Monitoring

Key Responsibilities

- Assist in the resolution of data communication problems with all CRDC service systems (Participants, etc.)
- Provide technical assistance to CRDC Participants experiencing problems accessing the system
- Support and monitor the different type of accesses and communication methods (LL, xDSL, …)

(FNP production system “provisioning & reporting”; GUI, Semi-automated, full automated Participants and NPA SM remote access -NP Test system: usage)

- Monitoring of the redundant link when activated or tested
- Monitoring the fall back access & restoration to normal
- Monitoring the bandwidth usage and throughput per access path by the use of leased lines

4.2.15 Data and system Integrity.

- Identify Originator of System Resources

  CRDC shall identify the originator of any accessible system resources.
- Identify Originator of Information Received Across Communication Channels

  CRDC shall be able to identify the originator of any information received across communication channels.
- Monitor System Resources

  CRDC shall use a product to monitor the system resources.
- Detect Error Conditions

  The CRDC shall use a product to detect error conditions.
- Detect Communication Errors

  The CRDC shall use a product to detect communication errors.
- Detect Link Outages

  The CRDC shall use a product to detect link outages.
- Rule Checking on Update

  The CRDC shall ensure proper rule checking on data update.
- Handling of Duplicate Inputs

  The CRDC shall handle duplicate/multiple inputs.
- Check Return Status

  The CRDC is responsible for checking all the return statuses.
- Validate Inputs

  The CRDC shall validate inputs for reasonable values and content.
- Transaction Serialisation

  The CRDC shall ensure proper serialisation of update transactions.
- Database Integrity Checking

  The CRDC shall include database integrity checking utilities for the CRDB.
- System clock synchronisation

  The CRDC shall ensure proper synchronisation between CRDB and Participants by use of an atomic clock source.
- Database back up and restoration

  The CRDC shall ensure an adequate and integrity save method for the planned back-ups and restore duties

4.2.16 Continuity of Service

- System Made Unavailable by Participant

  CRDC shall ensure that no Participant action, either deliberate or accidental, should cause the system to be unavailable to other Participants.
- Detect Service Degrading Conditions

CRDC shall report conditions that would degrade service below a specified minimum, including high memory, CPU, network traffic, and disk space utilisation.

- System Recovery After Failure

  CRDC shall provide procedures or mechanisms to allow recovery after a system failure without a security compromise.

- Software Backup Procedures

  CRDC shall have documented procedures for software backup.

- Data Backup Procedures

  CRDC shall have documented procedures for data backup.

- Software Restoration Procedures

  CRDC shall have documented procedures for software restoration.

- Data Restoration Procedures

  CRDC shall have documented procedures for data restoration.

- Software Version Number

  CRDC shall record the exact revision number of the latest software installed. This information is available at all times.

- System Power Supply

  CRDC shall provide sufficient backup power to maintain operation through electrical outages by means of UPS systems.

- Redundant Access

  The production system shall be accessible on a redundant path E.g. ISDN dial UP

- Test System

  A Test System will be accessible for conformance testing, release update, patch approval or new main releases through the same access paths as the production system as well as access through the Internet on request of a Participant.

  A specific Internet access needs to be provided for conformance testing and training purposes of expected new Participants.

4.2.17 Security Requirements

4.2.17.1 Threats

Attacks against the CRDC may be perpetrated in order to achieve any of the following:

- Denial of service to a Subscriber by placing wrong translation information in the CRDB
- Denial of service to a Subscriber by preventing a valid message from reaching the CRDB
- Disrupting a carrier's operations by having numerous spurious calls (to Participants who are not clients of that carrier) directed to that carrier
- Switching Subscriber to various carriers without their consent
- Disrupting the functioning of the CRDC / CRDB by swamping it with spurious messages

4.2.17.2 Security Services

- Authentication

  The interface between the CRDC and the Participant database shall support Authentication (at association set-up).

- Data Origin Authentication

  The interface between the CRDC and the Participant database shall support data origin authentication for each incoming message.

- Detection of an information send replay

  The interface between the CRDC and the Participant database support detection of replay.

- Modification of a Message

  The interface between the CRDC and the Participant database shall support detection of message modification.

- Delay of an information sent

  The interface between the CRDC and the Participant database shall support detection of the message time frame.

- Access Control

  The interface (GUI, XML,…) between the CRDB and the Participant database shall allow only authorised parties (i.e. carriers serving a given Participant) to cause changes in the CRDB database. To achieve this they will make use of security group's examples (but not limited):

  - Type of Participant (Operator, administrator, FOLO and MOLO Participant, ….)
  - Type of message (Audit, Synchronise, …)

- Security services by use of xDSL connections

  To access the production and NLI system (e.g. https with appropriated user(s) certificates.)

4.2.17.3 Security Mechanism

This section outlines the requirements to specify security mechanism of the CRDC.

A. Encryption

1. Public Key Cryptographic System (PKCS)

The interface between the CRDC and the Participant database shall use a public key cryptographic system (PKCS) to provide digital signatures. Since there is no requirement for confidentiality service there is no need for any additional encryption algorithms.

2. Digital Signature Algorithms

The interface between the CRDC and the Participant database shall support one of the digital signature algorithms.

B. Authentication

1. Digital Signature Algorithm

The interface between the CRDC and the Participant database shall apply the digital signature algorithm to the fields' specified below without any separators between those fields or any other additional characters.

- The unique identity of the sender
- The time, corresponding to the issuance of the message
- A sequence number
- A key identifier
- Integrity protection.
- Check system signature.
- Key list ID

2. Authenticator Contents

The interface between the CRDC and the Participant database shall provide authentication consisting of the following:

- The unique identity of the sender
- The Generalised Time, corresponding to the issuance of the message
- A sequence number
- A key identifier
- Check-sum data content embedded within authentication
- The digital signature of the sender's identity, Generalised Time and sequence number listed above
- Key list ID

3. Authenticator in Access Control Field

The interface between the CRDC and the Participant database shall convey the authenticator in the access control field.

C. Data Origin Authentication

1. Subsequent Messages Contain Access Control Field

The interface between the CRDC and the Participant database shall ensure that every subsequent message that contains the access control field carries the authenticator.

2. Separate Counter for Association Sequence Numbers

The interface between the CRDC and the Participant database shall verify that each party maintains a separate sequence number counter for each association it uses to send messages.

3. Increment Sequence Numbers

The interface between the CRDC and the Participant database shall verify that every time the authenticator is used a certain algorithm will change the value of the sequence number.

4.2.17.4 Integrity and Non-repudiation

A. Security Field

The interface between the CRDC and the Participant database shall ensure that all the notifications defined for the number portability application contain a security field.

B. Security Field Syntax

The interface between the CRDC and the Participant database shall ensure that the syntax of the security field used for the notification corresponds to the authenticator.

C. Notifications in Confirmed Mode

CRDC shall ensure that all the notifications are sent in the confirmed mode.

4.2.17.5 Access Control & Application Monitoring

CRDC shall be responsible for access control on the CRDC interface and the CRDC interface to the CRDB interface.

- Monitor the system response times
- Monitor End to End message delivery
- Monitor the access link capacity usage

Access control and application monitoring is based on the CRDC SLA parameters , agreed triggering and calculation method , especially what regards the CRDC end to end transaction performances.

4.2.17.6 Audit Trail

Log Contents

The interface between the CRDC and the Participant database shall keep a log of all of the following:

- Incoming messages that result in the set-up or termination of associations

- All invalid messages (invalid signature, sequence number out of order, Generalised Time out of scope, sender not authorised for the implied request)
- All incoming messages that may cause changes to the CRDB database

4.2.17.7 Key Exchange

A. Lists of Keys

CRDC shall ensure that during a security key exchange, each party provide the other with a list of keys.

B. Keys in Electronic Form

CRDC shall provide the list of keys in a secure electronic form on CDROM support.

C. Key List Exchange

CRDC shall support exchange of the list of keys in person or remotely.

D. Keys Not Reused

CRDC shall reject messages that use a key whose usage has stopped.

E. Key Change or maintenance

CRDC shall, free of charges, change or maintain the key used between the CRDC and the Participants at least once a year or at Participants specific request. Synchronisation of the key exchange or renewal process per access method is expected to be conducted by the CRDC.

4.2.18 Disaster Recovery and Backup Process. (Operation)

These process flows define the backup and restore activities performed by the CRDC and the Participants. The disaster recovery procedure must be transparent to all Participants.

If there is a planned downtime for the CRDB, the CRDC will send a notification (see 4.3) to the Participants that includes information on when the downtime will start, how long it will be, and if they will be switched to the back-up or disaster recovery machine. Downtime is considered planned when the CRDC can provide notification to the Participants at least 2 weeks in advance.

If there is an unplanned downtime, the CRDC will assess how long the primary machine will be down. The CRDC will notify all of the Participants by electronic notification and telephone calls to the Participants' contact numbers. The notification will describe the situation and the planned action.

- CRDC notifies Participants of switch to backup CRDB.

  The Participants will switch to the backup or disaster recovery machine as indicated in the notification.
- Participants connect to backup CRDB.

  The CRDC is responsible to route all connections to the back-up system.
- Participants conduct business using backup CRDB.

  The Participant should continue to process as normal when connected to the backup CRDB.
- Backup CRDB notifies Participants of switch to primary CRDB.

  The CRDB sends a message when the primary system is on line.
- Participants reconnect to primary CRDB.

  The Participants re-establish associations with the primary CRDB application using their normal connections.
- Primary CRDB notifies Participants of availability of primary system.

  When the primary CRDB is available, CRDC personnel will notify Participants of the system availability.

4.2.19 Administration

The administrative staff must provide support and direction for the operational CRDB groups and manage the business and technical issues affecting the performance of CRDB services.

Key Responsibilities

- Plan CRDC staff for software acceptance testing, report acceptance results, and ensure problem resolution of discrepancies.
- Schedule staff training for new software features and updates. Analyse documentation and training impact.
- Co-ordinate testing and cut over with CRDC data centre operations.
- Co-ordinate critical software release cut over.
- Adjust Staffing Level Based on Forecast System Usage Demands
- Plan capital equipment based on required staffing levels and CRDC performance standards
- Manage CRDC facilities
- List of trouble reports, with a breakdown between CRDB and CRDB Participant complaints
- List of cleared trouble reports

4.2.20 Facilities Requirements

The CRDC must provide an operational point of presence within Belgium by which Participants can connect to the CRDC. Participants will be able to connect to the CRDC by connecting to the CRDC facility location.

The physical location of the CRDC facility is at the discretion of the CRDC. The facility may be a separate building or be part of a larger facility owned or leased by the CRDC. If the CRDC is located within a larger facility, space allocated to the CRDC must have the following characteristics:

- Be dedicated entirely for CRDC use
- Be a distinguishable area, separate from other parts of the facility by use of secure access points
- Any access - physical or electronic - to the system, must be logged and accessible for the NPA manager
- Be contiguous space so that all CRDC staff members are physically located within the same secure area
- Serve as the primary (and, if applicable, secondary) work areas for all CRDC functions to be performedHave sufficient and suitable telecommunications links available with diverse routing disaster protection

4.2.21 Telecommunications Requirements

Key Requirements

- Individual phone lines for staff members
- 24 hour HOTLINE / Service Desk
- Voice messaging system
- Data communication facilities, fixed and mobile
- Voice communication facilities, fixed and mobile
- Faxes
- E-mail (group addresses preferable over named addresses in case of personnel changes)
- Guaranteed Access to an Actual CRDC Staff Member 24 Hours a Day
- The latest CRDC status available at times when the system may be unavailable during scheduled or unscheduled downtime.
- The choice of voice communication architecture, vendors, equipment, and services is totally at the discretion of the CRDC. The goal of these choices should be to best meet the functionality and service requirements described above. The CRDC will be responsible for the cost and services management and maintenance of its voice communication facilities. The CRDC will also be responsible for meeting or exceeding the required qualitative and quantitative performance levels that will be part of the regular service monitoring audits
- Procurement and management of the data communication facilities required between the CRDC, the data centre, and the system vendor are the responsibility of the CRDC. The contractor must provide re-

dundant data communication facilities to provide for disaster recovery due to facility outages. It will be the responsibility of CRDC to meet the data communication specifications of the CRDC system vendor. Data Communication must also include the ability to input into the appropriate trouble reporting systems.

4.2.22 CRDC/CRDB Reliability and Availability

This section defines the reliability and availability requirements for the CRDC/CRDB.

The final contractually agreed requirements will be written down in a separate SLA document.

The CRDC will be designed for high reliability, including redundancy and data integrity features, symmetrical multiprocessing capability, and allow for economical and efficient system expansion. The system will adhere to the following availability and reliability requirements:

- The centre will be functional 24 hours a day, 7 days a week.
- Its reliability will be 99.9% per segment for the total solution. This applies to functionality and data integrity.
- The amount of unscheduled downtime per year will be <= 9 hours.
- For unscheduled downtime, the mean time to repair will be <= 1 hour.
- The amount of scheduled downtime per year will be <= 24 hours.
- The scheduled downtime will be less than 4 hours off-peak within a 24 hour period
- It will be capable of monitoring the status of its entire communication links and be capable of detecting and reporting link failures and security malfunctioning.
- If a failure occurs resulting in downtime of any functionality, affected transactions received immediately prior to the failure must be queued and processed when functionality resumes.

The design will provide:

- Functional components with on board automatic self-checking logic for immediate fault locating.
- Continuous hardware checking without any performance penalty or service degradation.
- Installing redundancy of all major hardware components for continuous operation in the event of a system hardware failure.
- Hardware redundancy that is transparent to the Participants.

If the system becomes unavailable for normal operations due to any reason, including both scheduled and unscheduled maintenance; Participants must be notified of the system's unavailability.

- When possible, the notification will be made via an electronic broadcast message to the Participants. When this is not possible, the CRDC will notify the Participants via their contact numbers.
- The notification will include, at a minimum, the functionality that is unavailable, and the reason for the downtime, estimated length of the downtime and a CRDC contact number.

During any maintenance, if resources allow only partial functionality, the capability of receiving, processing and broadcasting updates will be given the highest priority.

It must provide system tolerance to communication link outages and offer alternate routing during such outages.

For any downtime, either scheduled or unscheduled, lasting more than 1 hour, the CRDC will switch Participants to a backup or disaster recovery machine. In most cases, the time to switch the Participants to another machine and provide full functionality must not exceed the mean time to repair. However, in the event of a disaster that limits both the CRDB and CRDC ability to function:

- The capability of receiving, processing and broadcasting updates must be restored within 12 hours.
- Full functionality must be restored within 48 hours.

Reports documenting the performance of the CRDC in regards to the above requirements will be provided.

4.2.23 Maximum CRDB access times with GUI interface

The final contractually agreed requirements will be written down in a separate SLA document.

- Access time to login into the CRDB must be ≤ 120 seconds
- End to end transaction time for one NP process (message) for a single number must be for 95% less than 20" and no more than 2'
- Worklist operational queries must not exceed 2' and in 95% less than 1'.
- Returns on reporting requests:
  - On production system < 120"
  - On DWH < 120"
- Synchronisation reports < 15'
- Transaction time to process an end to end NP transaction for multiple numbers must be ≤ 180 seconds (Average150 Sec) in 99.9% of the cases

4.2.24 Maximum CRDB access times with web browser and XML/Soap interface

The final contractually agreed requirements will be written down in a separate SLA document.

- Access time to login into the CRDB must be ≤ 120 seconds
- End to end transaction time for one NP process (message) for a single number must be for 95% less than 10" and no more than 2'
- Worklist operational queries must not exceed 2' and in 95% less than 1'. with an average < 15"
- Returns on reporting requests:
  - On production system < 120"
  - On DWH < 120"
- Synchronisation reports < 15'
- Transaction time to process an end to end transaction for multiple numbers must be ≤ 120 seconds in 99.9% of the cases

4.2.25 Prioritisation of CRDB messages flows and message type threshold management.

The CRDC *always* handles the exchange of FNP messages according to their priority. The priority is controlled by the CRDC internally using a configurable table ensuring that messages are globally handled according the same priority throughout the full NP process.

FNP Message	FNP Priority	Participant
Fnprequest	Medium	Recipient
Fnpreject	Medium	Donor
Fnpexec	High	Recipient
Fnpready	High	Donor
Fnprfs	Medium	Recipient
Fnpnonrfs	Medium	Recipient
fnprfsbroadcast	Medium	CRDB

fnpactivated	Low	All
Fnpaccept	Medium	Donor
Fnpchange	Low	Recipient
fnpchangereject	Low	Donor
fnpchangeaccept	Low	Donor
Fnpcancel / Cancelled by CRDC	Medium	Recipient
Fnphold	Low	Donor
Fnpabort	High	Recipient
fnpabortactivated	Medium	Donor
fnpdisconnect	Low	Recipient
fnpdiscdone	Low	Donor
fnpdeactivated	Low	Recipient
fnpdeactbroadcast	Low	CRDB
fnpdeactdone	Low	Participant & Donor
fnpupdate	Low	Recipient
fnpupdatecompleted	Low	Participant(s)
Npbroadcast (mobile)	High	MOLO
Npdisconnect (mobile)	High	MOLO

NOTE: NP messages threshold management:

Due to OLO's network system management constraints some volume of specific NP messages may not exceed a threshold specified and agreed between the Participants for message exchange. (Especially MNP Broadcast messages who forces some Participants to update ASAP their IN platform)

The monitoring of this threshold shall be managed operated and maintained by the CRDB with the use of parameter tables. Warnings will be sent to the involved Participant taking into account a real-time volume counter feed by (F) NP message types.

Note 1: MNP messages (Broadcasts) towards FOLOs, no more than 83 messages per 5 minutes

Note 2 : Possibility to FNP Broadcasts and MNP broadcasts message per type, to follows a specified Participant variable profile (maintained in Participant's specific profile data table). This profile and data table with its parameters need to be accessible by the involved Participant through the GUI in a read only mode as well as by the NPA SM.

4.2.26 CRDB recommended access and interfaces

A secure IP based VPN access method with XML for small operators or as redundant interface a GUI is recommended. Other access paths like LL or Dial In access (as redundant bypass) has to be negotiated with the body managing the CRDC.

5 Processes for Interaction

This section describes the requirements for interactions which can be identified in the scenario's for FNP as described in PT2 deliverables for geographical and non-geographical FNP, i.e. currently the Onward Routing (OR) and All Call Query (ACQ). It is to the discretion of two involved parties to select one of the scenarios on a bilateral basis. This choice, however, should have no influence on the operational aspects and the CRDB as discussed in this document.

The diagrams of this section show the data flows without highlighting of underlying protocols responsible to guarantee delivery of the messages. It means that, outside the scope of this description, a secured and protected environment must be defined supporting the transfer of data without loss, corruption or duplication of the original information.

Explicit acknowledge messages, e.g. 'FNP Ready', are specified at the application level when an explicit action is required following the request for action and where the timing is important.

Reject messages are used in the case that a request cannot be executed, meaning that the action on a corresponding request is refused.

Different phases are distinguished in the process of service delivery for FNP; each with their own characteristics of timing, involvement of various parties, exchange of information, etc. Specific data and events are specified per individual process.

Messages in the diagrams that leave one of the parties without being separated by a process are to be considered as sent simultaneously.

All timers and time frames applicable to the following processes are defined in the section 'Time frames and Timers'. Values are specified; see 6.4.10, to put the processes in the right perspective. All time stamps are specified by the CRDB.

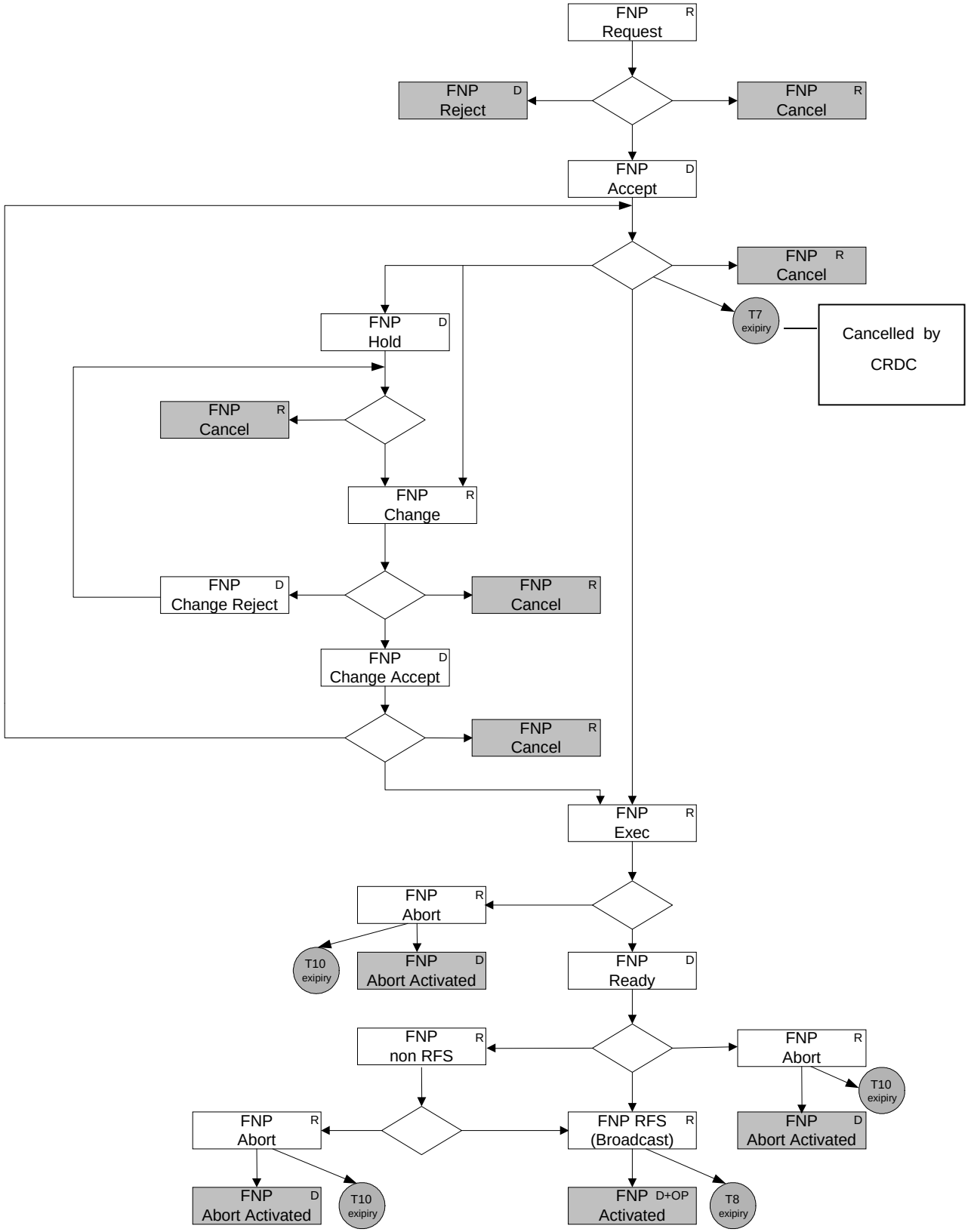
Referring to the definition of FNP services, the previous Recipients/Donors must take the appropriate action when routing information is changed. The purpose of this requirement is to avoid chaining in the case of subsequent portability. Within this section this applies specifically to the following processes of the technical, operational and maintenance phases.

Number ranges or numbers belonging to the same physical installation address can be grouped together using the FNP grouping features. The rule is that all Participants in the process as a whole treat grouped ports.

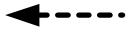
Finally, in the following processes the role of Network Operators and Service Providers should be comparable with respect to geographical and non-geographical numbers as well as for Operators influencing the FNP RFS Broadcast messages.

Errors that are returned by the CRDB are called faults that results of errors found during the validation by the CRDC and performed in three stages; - message format validation, -element validation, - transaction and consistency check validation. This rule is applied for every incoming message from Recipient, Donor and Participant towards the CRDB.

FNP Process flow


FNP Request R
FNP Reject D
FNP Cancel R
FNP Accept D
FNP Cancel R
T7 exipiry
Cancelled by CRDC
FNP Hold D
FNP Cancel R
FNP Change R
FNP Change Reject D
FNP Cancel R
FNP Change Accept D
FNP Cancel R
FNP Exec R
FNP Abort R
T10 exipiry
FNP Abort Activated D
FNP Ready D
FNP non RFS R
FNP Abort R
T10 exipiry
FNP Abort R
FNP RFS (Broadcast) R
FNP Abort Activated D
FNP Abort Activated D
T10 exipiry
FNP Activated D+OP
T8 exipiry

Message sent, e.g. Fixed Number Portanility Request



Message response sent by the CRDB, e.g. Fault code.

P1 **Procees to the next step with execution of process P1**

t-0 **Reference point for timing applicable to current diagram**

Link to the following diagram

[HOLD] **reference to a possible interfering process**

Figure 1 Keys to the diagrams

Identification of the different Participants in FNP:

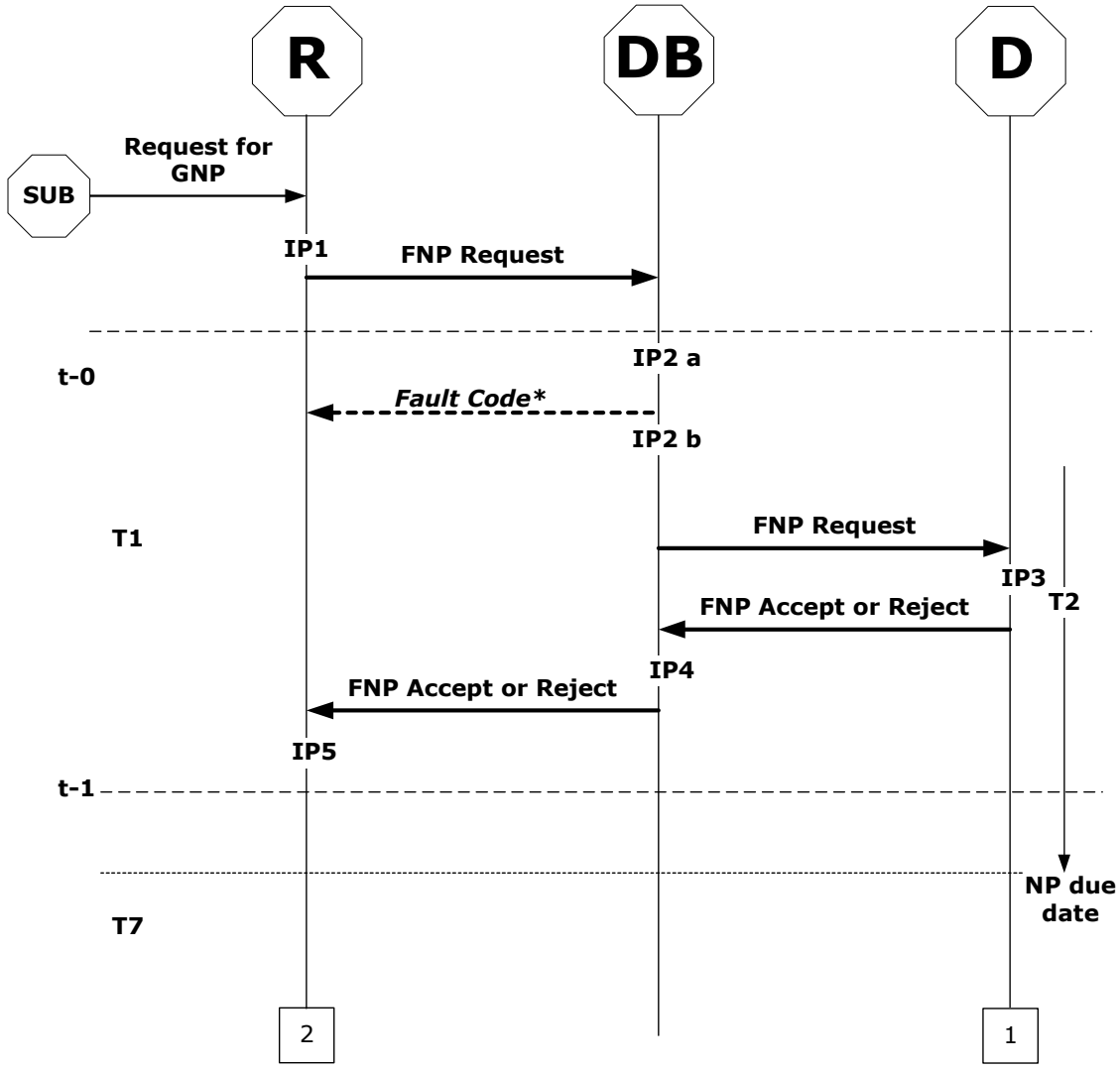
R =	Recipient	**O** =	other Participant	**DB** =	Common Reference Database Centre
D =	Donor	**sub** =	Subscriber	**OD** =	Original Donor

5.1 Initiation phase

5.1.1 Recipient requests FNP

Initial remark: All requests for non-geographic FNP (including Free Phone (FPH), Split Charges (SPL), Universal Access Numbers (UAN), Personal Number Services (PNS), Premium Rate (PRM), kiosk, …) have an indication whether the intended traffic profile will be “ATYPICAL” or “NON-ATYPICAL” .

The process names of the following description refer to the initiation phase and are named as “**IPx**”.



*: An 'FNPR fault code' response is sent on initiative of the CRDB or FNP Reject by the Donor when abnormal conditions are met as described in section about IP3. For details, see process description IP3 below.

T1 = (t-1 minus t-0) is the delay allowed for the Donor to respond to the request. For the definition and value of T1 refer to section 6, please.

T2 = (FNP Due Date minus t-0) is the minimum time that the Recipient is required to respect. For the definition and value of T2 please refer to section 6.4.

5.1.1.1 IP1

- A Subscriber (also for NGNP, service Subscriber or end user) requests FNP service from the Recipient, i.e. with the retention of his/her current [telephone] number (DN)
- The Recipient therefore obtains all information required to document this new FNP case and to co-ordinate FNP with the other parties. The Recipient sends an 'FNPR' message [6.3.1.1] to the CRDB
- if necessary for NGNP, additional information is provided in the FNPR message; for cases where the porting of 'Atypical calls' numbers is considered an explicit indication must be given of the future nature of the traffic pattern at this moment of request

Remarks:

- The timers T1 and T2 limit the shortest allowed due-date. There is a control by the CRDB on the latest allowed due-date. However since only one porting request can be active for a particular number, a very long due-date would prohibit any other porting of this number. The maximum due-date will be defined in the service description but cannot exceed one year.

- If either the Recipient or the customer feels that a field engineer of the Donor needs to be on-site during the technical phase of the port, the Recipient needs to request this at this stage of the process. This request is not handled by the CRDB and the practical arrangements are defined in bilateral service description.

5.1.1.2 IP2 (a and b)

- The CRDB verifies the request for FNP and forwards the 'FNPR' to the Donor
- a log is maintained of the request by the CRDB
- the CRDB can reject the request with a 'fault code' [6.3.1.3] if:
  - the Recipient sends an incomplete or incorrect request
  - a previous porting request for the same number is not finished, yet, and must be completed first

Remark:

- When the Recipient has submitted a FNPR, no other messages should be submitted on that number before the Donor has sent the FNP-Accept or FNP-Reject with the exemption of a FNP Cancel.

5.1.1.3 IP3

- The Donor verifies the 'FNPR' message and as outcome of this step the request is accepted or rejected via the transmission of a corresponding message. With one of these messages the Donor confirms the receipt of this request within the time frame T1:
  - The Donor checks if the request contains valid FNP information and answers with an 'FNPR Accept' [6.3.1.4] when the FNP can continue. At this point in the process, the Donor can modify the complexity class of the FNPR in case this is not correct. The Donor still needs to respond with a 'FNPR Accept' within the T1 time frame of the original request.
  - The Donor may answer with an 'FNPR Reject' when an abnormal condition is met [6.3.1.5]. The reasons for rejects are included in appendix E. In case of a "FNPR Reject" , the Donor will correct the complexity class if possible. This will allow the Recipient to correct as much as possible prior to resubmitting the FNPR.
  - The Donor initiates the process for FNP when it sent an 'FNPR Accept' message (see "FNP Activation")

- The Donor must be aware that the porting of the DN is, possibly, a porting back to the original Donor.

Remarks

- If the FNP-Exec has not yet been sent: the Donor can send an FNP-Hold message before the FNP Due date to postpone the porting process.

- When a grouped port request is rejected, the number that contains the problem is rejected using the appropriate code (see annex E). The other accepted numbers or range(s) that are part of the group are labelled with a specific code in the Reject field "1000" (see annex E).

5.1.1.4 IP4

- on receipt of an 'FNPR Accept' the CRDB will forward the message to the Recipient
- or, the CRDB will forward the 'FNPR Reject'
- the CRDB completes and adapts the CRDB according to the received accept or reject

5.1.1.5 IP5

- the Recipient initiates the number porting on receipt of the 'FNPR Accept'
- This process finishes on receipt of the 'FNPR Reject', (After treatment of the problem as reported by 'FNPR Reject', the Recipient has the option to send a new, revised 'FNPR' message or to abandon the number porting request).
- With or without response of the Donor the CRDB will cancel the FNPR after the expiration of timer T7.

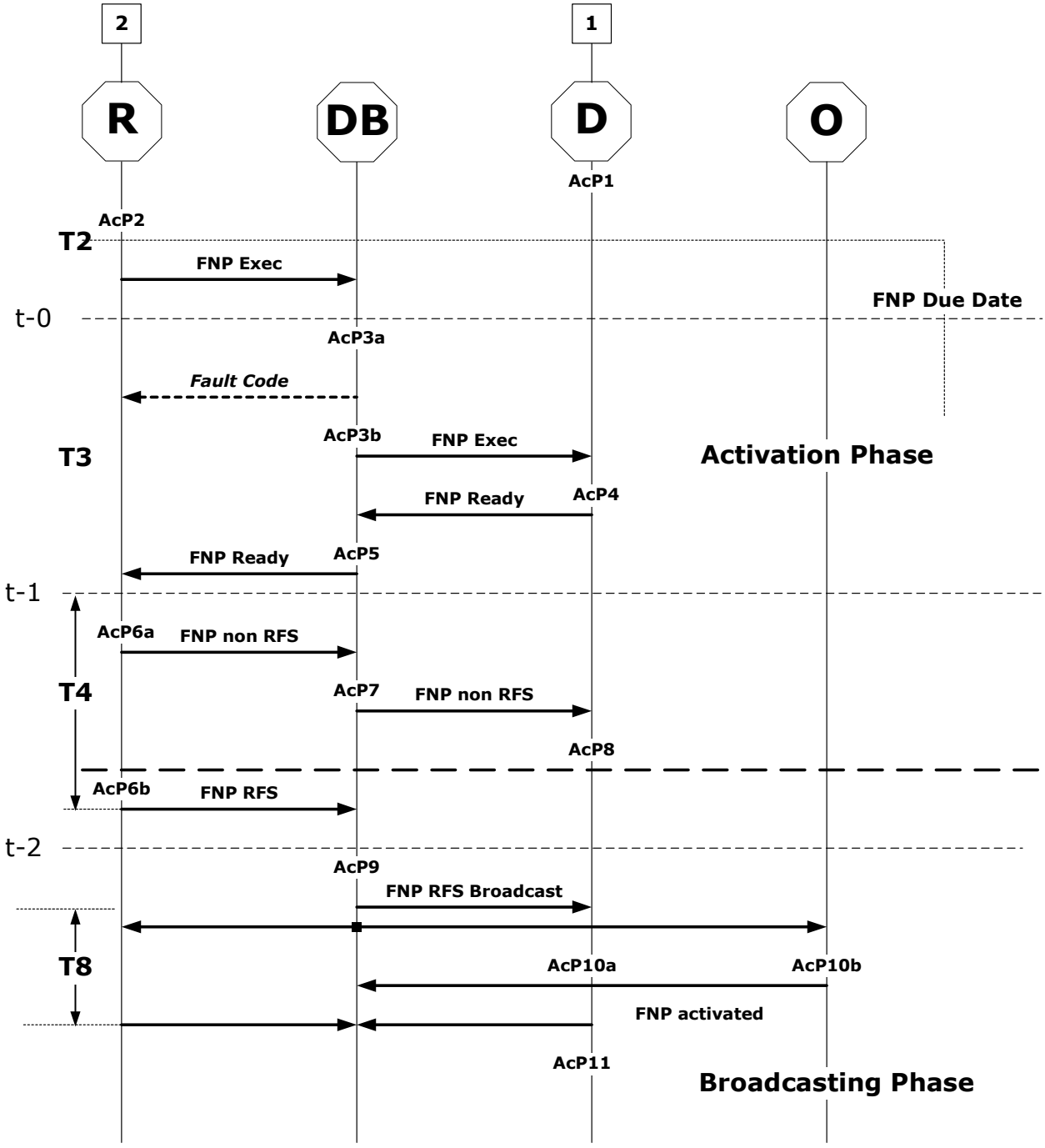
5.1.1.6 IP6

- The CRDB shall detect and log, independent of the FNPR status, all FNPRs impacted with a timer T7 expiration status. (Cancelled by CRDC log report available)
- The CRDB send a “Cancelled by CRDC” message to the Donor and Recipient after expiration of the timer T7.
- The involved NP case is cancelled and the CRDC system accepts a new NPR from any FNP Participant for the previously involved directory number , range or grouped request.
- The “Cancelled by CRDC” message generate and count an additional transaction record for the involved Participant “Recipient” in the FNP Volume Statistic Report.

5.2 Technical phase

5.2.1 FNP Activation

The process names of the following description refer to the FNP activation and are named as **AcPx**".



t-0 refers to the instance that the Recipient concludes to activate the FNP.

t-1 refers to the instance that actual implementation is configured by the Donor.

t-2 is the moment when FNP is actually available as service, and supported by the Donor and Recipient

T3 = (t-1 minus t-0) is the time given to the CRDB and the Donor to verify and execute the FNP. The definition of T3 and the corresponding value is specified in section 6.

T4 = (t-2 minus t-1) is the allowed elapse time given to the Recipient to verify end-to-end support of FNP. The definition of T4 and the corresponding value is specified in section 6.

- The porting of non-geographical numbers (NGN), classified as a "complex" installation (see in section 6 'Time frame and Timers', is subject to the following additional constraints:

  'FNP Exec' messages are exchanged between 13:00 (or before when non-geo OBH) and 14:00 hours local Belgian time on business days.

  (Messages arriving later than 14:00 are treated the following business day).

  - A timer T3 is respected for implementation that means that under normal circumstance porting is completed by 15:00 hours for all requests. A period T4 is available for non-RFS status.
  - The messages 'FNP Exec', 'FNP RFS' and 'FNP RFS Broadcast' contain identical additional information when it relates to "Atypical" traffic. The Coded ID 005 is used to mention a non- geographical number that could generate Atypical traffic.

5.2.1.1 AcP1

- The Donor prepares the provisioning of FNP in response to the agreed FNP Due Date in the FNP request and/or a request for change(s).
- Remark: The operational processes in this document don't describe the internal actions required by the various parties for a jointly support of FNP. It is therefore expected that the Donor prepares all necessary activities to implement the requested FNP and is ready for action by the FNP Due Date (and t-0 of the diagram). This includes any contributions of third parties that the Donor may depend on, e.g. for bilateral agreed transit services.

5.2.1.2 AcP2

- The Recipient prepares the provisioning of FNP in response to the agreed FNP Due Date in the FNP request and/or a request for change(s)
- The Recipient activates the FNP service - in principle, outgoing Subscriber traffic is supported by the Recipient at this stage – and sends an 'FNP Exec' to CRDB to ask the Donor for activation of this number porting. The information in this message is the consolidation of all previously exchanged data. This message is sent after the FNP Due Date has expired, this to ensure that the Donor is ready for the technical phase"

5.2.1.3 AcP3 (a and b)

- The CRDB checks if the execution request can be continued, i.e. whether the FNP Due Date and T7 have been respected - please, see section 6 for definitions and values of timers and time frames.
  - if YES, i.e. the execution can continue,
    - the CRDB takes notice that the FNP is activated by the Recipient and
    - forwards the 'FNP Exec' to the Donor
  - if NOT
    - The CRDB will send a 'fault code' to the Recipient when the FNP Exec is sent before the actual agreed FNP Due Date.
    - When the FNP Due Date + Timer T7 is expired, the CRDB will automatically set the FNP case in a "Cancelled by CRDC" status. [1]

5.2.1.4 AcP4

- After receipt of an 'FNP Exec' the Donor starts taking the necessary measures to activate the requested FNP within the expected time frame T3.

[1] In a future release it should be more user friendly for Donor and Recipient that a message "Cancelled by the CRDB" is send

- Remark 1: as mentioned in AcP1, it is the Donor's responsibility to take the necessary ["internal"] actions to support the 'Donor-to-Recipient' hand-over of responsibilities. This includes the actions of third parties subject to a bilateral agreement with the Donor. The resulting set-ups must give the Recipient the capability to continue with number porting at t-1 when the Donor confirms completion of the work

  Remark 2: if this should be the case, the Donor must be aware that the porting is back to the original Donor and is therefore allowed to undo the number porting
- The Donor sends an 'FNP Ready' to the CRDB when the activation is finished and tested
- If a service Subscriber is porting his/her non-Geo number from Donor A to Recipient B and if due to a (bilateral) interconnect agreement between A and C service users of C have access to the non-Geo number, Donor A must co-ordinate with C as specified in their bilateral agreement.

5.2.1.5 AcP5

- The CRDB takes notice of the Donor's response that activated the number porting and forwards the 'FNP Ready' message to the Recipient.

5.2.1.6 AcP6 (a , and b)

- The Recipient is now able to verify, end-to-end, that the FNP service implementation of Recipient and Donor is correctly completed.
- The Recipient makes sure that the delay between service activation and the confirmation message is kept to a minimum and less than T4.
- An 'FNP RFS' message (RFS: Ready for Service) is sent when the service is actually operational.(AcP6b)
- In case of problems, there is the possibility that T4 cannot be respected.
  - In this case, Recipient and Donor shall do their best effort to resolve the problem(*), and
  - an 'FNP non RFS' message is sent to the CRDB and Donor

*: Within this action AcP6 and together with activities in AcP8 a provisioning repair process is activated to resolve the problem and produce ASAP the requested and expected results

5.2.1.7 AcP7

- The CRDB takes notice that the number cannot be ported as planned, and
- forwards the message to the Donor

5.2.1.8 AcP8

- On receipt of the 'FNP non-RFS' message, the Donor takes the necessary measures to solve the problem in co-operation with the Recipient.
- After the expiration of the timer T4 (started after the FNP Ready originated by the Donor) the CRDC generate a notification , escalation request, to the CRDC Helpdesk (logged with a Trouble Ticket) for the co-ordination and Follow-Up of the problem resolution between the two involved Participants or Hosting Party.
- Such Interventions will be reported on a monthly basis to the NPA SM.
- The initiative to send a NPRFS is returned back to the Recipient when the problem is solved.

5.2.1.9 AcP9

- From here the **FNP Broadcast phase** is initiated.
- The receipt of an 'FNP RFS' message is for the CRDB an indication that the FNP service can be registered as operational for Donor , Recipient and Participants
- the CRDB sends the 'FNP RFS Broadcast' message to all the parties .
  - to request the Donor for confirmation of service availability after it implemented specific configuration(s) for this purpose (via the above steps), and

- to instruct the other Participants to update their routing information (after which they confirm their support of the new situation)
- However in case that the Recipient is identical as the original Donor, all Participants will undo the number porting to return the situation back as before the first successful porting request. This can be recognised by receipt of a “CNANO” as routing information from the CRDB.

5.2.1.10 AcP10 (a and b)

- The original Donor, if different than the Donor, and the other Participants adapt to the new routing following the information as received in the ‘FNP RFS Broadcast’ message.
- All Participants, after having adapted to the new routing condition, send an ‘FNP Activated’ message as a response to the receipt of the broadcast.

Note: The FNP broadcasted content is the information that needs to be available for real time online queries.

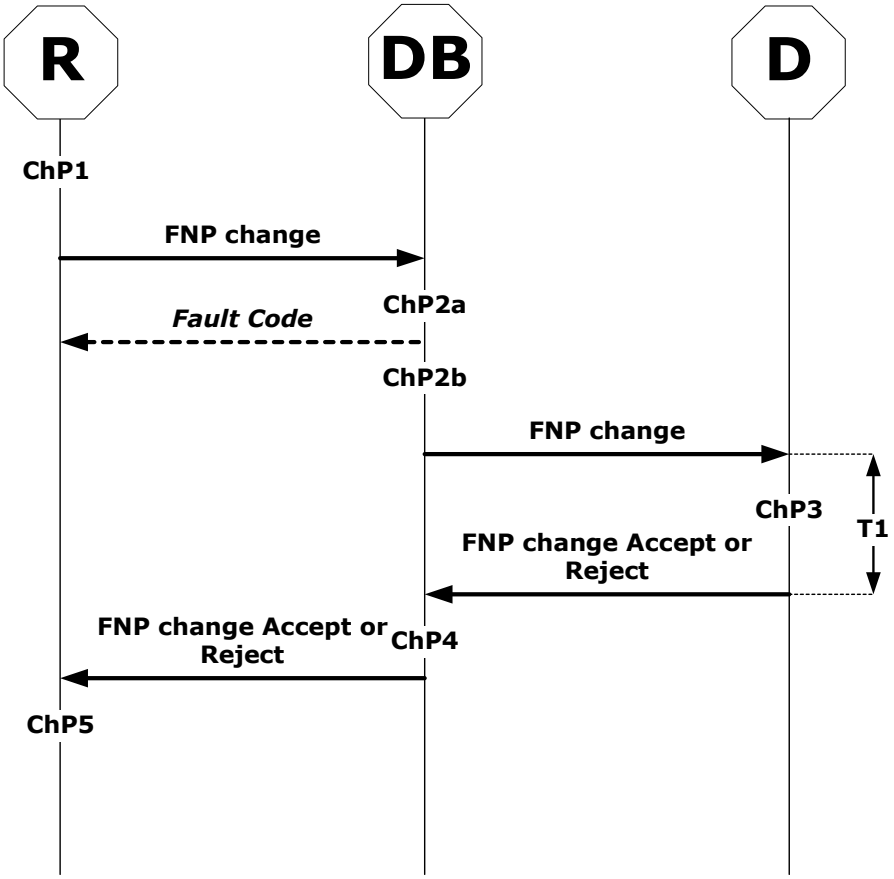
5.2.1.11 AcP11

- The CRDB takes notice of the ‘FNP Activated’ messages in a similar way as the ‘FNP Exec’ for the Recipient and the ‘FNP Ready’ from the Donor.
- The CRDB assumes that the Participant activated the FNP if it didn’t receive a message before T8 expired (the CRDB keeps track of this assumption).

5.2.2 Change Number Porting

A ‘Change’ can be given after the ‘FNPR Accept’ and before the ‘FNP Exec’ is sent from the CRDB to the Donor. Only the Recipient can send a change message and this triggers the T7 timer.

The process names of the following description refer to the requested changes in FNP Due Date and/or Routing number and/or Coded ID are named as “**ChPx**”.



5.2.2.1 ChP1

When the Recipient detects anomalies in the information which it provided in the original FNP request, it can send an ‘FNP Change’ [6.3.2.8] to the CRDB who informs the Donor.

A new due date can not be earlier than T1 plus T2 relative to the FNP Change message time stamp.

In case the Recipient and the Donor have agreed upon the presence of a field technician from the Donor, a change in due date will require a new appointment. This is handled outside the CRDB communication flow as agreed through service plans.

5.2.2.2 ChP2 (a and b)

- The CRDB takes notice and forwards the change request to the Donor.
- As a result of the FNP Change request the necessary changes will temporarily be updated.
- The CRDB will not accept the request and return a ‘fault code’ when the execution is started or if information in the request is incorrect.

5.2.2.3 ChP3

- The Donor verifies the ‘Change’ message and as outcome of this step the request is accepted or rejected via the transmission of a corresponding message. With one of these messages the Donor confirms the receipt of this request within the time frame T1 [6.3.2.9]
- See IP3 from initiation phase.

5.2.2.4 ChP4

- The CRDB inserts the necessary changes in the database when the request is accepted and forwards the ‘FNP Change Accept’ [6.3.2.10] to the Recipient. The FNP Change FNP Due Date is the trigger for the timer T7 calculation.
- If it received a reject the CRDB will forward the reject message, the initial FNP Due Date will be kept for T7 calculation.

5.2.2.5 ChP5

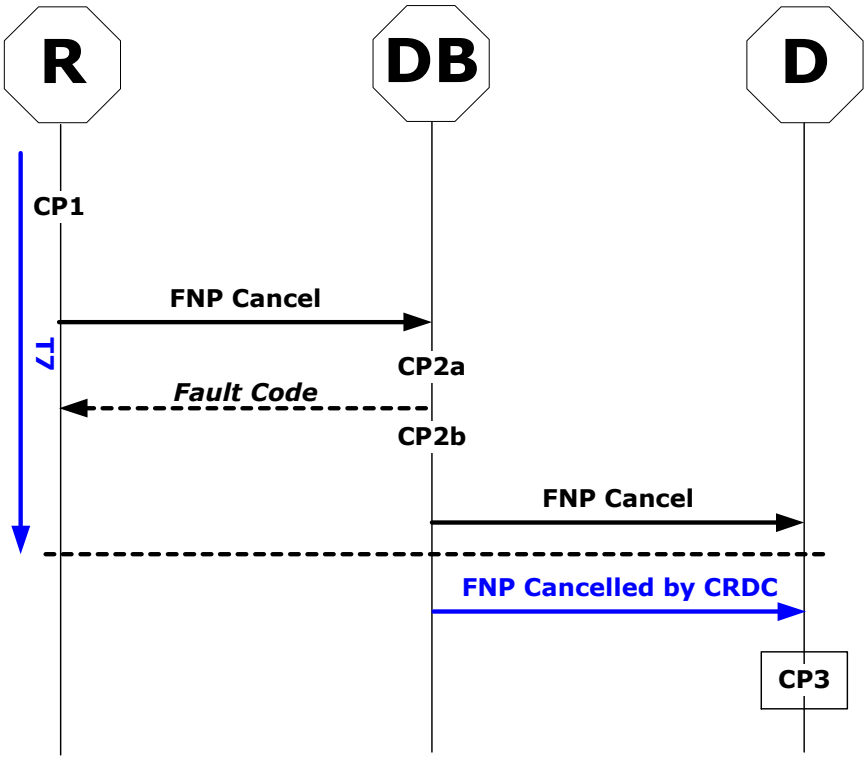
- If the Recipient received a reject message a new and/or revised ‘FNP Change’ will be required or a cancellation request could be sent.

5.2.3 Cancel Number Porting

A “FNP Cancel” can be sent at any moment in the porting process as soon as the CRDB has acknowledged the FNP Request and before the “FNP Exec” is sent from the CRDB to the Donor. FNP cancels are given for a complete FNPR (fragments of an FNPR can not be cancelled by itself). Only the Recipient can send a cancel message.

A previous request is cancelled.

The process names of the following description refer to the cancellation and are named as “**CPx**”.



5.2.3.1 CP1

The Recipient may request to cancel the GNP with an ‘FNP Cancel’ message [6.3.2.11].

5.2.3.2 CP2 (a and b)

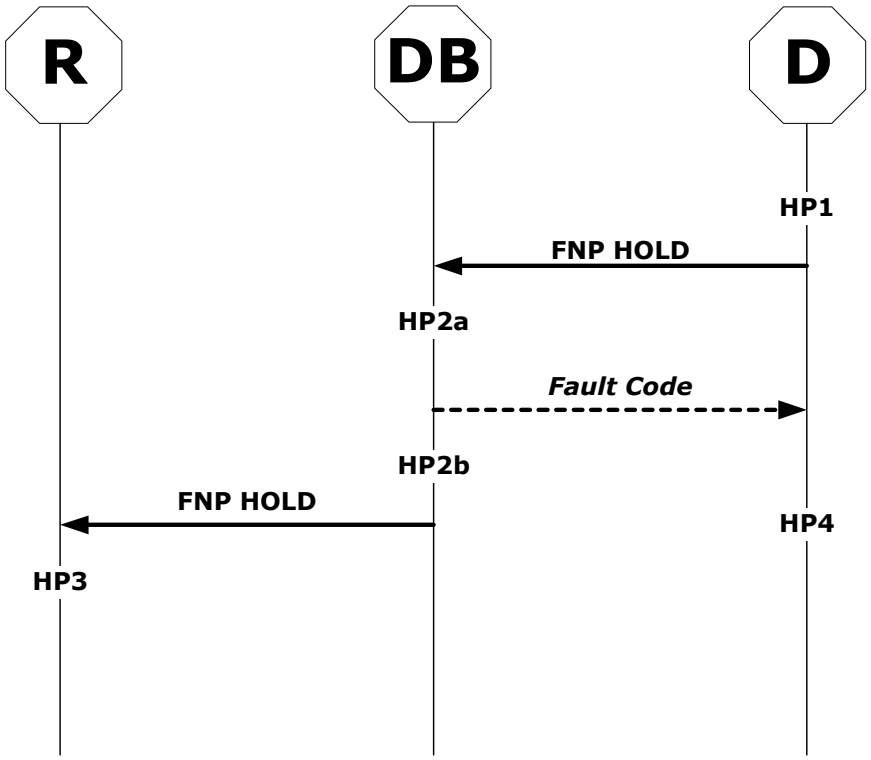
- The CRDB will respond with an “Acknowledgement” when the request is valid or shall reject the request and return an ‘fault code’ [6.3.2.12 – 6.3.1.3],
- Else, the CRDB will forward the cancel request to the Donor or generate a Cancelled by CRDC message after expiration of the timer T7.

5.2.3.3 CP3

- The Donor processes the cancellation: Hold Number Porting

A ‘hold’ can be given, after the ‘FNPR Accept’ and before the ‘FNP Due Date’, to the Recipient. Only the Donor can send a hold message. A previous request is put on hold and the implementation phase is interrupted.

The process names of the following description refer to the FNP activation and are named as “**HPx**”.



5.2.3.4 HP1

- A request to hold the GNP process can be given by the Donor, after it returned an 'FNPR Accept' or a FNP Change Accept in the Initiation phase. A 'FNP Hold' message [6.3.2.13] is sent for technical reasons only.
- The hold request includes a proposal for a new FNP Due Date but the current FNP Due Date stays/remains the only reference.

5.2.3.5 HP2 (a and b)

- hold messages are sent unsolicited after the 'FNPR Accept' and before 'FNP Exec' or other timing constraints which are applicable to this FNP process
- A 'fault code' [6.3.1.3] is replied by the CRDB if the FNP Due Date is passed

5.2.3.6 HP3

- The Recipient put the GNP process on hold when it received the request.
- New arrangements are made with the Subscriber to agree on a new activation date/time.
- If the CRDC rejects , with a fault code, the FNP Hold, the initial FNP Due Date will be kept for T7 calculation.

5.2.3.7 HP4

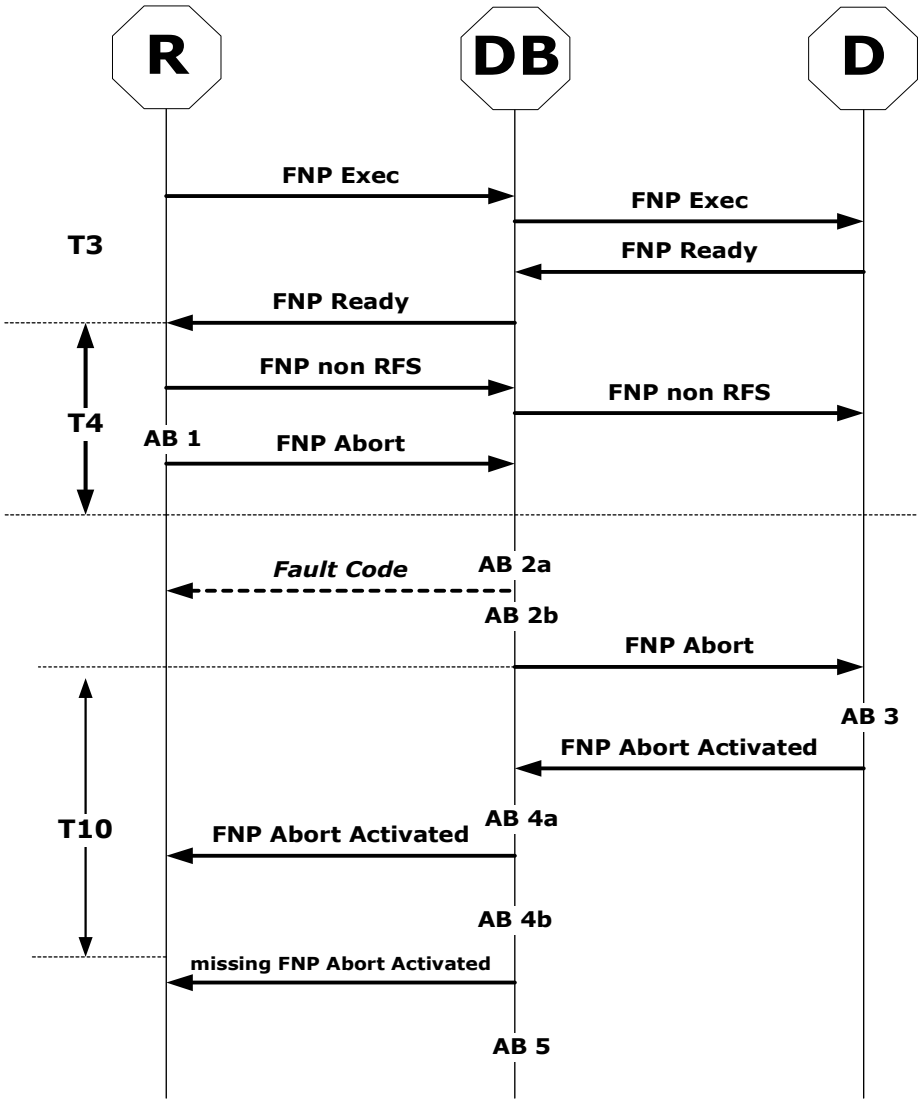
- The Donor now waits for a FNP change request or a FNP cancel from the Recipient.

5.2.4 FNP Abort

5.2.4.1 Abort porting process "FNP Abort"

A "FNP Abort" can only be send after a "FNP Exec" and before the "FNP RFS" message. Sending "FNP Abort" results in a deletion of all activation steps for the same FNPR and the activation phase is definitively interrupted and cleared in the CRDB. [FNPR must be cleared as well]

The process names of the following description refer to the FNP Abort and are named as "**ABx**"



5.2.4.2 AB 1

- The Recipient must send a "FNP Abort" message after T3 starts and before T4 expires.
- It is the task of the Recipient to inform, if any, the Transit operator that the porting will be aborted.
- The CRDB will reject, with the fault code 225, the "FNP Abort "if sent before a FNP Exec.

5.2.4.3 AB 2a

- When initiated the CRDB logs the "FNP Abort" message with the time and date.
- The CRDB replies the "FNP Abort" message [6.3.4.1] to the Donor

5.2.4.4 AB 2b

- The CRDB replies with a “fault code” [6.3.1.3] when the condition is not met
- Condition to reject the “FNP Abort” , when initiated before the FNP Exec or after the FNP RFS

5.2.4.5 AB 3

- The Donor sends a “FNP Abort Activated” message before the timer T10 expired. The “FNP Abort Activated” message [6.3.4.2] indicates when issued that a new FNPR can be generated.

5.2.4.6 AB 4a

- The CRDB replied the “FNP Abort Activated” message to the Recipient.

5.2.4.7 AB 4b

- When the timer T10 expires the CRDB assumes that the Donor has activated the FNP Abort message and sends the “FNP abort Activated by CRDC” message.

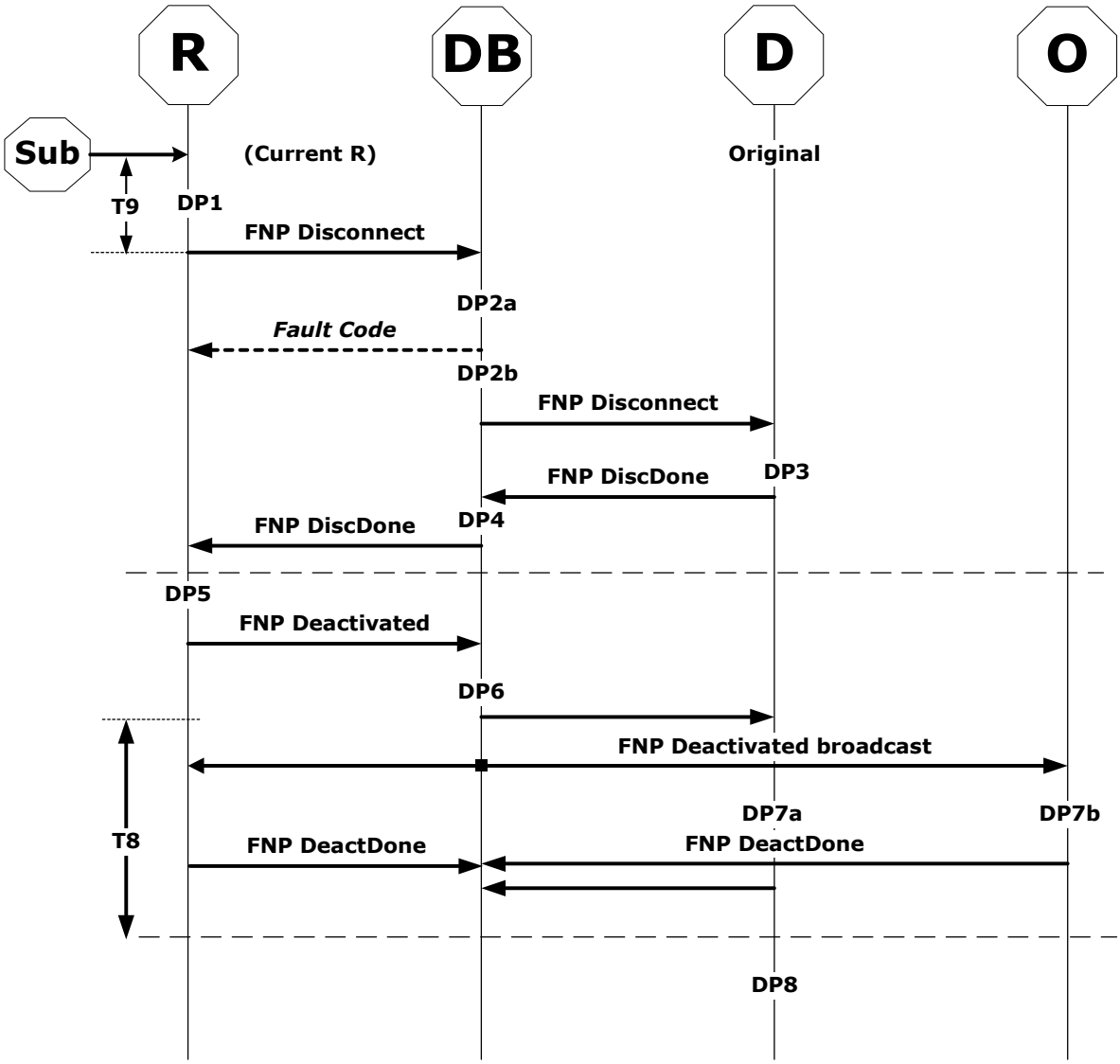
5.2.4.8 AB 5

- The CRDB will purge all validation and activation messages related to the involved FNPR ID.
- The CRDB will accept any new FNPR for this telephone number, range or grouped ID after the expiration of timer T10.
- The CRDB “Mgt report” shall report the “FNP Aborts” per Participant & Complexity code for a given period.

5.3 Operational phase

5.3.1 Disconnection

The process names of the following description refer to the disconnection and are named as "**DPx**".



5.3.1.1 DP1

- Deactivate the FNP takes place on request of the Subscriber or when the Subscriber's telephony service is terminated on that DN on Recipient's network.
- The [last] Recipient disables the DN and activates an announcement with the message that the number is no longer in use.
- The Recipient starts a, CRDB independent, timer T9.
- Any announcement on Recipient's network for this DN is removed after T9 expired.
- A "FNP Disconnect" [6.3.3.2] is sent to the CRDB for further co-ordination.

5.3.1.2 DP2 (a and b)

- The CRDB forwards the 'FNP Disconnect' message to the original Donor.
- A 'fault code' [6.3.1.3] is sent for an inappropriate request.

5.3.1.3 DP3

- The original Donor returns the number back to its number pool and the number will eventually be re-used in its own network.
- The original Donor deactivates the routing set-up for the deactivated FNP.
- The Donor returns an 'FNP DiscDone' message [6.3.3.3] when the task is finished.

5.3.1.4 DP4

- The CRDB registers the confirmation of the original Donor, and
- forwards the message to the Recipient

5.3.1.5 DP5

- The current Recipient can now take the necessary measures to deactivate the DN completely, and
- Then sends the "FNP Deactivated" message [6.3.3.4] to the CRDB for distribution to the other Participants.

5.3.1.6 DP6

- The CRDB informs all Participants by sending a 'FNP Deactivate Broadcast' message [6.3.3.5].

5.3.1.7 DP7 (a and b)

- On receipt of the message a Participant deactivates the routing - please, be aware that the original Donor already deactivated FNP routing in DP3 -which was set-up for this DN.
- The Participant sends an 'FNP DeactDone' message [6.3.3.6] to the CRDB as confirmation that the routing is disabled.

5.3.1.8 DP8

- The CRDB keeps track of all responses on the broadcast message.
- The CRDB assumes that the Participant deactivated the FNP and updated its legacy database; if it didn't receive a message before T8 expired (the CRDB keeps track of this assumption).

5.4 Operational phase - Customer Care

Due to the general requirement to respond to questions of the public the ”Subscriber” has a broader meaning in this context of customer care.

5.4.1 Responsibilities and Process

- The **operator where a Subscriber has a contract** is responsible to solve the problem for his customer (front-end process). If a Subscriber calls in to another operator (where he has no contract), this operator can inform the Subscriber of the correct operator by consulting or directing the Subscriber to e.g. “www.1450.be”.
- The **Recipient** is responsible to solve a problem with a ported number (back-end process) that he owns. In this process, it is the Recipient who takes the lead.
- The **Originating Donor** is responsible to inform a Participant of the current Recipient of a ported number (who will handle the problem) in case of a reported problem with this number. This basic principle does not exclude bilateral commercial agreements between agreed third parties seen as a non Participants and Participants to handle porting problems
- All **Participants**, including the Donor, are responsible to work together with the Recipient to solve a problem.
- The **CRDB** will **not** act as a central logging database for repair and fault handling issues after a successful port (end of provisioning process). The Participant’s NOC (Network Operation Centre) channel and processes will be used to address repair and fault handling issues. Only Participants (direct contact with a Subscriber will be rejected) may have contact with Participant’s NOC. The NOC is by default a different entity and handles no provisioning issues. It is the FNP customer service centre were provisioning problem have to be reported E.g. for FNP Non RFS issues and follow up.

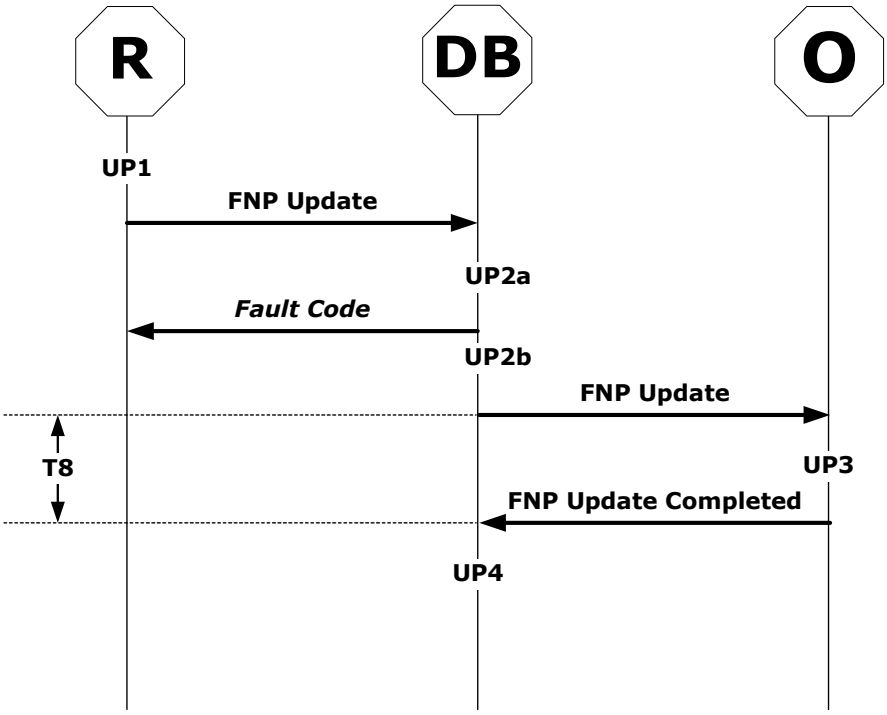
5.4.2 Service level Agreement

A basic FNP SLA does not exclude bilateral (more restringing) SLA’s between operators. The basic FNP SLA document is part of the FNP documents agreed between the involved parties.

5.5 Maintenance phase

5.5.1 FNP Update

The process names of the following description refer to the update process of routing information or for the Coded Id field status condition and are named as "**UPx**".



5.5.1.1 UP1

- The Recipient changes the routing information or the coded ID to support the new situation with guaranteeing the continuity of service, and
- Sends an 'FNP Update' message [6.3.5.1] with the routing or new coded ID status to inform about the new situation.

5.5.1.2 UP2 (a and b)

- The CRDB informs all other Participants about this change with a "FNP Update" message.
- However, the CRDB is allowed to return a fault code if the update request should contain in-appropriate information.

5.5.1.3 UP3

- After implementation the concerned Participants inform the CRDB about the updates process with a "FNP Update Completed" message [6.3.5.2]

5.5.1.4 UP4

- The CRDB registers the responses of all Participants.
- The CRDB assumes that the Participant adapted the routing information or Coded ID; if it didn't receive a message before T8 expired (the CRDB keeps track of this assumption).

5.5.2 Installation of a new CRDB release

Please, refer to 4.2.4 and 4.2.7 for details about the installation of a new release of the CRDB system.

5.6 Synchronisation phase

5.6.1 Audit process

5.6.1.1 Number Location Report (GUI only)

An operator asks the CRDB for audits of a specific DN.

This action results in a real time, online available information, based on the latest "FNP RFS Broadcast" for this case and recorded as such in the CRDB. This historical information is stored in the CRDB.

5.6.1.1.1 Current

- A Participant requests an update (query) from the CRDB on information concerning a DN with the Number location report [6.3.6.1]
    - Mostly all message fields send in the FNP RFS broadcast; IdNumber, Directory Number, Recipient Id, Activation Time, New Route and Coded Id Field content for this DN should be showed.

5.6.1.1.2 History

- Subsequent porting history is kept during 1 year in the report.

5.6.2 Synchronisation reports

Besides the Audit process there are synchronisation processes foreseen between the databases. These functions are available for when the Participant requires recovering from loss of information, to get information about a defined Recipient or when a new Participant needs to get the information to synchronise with the current status of FNP.

Synchronisation needs 2 different processes:

- Bulk synchronisation: this process delivers to a Participant (new Participant or disaster recovery) a copy of the CDRB for all the activated numbers (Report)
- Open porting synchronisation: in the previous case, a Participant must be able to receive back all messages about not yet activated porting for which he is the Recipient or Donor ; the smallest amount of data authorises unlimited back period. (Soap Replay)

5.6.2.1 Bulk synchronisation report

Based on current number location report, the requested day = previous business day.

5.6.2.2 SOAP Replay

As part of a re-synchronisation method, especially when a Participant has undergone a malfunctioning of its own system, the period suspected to have missing elements can be re-emitted played back by the CRDB by use of a specific GUI request emitted by the party requesting a synchronisation. The SOAP replay is seen as a report but the outcome is a reply of all the messages requested by the Participant for a specific period.

5.6.3 Participant System Down and System UP status , plus link status

A change in operational availability by a FNP Participant, from System UP to System Down and vice versa, is an information generated by a Participant through his GUI interface or ultimately and on request of the involved Participant or NPA SM, by the CRDC Helpdesk.

A System Down status issued by a Participant will generate a notification towards the CRDC helpdesk as well as in a real-time monitoring dashboard available to all CRDC Participants (Fix and Molo), status hat can be consulted through the GUI. The System status dashboard will reflect the individual Participant System status based on the "Mnemonic" ID of the Participant, flagging if the system is up or down as well as the date and time of the latest status change or and the condition of the access link.

E.g.

Molo1 System UP since 08:00 dd/mm/yy link OK

Molo 2 System Down since 13:00 dd/mm/yy link OK

Molo x System UP since 09:00 dd/mm/yy link NOK

Folo 1 System UP since 08:00 dd/mm/yy link OK

Folo 2 System Down since hh:mm dd/mm/yy link OK

Folo x System UP since hh:mm dd/mm/yy link NOK

CRDC System UP and operational since 06:00 dd/mm/yy all links OK (request daily update during CRDC Service Windows) , System Down or System in Maintenance is also a status

When a System Down status or/and link NOK is observed for a specific Participant the CRDC shall generate a fault code when a FNP Recipient operator tries to send a FNP Execution message to the involved Participant and this untill the status is back in a "System UP" and link OK state. The CRDC helpdesk monitor the access link(s) towards the CRDC and can initiate, after consultation of the involved party or after the escalation process with agreement of the NPA SM a System Down status in the name of the involved Participant. The link (connection) status is supervised and updated by the CRDC Helpdesk. A daily log will be kept and reporting of incidents will be communicated to the NPA SM at least once in a month or during the SM meetings.

5.7 Escalation processes

In this section the exception handling is described in case the process flows reach a state not described in the previous sections. This is not an exhaustive list and in general the process is handled manually and on a case by case basis. For the following situations a more formal approach is necessary.

5.7.1 Process after a timer violation

This section describes how the processes continue in case of a violation of one of the timers. It is organised by timer Tx.

5.7.1.1 T1

Timer T1 is relevant for both an FNPR and FNP Change. The following needs to happen in case the timer is surpassed.

- The formal porting process continues.
- A violation is logged and flagged by the CRDB.
- The Recipient contacts the Donor to identify the problem and to expedite the processing of the FNPR (FNP Change)

5.7.1.2 T2

A violation of T2 can only occur when the Recipient tries to send the FNP-Exec too soon.

The Minimum FNP Due date = T1 + 0 business days (independent when it starts)

5.7.1.3 T3

The following needs to happen in case the timer is surpassed.

- The formal porting process continues.
- A violation is logged and flagged by the CRDB.
- The Recipient contacts the Donor to identify the problem and to expedite the processing of the FNP Exec.

5.7.1.4 T4

The phase that is controlled by timer T4 can either include a non-RFS or not. In all cases the formal process continues and the phase can only be concluded by an RFS message. If relevant for some cases the Transit operator need to have changed the routeing path as well. (See Annex B)

In the case a technical problem is prohibiting the RFS; the following process needs to occur.

1. Recipient and Subscriber agree on a possible approach. This can either be to continue the trouble-shooting or to ask the Donor for an intermediate solution.
2. If Transit operator(s) are involved; is the routeing path updated accordingly the new port. (non-automated process)
3. In case Recipient and Subscriber want an intermediate solution, the Recipient contacts the Donor if a roll-back (full or partial) is possible at the Donor side. This needs to be evaluated on a case by case basis and is not necessarily possible or the Recipient decides to send a FNP abort.
   In case Recipient and Subscriber want to continue the trouble-shooting, the Recipient contacts the Donor's technical centre.
4. The Recipient keeps the Subscriber informed about the progress of the port and the solutions that have been worked out.

5.7.1.5 T7

After Timer T7 expires, the process flow stops and the CRDB generate a "Cancelled by CRDC" status. If the port needs to happen anyway, a new FNPR needs to be issued by the Recipient.

5.7.1.6 T8

When T8 expires the broadcast is considered as activated by the Participant and no FNP Broadcast Activation message needs to be sent.

5.7.1.7 T10

When T10 expires the Donor's "FNP Abort Activated" message is considered as activated by the CRDB and a new FNPR message shall be accepted for this DN or range.

Remark: A rollback is expected at the Donor's side to activate and restore the situation as just before the FNP activation phase.

5.7.2 Process after a technical problem occurs

5.7.2.1 Porting process needs to be aborted during the activation phase

The Recipient can be put in a situation (for technical reasons related to Subscriber, Recipient or Donor) where the porting process needs to be aborted by use of a FNP abort.

In the case a technical problem is prohibiting the RFS; the following process needs to occur.

1. Recipient and Subscriber agree on a possible approach. This can either be to either continue the trouble-shooting or to ask the Donor for an intermediate solution.
2. Transit operator, if relevant, is contacted to change back the routeing path.
3. The Recipient keeps the Subscriber informed about the progress of the port and the solutions that have been worked out.

5.7.2.2 Problem analysis prior to a customer care (Repair or Fault handling) action request

When an operational problem is found, related to a ported number who was successfully ported, all operators who are confronted with the problem are requested to check the following items prior to passing on the problem to another operator.

This will ensure that no unnecessary escalation of the problem takes place.

Some checks need to be done before issuing a customer care action request for a ported number:

- As Recipient:
  - Verify if the number is still correctly "ported-in" on the right Recipient Exchange
  - Verify the routing of the RN+DN (eventually by using a test number having the same RN)
  - Verify if calls to this number are still coming with the right format on the Interconnection (RN+DN)
  - Verify the status in the CRDB
  - Check if a transit operator is involved (loss of routeing path)

- As Donor :
  - Verify the RN in the IN platform and compare it with the CRDB value
  - Verify the "ported-out" configuration in the Donor Exchange
  - Verify the routing of the RN+DN
  - Verify the triggering mechanism
  - Verify the status in the CRDB
  - If a transit operator is involved, check if the routeing path is still correct

- The FNP SLA will force the parties to follow the agreed process steps and when evidences are found that no checks prior a fault or repair handling request was executed, the requesting Recipient will be charged to compensate the work done by the Donor.

6 Messages and Time frames

6.1 Summary of messages (Indicative)

Detailed description with the CRDB priority of the messages that are exchanged during the FNP provisioning of the above scripts. The level high and low is used to differentiate FNP executions by the CRDB; High will mainly be used for broadcast messages generated for MNP events. When there is a mention of a “fault code” please refer to the comments in 6.3.1.3.

Paragraph	Message name	Message Phase	Priority level
6.3.1.1	FNPR	INITIATION	Medium
6.3.1.2	Acknowledgement		
6.3.1.3	Fault code		
6.3.1.4	FNPR Accept		Medium
6.3.1.5.	FNP Reject		Medium
6.3.2.1	FNP Exec	ACTIVATION	Highest
6.3.1.3	Fault code		
6.3.2.2	FNP Ready		High
6.3.2.3	FNP RFS (Ready for Service)		Medium
6.3.2.4	FNP nonRFS		Medium
6.3.2.5	MNP RFS Broadcast	BROADCAST	High
6.3.2.6	FNP RFS Broadcast		Medium
6.3.2.7	FNP Activated		Low
6.3.2.8	FNP Change	CHANGE	Low
6.3.1.3	Fault code		
6.3.2.9	FNP Change Reject		Low
6.3.2.10	FNP Change Accept		Low
6.3.2.11	FNP Cancel	CANCEL	Medium
6.3.1.3	Fault code		
6.3.2.13	Acknowledgement		
6.3.2.12	FNP Cancelled by CRDC	CANCEL	Medium
6.3.2.14	FNP Hold	HOLD	Low
6.3.1.3	Fault code		
6.3.3.1	MNP Disconnect	DISCONNECT	High
6.3.1.3	Fault code		
6.3.3.2	FNP Disconnect		Low
6.3.3.3	FNP Disc Done		Low
6.3.3.4	FNP Deactivated		Low
6.3.3.5	FNP Deact Broadcast		Low
6.3.3.6	FNP Deact Done		Low
6.3.4.1	FNP Abort	ABORT	High
6.3.1.3	Fault code		
6.3.4.3	FNP Abort Activated		Medium
6.3.4.4	FNP Abort activated Send by the CRDC		Medium
6.3.5.1	FNP Update	UPDATE /Maintenance	Low
6.3.5.2	FNP Update Completed		Low
6.3.1.3	Fault code		Low

6.2 General Message Description

6.2.1 Message fields (Indicative)

Element Name	Element Description	Element Type	Data Type	Element Example
accountnumber	Customer account number under which the service is built/known at the Donor operator.	string	{30}	
datetime	Date & Time when message is sent for MNP & FNP messages. Date & Time of 'original' broadcast message for FNP messages.	dateTime	ccyy-mm-ddThh:mm:ss	*2001-02-22T23:12:56*
elementcontent	Content of the element the fault string refers to.	string	{60}	*27*
elementname	Element the fault string refers to.	string	{30}	*accountnumber*
faultcode	Unique error number generated by the CRDC.	integer	{3}	*225*
faultstring	Detailed error message generated by the CRDC.	string	{60}	*Message not allowed*
rejectcode	Unique error number generated by the Donor operator.	integer	{4}	*2012*
rejectstring	Detailed error message generated by the Donor operator.	string	{60}	*DDI range incomplete*
numberfrom	First number in the number-range.	integer	Minimum {8} Maximum {15}	*015355488*
numberto	Last number in the number-range.	integer	Minimum {8} Maximum {15}	*015355499*
routinginfo	Routing identification (network number for Mobile and Non-Geo or Switch number for Geo) used within the network.	string	C char{4}	*C1966*
vat	Company legal taxation number (BTW/TVA)	string	{30}	*BE343787789*
version	The <version> and root element identifies the method handler to be called. Use of <version> element allows migration of the XML content newer version.	string	digit {2}. digit{2}	*01.00 (=Initial version)*
idnumber	Unique number generated by the CRDC identifying the Number Porting Request for FNP.	string	(P|U|D) datetime {14} sequence# {4}	*P2002012813330972 79*

donorid	Unique operator identification of the party Donor.	string	{4}	*TELE*
recipientid	Unique operator identification of the party Recipient.	string	{4}	*BGC*
npduedate	Duedate on which the porting can be started.	dateTime	ccyy-mm-ddThh:mm:ss	*2001-02-22T23:12:56*
numbercount	The total amount of DNs (Directory Number for Geo) or SNs (Service Number for Non-Geo) within the NP message.	integer		*100*
complexityclass	Code used to identify the installation type and can be modified by the Donor. Values are: 'Simple' or 'Complex'	string	{30}	*Simple*
codedid	Used to flag specific conditions impacting the NP process	integer	{3}	*255*
zipcode	Postcode based on Subscriber's current installation address	integer		*1831*
housenumber	Housenumber based on Subscriber's current installation address	integer		*19*
street	Street based on Subscriber's current installation address	string	{30}	*Bessenstraat*
Activation Time	Date/Time of the Latest Activation Broadcasted	date/Time		
Created Time	Date/Time of the creation	date/Time		

For parameter formats, please, check section 7 with details on the database contents.

Fields with Subscriber's private information is kept, to avoid problems with the Privacy law, during 7 business days in the database, after FNP reject by the Donor or FNP Cancel by Recipient (if not yet accepted by Donor) but must disappear immediately after the FNP Accept from the Donor.

6.2.2 Message structure

General Section		
Idnumber	Value is system generated and displayed when the message is accepted.	
DonorID	Retrieved from Participant table.	
RecipientID	Retrieved from Participant Name in Participant table using the requesting user information. System generated.	
NP Due Date	Format yyyy/mm/dd hh:mm:ss	
Complexity	Simple, Complex	
Routing Info	Format Cnnnn	
Number Count	Total of numbers involved in the porting. This value is calculated when the Calculate button is pressed. If the Calculate button has not been pressed, before pressing the Submit button, the value is system generated.	
Customer Type	RESIDENTIAL	BUSINESS
VAT nº	Optional	Optional
Account number	Optional	Optional
Street	Optional	Optional
House number	Mandatory	Mandatory
Zip code	Mandatory	Mandatory
Detail Section		
Number From	Start of number range	
Number To	End of number range	
Coded ID	Optional field, Contains Coded ID and Description from Coded Id entity.	

Function is supplier dependant

The messages have a two level hierarchy. This parent-child relationship is a one-to-many relationship whereby the "message" (or "group") is the parent and the "range" is the child. There is always at least one parent and child. A conceptual model is shown in the following diagram. Maximum range message "25" (Dynamic)

6.2.3 Specific for a FNPR during the initiation phase:

- The total of telephone numbers to be ported in the FNPR "From" – "To" field contains maximum 10.000 consecutive DNs for Geo numbers and 1.000 for Non-Geo numbers
- The CRDB should control and compare the total of phone numbers mentioned in the FNPR "Control total # of FNPR" and if needed will reject with the fault code 325 "Total to port number(s) don't match" the FNPR.
- The original timer T1 does not change when the Donor changes the complexity class, all the following timers are related to the new complexity class.

6.2.4 General message layout (Indicative)

The following diagram shows the most important fields and in which messages they are mandatory.

Message field / Message	ID Number	Date Time	Number from	Number To	Complexity Class	Donor id	Recipient id	NP due date	Routing Info	Version	Coded id (optional)	Numbercount	Account number	Zip code	Housenumber	Street (residential optional)	VAT (business)	Reject code	Reject string
FNP Request	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X			
FNP Accept	X	X	X	X	X	X	X	X		X	X	X							
FNP Reject	X	X	X	X	X	X	X	X		X	X	X					X	X	X
FNP Exec	X	X	X	X	X	X	X	X	X	X	X	X							
FNP Ready	X	X	X	X		X	X	X		X	X	X							
FNP Non RFS	X	X	X	X		X	X	X		X		X						X	X
FNP RFS	X	X	X	X		X	X	X		X	X	X							
FNP RFS Broadcast	X	X	X	X		X	X	X	X	X	X	X							
FNP Activated	X	X	X	X		X	X	X		X		X							
FNP Change	X	X	X	X	X	X	X	X	X	X	X	X							
FNP Change Reject	X	X	X	X		X	X	X	X	X	X	X						X	X
FNP Change Accept	X	X	X	X		X	X	X	X	X	X	X							
FNP Cancel / cancel by CRDC	X	X	X	X		X	X	X		X	X	X							
FNP Hold	X	X	X	X		X	X	X		X	X	X							
FNP Abort	X	X	X	X		X	X	X		X	X	X							
FNP Abort Activated	X	X	X	X		X	X	X		X	X	X							
FNP Disconnect	X	X	X	X		X	X			X	X	X							
FNP Disc Done	X	X	X	X		X	X			X	X	X							
FNP Deactivated	X	X	X	X		X[2]	X			X	X	X							
FNP Deact Broadcast	X	X	X	X		X	X	X		X	X	X							

[2] Element <donorid> will be filled with 'original' donor id=NANO

Message field / Message	ID Number	Date Time	Number from	Number To	Complexity Class	Donor id	Recipient id	NP due date	Routing Info	Version	Coded id (optional)	Numbercount	Account number	Zip code	Housenumber	Street (residential optional)	VAT (business)	Reject code	Reject string
FNP Deact Done	X	X	X	X		X	X			X	X	X							
FNP Update	X	X	X	X		X	X	X	X	X	X	X							
FNP Update completed	X	X	X	X		X	X			X	X	X							

6.2.5 Participant identities

The different Participants will be uniquely identified. The annex “PARTICIPANTS” gives an overview of the identified operators and users of the CRDC/CRDB. Please, refer to the definition of ‘Participant’ for a description of possible users.

6.2.6 Sequencing of messages

The next matrix displays the valid sequence of the messages depending on its status. This matrix is illustrating what message(s) are allowed to be sent and by whom, for instance when a FNP Exec is sent, this message is only allowed when the case status contains an FNP Accept status or a FNP Change Accept status and can only be sent by the Recipient. The matrix underneath is subject to changes dependant on the process flow or/and business rules forwarded to the supplier of the CRDB.

The listed abbreviations are used to explain the usage:

- D: Only the Donor can send this message
- R: Only the Recipient can send this message
- P: Each Participant is allowed to send this message
- S: Serving Participant, could be the Recipient or the NANO
- C: Broadcast message forwarded from the CRDC to all Participants
- N: Only the original Donor (NANO) can send this message

Remarks:

- Combinations of abbreviations, separated by a slash “/”, e.g. “S/C”, means that the Serving Participant can send this message and the message is Broadcasted from the CRDC.
- Status “Not Ported”, not showed in the matrix, means that the number handled is recorded, updated or deactivated in the Number Location database in combination with its specific and relevant Coded ID, this Coded ID indicate a specific usage or domain for this number. The FOLO handling the number in combination with the used Coded ID attribute is responsible for the correctness of it. The method to exchange such information with the CRDB is handled with the “FNP Update” of the Maintenance phase (5.5). For more detail refer to annex G

Message / Status	FNP Request	FNP Accept	FNP Reject	FNP Exec	FNP Ready	FNP Non RFS	FNP RFS	FNP RFS Broadcast	FNP Activated	FNP Change	FNP Change Reject	FNP Change Accept	FNP Cancel/ CRDC	FNP Hold	FNP Abort	FNP Abort Activated/dent by CRDC	FNP Disconnect	FNP Disc Done	FNP Deactivated	FNP Deact Broadcast	FNP Deact Done	FNP Update	FNP Update Completed
Initiated		D	D [3]										R [3]										
Reject	R	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	R [4]					S/C [6]	
Accept				R						R			R [3]	D [5]									
Exec					D										R								
Ready						R	R								R								
Non RFS							R								R								
RFS								C															
Broadcast									P														
Activated	R	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	R [4]					S/C [6]	
Change											D	D	R [3]										
Change Reject										R			R [3]										
Change Accept				R						R			R [3]	D [5]									
Cancelled by Recipient / CRDC	R/C	C	-	-	-	-	-	-	-	-	-	-	-	-	-	-	R [4]					S/C [6]	
Hold										R			R [3]										
Abort	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	D [3]							
Abort Activated by Donor / CRDC	R	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	R [4]					S/C [6]	
Disconnect Initiated																		N					
Disc Done																			R				
Deactivated																							
Deact Done by Participant	R																			C		N/C [6]	
Deact Done by CRDC	R																					N/C [6]	

[3] Terminates the process and closes the FNP Case

[4] Only when the specified numbers not belongs to the NANO and are not local ported (FNP Update from the NANO)

[5] Must be send before due date, generates faultcode: 225, “Message not allowed”

Message / Status	FNP Request	FNP Accept	FNP Reject	FNP Exec	FNP Ready	FNP Non RFS	FNP RFS	FNP RFS Broadcast	FNP Activated	FNP Change	FNP Change Reject	FNP Change Accept	FNP Cancel/ CRDC	FNP Hold	FNP Abort	FNP Abort Activated/dent by CRDC	FNP Disconnect	FNP Disc Done	FNP Deactivated	FNP Deact Broadcast	FNP Deact Done	FNP Update	FNP Update Completed
Update																							P
Update Completed	R	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	R [4]					S/C [6]	
Update Completed by CRDC	R	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	R [4]					S/C [6]	
FNP Deact Broadcast																					P		

6.3 Message details

Messages (such as FNPR, FNP Exec, etc.) have 2 fields of free text for the exchange of additional information. This data is not necessarily logged in the database.

Interactions between Recipient/Donor and Subscriber are beyond the scope of the CRDC. Processes for obtaining authorisation from the Subscriber to port a number are defined by the Participants and the CRDC is not involved in obtaining or verifying Subscriber authorisation. Details of steps in those processes do not involve the CRDC, and are beyond the scope of the CRDC functionality.

6.3.1 Initiation Phase

6.3.1.1	FNPR
6.3.1.2	Acknowledgement
6.3.1.3	Fault Code
6.3.1.4	FNP Accept
6.3.1.5	FNP Reject

6.3.1.1 Number Portability Request - FNPR

The Recipient requests the porting of a number which is currently receiving service from the Donor.

A FNPR request can be sent from Recipient to CRDB and from CRDB to Donor.

Before sending a FNPR to CRDB, the Recipient validates the data received by the Subscriber and from its commercial/technical departments and which have to be contained in the FNPR. If data are missing, the Recipient takes care to obtain it from the Subscriber or internally. The data must contain all necessary information to document this new GFNP case and to co-ordinate FNP with the other parties. IP1 has therefore no limit in timing.

Once all data is collected, the Recipient sends a FNPR message to the CRDB by which the Recipient requests the porting of a number which is currently receiving service from the Donor.

6.3.1.2 Number Portability Request Acknowledgement

The CRDB validates the data send an acknowledgement for each notification [6.3.1.4] and send an acknowledgement [6.3.1.4]attempts to match the notification with its own data if any (e.g. in case of a number already

[6] The FNP Update messages is sent from the recipient and Broadcasted by the CRDC to each other Participant.

ported before. If the data provided with the notification is valid, the CRDB replies to the Recipient with an Acknowledgement.

6.3.1.3 Number Porting Request Reject – fault code

If data are missing, irrelevant, corrupt or not expected coming from the Recipient or if the porting concerns a number which is either already in progress by an other Recipient or for a number that cannot be ported, the CRDB sends a fault code to the current Recipient. The replied fault code is dependant of the NP process stage or/and by the business rule implemented in the CRDB. Number Portability Request Accept – FNP Accept.

The Donor checks the validity of the information contained in the FNPR received from the CRDB and verify whether the number can really be ported. The FNPR Accept is forwarded from the CRDB to the Recipient. Number Portability Reject – FNP Reject

6.3.1.4 Number Portability Request Reject – FNP Reject

The Donor checks the validity of the information contained in the FNPR received from the Recipient through the CRDB and verify whether the number can really be ported. If this is not the case, the Donor will forward an FNP Reject with the appropriated reject code to the CRDB for each number or range impacted (see annex E). The FNP Reject is forwarded from the CRDB to the Recipient.

6.3.2 Technical Phase

6.3.2.1	FNP Exec
6.3.1.3	Fault code
6.3.2.2	FNP Ready
6.3.2.3	FNP RFS (Ready for Service)
6.3.2.4	FNP nonRFS
6.3.2.5	MNP RFS Broadcast
6.3.2.6	FNP RFS Broadcast
6.3.2.7	FNP Activated
6.3.2.8	FNP Change
6.3.1.3	Fault code
6.3.2.9	FNP Change Reject
6.3.2.10	FNP Change Accept
6.3.2.11	FNP Cancel
6.3.2.13	Acknowledgement
6.3.1.3	Fault code
6.3.1.12	FNP Cancelled by CRDC
6.3.2.14	FNP Hold
6.3.1.3	Fault code

6.3.2.1 Number Porting Execution - FNP Exec

The FNP Exec is sent to the CRDB (and Donor) after the Recipient is ready to activate the GNP service. With this message he asks the Donor for activation of the number porting related to the unique ID number. This message is sent after the FNP Due Date has expired, this to ensure that the Donor is ready, but before the expiration of T7.

6.3.2.2 Number Porting Execution Rejected – Fault code

This fault code is issued by the CRDB when the execution request cannot be continued.

Between involved parties, a system down status by a Donor shall also generate a Reject – fault code to the Recipient when he sends out the FNP Exec message to the Donor.

6.3.2.2 Number Porting Ready - FNP Ready

The FNP Ready is sent to the CRDB (and the Recipient) after the Donor has finished and tested the activation. Time frame T3 must be taken into account.

6.3.2.3 Number Porting Ready for Service - FNP RFS

The FNP RFS is sent from Rec. to the CRDB when de service is operational and end to end tested. Time frame T4 must be taken into account.

6.3.2.4 Number Porting non-RFS – FNP nonRFS

The FNP Non RFS is sent from Rec. to the CRDB (and Donor) when the end to end test failed. Time frame T4 must be taken into account.

6.3.2.5 Mobile Number Porting Execution Broadcast – MNP RFS Broadcast

Broadcast of the “MNP RFS Broadcast” message to all operators. This message must contain the routing information, the Recipient ID and MSISDN number information. The Due date field will be filled automatically through the CRDB on receipt of the “MNP RFS Broadcast ” message with its current date and clock time. With this message all other parties could implement the new routing information but its CRDB priority for treatment is high.

6.3.2.6 Number Porting Execution Broadcast - FNP RFS Broadcast

Broadcast of the ”FNP RFS Broadcast” message to all operators. This message must contain the routeing information, the Recipient ID , the Donor ID, the Coded ID (optional) , the involved “To-From” directory number information , the “FNP RFS broadcast” CRDB current date and time, the CRDB software version number and the numbercount. The date and time field will be filled automatically in the” FNP Due Date” field through the CRDB on receipt of the Recipient’s “FNP RFS ” message with its current date and clock time. With this message all other parties can implement the new routeing information but the CRDB priority for treatment is medium. When it is a port back to the original Donor, the CRDB will replace the actual routeing number with CNANO. This to inform the operators, that the number is ported back to the original Donor.

6.3.2.7 Number Porting Activated - FNP Activated

This message is sent by all operators that have made changes to their routing information after the FNP RFS Broadcast.

6.3.2.8 Number Porting Change - FNP Change

A ‘FNP Change’ can be given after the ‘FNPR Accept’ and before the ‘FNP Exec’ is sent from the CRDB to the Donor. Only the Recipient can send a change message. The change message allows the Recipient to change the routing information and/or the FNP due date.

6.3.1.3 Number Porting Change Rejected - Fault Code

If data are missing or the data is not correct, a fault code will be send from the CRDB to the Recipient.

6.3.2.9 Number Porting Change Rejected - FNP Change Reject

The ‘FNP Change Reject’ can be sent by the Donor.

6.3.2.10 Number Porting Change Accepted - FNP Change Accept

‘Change accept’ will be send from Donor to Recipient when the Recipient agrees upon the change and took the according actions.

6.3.2.11 Number Porting Cancellation - FNP Cancel

A ‘FNP Cancel’ can be given after the ‘FNP Request’ and before the ‘FNP Exec’ is sent from the CRDB to the Donor. Only the Recipient can send a cancel message. This cancel message aborts the porting case.

6.3.2.12 Number Porting Cancellation - FNP Cancelled by CRDC

A ‘ FNP Cancel by CRDC’ shall be given after the ‘ FNP Accept’ when the timer T7 is expired.

The cancel by CRDC message aborts the porting case and permit to any Participants to introduce a new FNPR.

6.3.2.13 Number Porting Cancellation Acknowledgement –Acknowledgement

The CRDB validates the data for each notification and attempts to match the notification with its own data. If the data provided with the notification are valid, the CRDB replies to the Recipient with an “acknowledgement” message response.

6.3.1.3 Number Porting Cancellation Rejected – Fault code

The Fault code can only be send from the CRDB to the Recipient.

6.3.2.14 Number Porting Hold - FNP Hold

A ‘FNP hold’ can be given, after the ‘FNPR Accept’ and before the ‘FNP Due Date’, to the Recipient. Only the Donor can send a hold message. A previous request is put on hold and the implementation phase is interrupted.

6.3.1.3 Number Porting Hold Rejected – Fault code

A ‘fault code’ is replied by the CRDB if the FNP Due Date is passed.

6.3.3 Operational phase.

6.3.3.1	MNP Disconnect
6.3.3.2	FNP Disconnect
6.3.3.3	FNP Disc Done
6.3.3.4	FNP Deactivated
6.3.3.5	FNP Deactivated Broadcast
6.3.3.6	FNP Deact Done

6.3.3.1 Mobile NP Disconnect – MNP Disconnect

A “MNP Disconnect “is sent by the CRDB when a previously ported mobile number is disconnected

6.3.3.2 Number Porting Disconnect - FNP Disconnect

A ‘FNP Disconnect’ is sent to the CRDB for further co-ordination.

The CRDB informs the original Donor by forwarding the ‘FNP Disconnect’.

6.3.3.3 Number Porting Disconnect Done - FNP Disc Done

The Donor sends an ‘FNP Disc Done’ message to the CRDB after the ‘FNP Disconnect’, and the CRDB forwards the message to the Recipient after registration.

6.3.3.4 Number Porting Deactivated - FNP Deactivated

After the ‘FNP Disconnect’/’FNP Disc Done’ cycle, the Recipient finishes the deactivation and sends an ‘FNP Deactivated’ message for distribution.

6.3.3.5 Number Porting Deactivation Broadcast - FNP Deact Broadcast

A ‘FNP Deactivate Broadcast’ is sent to all Participants by the CRDB.

6.3.3.6 Number Porting Deactivation Done - FNP Deact Done

A ‘FNP Deact Done’ is sent to the CRDB by the Participants, when done.

6.3.4 Number Portability Abort

6.3.4.1	FNP Abort
6.3.1.3	Fault code
6.3.4.2	FNP Abort Activated
6.3.4.3	FNP Abort Activated send by the CRDB

6.3.4.1 Number Portability Abort – FNP Abort

The Recipient is the only entitled party who can send a “FNP Abort”, this message will be accepted by the CRDB starting after a “FNP Exec” and till a “FNP RFS” message is emitted. The “FNP Abort” message kills the running process and impact’s single, full range(s) or grouped FNPR. In this stage of the process no link or mention will be done with any previous information recorded in the “Coded Id field”. The “FNP Abort” will initiate a fall back process at Donor’s network.

E.g. wrong Subscriber’s number is ported out and the issue detected by the Recipient during a -FNP non RFS-check.

6.3.1.3 Number Portability Abort Reject – fault code

The CRDB fault code the “FNP Abort” message when any abort condition is not met .

6.3.4.2 Number Portability Abort Activated – FNP Abort Activated

A “FNP Abort Activated” is the acknowledgement by the Donor after a receipt of a “FNP Abort” message. The acknowledgement needs to be replied during the timer T10.

6.3.4.3 Number Portability Abort by CRDB – missing FNP Abort Activated

After T10, by no receipt of the FNP Abort activated , by the Donor, the CRDC presume that the task is executed and send a “missing FNP Abort Activated” message to the Recipient.

6.3.5 Maintenance phase.

6.3.5.1	FNP Update
6.3.1.3	Fault code
6.3.5.2	FNP Update Completed

6.3.5.1 Update of Information – FNP Update

The Recipient who performs internal modifications which have an influence on his (in-)ported numbers sends an Update message to CRDB to notify the changes. The message contains:

- The ID number, new routing info, Coded Id field (if any)
- In case of porting of number ranges, the ported number range to which the modification relates. In that case Nr From and Nr To must be filled.
- If the set of individual ported numbers forms a continuous series, one can also use Nr From and Nr To for practical convenience.

A time T8 is foreseen in order to give a mandatory time frame to Participants to correct their routing tables.

CRDB transfers the Update message to the Participants in the same format.

6.3.1.3 Number Portability Abort Reject – fault code

The CRDB fault code the “FNP Abort” message when any abort condition is not met

6.3.5.2 Completion of Update - Update Completed

All Participants send an Update Completed message to the CRDB. CRDB logs the information for reporting purposes.

6.3.6 Synchronisation report

See section “Reports”

6.3.6.1 Current Number location

This message is sent to request information about a specific DN as well as to update the Participant database which wants to check information for any task (e.g. trouble ticket).This information is available on line and in real time.

6.3.6.2 Number Porting Audit Response – FNP Audit Response

The database provides the requested information. All fields of the message are completed to provide all information available.

6.3.6.3 FNP Bulk synchronisation request - FNP Bulk Sync Report

Report is supplier dependant.

6.3.6.4 FNP Bulk synchronisation answer- For new Participant

CDROM or Zip file with copy of database for all activated numbers.

The flat file containing: Time stamp of the last broadcast message included in the copy for each activated or updated number:

ID number	unique identity assigned by the CRDB to be used in messages referring this porting case
Nr. From	the (first) Directory Number (of the range) to which the activated number is referring at
Nr. To	the last Directory Number if the activated number concerns a DN range
Donor Id.	the identity number of the Donor
Recipient Id.	the identity number of the Recipient
New Route	Route identified for the new FNP situation; i.e. Route Nr. or Network Identity
	Broadcast message type
	Time stamp of latest FNP emitted broadcast
Coded Id field	Hexadecimal field which represent a specific event (flag)

Original Donor ID: Original Donor ID is the current operator in possession of the allocated Number block.

6.3.6.5 Soap Replay

See 5.6.2.2 , type(s) of NP messages for a requested period are replied through the Soap interface.

Mainly requested for a re-synchronisation need of a FOLO’s automated or semi-automated legacy systems.

6.3.6.6 FNP Open porting synchronisation request- FNP Open Porting

Message to request all messages concerning non-ported numbers where the Participant is Recipient or Donor and sent from a given date and time ; two parameters are used, Participant Id and Date/time for first retransmitted message.

6.3.6.7 FNP Open porting sync answer- FNP Open Porting Answer

Supplier dependant

6.3.7 Operational phase - Customer Care

For FNP Fault handling and FNP repair services, please refer to the process, contacts and documents used within the Participant’s NOC services.

6.4 Time frames and Timers

If a timer expires the Participants have the right to start an escalation process. Please, refer to the FNP SLA for details.

Business hours referred to in this document are from 8:00 AM to 17:00 PM local Belgium time. Business days are from Monday to Friday excluding bank holidays and agreed excluded closing days.

Refer to the NP SLA for the value of a Business Day.

6.4.1 T1

The Recipient receives a response on the request within T1.

6.4.2 T2

T2 is the minimum time that the Recipient is required to respect before the FNP Due Date.

Minimum FNP Due date = T1

6.4.3 T3

The maximum elapse time between the execution command and actual activation of FNP by the Donor.

6.4.4 T4

Maximum elapse time given to the Recipient, between the receipt of a ready for service indication and the confirmation of service availability, can be concluded by a “FNP RFS” or “FNP Abort” message.

6.4.5 T5

During time frame T5 a Participant should confirm that the received Log report is correct. It is assumed that the information is correct if no response is received by the CRDB before the timer expires.

6.4.6 T6

T6 is the minimum elapse time between the current date/time and the activation of synchronisation.

6.4.7 T7

T7 is the period following the FNP Due Date during which the FNP can be activated. When the timer T7 expired the porting case is automatically cancelled by the CRDC.

6.4.8 T8

A Participant is expected to confirm the FNP is activated, deact done or updated completed within a time frame of T8. If this timer expires, the CRDB can assume that actual (de-)activation or update took place.

6.4.9 T9

Internal timer of the Recipient to guarantee a minimum elapse time before a number can be re-used by the Donor.

6.4.10 T10

When T10 expired the CRDB is considering that the Donor has omit to send the “FNP Abort Activated” in due time. It will start, after a “FNP Abort” event log, the deletion of the relating messages of this FNPR, this to permit the introduction of a new FNPR for this number, range or grouped FNPR.

6.4.11 Timer values

The current operational timer values and FNP Service Windows are these confirmed in the latest edited NP basic SLA on the BIPT website.

Timer	Values for Simple	Values for complex installations
T1	1 business day	2 business days
T2	T1	T1
T3	15 min's 85% of the cases, 30 minutes maximum	3 min's per DN or number range + 5 min's (85% of the cases), 120 min's max.
T4	4 business hours	4 business hours
T5	3 business days	3 business days
T6	10 business days	10 business days
T7	10 business days	10 business days
T8	5 business days	5 business days
T9	Minimum 6 months and maximum 12 months	Minimum 6 months and maximum 12 months
T10	24 hours	48 hours

The above timing constraint refer to "simple" installations (E.g. PSTN or full ISDN or HFC coax based connections) and to more complex configurations (E.g. partial ISDN , Fibre , ……)In general terms, a difference between possible installations is therefore described as follows.

Simple installations are single connections of telephone lines with one or a multiple of individual numbers assigned on the same physical installation. It concerns an analogue line, in the case of PSTN, a full basic access connection for ISDN (main number and all its Multiple Subscriber Numbers) or a HFC coax connection.

Complex installations refer to configurations on the same physical installation, which don't fall under the above descriptions. Typically, they are hunt groups, in dialling, services, partial porting on an ISDN or other fibre connection carrying multiple numbers. In these cases the signalling takes place at the level of R2 (analogue) or PRA (digital) connections. For the timer values, the NGFNP are considered as Complex installations. Any installations were the Subscriber is already disconnected with a minimum of 7days and a maximum idle period of x months in Donor's network is treated as complex , after the x months we can not speak about an previous installation. (x is bilaterally agreed between the two parties , Donor and Recipient)

6.5 Reject & Blocking Reasons

As initial remark, this list is non-exhaustive. The annex E: “Codes” is therefore referring to the values that are currently defined.

A state level specifies the interpretation in relation to the code; it could be seen as a reject, blocking or information state.

Status “R” is an unconditional reject cause for the full FNPR.

Status “B” is a conditional situation, meaning that when the constraint is corrected or settled, a new porting will be accepted.

Status “I” is to inform the Recipient or Participant of a specific condition who could impact the porting request.

7 Database (Indicative)

7.1 Common information

- local operator reference
- GNP capabilities (e.g. OR, ACQ)
- information for audit
- accounting and charging data
- Tables like;
  - Allocated Number Block tables
  - Agreed Routing number tables
  - OLO's mnemonic table
  - Coded ID ref. table
  - Rejection codes and fault error codes tables
  - Participant's with Geo & Non-Geo porting rights table
  - Timers table
  - Official Holidays table
  - Serving window table
- Documentation depository system: system related documentation

7.2 Bilateral Information (Indicative)

There is no intention to keep track of the Subscriber information in the CRDB.

If Subscriber information is exchanged during the FNPR and this to guarantee a cross check between the DN / range and the holder known as Subscriber, for privacy reasons, the Subscriber's information has to be cleared ultimately by the CRDC when the FNP is accepted by the Donor.

The fields; any type of Subscriber ID, the VAT fields and the address data fields need to be emptied as soon as the FNPR is accepted

To comply on the privacy regulations this information will only be kept in the CRDB as long as needed for the FNP validation process.

7.3 Historical data (Reference data)

The only stored historical data at any level is the all type of "FNP broadcasts" information, who need in real time and on-line to be available and this for all Participant's public information on ported numbers.

This information will be limited in content to identified single or a range of numbers belonging to the same grouped porting. The online data consists of;

- **The FNP Directory Number** (Public)
- **The Recipient ID** (Public)
- **The FNP Broadcast Time** (Day + Hour) (Public)
- **The New Route** = Routing Number (Participant)
- **The Coded Id field (Private ; only for FNP Participants and agreed 3rd parties)**
- The FNP ID number (only for Fix FNP Participants)
- The Original Donor (Private)

Period the historical data is kept and available by the CRDC depend on the application

- Production system : six months
- Judicial system : one year (with data of subsequent ports involved *)
- DWH : * with or without subsequent porting case(s) , the date and time of the first port from the NANO stays always recorded in the DWH as historical data .

7.4 CodedID Field “Flag”

CodedID field.

The CodedID field, 3 decimal characters (XYZ), gives a specific condition or situation were the recorded number, in the CRDB, could be impacted with. This information is relevant for FNP customer care, FNP disconnection and similar issues as well as for some types of coded ID for tracking of elements by the Judicial Authorities.

The CodedID shall reflect a specific condition(s) regarding a specific directory number recorded in the Common Reference Data Base.

The CodedID could e.g. be used as coding for synchronisation purposes during a NP validation process in relation with an other parallel involved process impacting the porting (e.g. CodedID 001), to be used to inform other operators about a specific impact on a ported number or to make it possible to trace ,after a while, for repair or fault management a field condition on a specific number or to indicate the nature of the directory number in the location Database.

The CodedID is a three digit number starting from 000 till 999, some of these Coded ID’s could be validated by the CRDB, following predetermined business rules.

Other could be used only to inform a technical stage on a ported number or number recorded in the CRDC DWH for number location purposes.

The CodedID can be managed (created or updated) with the FNP Update message, created during a FNPR or removed (number + CodedID) from the DWH with the NP disconnect message.

The content of the CodedID field will still remain in the DB as value information per recorded number but could also be empty for a normal case (most common situation)

The FNP Worklist Screen[7] (reporting) will display the value and description of the CodedID if requested and present in the online DB.

A view and CSV output format need to be available through the GUI. (Filter; Participant, DN, Date from – date To, routing or network Identifier and CodedID)

Reply of the query; Participant, Start date, DN, routing info, CodedID value + description.

Some CodedID values will be displayed, only with its specific description on the 3rd Party interface as additional information for the Judicial Authorities (E.g. for the CodedID: 002 and 004) could be later also the case for the Public Interface (Number location Database for specific codes, e.g. 004 CodedID)

Additional CodedID values and descriptions recorded in the CRDB table need to be validated through the NPA Service Manager and documented if a business rule is expected during the validation process.

For the “CodedId field” list please refer to Annex G. E.g. Imagine code 001 is the code used to flag a FNP + LLU impact. Allocated Number blocks and exchange identification routing number format

7.5 Allocated Number Block Number Range format

The number ranges allocated by BIPT to the Number Range Holders (NRH) may have the following format:

PQY(Z) (K) (L) : 3 to 6 numeric digits representing the number range (first significant digits without leading '0') that has been allocated by the BIPT to a specific NRH and activated by the NRH.

Examples :

2400 : for a geographic number range of Brussels zone: (0)2-400 xx xx
476 : for a mobile number range: (0)476-xxx xxx

[7] The FNP Worklist screen is supplier dependant.

80063 : for a non-geographic (0800) number range: (0)800-63 xxx

7.5.1 Exchange Identification Routing Number format

The Routing Numbers (RN) used for number portability for geographic, non-geographic and mobile numbers have the following format:

CXXXX : 5 hexadecimal digits with:
- C : the hexadecimal digit 'C'
- XXXX: 4 numeric digits identifying the Recipient network or Recipient network entity

Examples:

C5631 : Routing number used for geographic number portability
C4700 : Routing Number used for mobile number portability
C0016 : Routing Number used for non-geographic number portability

7.5.2 Data changes “CRDC Table” of Routing Numbers or allocated Number blocks

The Recipient is always responsible to request an update, deletion or change of data recorded in the CRDC Data tables. He needs to forward this request to the NPA Service manager after a real time implementation check with the transit operator(s) involved. Only allocated Number blocks (not reserved number blocks) are taken into account as new data for the CRDC, as well as operation Routing Numbers (Interconnection).

If a FOLO as no Porting obligation anymore or if it disappears as National operator, the BIPT will grant the NPA Service Manager to request to the CRDC to clear the appropriated and involved data tables in the CRDB. If this impact already ported numbers an agreed solution and time will be communicated by the NRA to clear and adapt the CRDC tables.

8 ANNEX A : Service Level Agreement

Refer to the FNP Basic SLA document for more details.

(FNP Basic SLA is part of the bundle of the FNP contractual documents that can be consulted on the BIPT Web-site)

- FNP Service Windows with the agreed operation FNP timers are recorded in this NP Basic SLA.[8]
- These documents are approved and signed by the Minister of Telecommunications.

[8] The FNP STC (Representation of Folo's and NRA) could agree to adapt the FNP Service Windows and timer values.

9 ANNEX B : LOOP PROBLEM

This annex is included for clarification of the above sections on Initiation and Activation. It forms no part of the agreements but shows the consensus that exists on interpretations of these sections.

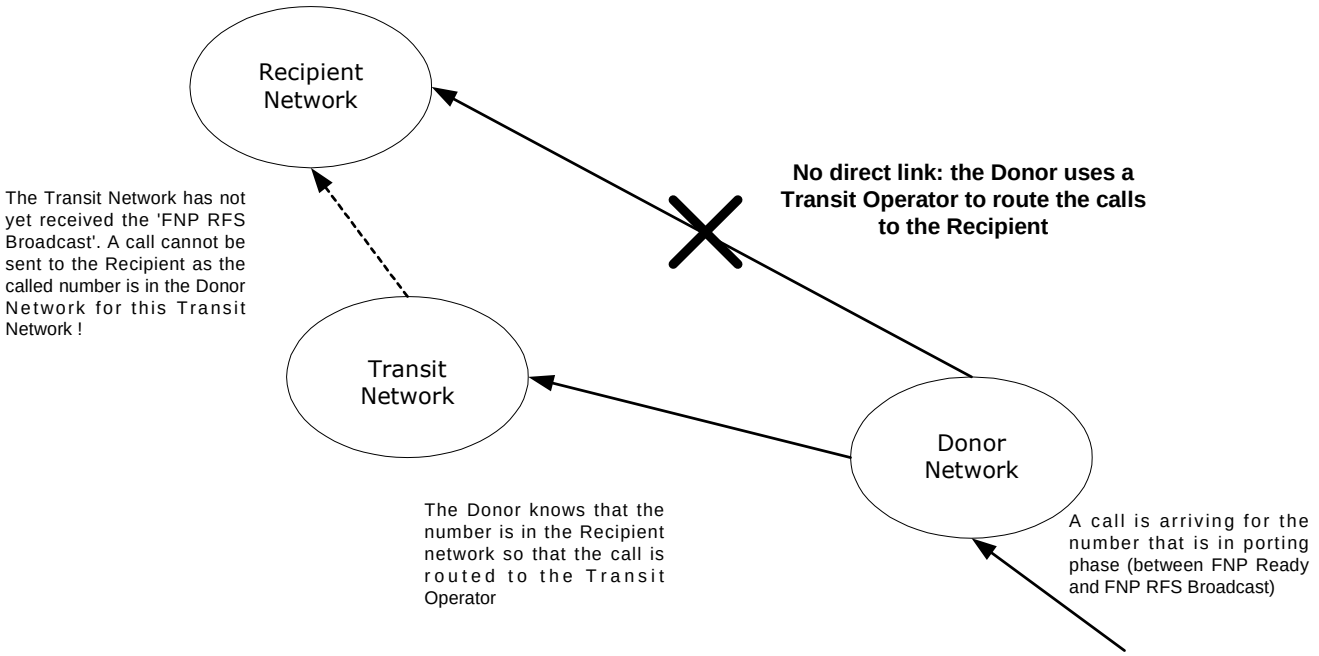
The possibility of a loop is explained when routing calls in the period between an 'FNP Ready' and 'FNP RFS Broadcast' message are exchanged for the GFNP Activation process, § 5.2.1. The situation may occur when a transit operator is involved. The following discusses the solution for this problem in the context of inter-operator co-operation.

In case of Non-geographic number porting, the loop problem is not applicable after the Donor applied the correct routing.

9.1 Description of the Problem

Key Participants in the FNP process are (see figure):

- A Donor Operator
- A Recipient Operator
- A Transit Operator utilised by the Donor Operator to route the calls to the Recipient.



In this case, any call initiated between the exchange of 'FNP Ready', as sent by the Donor, and the 'FNP RFS Broadcast', sent by CRDB, will not be terminated.

The Donor has sent a 'FNP Ready' which means that the Donor database is updated and informs its own systems that the number has been ported to the Recipient. A call which arrives to that number is re-routed to the Transit Operator in order for him to route the call to the Recipient.

Unfortunately, the *Transit Operator has not yet received the FNP RFS Broadcast* so that it is not known that the call must be routed to the Recipient. On the contrary, the Transit Operator will send the call back to the Donor as for the number has not yet been ported and is therefore still owned by the Donor.

Furthermore, it is impossible for the Recipient to complete the end-to-end tests before sending the 'FNP RFS' message about the new ported number.

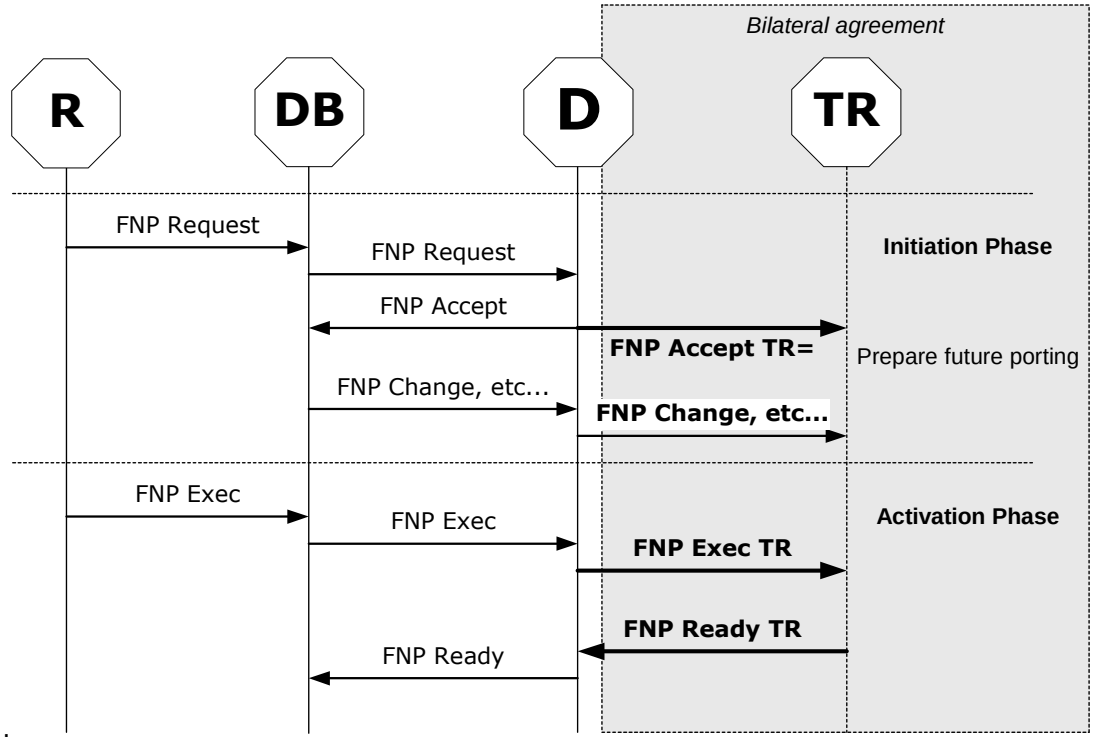
9.2 Solutions

In the following scenarios a co-ordination is required between the Donor and the Transit Operator to handle the above problem and make it transparent for the other parties; the Donor is responsible for the overall results (a principle applied during the development of the FNP concept is the autonomy of Participants. I.e. the Recipient has no capability to control bilateral agreements between the Donor and the Transit Operator). Donor and Transit Operator work together to perform the "Donor" functions as described in this document. Consequently, all messages exchanged between the Donor and the Transit Operator as identified below have a format and content which is mutually agreed between these Participants.

The result of this interaction corresponds with, and finds its constraints in, the description found in the above sections. [*Editor's note: this text is the annex to the deliverable of PT3 and highlights certain interpretations created in consensus between the members of the project team*] There exist the following three scenario's to achieve the overall "Donor" objective as described in the sections 'Initiation phase' and 'Technical phase', i.e. § 5.1 and § 5.2.

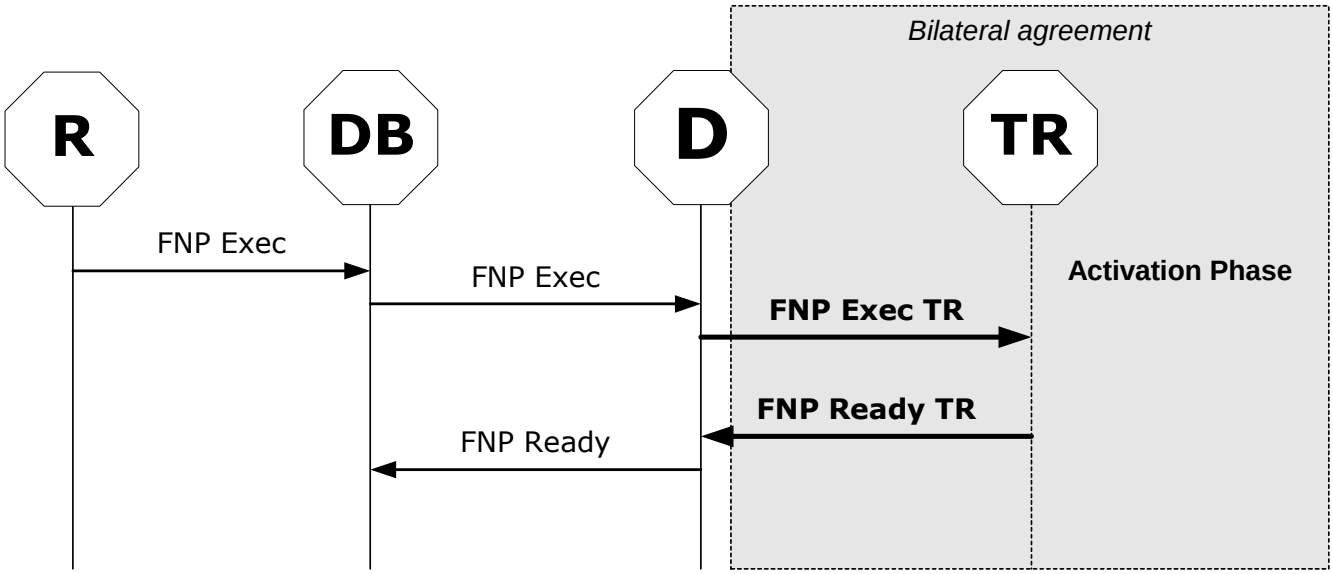
9.2.1 Scenario A

The Donor exchanges messages with the Transit Operator on a bilateral basis. The identified messages are 'FNPR Accept TR', various data transfers related to changes in the FNP process, 'FNP Exec TR' and 'FNP Ready TR'



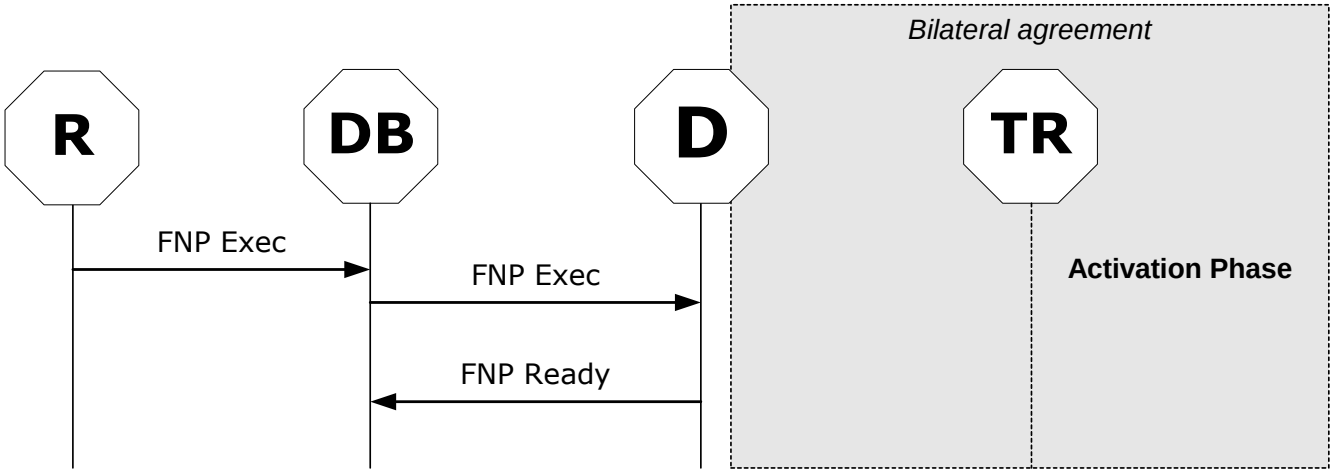
9.2.2 Scenario B

The Donor exchanges the 'FNP Exec TR' and 'FNP Ready TR' messages with the Transit Operator. The "Donor" therefore waits for the corroboration of the Transit Operator before sending "FNP Ready".



9.2.3 Scenario C

This scenario makes use of the capabilities foreseen in the signalling between the switches of the Participants. In the stage of porting it is expected that the Donor sends the Routing Id. to the Transit Operator; the combined information sent by the Donor contains the DN and the RN or Network Id. The transit network is informed about the new routing condition and will act appropriately.



10 ANNEX C : COMPLEX INSTALLATIONS

This annex is included for clarification of the installations which are not considered as “simple” and therefore require additional attention.

10.1 Grouping of numbers

The following grouping of DN numbers exist to handle complex installations:

- single DN DN0
- multiple DN’s DN1, DN2, DN3, ...
- DN ranges + individual DN’s DN1-to-DN2, DN3-to-DN4, ..., DN5, DN6, ...

10.2 Types of complex installations

Three typical forms of complex installations are identified. The first one relates to the treatment of ISDN-BA numbering and the two following are coupled with the usage of PABXes. A description of each of these cases is given below.

10.2.1 Partial ISDN-BA

The porting of a “Partial ISDN-BA” compared with a “Full ISDN-BA”, situations were the main DN and/or some of the MSNs are not ported and remains the propitiatory of the Donor. (Full ISDN-BA = one main DN and max. 7 MSNs recorded to the same BA).

10.2.2 Huntgroup

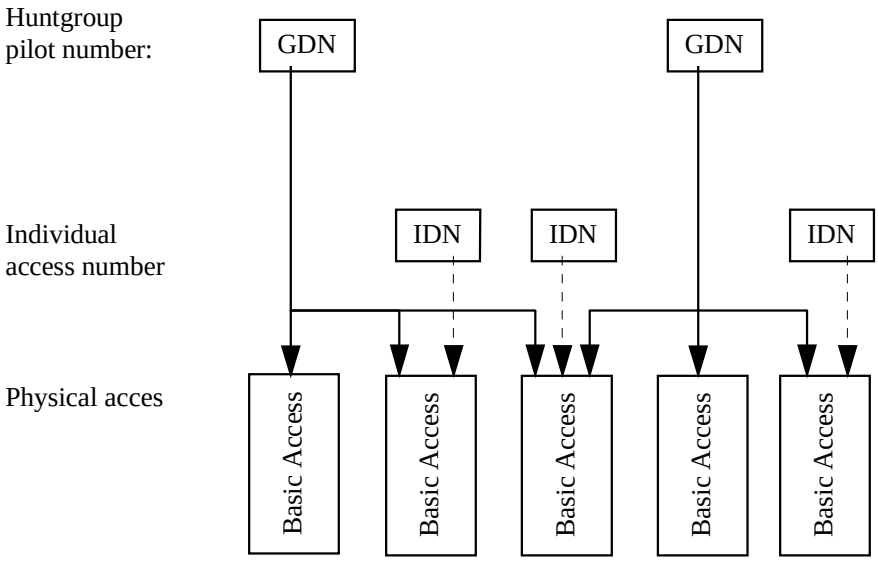
It is identified by a General Directory number (GDN). For all calls to this GDN, the exchange will have to select a free access towards the PABX. This process is called 'hunting'. Inside the PABX, the calls are routed to an attendant. This attendant can establish a connection between the incoming call and the desired PABX extension. The same PABX without in dialling might be connected via several huntgroups (i.e. several GDNs 'Search Directory Number’). Accesses can be defined as being part of more than one huntgroup. An 'Individual Directory Number (IDN)' can be assigned to each individual access, in order to address the access directly without using a hunting mechanism.

The following physical accesses can be used:

- Analogue line.
- Basic Access.
- Primary Rate Access.

Different types of accesses can be combined in the same huntgroup.

Example:



10.2.3 In dialling

PABX with In dialling (also called **D**irect **D**ialling **I**n - PABX): In this case the extensions can be reached directly from the public exchange. Then the signalling towards the PABX must contain at least the dialled extension number. The PABX is also identified by a GDN and a DDI in dialling plan is assigned to the PABX.

The following physical accesses can be used:

- Analogue line.
- Basic Access.
- Analogue Trunk. (R2)
- Primary Rate Access (PRA).

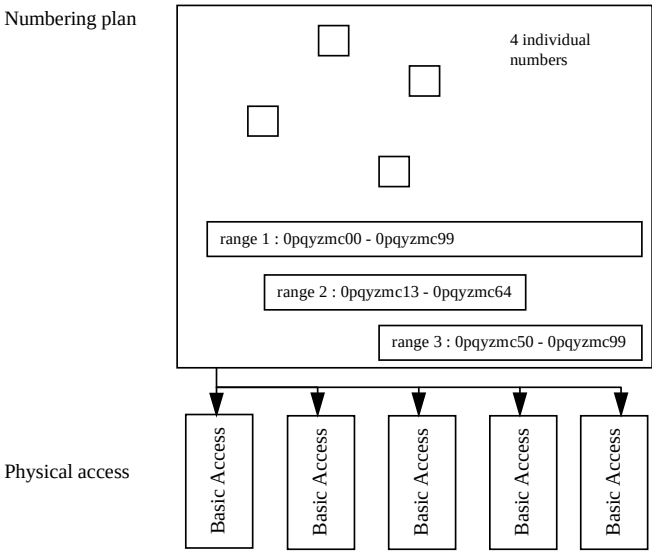
Different types of accesses can be combined in the same in dialling.

The in dialling plan is defined as a the group of numbers assigned to the group of accesses, and which consists of

- - one or multiple ranges of consecutive numbers,
- - one or more individual numbers added (not consecutive).

The in dialling plan is dependent of the physical access type.

Example:



10.3 (more) Candidates for further detailed evaluation

The following summarises the (additional) possible complex cases for FNP installations.

- PSTN Distinctive Ringing: One line has multiple DN's assigned. A different ringing is assigned for each DN.
- PSTN /Convergence: One line with two or more DN's. All numbers ported or partial porting.
- ISDN-BA /Convergence: One line with two or more DN's. All numbers ported or partial porting.
- Huntgroup analogue PBX: One pilot line with a geographical number and 'n' additional number which are used when the pilot line is busy. Possible number assignment is one hunt DN plus n x DN's. The later can also be called directly.
- ISDN Cascade: One pilot line with a geographical number and 'n' additional number which are used when the pilot line is busy. Possible number assignment is one hunt DN plus n x DN's. The later can also be called directly.

The cases that need more clarification are:

- Centrex PSTN / ISDN-BA: [to be specified]
- A DN to port who is allocated , reserved or resigned and out of service, for a period not exceeding 90 days after the effective terminating date.

11 ANNEX D : Reporting

11.1 Scope

The content hereunder reflects the minimum requirements expected from the CRDB reporting facilities.

These reports are split in management and operational reporting. The management reporting is based on neutral information which can be shared between all entitled and recognised as right to have parties.

The operational reports are needed for the daily, weekly or monthly operational follow up an issue tracking and are the base figures for the FNP SLA compensation calculation.

There were needed all reports will differentiate a Participant as report requestor and a Participant involved in a reported case.

11.2 CRDC REPORTING

CRDB reports are generated in a Web-page format and via file downloads , e.g. CSV-format.

Some consolidated (all FOLOS) reports are only retrievable by the NPA Service Manager (E.g. NRA statistical reports)

11.2.1 Type of reporting

Four type of reports are generated by the CRDC

1) Reports needed for the NRA and recharging usage (consolidation of figures of all FOLO Participants)

a) Volume Statistics (Transactional) report will comprise the requirement listed below:

Number of "fnpr" (All NP Requests send to the CRDC = accepted and rejected by the CRDC) emitted as Recipient

- Number of "fnpcancel" emitted as Recipient ,added with the Cancels generated automatically by the CRDC, after expiration of the timer T7, by lack of the FNP settlement through the Recipient
- Number of "fnpchange" emitted as Recipient
- Number of "fnphold" emitted as Donor
- Number of "fnprejects" received by Donor
- Number of "fnpexec" (without timer T7) emitted as Recipient
- Number of "fnpready" emitted as Donor towards a specific Recipient with a split between 08:00 - 17:00 and outside this time window
- Number of "fnpabort" emitted as Recipient
- Number of "fnprfs" emitted as Recipient
- Number of "fnpdisconnect" emitted as Recipient
- Number of "fnpupdate" emitted as Recipient
- Number of "npbroadcast" received from MNP application
- Number of "npdisconnect" received from MNP application
- Number of ported in directory numbers with the "nprfs" as Recipient
- Number of ported out directory numbers with the "npready" as Donor
- Total directory numbers ported (volume) per reported line

b) Data Warehouse Storage report (DWH Storage)

Number of Geo, Non-Geo and mobile numbers currently recorded in the CRDC Database as Recipient

- Number of ported Geo Numbers
- Number of ported Non-Geo numbers

- Recorded number of ported Mobile numbers still in the DWH

Storage as totals shall include

- Volume of numbers received, acting as Recipient
- Volume of numbers ported out, acting as Donor
- Volume of Updated numbers (only fixed local ports), acting as Recipient and Donor.

E.g. Storage as Recipient

Volume of numbers received from a NANO

Volume of numbers received from a Donor (subsequent porting)

Volume of numbers disconnected by Recipient (back to NANO)

Storage as Donor

Volume of numbers given as NANO to a Recipient

Volume of numbers given as Donor to a Recipient

Storage calculation method

Start position as Recipient

The numbers ported in from NANO and Donor (subsequent porting), Due to the very low subs. ports all imported numbers are considered as coming from the NANO.

Start position as Donor

The numbers ported out to a new Recipient or numbers ported back to the NANO.

Calculation method:

Imagine 3 FOLOs , they could each have the status of Recipient , Donor or NANO Donor.

Situation 1 : FOLO3 $NANO^{Donor}$ port to $FOLO1^{Recipient}$ = +1 for FOLO3 $NANO^{Donor}$ + 1 for $FOLO1^{Recipient}$

Situation 2 :$FOLO1^{Donor}$ subsequent port to $FOLO2^{Recipient}$= + 1 for $FOLO1^{Donor}$ + 1 for $FOLO2^{Recipient}$ - 1 for $FOLO1^{Recipient}$

Situation 3 : $FOLO2^{Donor}$ port back to FOLO3 $NANO^{Donor}$ = - 1 $FOLO2^{Recipient}$ – 1 FOLO3 $NANO^{Donor}$ - 1 for $FOLO1^{Donor}$

2) CRDC Operation & SLA reporting

The Operational Reporting will be available using the GUI, or on request (special cases) it will be supplied on paper or via mail.

More detail will be provided in these reports

c) Timers expired report (based on Timers violation following the FNP Basic SLA principle)

Requestor ID as Donor or Recipient and Involved Participant ID are mentioned , trigger are the violated timers T1 ,T3 and T4 per involved porting case

d) Message List reporting

Report that permit to trace the history of a porting case, message type is the trigger

e) Monthly FNP Business Management report (unique report with 3 types of data)

- Report requestor has the role of Donor :

  Trigger are the “fnpready” messages emitted as Donor toward the Recipient OLO.
- Report requestor has the role of Recipient :

  Trigger are the “fnpready” messages received from Donor as Recipient OLO

- Report requestor has the role of Participant :
  Trigger are the “fnpbroadcast” messages received as Participant OLO

f) Number Location Information access report

Logs access and transactions done by individual parties when retrieving NLI updates in the NLI repository system

System Reporting

CRDC Downtime

Unauthorised System Access Attempts

Data and System Integrity

Continuity of Service

CRDB Reachable

- Quantity and total time the CRDB was not reachable or in service during the Business Hours.

Intrusion detection

- Exception reports
- Summary reports
- Detailed reports
- Test System Availability
- Production System Availability
- Front End System Availability
- Specific Availability and Performance requirements

Operational SLA Reporting

CRDC/CRDB Reliability and Availability

- Production System Availability
- Specific Availability and Performance
- CRDC Access Time with GUI Interface

- Reliability. This applies to functionality and data integrity.
- The amount of unscheduled downtime per year.
- For unscheduled downtime, the mean time to repair.
- The amount of scheduled downtime per year.
- Monitoring the status of entire communication links and reporting link failures and security malfunctioning.
- Front End System Availability

Test System Availability

Usage Statistics

Third party access Reporting

- N° of transaction logs of Judicial Authorities

3) Daily FOLO's operational reporting

- **Timer expiration reports (between FOLOs NP SLA based)**

This statistical report will show the percentage of timers exceeded for Simple and Complex ports. The FNP Cases which are viewed are all Cases which have open ports in progress , except for the T7 timer expired closed by CRDC. The report will comprise the requirements listed below:

- Number of times timer T1 is exceeded.
- Number of late and unsent NP RFS after T4 (T4 expired).
- Number NP Readies exceeding the maximum value of the T3 timer.
- Number of times the value of the timer T7 was exceeded.
- Number of times the T7 expired was closed by the CRDC.

- **FNP Worklist based reporting (GUI)**

The FNP Worklist [9] based reporting(s) provides a comprehensive selection to view/report a FNP messages and Mobile Broadcast messages based on user-defined criteria. A Participant can only view messages which are sent to the Participant in question (received and sent). After a selection has been made the messages, which are in the online database, are retrieved. They are shown on the detail section of the screen or downloaded in a CSV format.

The user can then start a responsive action by clicking on the Idnumber field on one of the messages that is displayed. The Worklist screen will automatically open a new screen to perform the action needed to respond to the FNP message (e.g. FNP Accept/Reject) or will display the details of the message when no action is required or no action is possible (e.g.: FNP RFS, FNP Activated, etc.).

The new screen that is opened is depending on the message status of the selected message, which is explained in the Recipient / Donor Screen Hierarchy.

A High Priority Indicator (only in a GUI view) is as default on. This means that there is a check running every 5 min for high priority FNP messages (ref. to TIS document of the supplier) sent to the Participant. If a high priority message occurs the High Priority Indicator will start blinking.

11.2.2 Management Reporting (NPA members & NRA)

Monthly Number of elements per category (Simple/Complex) per quarter

- Number of FNPR's (FNP Request).
- Number of FNP Readies with split, between 08:00 and 18:00 and outside this time window.
- Number of FNP Disconnects
- Number of FNP Cancels volume.
- Number of FNPR's without (timer T7) FNP Exec.
- Number of Participants who have access to the CRDB+ID list.
- Number of FNP Abort

Quality parameters *per category (Simple/Complex) and per quarter*

- Number of FNP Non-RFS (Ready for services)

[9] The FNP Worklist view is supplier dependant

- Number of times timer T1 is exceeded
- Number of late and unsent FNP RFS after T4
- Number FNP Readies exceeding the maximum of n times the value of the T3 timer.
- Quantity and total time the CRDB was not reachable or in service during the Business hours.
- Average processing time per processed consultation / data entry of the CRDB via a specific interface.

11.2.3 Operational Reporting per Participant

Reporting per Participant based on the complexity code, weekly (W) or monthly (M)

The weekly reports are generated as a list where the FNPR ID, the “TO” – “From”, Donor ID, date and time are mentioned, sorted by Donor and Complexity Class.

- Grand total own FNPR's (FNP Request) sent out (Monthly)
- Total own FNPR's (FNP Request) sent out towards specific Participant (Weekly)
- Own FNP Ready (with split), between 08:00 and 18:00 and outside this time window towards specific Participant. (Monthly)
- Own grand total FNP Disconnects. (Monthly)
- Own total FNP Disconnect towards specific Participant (Monthly)
- FNP Cancels towards specific Participant. (Weekly)
- Own Number FNPR's without (timer T7) FNP Exec. (Weekly)
- Number of emitted FNP Aborts (Monthly)

Quality parameters per category (Simple/Complex) and per quarter towards a Specific Participant.

(On request additional details could be forwarded as well.)

- Number of FNP Non-RFS (Ready for services) sent out
- Number of times the timer T1 was exceeded
- Number of late and unsent FNP RFS after T4
- Number of FNP Ready's exceeding n times the value of the timer T3
- Number of times the value of the timer T7 was exceeded
- FNP ID with a T7 exceeded
- Number of FNP Abort

12 ANNEX E : Codes

12.1 Introduction

This section tries to identify the circumstances in which the different blocking, reject or information codes can be used. This document gives an exhaustive list of circumstances; i.e. if a particular case is not described in this document, no blocking or reject code shall be used.

The document also describes which party can use which blocking, reject or an information code.

A state level field has been added to each code, in which will be specified what the interpretation is of the code. The state level of the code can be:

- **Reject (R)**: in this case, an unconditional reject reason causes the current process to abort. A new porting process can be started in order to continue as soon as the state becomes acceptable. States related to the FNP Process agreed technical constraints or when long term resolution is expected to clear the reject cause.
- **Blocking (B):** In this case, the nature of the blocking code causes the current process to abort. A new porting process has to be started which fulfil the FNP precondition in order to be successful. Precondition expressed in the logical flow of the FNP processes, with agreed timers in relation to the FNP classification, technical prerequisites and administrative or legal resolution for short term blocking issues.
- **Information (I):** In this case, the current process continues. The code is filled for informational reasons only or used to clarify a situation. A rejection may not arise out of the usage of such codes.
- Codes without consensus of the PT3 members are not frozen

12.1.1 Family of codes used by the CRDB only, "[CRDB and/or Donor]"

The codes between square brackets can be used by either the CRDB (if implemented) or Donor.

Fault Codes / Reject code	Information	Not implemented / Other
200, 205, 210, 215, 225, 299, 300, 305, 306, 310, 315, 316, 320, 321, 325, 335, 340, 345, 350, 355, 370, 380, 381, 385 [1000]		

12.1.2 Family of codes used by the Donor

The codes between square brackets can be used by the Donor.

Blocking	Rejects	No consensus / Other
1050, 1051, 1052, 1053, 1054, 1055, 1056, 1057, 1058, 1059, 2010, 2011, 2012, 3015, 3017, 3018, 3019, 4014, 4018, 4019, 4020, 4021	3010, 3013, 3014, 3020, 3110, 4011, 4012, 4015, 4016, 4017, 5010, 9999	

12.1.3 Non-RFS codes used by the Recipient

Information	Rejects	No consensus / Other
8110, 8120, 8130,		

12.1.4 Non PT3 process related Economical or commercial codes used by the Donor

Blocking	Reject	No consensus / Other
	6013, 6014, 7010, 7011, 7012	

12.2 Codes

12.2.1 Normal Case

12.2.1.1 1000 No reject

Code	Family	Code	Description	Explanation	Code	State level
10	None	10	No reject	Default situation, filling up code	1000	I

Originator of the reject code: Donor, and Recipient.

Use of this reject code: this code can be used by the Participants when no reason for rejection is encountered, i.e. the normal case or to solve issues when a non process impacting code is expected to forward a condition, a fill the gap code e.g. by usage of the FNP grouping message.

12.2.2 CRDB Internal fault codes

12.2.2.1 200 Invalid Data

Code	Family	Code	Description	Explanation	Code	State level
200	CRDB	200	Invalid Data	Data out of format (PT3) or inconsistent	200	R

Originator of the fault code: CRDB

Use of this fault code: this code can be used by the CRDB when inconsistent data or data format is used to fill the message fields.

12.2.2.2 205 Message Not Complete

Code	Family	Code	Description	Explanation	Code	State level
205	CRDB	205	Message Not Complete	Data is missing in some message fields	205	R

Originator of the fault code: CRDB

Use of this fault code: this code can be used by the CRDB when message fields stay empty or when some fields are not fully filled up.

12.2.2.3 210 Message Format incorrect

Code	Family	Code	Description	Explanation	Code	State level
210	CRDB	210	Message Format incorrect		210	R

Originator of the fault code: CRDB

Use of this fault code: this code can be used by the CRDB when a Donor, Recipient or Participant sends a message with a non-adequate format.

12.2.2.4 215 DN format error

Code	Family	Code	Description	Explanation	Code	State level
215	CRDB	215	DN format error		215	R

Originator of the fault code: CRDB.

Use of the fault code: This fault code shall be used by the CRDB if the format in the DirectoryNumberFrom field or in the DirectoryNumberTo field has a wrong format. The correct format is:

0PQYZKHDU or 0PXYZKHDU for geographic numbers

0800AKHDU, 090ABKHDU, 070ABKHDU, 078ABKHDU for non-geographic numbers

The length of the number is in any case 9 digits, and shall always start with a 0.

12.2.2.5 215-205-385 DN range error

Code	Family	Code	Description	Explanation	Code	State level
215 205 385	CRDB	215 205 385	DN range error		215 205 385	R

Originator of the fault code: CRDB.

Use of the fault code: this fault code shall be used by the CRDB in the following cases:

- the value of the DirectoryNumberFrom field is higher than the value of the DirectoryNumberTo field
- only DirectoryNumberTo is filled out, nothing in the DirectoryNumberFrom field
- the porting range crosses the boundaries of the by the BIPT allocated number blocks, e.g. for geographic numbers: the PQYZ or PXYZ of the DirectoryNumberFrom field and the PQYZ or PXYZ of the DirectoryNumberTo field don't have the same value.

12.2.2.6 225 Message not allowed in this phase

Code	Family	Code	Description	Explanation	Code	State level
225	CRDB	225	Message not allowed in this phase	Same as 0012	225	R

Originator of the fault code: CRDB

Use of this fault code: this code can be used by the CRDB when it encounters a process flow outrage or processes sequence mismatch.

12.2.2.7 225 Message sequence error

Code	Family	Code	Description	Explanation	Code	State level
225	CRDB	225	Message sequence error	message to the CRDB not allowed or incorrect in this stage of the process	225	R

Originator of the fault code: CRDB.

Use of the fault code: This reject code shall be used by the CRDB if any of the parties sends a message that is not allowed in that particular stage of the porting process.

12.2.2.8 225 Porting order already cancelled

Code	Family	Code	Description	Explanation	Code	State level
225	CRDB	225	Porting order already cancelled		225	R

Originator of the fault code: CRDB.

Use of the fault code: This fault code shall be used by the CRDB in the FNP Cancel Reject message when the Recipient has sent an FNP Cancel message for a particular DN or range of DN's and the porting process was already cancelled by the Recipient.

12.2.2.9 299 Message coding error

Code	Family	Code	Description	Explanation	Code	State level
299	CRDB	299	Message coding error	message to the CRDB is incorrect or incomplete	299	R

Originator of the fault code: CRDB

Use of this fault code: This fault code shall be used by the CRDB in case an error is encountered in the message coding and the error can not be described by one of the other CRDB family fault codes.

12.2.2.10 300 Number not in database

Code	Family	Code	Description	Explanation	Code	State level
300	CRDB	300	Number not in database	No valid information available	300	R

Originator of the fault code: CRDB

Use of this fault code: this code can be used by the CRDB when the ID, DN or Range(s) is not recorded in the CRDB.

12.2.2.11 300 Number block not allocated or not active

Code	Family	Code	Description	Explanation	Code	State level
300	CRDB	300	The DN or Range belongs not to a Recipient's activated or allocated Number block .		300	R

Originator of the fault code: CRDB.

Use of the fault code: This fault code shall be used by the CRDB in the following cases:

When the DN, range or Range is not recognised as being in a number block that is allocated or activated in part of the Recipient's network.

12.2.2.12 305 Invalid range

Code	Family	Code	Description	Explanation	Code	State level
305	CRDB	305	Invalid range: The range already exists		305	R

Originator of the fault code: CRDB

Use of this fault code: this code can be used by the CRDB when the Recipient requests a porting for a range that was already ported in.

12.2.2.13 306 Some or all numbers in the range do not belong to the Donor

Code	Family	Code	Description	Explanation	Code	State level
306	CRDB	306	Some or all numbers in the range do not belong to the Donor		306	R

Originator of the fault code: CRDB

Use of this fault code: this code can be used by the CRDB when a Recipient requests a porting of a range including ranges belonging to another Donor. Could be the case by subsequent porting.

12.2.2.14 306 DN / Range already ported

Code	Family	Code	Description	Explanation	Code	State level
306	CRDB	306	DN / Range already ported		306	R

Originator of the fault code: CRDB.

Use of the fault code: This fault code shall be used by the CRDB when an FNPR message is received for a particular DN or range with a DonorId that refers to a previous executed porting of this DN or range of DN's

12.2.2.15 310 No Data exist for this line numbers

Code	Family	Code	Description	Explanation	Code	State level
310	CRDB	310	No Data exist for these line numbers		310	R

Originator of the fault code: CRDB

Use of this fault code: this code can be used by the CRDB when no data is recorded or exists

12.2.2.16 310 ID Number not in DB

Code	Family	Code	Description	Explanation	Code	State level
310	CRDB	310	ID Number not in DB		310	R

Originator of the fault code: CRDB

Use of the fault code: This fault code shall be used by the CRDB when the CRDB does not recognise the value n the IdNumber DonorId field in the main record. This error cannot occur when the Recipient sends the initial FNP Request message, since it is the CRDB that will allocate the IdNumber.

12.2.2.17 315 DN/Range is in progress stage by Donor

Code	Family	Code	Description	Explanation	Code	State level
315	CRDB	315	DN/Range is in progress stage by Donor		315	R

Originator of the fault code: CRDB.

Use of the fault code: This fault code shall be used by the CRDB when the CRDB detects that the DN, range or a part of the range of directory numbers is already involved in another porting request.

12.2.2.18 315 Already Ported, FNPR by other OLO

Code	Family	Code	Description	Explanation	Code	State level
315	CRDB	315	Already Ported, FNPR by other LO	Same as 1610	315	R

Originator of the fault code: CRDB

Use of this fault code: this code can be used by the CRDB when a second or x^{Th} FNPR is introduced for the same DN or range(s) by a different LO. The initial FNPR is still under process by the Donor.

12.2.2.19 315 Invalid range / subset of the existing range

Code	Family	Code	Description	Explanation	Code	State level
315	CRDB	315	Invalid range: The range is a subset of the existing range		315	R

Originator of the fault code: CRDB

Use of this fault code: this code can be used by the CRDB when the received data is invalid or when the DN or Range is not recorded in the CRDB.

12.2.2.20 315 Some/all numbers in the range are already being ported

Code	Family	Code	Description	Explanation	Code	State level
315	CRDB	315	Some/all numbers in the range are already being ported		315	R

Originator of the fault code: CRDB

Use of this fault code: this code can be used by the CRDB when a Recipient requests a porting for a subset or a full range that was already ported in.

12.2.2.21 316 Invalid range / spans existing range

Code	Family	Code	Description	Explanation	Code	State level
316	CRDB	316	Invalid range: The range spans existing range		316	R

Originator of the fault code: CRDB

Use of this fault code: this code can be used by the CRDB when a Recipient requests a porting of a new range that spans an already ported in smaller range.

12.2.2.22 320 Port Due Date not acceptable

Code	Family	Code	Description	Explanation	Code	State level
320	CRDB	320	Port Due Date not acceptable	Same as 1018	320	R

Originator of the fault code: CRDB

Use of this fault code: this code can be used by the CRDB when the due date coupled on the complexity code does not respect the agreed timer (T1&T2) settings.

12.2.2.23 320 FNP Due Date not conform PT3 rules / Donor's System not ready for activations

Code	Family	Code	Description	Explanation	Code	State level
320	CRDB	320	FNP due date not conform PT3 rules	- no conform PT3 rules, Donor System Down or link down	320	R

Originator of the fault code: CRDB.

Use of the fault code: This fault code shall be used by the CRDB when the requested value of the ActivationTime field (i.e. the FNP due date) exceeds the limits as defined in clause 6.4 of the FNPTF PT3 deliverable for this request.

12.2.2.24 321 FNP due date error

Code	Family	Code	Description	Explanation	Code	State level
321	CRDB	321	FNP due date error		321	R

Originator of the fault code: CRDB.

Use of the fault code: This fault code shall be generated by the CRDB in the following cases:

- The date in the ActivationTime field is in the past or has a wrong format.
- The date in the ActivationTime field is beyond the limit in the future (12 months)

12.2.2.25 325 Total to port number(s) don't match

Code	Family	Code	Description	Explanation	Code	State level
325	CRDB	325	Numbers counted in the "Control total # of FNPR " don't match.	The total amount of ported number for this FNPR don't match the data of total # of FNPRs field.	325	R

Originator of the fault code: CRDB

Use of this fault code: this code can be used by the CRDB when the checksum is invalid

12.2.2.26 335 RN error

Code	Family	Code	Description	Explanation	Code	State level
335	CRDB	335	RN error		335	R

Originator of the fault code: CRDB.

Use of the fault code: This fault code shall be used by the CRDB in the following cases:

- The value of the NewRouteInfo field is not recognised by the CRDB
- The CRDB detects that the Recipient does not own the RN provided by the Recipient.

12.2.2.27 340 Recipient equals Donor

Code	Family	Code	Description	Explanation	Code	State level
350	CRDB	350	Recipient equals Donor		350	R

Originator of the fault code: CRDB

Use of the fault code: This fault code shall be used by the CRDB when the value of the DonorId field equals the value of the RecipientId field.

12.2.2.28 340 Recipient same as Donor

Code	Family	Code	Description	Explanation	Code	State level
350	CRDB	350	Recipient same as Donor		350	R

Originator of the fault code: CRDB

Use of this fault code: this code can be used by the CRDB when the Recipient and Donor codes are the same.

12.2.2.29 345 DN / Range on Hold

Code	Family	Code	Description	Explanation	Code	State level
345	CRDB	345	DN / Range on Hold		345	R

Originator of the fault code: CRDB.

Use of the fault code: This fault code shall be used by the CRDB in the FNP Exec Reject message when the Donor has sent a valid FNP Hold message and subsequently, the Recipient sends an FNP Exec message.

12.2.2.30 350 DN / Range deactivated

Code	Family	Code	Description	Explanation	Code	State level
350	CRDB	350	DN / Range deactivated	DN/Range is in process to be relieved to the Original Donor	350	R

Originator of the fault code: CRDB.

Use of the fault code: This fault code shall be used by the CRDB as FNPR Reject message when the Recipient of the deactivated DN or range of DN's has sent a FNP Disconnect message. This whereas another Participant sends during T9 a FNP Request message for that DN or range of DN's.

12.2.2.31 355 Change or Cancel received after agreed cut-off time

Code	Family	Code	Description	Explanation	Code	State level
355	CRDB	355	Change or Cancel received after agreed cut-off time		355	R

Originator of the fault code: CRDB.

Use of the fault code: This fault code shall be used by the CRDB in the following cases:

- The Recipient sends a FNP Change message to the CRDB after the agreed FNP Due Date and Time (Activation Time field).

12.2.2.32 370 Cancel request not from Recipient

Code	Family	Code	Description	Explanation	Code	State level
370	CRDB	370	Cancel request not from Recipient		370	R

Originator of the fault code: CRDB.

Use of the fault code: This fault code shall be used by the CRDB in the FNP Cancel Reject message when the originator of the FNP Cancel message for a particular DN or range of DN's is not the Recipient of that DN or range of DN's.

12.2.2.33 370 Donor ID number error

Code	Family	Code	Description	Explanation	Code	State level
370	CRDB	370	Donor ID number error		370	R

Originator of the fault code: CRDB.

Use of the fault code: This fault code shall be used by the CRDB when the value of the DonorId field can not be recognised by the CRDB.

12.2.2.34 370 Recipient ID number error

Code	Family	Code	Description	Explanation	Code	State Level
370	CRDB	370	Recipient ID number error		370	R

Originator of the fault code: CRDB.

Use of the fault code: This fault code shall be used by the CRDB when the value of the RecipientId field cannot be recognised by the CRDB.

12.2.2.35 380 - 381 Porting request out of scope

Code	Family	Code	Description	Explanation	Code	State level
380 381	CRDB	380 381	Porting request out of scope.		380 381	R

Originator of the fault code: CRDB.

Use of the fault code: This fault code shall be used by the CRDB when the CRDB detects that the DN or range of DN's is not within the scope of number portability, as defined in the PT3 document.

12.2.3 Data and format codes

12.2.3.1 2010 Mismatch between VAT number and DN / Range

Code	Family	Code	Description	Explanation	Code	State level
20	DATA & Format	10	VAT number error	Mismatch between VAT number and DN / Range	2010	B

Originator of the code: Donor.

Use of the code: This blocking code shall be used by the Donor when the Donor detects that a DN or Range of DN's and the VAT number are not referring to the same Subscriber.

This blocking code shall not be used when the Recipient gives no VAT number.

12.2.3.2 2011 Subscriber id number error

Code	Family	Code	Description	Explanation	Code	State level
20	DATA & Format	11	Subscriber id number error	Mismatch between Subscriber ID and DN / Range	2011	B

Originator of the fault code: Donor.

Use of the fault code: This blocking fault code shall be used by the Donor when the Donor detects that a DN or range of DN's and the Subscriber Id are not referring to the same Subscriber.

This blocking code shall not be used when the Recipient gives no Subscriber Id number.

12.2.3.3 2012 DDI range incomplete

Code	Family	Code	Description	Explanation	Code	State level
20	DATA & Format	12	DDI range incomplete	The NANO's minimal DDI format is not respected	2012	B

Originator of the fault code: Donor

Use of the fault code: This blocking fault code shall be used by the Donor to inform the Recipient that the range that was requested to be ported is not a complete DDI range. The use of this blocking code shall be a trigger to start trilateral negotiations between the Subscriber, the Donor and the Recipient.

12.2.4 Technical codes

12.2.4.1 1050 FNP Grouping of numbers is not correct [1051 till 1059]

Code	Family	Code	Description	Explanation	Code	State level
10	TECHNICAL	50	RN or Ranges belongs to different physical installations RN or Ranges in FNPR can not be grouped, a grouping identifier will be used to inform the Recipient how to group the DN or ranges for a same physical installation	The codes 1051 till 1059 will be used to indicate to which physical installation the DNs or ranges belongs . All the DNs or Ranges belonging to the same physical installation will have the same reject grouping identifier in the initial rejected FNPR. e.g. DN 02.1321111 and 02.1331112 both with reject code 1051, belongs to the same physical installation. A new grouped FNP can be generated by the Recipient grouping both DNs.	1050	B

Originator of the code: Donor.

Use of the code: This blocking code shall be used when the FNP Grouping could not be validated due to a mix of physical installation types into the same grouped FNPR. The rejection code(s) (1051 till 1059) shall reflect the order the Recipient need to send new FNPR(s) with a potential new grouping (All rejection with the same rejection code can be grouped together.)

12.2.4.2 3010 not portable geographical number

Code	Family	Code	Description	Explanation	Code	State level
30	TECHNICAL	10	Not portable geographical number	Refer to section 10.3	3010	R

Originator of the reject code: Donor

Use of the reject code: This reject code shall be used by the Donor when the DN or range of DN's in the FNPR message is served by the Donor and impacted with a case referred in chapter 10.3.

12.2.4.3 3013 DN or Range not allocated to a Subscriber or do not belongs to the same Subscriber

Code	Family	Code	Description	Explanation	Code	State level
30	TECHNICAL	13	DN or Range not allocated to a Subscriber or not from the same Subscriber	The DN/range is not activated or is in freezing condition in NANO's network	3013	R

Originator of the code: Donor

Use of the code: the Donor shall use this code when the number(s) or range(s) is not subject of a subscription by the Donor or allocated to different Subscribers.

12.2.4.4 3014 Technical number

Code	Family	Code	Description	Explanation	Code	State level
30	TECHNICAL	14	Technical number	number not used by the Subscriber but by the OLO to identify the physical lines	3014	R

Originator of the reject code: Donor.

Use of the reject code: This reject code shall be used by the Donor when a DN or (part of) the range of DN's meets the definition of Technical Numbers as given in the document.

12.2.4.5 3015 FNP blocking period

Code	Family	Code	Description	Explanation	Code	State level
30	TECHNICAL	15	FNP blocking period	Freezing period, exceptional non scheduled system shutdown by Donor	3015	B

REMARK: Freezing periods, planned maintenance's are to be communicated up-front, shall be agreed upon by all involved parties and should not be the answer to a FNP Request or a FNP Exec message.

Originator of the code: Donor.

Use of the code: this blocking code shall be used by the Donor when the Donor is unable to meet the FNP due date, due to planned maintenance on its legacy systems. This blocking code shall only be used when a timer cannot be respected. This blocking code shall never be used as an answer on a FNPR message.

12.2.4.6 3017 DN/Range is in repair mode by Donor

Code	Family	Code	Description	Explanation	Code	State level
30	TECHNICAL	17	DN/Range is in repair mode by Donor (Switch impacted)	Unable to port before closing of event (Due date to short)	3017	B

Originator of the code: Donor.

Use of the code: This blocking code shall only be used in a Hold message.

12.2.4.7 3018 DN is a mass calling / media number

Code	Family	Code	Description	Explanation	Code	State level
30	TECHNICAL	18	DN is a mass calling / media number	wrong classification of request	3018	B

Originator of the code: Donor.

Use of the code: This blocking code shall be used by the Donor when the atypical traffic indicator in the free text formatting fields does not match the kind of traffic of the non-geographic number series.

12.2.4.8 3019 Conflict with FNP process with current coded ID field

Code	Family	Code	Description	Explanation	Code	State level
30	TECHNICAL	19	Timing conflict, for Donor, detected for an activation or impacting an initiated process addressed in the Coded ID field		3019	B

Originator of the code: Donor

Use of the code: This blocking code can be used by the Donor when he detects a conflict of impact with a process in relation with this DN or range as mentioned by the Recipient "coded ID field" field.

12.2.4.9 3020 DN not in use by Donor

Code	Family	Code	Description	Explanation	Code	State level
30	TECHNICAL	20	DN not in use by Donor		3020	R

Originator of the reject code: Donor.

Use of the reject code: the Donor shall use this reject code when a DN or a range of DN's is neither allocated nor reserved to a Subscriber. Numbers that are in the 'ageing' period after being deactivated can't be requested to be ported by the Subscriber who has his number deactivated.

12.2.4.10 3110 Installation too complex to enable Donor to meet Due date

Code	Family	Code	Description	Explanation	Code	State level
31	TECHNICAL	10	Installation too complex to enable Donor to meet Due date	Subscriber's configuration is very complex and does not allow to meet the due date before changes or reconfiguration	3110	B

Originator of the code: Donor.

Use of the code: the Donor shall use this blocking code if the Donor cannot meet the due date due to the technical complexity of the installation.

12.2.5 Administrative and legal codes

12.2.5.1 4011 LO no porting right

Code	Family	Code	Description	Explanation	Code	State level
40	ADM/LEGAL	11	No porting right	OLO has no right to port numbers in that zone	4011	R

Originator of the reject code: Donor

Use of the reject code: This reject code shall be used by the Donor (or the CRDB) when the Recipient has sent an FNPR message with a DN or range of DN's that are geographical numbers when the Recipient has no geographical numbers allocated or for non-geographical number when the Recipient has no non-geographical numbers allocated.

12.2.5.2 4012 OLO's owned number

Code	Family	Code	Description	Explanation	Code	State level
40	ADM/LEGAL	12	OLO's owned number		4012	R

Originator of the reject code: Donor.

Use of the reject code: This reject code shall be used by the Donor when the DN or range of DN's is used internally in the network of the Donor (e.g. remote access numbers, voice mail numbers, Public own phone box,…).

12.2.5.3 4013 Reserved

Code	Family	Code	Description	Explanation	Code	State level
40	ADM/LEGAL	13			4013	B

Originator of the code: Donor.

- Use of the code: This blocking code shall be used

12.2.5.4 4014 Line in modification status

Code	Family	Code	Description	Explanation	Code	State level
40	ADM/LEGAL	14	Line in modification status	Adding/removing services are in process by the Donor on Subscribers demand for this installation	4014	B

Originator of the code: Donor.

Use of the code: the Donor shall use this blocking code when the DN or range of DN's refers to a line that is in modification status. The Subscriber need to cancel his request before a FNPR can be accepted or the Recipient need to wait the end of the modification process before sending his FNPR.

12.2.5.5 4015 DN or Range(s) overlap

Code	Family	Code	Description	Explanation	Code	State level
40	ADM/LEGAL	15	Different DN / range(s) from different Subscribers in same FNPR	DN or Range(s) overlap with other account number	4015	R

Originator of the reject code: Donor.

Use of the reject code: the Donor in the following cases shall use this reject code:

- Within one FNPR message, containing one range of DN's, DN's are belonging to different Subscribers.
- Within a grouping of FNPR messages, one FNPR message contains a DN or range of DN's which is not belonging to the same Subscriber as the DN or range of DN's in the other FNPR message(s) in that grouping.

12.2.5.6 4016 I-line number

Code	Family	Code	Description	Explanation	Code	State level
40	ADM/LEGAL	16	I-line number	Governmental subsidised line	4016	R

Originator of the reject code: Donor.

Use of the reject code: the Donor shall use this reject code when the DN requested to port is allocated as an I-line.

12.2.5.7 4017 missing LoA during the validation period for professional Subscribers

Code	Family	Code	Description	Explanation	Code	State level
40	ADM / LEGAL	17	no authorisation letter from Subscriber (LoA) presented by Recipient on Donor's request during the validation period for Subscribers subject to VAT	Authorisation letter not found / presented to prove the FNPR (Donor requested in the early stage of FNPR)	4017	R

Originator of the reject code: Donor

Use of the reject code: The Donor shall use this reject code when the Recipient cannot present a Letter of Authorisation within the validation period. This letter of Authorisation can be asked when the Donor suspect the ownership of the DN(s) / Range(s) subject to the porting request or the authorisation of the requestor for a Subscriber subject to VAT. (See FNP service Description for details)

12.2.5.8 4018 reserved numbers

Code	Family	Code	Description	Explanation	Code	State level
40	ADM/LEGAL	18	Reserved numbers	DN's not in use / DNs-range(s)need to be putted in service first to allow porting	4018	B

Originator of the code: Donor

Use of the code: The Donor shall use this blocking code when he detects that reserved ranges are not in service or put in service before the FNP Due date.

12.2.5.9 4019 Subscriber objects to Donor

Code	Family	Code	Description	Explanation	Code	State level
40	ADM/LEGAL	19	Subscriber objects porting during the validation period	Porting request is not affirmed/ confirmed by the owner of the DN or is contested	4019	B

Originator of the code: Donor

Use of the code: The Donor shall use this blocking code when the owner of the DN(s) or Range(s) is objecting the FNPR. The Subscriber needs to contact the Recipient asking to generate a cancel for this demand.

12.2.5.10 4020 Public utility access lines

Code	Family	Code	Description	Explanation	Code	State level
40	ADM/LEGAL	20	Public utility access lines associated with the installation where has been no order raised with the Donor to cease, interrupt or transfer that service	Number(s) are used of benefit to the public. Impacting emergency services (fire brigade, police, Health care emergency services,…)	4020	B

Originator of the code: Donor

Use of the code: The Donor shall use this blocking code in such cases. The use of this blocking code shall be a trigger to start trilateral negotiations between the Subscriber, the Donor and the Recipient..

12.2.5.11 4021 contractual issues

Code	Family	Code	Description	Explanation	Code	State level
40	ADM/LEGAL	21	Porting not possible due to contractual issues	Specific deals not respected before a FNPR can be send. Current contract do not authorise to port before all parties agree (e.g. security / fire/ burglary protection /emergency lines)	4021	B

Originator of the code: Donor.

Use of the code: The Donor shall use this blocking code in such cases. The use of this blocking code shall be a trigger to start trilateral negotiations between the Subscriber, the Donor and the Recipient.

12.2.6 Process related codes

12.2.6.1 5010 Conflict with timers

Code	Family	Code	Description	Explanation	Code	State level
50	PROCESS conflict	10	Conflict with timers		5010	R

Originator of the code: Donor

Use of the code: The blocking code shall be used when conflicts arise in the timers when not detected by the logic of the CRDB. Mostly by usage or combinations with Hold / Change messages and the recorded Due date.

12.2.7 Economical / commercial related codes

12.2.7.1 6013 involved numbers are blocked

Code	Family	Code	Description	Explanation	Code	State level
60	ECONOM.	13	Involved numbers are blocked by guardian (Curator)	Involved numbers subject of a deal for business take over	6013	R

Originator of the reject code: Donor.

Use of the reject code: the Donor shall use this reject code when a guardian (Curator) is blocking the numbers.

12.2.7.2 6014 Number(s) involved in bankruptcy case

Code	Family	Code	Description	Explanation	Code	State level
60	ECONOM.	14	Number(s) involved in bankruptcy case	Owner of the DN(s) – Range(s) be bankrupt	6014	R

Originator of the reject code: Donor.

Use of the reject code: the Donor shall use this reject code when the Subscriber who wants to port its numbers involved in a bankruptcy case.

12.2.8 Fraud codes

12.2.8.1 7010 Slamming

Code	Family	Code	Description	Explanation	Code	State level
70	FRAUD	10	Slamming	Term used to describe any practice that changes a consumer's operator without the Subscriber's knowledge or consent.	7010	R

Originator of the reject code: Donor

Use of the reject code: the Donor shall use this reject code in case the Subscriber complains about slamming practices by the Recipient.

12.2.8.2 7011 Cramming

Code	Family	Code	Description	Explanation	Code	State level
70	FRAUD	11	Cramming	The unauthorised adding of features to a consumer's service without permission.	7011	B

Originator of the code: Donor

Use of the code: the Donor shall use this blocking code in case the Subscriber complains about cramming practices by the Recipient.(Third party billing)

12.2.8.3 7012 Fraud monitoring

Code	Family	Code	Description	Explanation	Code	State level
70	FRAUD	12	Judicial authority authorised fraud monitoring in process on this DN / Range(s)	Fraud investigation on this DN/Range. Due date need to be agreed on between Donor and Recipient	7012	B

Originator of the code: Donor.

Use of the code: the Donor shall use this blocking code when the Donor is investigating fraud on the line of the Subscriber. In this case a future due date need to be agreed on between Donor and Recipient.

12.2.9 NP Non-RFS codes

12.2.9.1 8010 NP Customer care request exist for this porting

Code	Family	Code	Description	Explanation	Code	State level
80	NP Non RFS	10	NP Customer care request exist for this porting	Repair requested for this porting	8010	B

Originator of the code: Donor / CRDB

Use of the code: This blocking code shall be used by the Donor (or the CRDB) when the Donor (the CRDB) detects that the DN or (part of) a range of DN's is involved in a NP Non-RFS process.

12.2.9.2 8110 No access to the ported DN

Code	Family	Code	Description	Explanation	Code	State level
81	NP Non RFS	10	No access to the ported DN	Access to ported DN , initiated from Participants or Donor network unsuccessful	8110	I

Originator of the code: Recipient

Use of the code: This information code shall be used by the Recipient when he concludes that access initiation through the Donor's /original Donor or Participant is unsuccessful.

12.2.9.3 8120 Calls wrongly terminated

Code	Family	Code	Description	Explanation	Code	State level
81	NP Non RFS	20	Calls initiated towards the ported DN are terminated by a wrong Subscriber	The calls terminate to a wrong Subscriber, routing information could be corrupt or faulty routed	8120	I

Originator of the code: Recipient

Use of the code: the Recipient shall use this information code when he concludes that the call terminates by a different Subscriber, other than these from were the number was ported.

12.2.9.4 8130 Calls not terminated or NP Non RFS problem under study

Code	Family	Code	Description	Explanation	Code	State level
81	NP Non RFS	30	Unknown reason	The reason is not precisely determinate, the problem is reported for acknowledgement	8130	I

Originator of the code: Recipient

Use of the code: the Recipient shall use this information code when he is analysing the reason(s) that the call do not terminates by the in his network ported Subscriber and the analysis could take a longer time that normally expected.

12.2.10 Other codes

12.2.10.1 9999 not covered issue impacting the porting

Code	Family	Code	Description	Explanation	Code	State level
99	Other	99	These code can be used exceptionally to indicate a problem which is not yet recorded with a specific blocking or reject code	The operator may use this code to report an issue who is not covered by an existing code	9999	B

Originator of the reject code: Donor, Recipient and Participant.

Use of the reject code: This reject code shall be used by all parties, except the CRDB when during the FNP process a mayor issue is detected which could interfere in the normal agreed porting process

13 ANNEX F: PARTICIPANTS

A list is maintained of all 'Participant Id's' of Operators and Service Providers who exchange information with the CRDC, directly or through an agreed 3rd Party. A 4- digit, alpha numeric "mnemonic" code, is assigned to each Participant.

Please refer to the latest NP Certificate list of the NRA to trace the Number Portability obligation of any Participant. The NP certificate include the geographical areas (zones) were a geographical FNPR as Recipient is permitted as well as for non-geographical number portability requests, here allocated to a Service Provider for specific Value Added Services (VAS) type of marketing numbers . (070, 0800, 0900 etc..)

14 Annex G: Coded ID Field

A field with 3 numeric characters (0 to 9)

Coded ID			Description	Impact Level
0	0	0	FNP Only	
0	0	1	FNP + Local Loop Unbundling	High
0	0	2	European Telephony Numbering Space (ETNS) number implemented on National OLO network	Information
0	0	3	ENUM or Voice over IP impacted number	Information
0	0	4	Local Interconnection , impacted number	Medium
0	0	5	Atypical traffic (used in combination with non-geo numbers)	Information
0	0	6	Voice over DSL impacted number	Information
0	0	7	Carrier DSL impacted number	Information
0	0	8		
0	0	9		
0	1	0		
0	1	1		
0	1	2		

15 ANNEX H: Block reallocation process

15.1 Block reallocation (BR) - Framework

Block reallocation is an administrative and technical process with five potential involved parties:

- The regulator: who decided to reallocate the block on request of an operator and after consultation of other involved operators.
- The BR Recipient OLO: to whom the number block will be reallocated.
- The BR Donor OLO: the operator to whom the number block was initially allocated by the BIPT.
- The Participant BR operators: all other operators who will be informed of the reallocation.
- The Subscriber using the reallocated block.

This process is limited to a block reallocation where the full block with its 10.000 DNs is served by an unique operator were the numbers belongs to one and the same Subscriber and reallocated to a unique Recipient operator. No difference is made if some ranges are still in reserved status or put into service.

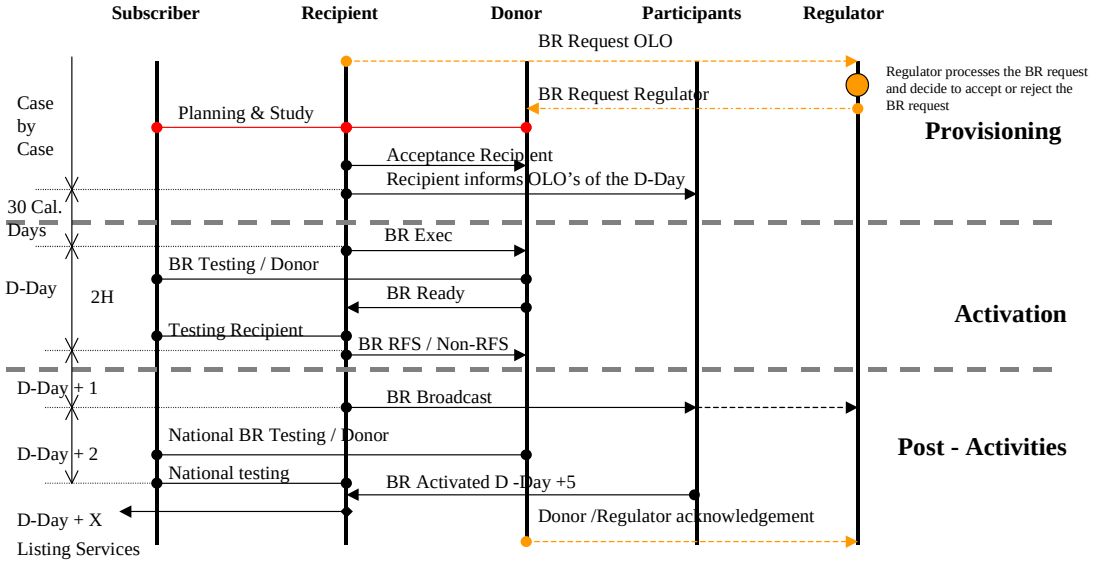
No processes are been described, agreed or tested so far for conditions were some numbers or number ranges belongs to a other Subscriber.

The CRDB is only involved, in a full block re-allocation process, to change the FOLO ownership in the allocated number block(s) tables. The NPA Service Manager must be informed by the NRA when such changes occur.

15.2 Reallocation Process

The full block reallocation process is shown in the following diagram.

Block Reallocation (BR)



The three phases: provisioning, activation and post-activities are described in the next sections.

15.2.1 Provisioning phase

A case by case study and planning is required prior to informing the participating operators. This needs to be done to take account of the specific network and customer configuration in order to guarantee the 30 calendar days notification towards the participating operators.

The preliminary work for the BR Recipient and BR Donor is to prepare their network for the block reallocation. These preliminary works make the switchover easier and reduce dramatically the risk of errors during the activation phase.

A fall back plan must be designed to recover to the previous situation in case of non-RFS stage.

The Recipient operator needs to notify the remaining operators ,as well as the transit operator if any, at least 30 calendar days before the switchover of the full block, switchover day named later in the document as the D-day.

Donor, Recipient and Subscriber accept the D-Day (day and time),"Acceptance Recipient" message.

The planning and process for the block reallocation will be approved by the Donor, Recipient and impacted Subscriber. To reduce operational reallocation risks and the impact for the Subscriber the best (switchover) activation time is during the noon (12:00-14:00).

We recommend to the Subscriber to provide one ore more test number(s) for every used 1000 ranges in the block.

15.2.2 Activation phase

The Recipient OLO assumes the accountability for the operation.

The Recipient will forward a Block Reallocation Exec message to the Donor operator.

The most appropriated communication method is the usage of phone or GSM followed by an E-mail confirmation message for all crucial exchanged messages. (Exec., Ready , RFS, Non-RFS)

All identified key persons must be reachable during the process.

The Donor is invited to test on a manual or automated way the block reallocation activation and if he feels confident to send the block reallocation "Ready" message towards the Recipient.

When the "Ready" from the Donor is given the Recipient will on his side terminate the reallocation process, test and he will close the process with a "RFS" message.

In case the Recipient conclude in a non-RFS status the fall back scenario need to be started after consultation of the three parties (Recipient, Donor and Subscriber).

The Recipient is the final decision-maker.

15.2.3 Post – activities phase

The Recipient needs to inform the other OLO's and the regulator that the block has really been reallocated.

The Recipient and Donor operator will perform national testing to guaranty national access towards the reallocated block and correct routing in their network if some problems occur

The testing is foreseen to be finalised D-day + 2.

Both parties will communicate their final testing results and will decide to abort or to continue the testing if needed.

The Participant OLOs needs to confirm with a written message the BR Activation[10] in a period of D – Day + 5.

The Recipient will perform the needed tasks to update and to guaranty accurate information for the listing services especially for the emergency services.

When the update for the listing services as been communicated and corrected the Donor operator will inform the regulator and will report the still open issues if any.

Finally the Donor will inform the regulator that the block reallocation is finalised.[11]

[10] The BR Activation message allows them to update their network elements and test the new configuration.

[11] If the donor is in charge to update the listing services, he will report that this is done. In particular for the emergency services this is a necessity.

16 ANNEX I : FOLO's Automated access

16.1 Different CRDC Participant Profiles

Actually there are 3 different FOLO Participant Profiles supported:

- GUI Only Participants, (GOP)
- Semi-Automated Participants, (SAP)
- Fully Automated Participants, (FAP)

16.2 GUI Only Participants

The GUI Only Participants make use of the CRDB GUI to access and to process the FNP provisioning on the CRDB. The GUI is an https Web Browser solution and access the CRDC through a secure IP/VPN connection.

All GOP's GUI Access is granted with a Private Authentication Certificate.

The GUI interface used is supplier dependant.

16.3 Semi-Automated Participants

The Semi-Automated Participants make use of the CRDC GUI to participate to the FNP process on the CRDC. They do use an automated interface (SOAP Server) linked to their internal systems to capture the FNP Messages. The OLO SOAP Server is operating in a "listen only" (read only) modus operandi. The FOLO SOAP Server is not sending any SOAP Messages to initiate or participate in the FNP Provisioning.
The FOLO SOAP server receives all CRDB messages and is not allowed to send any messages towards the CRDC. The FOLO SOAP server receives all CRDB FNP messages and will answer with "FNP SOAP Server Response" messages (= confirmation of CRDB SOAP message receipt) ≅ Acknowledgement on SOAP level.

Access as SAP is granted through a secure IP/VPN link with a Public Authentication Certificate.
General Remark:

A possibility for the SAP to send specific SOAP activated broadcast messages is not excluded and could be detailed in this annex.

16.3.1 Description of message protocol (for FOLO Participants)

Description of the message receipt and answered (acknowledgement on SOAP level is not described in this diagram):

Messages	Initiated with GUI	Captured by SAP	Sent by SAP
Fnprequest	**Yes**	**Yes**	**No**
Fnpreject	**Yes**	**Yes**	**No**
Fnpexec	**Yes**	**Yes**	**No**
Fnpready	**Yes**	**Yes**	**No**
Fnprfs	**Yes**	**Yes**	**No**
Fnpnonrfs	**Yes**	**Yes**	**No**
Fnprfsbroadcast	**No**	**Yes**	**No**
Fnpactivated	**Yes**	**No**	**No**

Fnpaccept	**Yes**	**Yes**	**No**
Fnpchange	**Yes**	**Yes**	**No**
Fnpchangeaccept	**Yes**	**Yes**	**No**
Fnpchangereject	**Yes**	**Yes**	**No**
Fnpcancel / CRDC	**Yes / No**	**Yes**	**No**
Fnphold	**Yes**	**Yes**	**No**
Fnpabort	**Yes**	**Yes**	**No**
Fnpabortactivated	**Yes**	**Yes**	**No**
Fnpdisconnect	**Yes**	**Yes**	**No**
Fnpdiscdone	**Yes**	**Yes**	**No**
Fnpdeactivated	**Yes**	**No**	**No**
Fnpdeactbroadcast	**No**	**Yes**	**No**
Fnpdeactdone	**Yes**	**No**	**No**
Fnpupdate	**Yes**	**Yes**	**No**
Fnpupdatecompleted	**Yes**	**No**	**No**

16.4 Fully Automated Participants

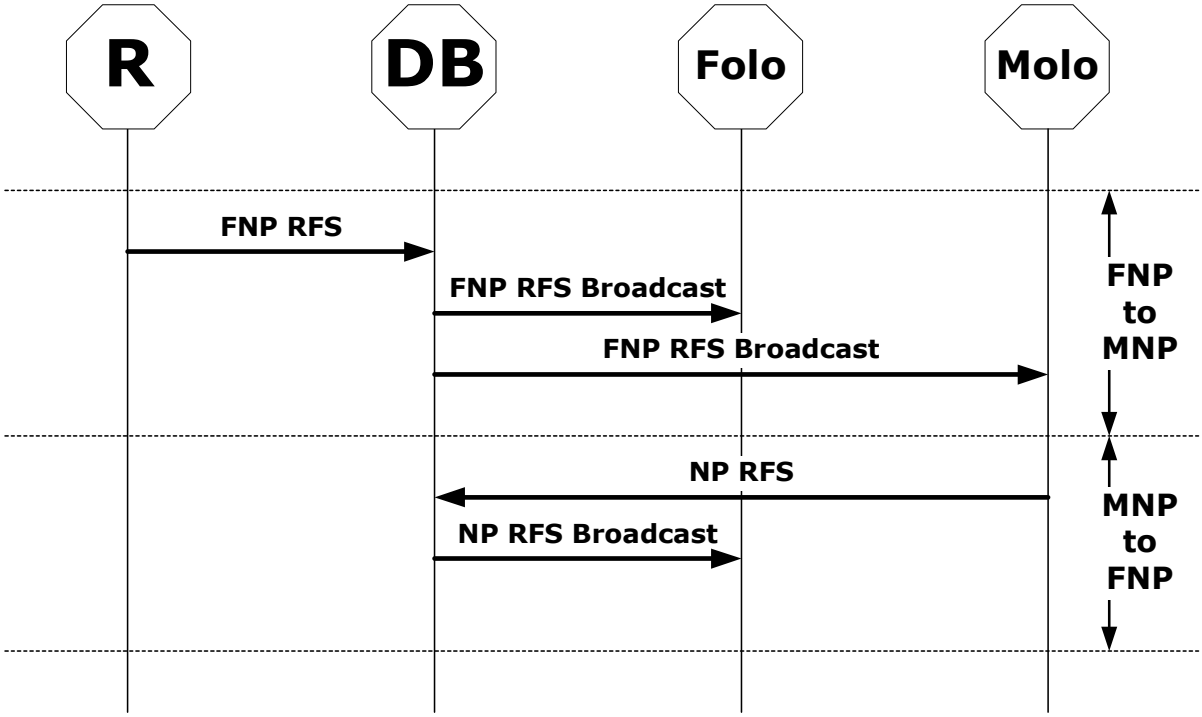
The Fully Automated Participants make use of a XML/SOAP (SOAP Server) access to fulfil the FNP Provisioning. Mainly all FNP messages are handled through this interface. Access is granted through a secure IP/VPN link with a Public Authentication Certificate. The Fully Automated Participants uses the GUI Interface to retrieve CRDB FNP Reports, to request a SOAP replay and to handle manually the FNP provisioning processes in case of incidents with the automated system.

17 ANNEX J : Mobile Number Portability Broadcasts

17.1 Activation Phase (Broadcast process)

FOLO to MOLO: When the FOLO Recipient sends a FNP RFS to the CRDB, this last one will as for the FOLOs forward this message as a FNP RFS Broadcast to all Mobile Operators. As a result the MOLO can update their routing info for Mobile to Fix traffic. The message lay out is the same as the message that is send to the Fixed Operators, but broadcasted per single number or single range (no grouping). The detailed FOLO broadcast flow is explained in section 5.2.1.

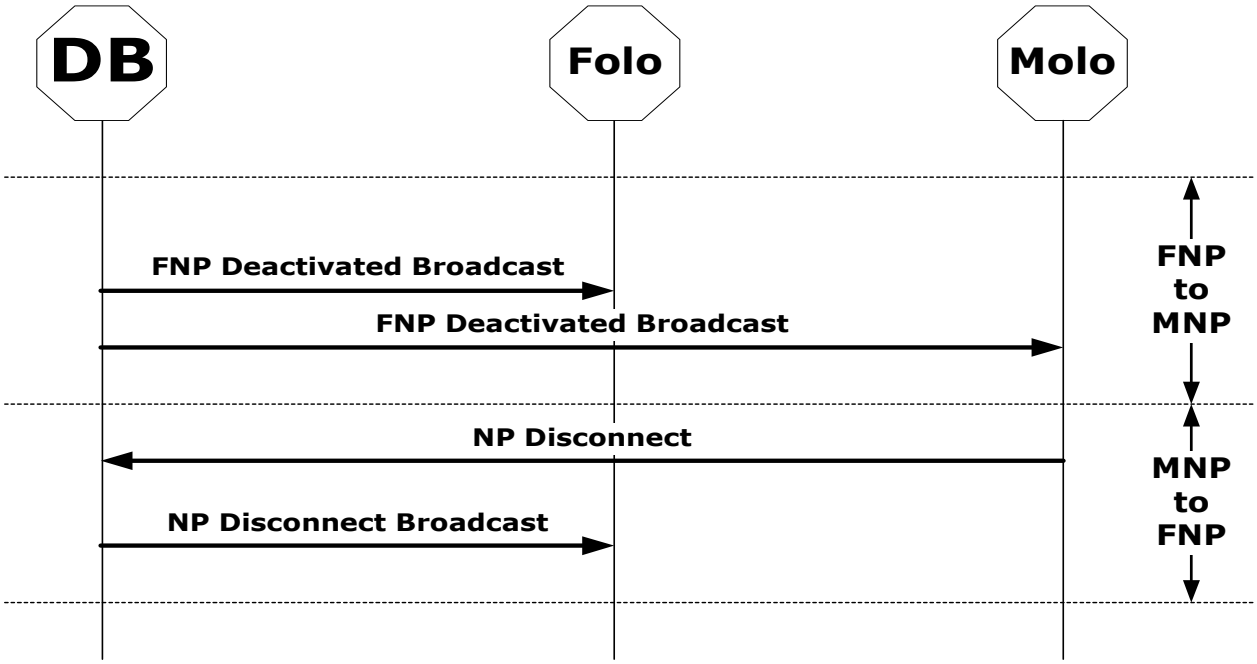
MOLO to FOLO: Mobile Operators are sending a NP Broadcast to the CRDB. The CRDB will forward this message to all FOLO's. As a result they can update their routing info. The NP Broadcast content is based per single ported MSISDN.



17.2 Deactivation Phase (Disconnect process)

FOLO to MOLO: when the FOLO Recipient sends a FNP Deactivated Broadcast to the CRDB as a result of the FNP Disconnect process, this last one will forward this message to all Mobile Operators. As a result they can delete this DN or Range as being ported. The message lay out is the same as the message that is send to the Fixed Operators. The detailed FOLO disconnection flow is explained in section 5.3.1.

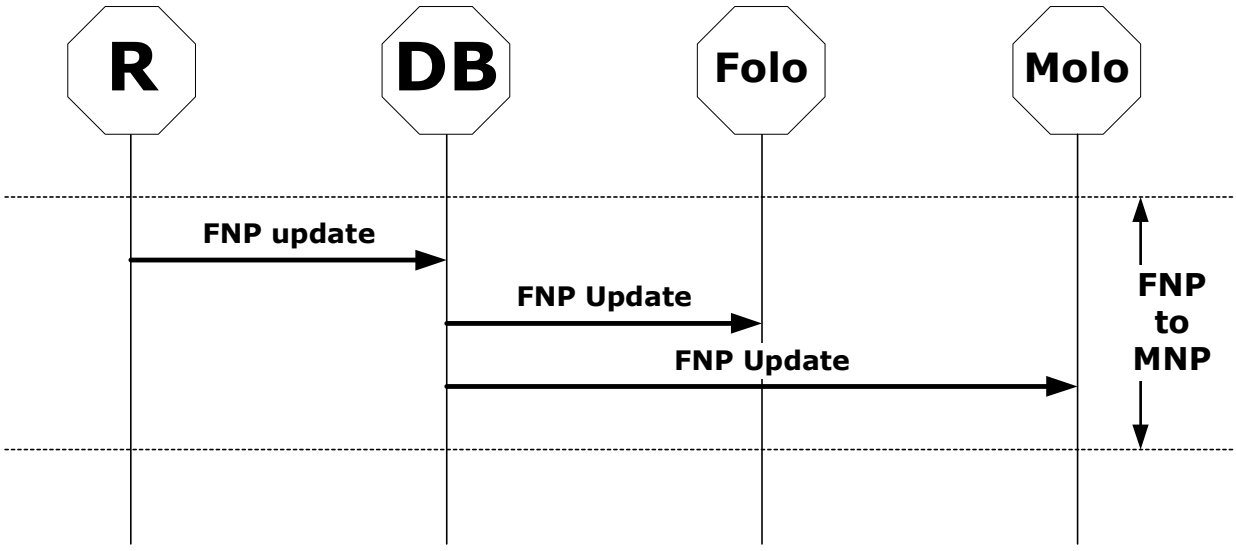
MOLO to FOLO: Mobile Operators are sending in the case of Deactivation a NP Disconnect to the CRDB. The CRDB will forward this message to all FOLO's. As a result they can update this case from their own NP database.



17.3 Maintenance Phase (Update process)

FOLO to MOLO: When a FOLO operator does an FNP update of a particular case, the update will be forwarded by the CRDB to the MOLO Operators. The detailed FOLO process for the NP Update is explained in section 5.5.1.

MOLO to FOLO: The Mobile Operators currently (2003) don't have the need of a NP Update process.



17.4 MOLO System Up – System Down

Every participating MOLO has the possibility to notify the other Participants that it is temporally unable to handle NP Execution requests. The result is a system down message that is sent to the CRDB, who forwards this to all MNP- & FNP Participants. As this is only an information message, the FOLO Participant's only answer with a SOAP response (acknowledgment).

The Participant who can resume request handling will generate a System Up message and sends this to the CRDB. The CRDB will forward this to the MOLO- and FOLO Participants. The FOLO Participant's will only answer with a SOAP response (acknowledgement).

18 ANNEX K: CRDC Hotline / Support Desk

This annex reflects the expected daily CRDC Support activities between the 3rd Party managing and maintaining the CRDC and the Participants as well as the tools (e.g. ticketing system) and method used to guaranty such activities.

The non exhausted list of Helpdesk features underneath reflect common industrial offering of the moment for a Support Desk application, features expected by the CRDC Participants.

“Call = Ticket opened by the Support Desk”

Generic features:

- User-friendly Call logging; keyboard, e-mail and browser-based (Web) interface
- Call Alerts based on e-mail (system down, performance issues, impact on,…)
- Notification : Email notification to notify changes in; status, escalation,….
- Fully Configurable SLA’s Tracking features.
- Participants Notice board to share ideas docs etc..
- Possibility of Re-assignment of calls
- Alerts and warning when Action times are breached
- Security ; Login and Password management of the Support desk solution (Https access)
- Workflow engine (Configurable Work-flow Management)
- Reporting (Investigation , Audit, SLA, Status etc…)
- Whiteboard (convey know issues to Participant community)
- Activity Management
- Contact Management & Customized messaging (Escalation and follow up)
- Scalability of system
- Search engine (filter, …)
- Back Up solution when system down
- Clock Synch with CRDC
- Multimedia Contact ; future proof

Participant:

- Can log their own call request (severity , incident + attachments, changes on previous input,…)
- Check on status (On Hold, In progress, Waiting Reply, Waiting Parts, Escalated, Assigned to …….)
- Dynamic update of open requests
- Use the knowledge base to find answers to FAQ
- Check on SLA deadline
- Pre-defined management reports
- Weekly own view of Call Statistics
- Run Reports over the Web
- Download reports (Format, CSV, Excel, ..)
- Can close and re-open Calls remotely
- Search engine (Filter,…)

Support Desk:

- Dynamic update of open requests (Participant , per Severity , per SLA deadline, …
- Remote desktop management
- Call Statistics
- Adding Quick Calls on the fly
- Auto-fill on fields to speed initial call logging
- Schedule Reports
- Audit trail to track changes in Call lifestyle
- Automated E-mail notification / acknowledgement
- SLA deadlines (approaching or exceeding)
- Alerts , escalation notification
- Receive file attachment into application within incoming E-mails
- E-mail out any File attachment with call and knowledgebase entries
- Background e-mail scan and import of Call into application
- Recording actions, steps people have taken to resolve
- Time recording “open-close” the call
- Ability to “Stop the Clock” for agreed actions
- Direct call to teams with specific skill sets
- Incident Monitoring per Participant , per topic
- Search engine
- Billing , charging for specific or agreed additional support
- Activity Management
- Scalability
- Contact Management

19 Annex L: Filtering of Number Portability Broadcasts

Due to specific business needs of CRDC Participants, the type of Broadcast messages is well or not relevant for their business or/and operations.

On the other hand for others, broadcasts with additional information is expected to permit them to route cost effectively calls or telecom services.

The data in the coded ID field, already present in the broadcast messages is therefore valid information that permits the Participant to filter per type of broadcast messages what is relevant for them.

Nevertheless, we could expect that mass of broadcasts are irrelevant for some parties but still need to be processed in their legacy system and this for automated or semi automated Participants.

For this reason the CRDC must be able to filter out broadcast messages before sending them to any Participants. This could be triggered, based on the data recorded in the Coded ID field.

Nevertheless a Participant directly involved in a porting process as Donor or Recipient shall receive as 'Close the loop principle '[12] all FNP types of broadcast.

The synchronisation report and bulk synch file, shall by default take care of the filtering values, specific for the requesting Participant, but on request (menu) a full synchronisation report or bulk sync file, without filtering, must be available for the requesting party.

========== THE END ==========

[12] For the "close the loop" principle the broadcast messages must still be forwarded to the OLO if it has the role of Donor or Recipient involved in the NP transaction process.